"Make Security Part of You and Your Institution's DNA!"

Threat Intelligence Newsletter: May 03, 2018

FIPCO®
IT Audit
Round Table
Discussions

If you would like to host an event, please contact: Becky Schowalter

Upcoming Threat Intelligence Peer Group Discussions
August 16 - Barron

Great Resource for Bank Lobby Customer Awareness Materials
Check this out for free awareness information from the Federal Trade Commission; can order bulk brochures, bookmarks, folders, etc... https://www.bulkorder.ftc.gov/publications/start-security-guide-business. Especially check out the "Pass it On" series.

Wisconsin Cyber Liaison Officer Training Opportunity (Milwaukee Area) no cost
Mark your calendar; CLO training event on May 31st from 8am-3pm will be held at 400 S. Executive Drive, Milwaukee; in the basement conference room. More information to follow, but this is preliminary information so you can mark your calendar. There may be CLO training coming to the Wausau area in a few months. More details to follow or contact Ken Shaurette directly to ensure you get notifications and contact information.

****

Alerts

BBB: New Phishing Con Nabs Your Browser Tabs
Scammers have a new technique called "tabnabbing. They hijack inactive browser tabs and trick people into giving up their login and password information. Here's how it works. Read more about "tabnabbing"… https://www.bbb.org/en/us/article/news-releases/17368-digital-spring-cleaning-why-you-need-to-know-what-tabnabbing-means

How do Hackers Hack your Passwords?
Here are the three ways that hackers use to hack your passwords. http://threatbrief.com/hackers-hack-passwords/

Scammers impersonate the Chinese Consulate

Have you gotten a call from someone saying they're from a Chinese Consulate office? If so, you're not alone – based on reports to the FTC and the real Chinese Consulates. But here's the thing: it's not a Chinese Consulate office calling. It's a scammer. These callers seem to be reaching people with Chinese last names but, as we know, scammers can change tactics quickly.
https://www.consumer.ftc.gov/blog/2018/04/scammers-impersonate-chinese-consulate?utm_source=govdelivery

Google cuts fake ad blockers from Chrome Store: Were you among 20 million fooled?
Bogus ad-blocker extensions in the Chrome Web Store trick millions of people into installing them.
https://www.zdnet.com/article/google-cuts-fake-ad-blockers-from-chrome-store-were-you-among-20-million-fooled/?ftag=TRE-03-10aaa6b&bhid=78480402

Copy and Paste Plea Exposes Your Identity
Why you should be wary of Facebook copy and paste requests. What crosses your mind when a Facebook friend asks you to copy and paste their post rather than just sharing it?
https://www.scambusters.org/copyandpaste.html

Two incident response phases most organizations get wrong
There is a baseline for incident response — six phases familiar to anyone who has spent time around a SANS classroom. Those phases — preparation, identification, containment, eradication, recovery, and lessons learned — define the basic outline constructed to help a business manage a situation while keeping damage and recovery time to a minimum. But there are some aspects to this baseline that organizations routinely get wrong. https://www.csoonline.com/article/3263794/security/two-incident-response-phases-most-organizations-get-wrong.html

Publishers Clearing House scams keep coming
Who wouldn't love to be that winner you see on TV holding a great big sweepstakes check? That's what con artists are counting on when they claim to be Publishers Clearing House. This trick is an oldie but goodie for scammers. https://www.consumer.ftc.gov/blog/2018/04/publishers-clearing-house-scams-keep-coming?utm_source=govdelivery

Internet Explorer 0 Day Attack Found in the Wild
A new Internet Explorer zero-day exploit it has seen exploited in the wild by an (unmentioned) APT group. Qihoo 360 has reported this to Microsoft on 4/19/2018. We have no news from Microsoft.
https://isc.sans.edu/forums/diary/New+IE+0day+in+the+wild/23581/

****

Hints & Tips plus Security Awareness

Webcast: NIST Cybersecurity Framework Version 1.1 Overview
The Framework for Improving Critical Infrastructure Cybersecurity ("The Framework") provides a prioritized, flexible, repeatable, performance-based, and cost-effective approach to managing cybersecurity risk at all levels in an organization. It is applicable to organizations of all sizes and sectors.
https://www.nist.gov/news-events/events/2018/04/webcast-cybersecurity-framework-version-11-overview

Security Awareness Training: One CISO's Journey from Doubter to Believer

Whether budgets are robust or restrictive, infosec teams are often skeptical about diverting dollars away from technical tools so they can better fund awareness training. Fortune 500 CISO, Alan Levine, felt the same—until a nation-state attack on his organization led him to re-examine employees' roles in cybersecurity and the value of defense-in-depth strategies at users' desktops. Join us to hear how Alan's journey with awareness training went from skeptic to advocate. Brought to you by Wombat Security. https://engage.vevent.com/index.jsp?eid=7019&seid=1419

Personal information tip posted on the global risk community
Don't take the Facebook quizzes!!! Your online security and Facebook privacy security settings. Good cyber citizens make good corporate citizens and online banking customers.
https://mediaexplorers.lpages.co/cyber-security-tips-series-tip-2-your-personal-privacy-and-security/

FTC to Introduce New Cybersecurity Education Series for Small Businesses
Last week, the Federal Trade Commission announced that they will launch a campaign designed to educate small businesses on cybersecurity issues such as phishing, ransomware attacks mobile device security and more… https://www.consumer.ftc.gov/blog/2018/04/coming-soon-new-cybersecurity-education-small-business

Special report: A winning strategy for cybersecurity
In this era of rapidly escalating cyberattacks, companies should protect themselves with a solid risk management strategy. This eBook offers a detailed look at how to build policies to protect your critical digital assets. http://b2b.cbsimg.net/downloads/Gilbert/SF_april_cybersecurity.pdf

CSIAC Physical Cyber Awareness Video
Tired of reading the same stale cyber awareness content? Lacking the time and/or resources to develop and deliver effective security content to your workforce? Strengthen your cybersecurity posture by implementing an ongoing awareness campaign that incorporates short, fresh video content created by the CSIAC. https://www.csiac.org/podcast/cyber-physical-security/

FEMA National Planning Frameworks
The purpose of this page is to provide information on the National Planning Frameworks (Frameworks). The Frameworks describe how the whole community works together to achieve the National Preparedness Goal (https://www.fema.gov/national-preparedness-goal). There is one Framework for each of the five mission areas, Prevention, Protection, Mitigation, Response, and Recovery. The intended audience for the page is individuals, families, communities, the private and nonprofit sectors, faith-based organizations, and local, state, tribal, territorial, insular area, and federal governments. https://www.fema.gov/national-planning-frameworks

Training Course web links are listed below. A revised course for the refreshed National Disaster Recovery Framework will be released at a later date.

IS-2000: National Preparedness Goal and System Overview:
https://training.fema.gov/is/courseoverview.aspx?code=IS-2000
IS-2500: National Prevention Framework, An Introduction:
https://training.fema.gov/is/courseoverview.aspx?code=IS-2500
IS-2600: National Protection Framework, An Introduction:
https://training.fema.gov/is/courseoverview.aspx?code=IS-2600
IS-2700: National Mitigation Framework, An Introduction:
https://training.fema.gov/is/courseoverview.aspx?code=IS-2700
IS-800.c: National Response Framework, An Introduction:
https://training.fema.gov/is/courseoverview.aspx?code=IS-800.c

GDPR Compliance MasterClass
The GDPR is the most significant change in data privacy regulation in more than 20 years. It comes into force on 25 May 2018 and will impact all businesses that process personal data or businesses that process personal data of EU citizens even if they are not in the EU. Obligations for compliance will affect both… Registration required: https://www.brighttalk.com/webcast/5586/297219

****

News & Views

EMV Cards Decrease In-Person Fraud But Still Aren't 100% Secure
In a time long ago, there were a couple of very large data breaches. You may remember them: Target and Home Depot. Way back then, in 2015, the payment cards customers used at point-of-sale (POS) systems at these places and everywhere else in the United States required swiping a card, so the machine could read the magnetic strip on the back. Well, as is now well known, it’s not so hard for cyberthieves to recreate cards and use them to make their own purchases…
https://www.sosdailynews.com/news.jspx?&articleid=7EAEAEEA7AAF6F385914CF7DA683B970&sx=79

Asset Focused Risk Management
There are many ways to manage risks and each one of them should fit business needs of organization. Here is one way to manage risks around assets. InfoGraphic: https://cypherowl.com/asset-focused-risk-management-infographics/

Bracing for Tomorrow's Threats with Behavioral Analytics
Bracing for Tomorrow's Threats with Behavioral Analytics , As the cybersecurity threat landscape becomes increasingly complex, attacks are growing in both volume and sophistication.
https://www.scmagazine.com/bracing-for-tomorrows-threats-with-behavioral-analytics/article/757046/?utm_source=newsletter&utm_medium=email&utm_campaign=SCUS_Newswire_20180419&DCMP=EMC-SCUS_Newswire_20180419&email_hash=305F40BE59A0DCB04476BF06C7E07DC9&spMailingID=19408780&spUserID=MjMzMTgxMDAzMgS2&spJobID=1241166881&spReportId=MTI0MTE2Njg4MQS2

RSAC TV: How Hackers Learn and Why You Want This in Your School
Schools around the world are trying to figure out how to best use technology to help students learn better but hackers have already done that. Hackers have figured out how to best learn with the technology they have. This is a look at how hacking skills impact student learning across all school subjects and how hackers use technology to learn more, learn faster and stay safe online.
https://www.rsaconference.com/videos/rsac-tv-how-hackers-learn-and-why-you-want-this-in-your-school

****

"Ctrl -F" for The Board

Framework for Improving Critical Infrastructure Cybersecurity
The U.S. Commerce Department's National Institute of Standards and Technology (NIST) has released version 1.1 of its popular Framework for Improving Critical Infrastructure Cybersecurity, more widely known as the Cybersecurity Framework. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSP.04162017.pdf
"Cybersecurity is critical for national and economic security," said Secretary of Commerce Wilbur Ross. "The voluntary NIST Cybersecurity Framework should be every company's first line of defense. Adopting version 1.1 is a must do for all CEO's." https://www.nist.gov/news-events/news/2018/04/nist-releases-version-11-its-popular-cybersecurity-framework

Cyber War: The Fastest Way to Improve Cybersecurity?

For all the benefits IT in general and the Internet specifically have given us, it has also introduced significant risks to our well-being and way of life. Yet cybersecurity is still not a priority for a majority of people and organizations. No amount of warnings about the risks associated with poor cybersecurity have helped drive… https://ctovision.com/cyber-war-the-fastest-way-to-improve-cybersecurity/

E-commerce fraud has increased 30% from 2016 to 2017.
Thanks mostly to the availability of compromised data. To help you better understand where fraud is being perpetrated and how best to protect against it, we analyzed millions of online transactions to identify fraud attack rates across the United States and incorporated our top insights into this infographic.
http://images.go.experian.com/Web/ExperianInformationSolutionsInc/%7Bfa8ac957-f57e-40ce-9179-ee01800ad90e%7D_18-EXp-14749_2016-17_Heat_Map-v5.pdf

Cost Of Cybercrime Increasing For Financial Sector
It's no secret that cybercrimes cost money to remediate. In fact, the bill can be rather high and in the financial sector, the cost of cybercrime has increased by 40% since 2014. In the past year, it rose 9.6% alone. This is all according to a report conducted by Accenture and the Ponemon Institute.
https://www.sosdailynews.com/news.jspx?&articleid=BF88B1149EFBF49838B60D770C3D7C17&sx=79

Questions
Contact FIPCO's Ken Shaurette at 800/722-3498 ext. 251 or email FIPCO IT Services for more information.

"Make Security Part of You and Your Institution's DNA!"

Threat Intelligence Newsletter: May 14, 2018

FIPCO®
IT Audit
Round Table
Discussions

If you would like to host an event, please contact: Becky Schowalter

Upcoming Threat Intelligence Peer Group Discussions
August 16 - Barron

****

Alerts

Microsoft Patches Two Windows Zero-Day Vulnerabilities:
Microsoft fixes over 60 vulnerabilities with May 2018 Patch Tuesday updates, including two Windows zero-day flaws… https://www.securityweek.com/microsoft-patches-two-windows-zero-day-vulnerabilities

BBB Scam Alert: Shimming is the New Skimming
The new credit card chips make it harder for scammers to steal your payment information, so con artists have created a different technique called "shimming." https://www.creditcards.com/credit-card-news/new-card-skimming-is-called-shimming.php

Bad bots detected on 100% of web login pages, here's how to protect your business
Every website with a login page faces Account Takeover attempts, which increase 300% after a data breach, according to Distil Networks. https://www.techrepublic.com/article/bad-bots-detected-on-100-of-web-login-pages-heres-how-to-protect-your-business/?ftag=TREa988f1c&bhid=78480402

Password behaviors remain largely unchanged
Despite today’s increased threat landscape and heightened global awareness of hacking and data breaches, password behaviors remain largely unchanged. Data from a survey conducted by Lab42 shows that 91 percent of people know that using the same password for multiple accounts is a security risk, yet 59 percent continue to use the same password. As a result, individuals’ behavior in creating, changing and managing passwords in both their professional and personal lives is slow to…
https://www.helpnetsecurity.com/2018/05/03/password-behaviors/

SamSam ransomware designed to inundate targeted networks with thousands of copies of itself
SamSam ransomware designed to inundate targeted networks with thousands of copies of itself
The ongoing SamSam ransomware campaign responsible for recently infecting the city of Atlanta, the Colorado Department of Transportation and an array of health care organizations represents an emerging operational model for malicious cryptors, according to researchers at Sophos. https://www.scmagazine.com/samsam-ransomware-designed-to-inundate-targeted-networks-with-thousands-of-copies-of-itself/article/762178/?utm_source=newsletter&utm_medium=email&utm_campaign=SCUS_Newswire_20180501&DCMP=EMC-SCUS_Newswire_20180501&email_hash=305F40BE59A0DCB04476BF06C7E07DC9&spMailingID=19481141&spUserID=MjMzMTgxMDAzMgS2&spJobID=1260043787&spReportId=MTI2MDA0Mzc4NwS2

Phishing alert: Hacking gang turns to new tactics in malware campaign
Off-the-shelf malware kits and mass phishing campaigns are enabling a small group of Nigerian cybercriminals to conduct hacking campaigns against targets around the world – and the threat they pose to organizations is increasing. The group, dubbed SilverTerrier, isn't a sophisticated operation, but has access to a number of malware families – including information stealers and remote access trojans – which are distributed with the aim of infecting victims and stealing data. Researchers at Palo Alto Networks have been tracking SilverTerrier and have attributed 181,000 attacks, using 15 families of malware, to the group in the last year. Over the past 12 months, the group has fired off an average of 17,600 spam emails a month, representing a 45 percent increase from 2016. "Sending malicious emails does not require a significant amount of resources, but monetizing these infections requires time and attention from the actors," Ryan Olson, intelligence director of Unit 42 at Palo Alto Networks told ZDNet.
https://www.zdnet.com/article/phishing-alert-hacking-gang-turns-to-new-tactics-in-malware-campaign/

Hackers Found Using A New Way to Bypass Microsoft Office 365 Safe Links
Security researchers revealed a way around that some hacking groups have been found using in the wild to bypass a security feature of Microsoft Office 365, which is originally designed to protect users from malware and phishing attacks. Dubbed Safe Links, the feature has been included in Office...
https://thehackernews.com/2018/05/microsoft-safelinks-phishing.html?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+TheHackersNews+%28The+Hackers+News+-+Security+Blog%29&_m=3n.009a.1739.aa0ao086k1.125v

ATM attacks: How hackers are going for gold
Imagine winning the lottery and having an ATM spit huge amounts of cash at you. That's exactly what some cyber criminals are after. They're targeting ATMs and launching "jackpotting" attacks, forcing them to dispense bills like a winning slot machine. Already this year, the U.S. Secret service has warned financial institutions of such attacks. Security researcher Barnaby Jack demonstrated such an attack and amazed attendees at Black Hat when he made two unpatched ATMs spit…
https://www.helpnetsecurity.com/2018/05/11/atm-attacks/

****

Hints & Tips plus Security Awareness

June, Internet Safety Month
Internet Safety Month is the 'purr-fect' excuse to organize a Cyber Safety Day in your community! Remind children the do's and don'ts of safe online posting, whether on vacation or at home. Cyber Safety Day is an ideal Garfield themed activity for summer camps or youth groups. Here's how YOU can get involved…(not a free resource) https://www.cybersafetykits.org/

Planning for Business Continuity and Disaster Recovery (registration required vendor sponsored)
In the current world laden with threat actors profiting from breaches, ransomware payouts and members of the public employing cybercrime-as-a-service, the need for data recovery in an automated, reliable and timely manner is critical for an organization's business continuity. It is no longer an issue of IF you need a business continuity/disaster recovery plan but a matter of WHEN you will deploy one. https://info.armor.com/05232018DisasterRecovery_Registration.html

Best Practices for Protecting Against Phishing, Ransomware and BEC Attacks
MIS-TI June 20, 2018 **|** 1:00 PM - 2:00 PM CT, 1 CPE (No cost to attend), Most organizations have been successfully infiltrated by phishing attempts, and a growing number are being hit by ransomware and other threats. Join us for a discussion on how phishing, ransomware and BEC attacks can be devastating and in some cases—force a business to close its doors.
https://engage.vevent.com/index.jsp?eid=7019&seid=1449

NIST Updates Risk Management Framework to Incorporate Privacy Considerations
Augmenting its efforts to protect the nation's critical assets from cybersecurity threats as well as protect individuals' privacy, the National Institute of Standards and Technology (NIST) has issued a draft update to its Risk Management Framework (RMF) to help organizations more easily meet these goals.
https://www.nist.gov/news-events/news/2018/05/nist-updates-risk-management-framework-incorporate-privacy-considerations

****

News & Views

DHS to roll out national cybersecurity strategy in mid-May
The Department of Homeland Security will issue a national cybersecurity strategy in mid-May, the DHS chief told a key House committee oversight hearing. https://fcw.com/articles/2018/04/26/nielsen-bug-bounty-hearing.aspx

Your next bank card will have a fingerprint scanner built-in
Visa and Mastercard have chips embedded in hundreds of millions of credit and debit cards around the world. They're used in more than 200 countries and process billions of payments each year. And they're both intent on creating bank cards that use your fingerprint instead of a PIN. Early trials of cards with fingerprint scanners built-in are underway and success could eventually result in the death of the humble PIN. "A four-digit PIN is pretty good security – obviously, six, seven or eight digits are better but it is very hard for people to remember," says Bob Reany, an executive vice president at Mastercard, who is working on the firm's biometric cards. "The security is going to be better than a PIN."
http://www.wired.co.uk/article/mastercard-biometric-card-testing-visa-gemalto-scanner-fingerprint-trial

NIST Releases V1.1 of Cybersecurity Framework
On April 16, the National Institute of Standards and Technology released Version 1.1 of its Cybersecurity Framework, which provides a prioritized, flexible, repeatable, performance-based, and cost-effective approach to managing cybersecurity risk at all levels of an organization. Version 1.1 is fully compatible with Version 1.0 and has revised provide a more comprehensive treatment of identity management and additional description of how to manage supply chain cybersecurity. nist.gov/cyberframework

****

"Ctrl -F" for The Board

Cybersecurity Roles and Responsibilities for the Board of Directors

Boards of Directors are ultimately liable and responsible for the survival of their organizations, and in today’s interconnected world, cyber resilience is big part of that responsibility. That means that Boards must take an active role in cybersecurity.

In this blog post we take a look at some of the responsibilities that Boards of Directors should consider as they take on the role of cybersecurity leaders within their organizations. https://www.sagedatasecurity.com/blog/cybersecurity-roles-and-responsibilities-for-the-board-of-directors?utm_campaign=Blog&utm_source=hs_email&utm_medium=email&utm_content=62496524&_hsenc=p2ANqtz-_S7njt8ziyFoCVug2TX0sUc2bEngr7K7MwLVkHw5_eqntR3hEGn4dsiAB4XLMwSPpOA3b9kIFPtic33vny4gKYJFrXcQ&_hsmi=62496524

Cybersecurity Questions Board of Directors Should Be Asking

As cybercrime continues to soar, it’s time for the Board of Directors to take responsibility. Directors and other Senior Managers need to gain an understanding of the cyber risks they are facing as an organization and stay informed on a continual basis. After all, they will be held responsible should a breach occur. In this post, we share a list of ten questions the Board needs answered, and why, in order to take on their cybersecurity roles and responsibilities. https://www.sagedatasecurity.com/blog/cybersecurity-questions-board-of-directors-should-be-asking?utm_campaign=Blog&utm_source=hs_email&utm_medium=email&utm_content=62496524&_hsenc=p2ANqtz-_S7njt8ziyFoCVug2TX0sUc2bEngr7K7MwLVkHw5_eqntR3hEGn4dsiAB4XLMwSPpOA3b9kIFPtic33vny4gKYJFrXcQ&_hsmi=62496524

Questions

Contact FIPCO’s Ken Shaurette at 800/722-3498 ext. 251 or email FIPCO IT Services for more information.

"Make Security Part of You and Your Institution's DNA!"

Threat Intelligence Newsletter: May 25, 2018

If you would like to host an event, please contact: Becky Schowalter

Upcoming Threat Intelligence Peer Group Discussions
August 16 - Barron

FBI Releases Article on Building a Digital Defense with Credit Reports
FBI has released an article on using credit reports to build a digital defense against identify theft. FBI explains how identity theft can deal a devastating blow to consumers' credit history. However, regularly checking the accuracy of credit reports can help consumers minimize risk. NCCIC encourages consumers to review the ***FBI Article*** (https://www.fbi.gov/contact-us/field-offices/portland/news/press-releases/fbi-tech-tuesday-building-a-digital-defense-with-credit-reports) and NCCIC's Tip on ***Preventing and Responding to Identity Theft*** **(**https://www.us-cert.gov/ncas/tips/ST05-019).

****

Alerts

Critical vulnerabilities in PGP/GPG and S/MIME email encryption, warn researchers
Efail flaw "might reveal the plaintext of encrypted emails". https://www.grahamcluley.com/critical-vulnerabilities-in-pgp-gpg-and-s-mime-email-encryption-warn-researchers/

PDF Exploit built to combine zero-day Windows and Adobe Reader bugs
A privilege escalation vulnerability that was patched last week in Microsoft Windows and an Adobe Reader remote code execution bug that was fixed yesterday in a product update were both jointly targeted by a PDF-based zero-day exploit prior to their discovery, researchers from ESET reported today.
https://www.scmagazine.com/pdf-exploit-built-to-combine-zero-day-windows-and-adobe-reader-bugs/article/766100/?utm_source=newsletter&utm_medium=email&utm_campaign=SCUS_Newswire_20180516&DCMP=EMC-SCUS_Newswire_20180516&email_hash=305F40BE59A0DCB04476BF06C7E07DC9&spMailingID=19571606&spUserID=MjMzMTgxMDAzMgS2&spJobID=1260998070&spReportId=MTI2MDk5ODA3MAS2

Masked Amplified DDoS Attacks
Surreptitious attackers have amplified DDoS assaults by delivering malicious payloads through nonstandard ports. Called Masked Amplification attacks, these attacks deliver payloads to nonstandard ports using Universal Plug and Play protocols (UPnP). https://security.radware.com/ddos-threats-attacks/threat-advisories-attack-reports/masked-amplified-ddos/?elqTrackId=e30e2de4a2cc4959a88ae71a2b88f3a1&elq=0e57c33e4af1435c95954972edc23099&elqaid=3467&elqat=1&elqCampaignId=2398

A scam story: Secret shopping and fake checks
Scammers need a good story to get to your wallet. Once they find one that works, they use it again and again. One of their old favorites brings together fake checks and secret shopping, and we've been hearing a lot about it lately. https://www.consumer.ftc.gov/blog/2018/05/scam-story-secret-shopping-and-fake-checks?utm_source=govdelivery

New Phishing Attack Will Drain Your Bank Account
Cryptocurrency is one of those things that most of us have heard about and maybe even discussed, even if we don't truly understand it. But for those who have a good grasp of it, opportunity awaits. Though there is not a centralized bank for cryptocurrency, it is not immune from people trying to rob it. Unlike the bank heists of the past, these crimes are committed purely online.
https://www.theregister.co.uk/2018/01/25/uk_prime_minister_encryption/

Banks Beware: Lawsuits Challenging Website Accessibility are Gaining Steam
As Americans become ever more reliant upon the Internet to obtain information and perform everyday tasks, companies' websites are increasingly being scrutinized to determine whether they are accessible to people with disabilities. This scrutiny has significant legal and financial implications, as an increasing number of lawsuits are being filed challenging website accessibility under the Americans with Disabilities Act (ADA). Subscription is required, however American Banker has a full article on this topic just published.
https://www.americanbanker.com/news/banks-are-sitting-ducks-for-ada-lawsuits
https://www.fosterswift.com/communications-banks-beware-lawsuits-website-accessibility.html

Critical Tech Firms Coordinate Disclosure of New Meltdown, Spectre Flaws
Intel, AMD, ARM, IBM, Microsoft and other major tech companies on Monday released updates, mitigations and advisories for two new variants of the speculative execution attack methods known as Meltdown and Spectre. https://www.securityweek.com/tech-firms-coordinate-disclosure-new-meltdown-spectre-flaws

New alert for Western Union refunds
Did you lose money to a scam, wiring the money via Western Union between January 1, 2004 and January 19, 2017? If so, you might know that May 31 is the deadline for filing your claim to get money back from the FTC's and the Department of Justice's settlement with Western Union. With the deadline fast approaching, we know two things: (1) there will probably be a rush of last-minute filers; and (2) scammers will try to take advantage of the people filing claims. https://www.consumer.ftc.gov/blog/2018/05/new-alert-western-union-refunds?utm_source=govdelivery

Brain Food botnet infected 5,000+ websites with malicious PHP scripts in past 4 months
The botnet tries to trick users into buying fake diet and brain-boosting pills in order to steal personal info. It does a great job of hiding itself, and it's spreading like wildfire. https://www.techrepublic.com/article/brain-food-botnet-infected-5000-websites-with-malicious-php-scripts-in-past-4-months/?ftag=TREa988f1c&bhid=78480402

****

Hints & Tips plus Security Awareness

Specops and Thycotic Password Auditor and IT Mgmt Tools
Authentication and password security is more important than ever. Free tool allows you to measure existing password policies against industry best practices and compliance standards. https://specopssoft.com/product/specops-password-auditor/?utm_source=Sponsored%20Article&utm_medium=Referral&utm_campaign=Helpnet%20security or https://thycotic.com/solutions/free-it-tools/secret-server-free/

How to Secure your PC after a Fresh Windows Installation
If you are planning on doing a fresh Windows installation on your computer, make sure you apply these security measures after this procedure. It's important to secure your PC and keep it safe from malicious actors trying to harvest your most valuable data. Consider reading this useful guide that will show you all the steps you need to take to enhance protection for your PC. https://heimdalsecurity.com/blog/fresh-windows-installation-security-guide/?utm_source=Heimdal+Security+Newsletter+List&utm_campaign=14c12a0ea9-EMAIL_CAMPAIGN_2018_05_18&utm_medium=email&utm_term=0_31fbbb3dbf-14c12a0ea9-194307777

How can Office 365 phishing threats be addressed?
With the rapid expansion of Office 365, more and more threats can emerge within its infrastructure, particularly via email. This is due in part to the size and ease of compromising Office 365 accounts and comes to the detriment of the same broad audience among which Office 365 has seen such massive adoption. Office 365 email security is now a common concern among many organizations small and large alike for exactly this reason. Some vendors… https://www.helpnetsecurity.com/2018/05/18/office-365-phishing-threats/

4 best practices for cyber intelligence in business
Researchers at Carnegie Mellon's Software Engineering Institute (SEI) have released a study (https://insights.sei.cmu.edu/sei_blog/2018/05/best-practices-for-cyber-intelligence.html) identifying the best practices and major challenges organizations face concerning cybersecurity. With funding from the US Office of the Director of National Intelligence, the report highlights what the best organizations are doing to protect themselves digitally. https://www.techrepublic.com/article/4-best-practices-for-cyber-intelligence-in-business/

CISO's Toughest Battle: Finding the Right Weapons to Fight
This and sever other articles in the CyberDefense Magazine.
http://www.cyberdefensemagazine.com/newsletters/may-2018/mobile/index.html#p=1

****

News & Views

DHS rolls out national cybersecurity strategy
The Department of Homeland Security issued a national comprehensive treatment of identity management and additional description of how to manage supply chain cybersecurity. This strategy provides the Department with a framework to execute our cybersecurity responsibilities during the next five years to

keep pace with the evolving cyber risk landscape by reducing vulnerabilities and building resilience; countering malicious actors in cyberspace; responding to incidents; and making the cyber ecosystem more secure and resilient. https://www.dhs.gov/publication/dhs-cybersecurity-strategy

Don't let attackers worm their way in: Increase password security
Passwords are inherently the weakest form of authentication, yet they remain the most prevalent. Many organizations realize that moving beyond this single point of vulnerability is required but replacing passwords or adding multi-factor authentication (MFA) to all use cases can be daunting if not impossible. As such, it is undoubtedly important to enforce strong password policies to ensure that this first and often time's only line of defense can withstand common attacks. In recent years, …
https://www.helpnetsecurity.com/2018/05/21/increase-password-security/

DHS NCCIC Ransomware Awareness Briefings
In the last few years, organizations around the world have lost tens of millions of dollars to ransomware – a type of malicious software, or malware, that threatens to publish the victim's data or perpetually block access to it unless a ransom is paid. https://share.dhs.gov/nccicbriefings

****

"Ctrl -F" for The Board

Staying One Step Ahead of Cyber Crime
Part 3 in a series. Read Parts 1 https://bankingjournal.aba.com/2018/05/innovating-and-automating-in-2018/ and 2 https://bankingjournal.aba.com/2018/05/the-ongoing-hunt-for-talent/.
With each passing year, the number of fraud victims continues to grow, and data breaches have become routine occurrences. The introduction of EMV technology has shifted the fraud landscape to include more instances of card-not-present and online fraud: from 2015 to 2016, card-not-present fraud increased 40 percent and account takeover fraud was up 31 percent, according to Javelin Strategy & Research.
https://bankingjournal.aba.com/2018/05/staying-one-step-ahead-of-cyber-crime/?utm_campaign=ABA-Newsbytes-052218&utm_medium=email&utm_source=Eloqua

Password pattern analysis: Risky, lazy passwords the norm
Dashlane announced the findings of an analysis of over 61 million passwords. The analysis was conducted with research provided by Dr. Gang Wang, an Assistant Professor in the Department of Computer Science at Virginia Tech. Researchers examined the data for patterns, illuminating simple...
https://www.helpnetsecurity.com/2018/05/24/password-pattern-analysis/

Questions
Contact FIPCO's Ken Shaurette at 800/722-3498 ext. 251 or email FIPCO IT Services for more information.

"Make Security Part of You and Your Institution's DNA!"

Threat Intelligence Newsletter: June 15, 2018

FIPCO®
IT Audit
Round Table
Discussions

If you would like to host an event, please contact: Becky Schowalter

Upcoming Threat Intelligence Peer Group Discussions
August 16 - Barron

****

Alerts & Warnings

VPNFilter malware infecting 500,000 devices is worse than we thought (power recycle your home routers)
Malware tied to Russia can attack connected computers and downgrade HTTPS. Two weeks ago, officials in the private and public sectors warned that hackers working for the Russian government infected more than 500,000 consumer-grade routers in 54 countries with malware that could be used for a range of nefarious purposes. Now, researchers from Cisco's Talos security team say additional analysis shows that the malware is more powerful than originally thought and runs on a much broader base of models, many from previously unaffected manufacturers. https://arstechnica.com/information-technology/2018/06/vpnfilter-malware-infecting-50000-devices-is-worse-than-we-thought/

BackSwap Trojan exploits standard browser features to empty bank accounts
Creating effective and stealthy banking malware is becoming increasingly difficult, forcing malware authors to come up with innovative methods. The latest creative burst in this malware segment comes from a group that initially came up with malware stealing cryptocurrency by replacing wallet addresses in the clipboard. About the BackSwap banking malware "To steal money from a victim's account via the internet banking interface, typical banking malware will inject itself or its specialized banking module into..."
https://www.helpnetsecurity.com/2018/05/29/backswap-trojan/

Asked to pay by gift card? Don't.
Has someone asked you to go get a gift card to pay for something? Lots of people have told us they've been asked to pay with gift cards – by a caller claiming to be with the IRS, or tech support, or a so-called family member in need. If you've gotten a call like this, you know that the caller will then demand the gift card numbers and PIN. And, poof, your money is gone. https://www.consumer.ftc.gov/blog/2018/05/asked-pay-gift-card-dont?utm_source=govdelivery

Con Artists Use Facebook Messenger to Contact Victims
If you are on Facebook, watch out for scams using Messenger. In the past month, BBB Scam Tracker has received dozens of reports about con artists using Facebook Messenger to promote phony grants. https://www.bbb.org/en/us/article/news-releases/16920-bbb-tip-government-grant-scam
Report scam accounts and messages to Facebook: Alert Facebook to fake profiles, compromised accounts, and spam messages by reporting them here.
https://www.facebook.com/help/181495968648557?helpref=faq_content

Sweepstakes, Lottery and Prize Scams: A Better Business Bureau Study of How "Winners" Lose Millions Through an Evolving Fraud
Sweepstakes, lottery and prize scams are among the most serious and pervasive frauds operating today. While the scams' roots go as far back in the culture as gambling, the fraud continues to evolve with the times. The scheme currently involves scammers telling people they have won a large amount of money in a lottery or sweepstakes, sometimes by misusing the established name of Publishers Clearing House Sweepstakes. https://www.bbb.org/en/us/article/news-releases/17786-sweepstakes-lottery-and-prize-scams-a-better-business-bureau-study-of-how-winners-lose-millions-through-an-evolving-fraud, Winners are Losers: https://www.consumer.ftc.gov/blog/2018/06/winners-are-losers-lottery-sweepstakes-scams?utm_source=govdelivery

Sophisticated keyloggers target the finance industry
Lastline found three separate strains of keylogger malware that are currently targeting finance. Lastline's analysis of the 100 most recent malware samples found among finance firms uncovered an unusually large number of iSpy keylogger samples, which is a variant of the notorious HawkEye logger, a fully functioning keylogger that sends victim's credentials to a server under the keylogger operator's control. By intercepting the communication with the command and control server, Lastline detected the active exfiltration…
https://www.helpnetsecurity.com/2018/06/06/keyloggers-finance-industry/

Combosquatting -- A New Fake Web Page Scam that Can Fool Experts
Internet crooks have come up with a new way of tricking users into visiting a fake website – combosquatting. https://phys.org/news/2017-10-combosquatting-plain-sight-users.html and https://www.scambusters.org/combosquatting.html

Untangling a robocaller web
Sick of getting robocalls and other unwanted calls? You can learn more about how to block them at ftc.gov/calls. You also might know that the FTC continues to go after the people and companies behind these calls. Case in point: today the FTC announced a case against a group of defendants that it alleges are responsible for billions of illegal robocalls. https://www.consumer.ftc.gov/blog/2018/06/untangling-robocaller-web?utm_source=govdelivery

BBB: Tech Support Scammers Offer Phony Refunds
In most tech support scams, a phony representative helps you "fix" a computer problem you didn't realize you had - for a fee. As more people catch on to this popular scam, con artists find new twists on the same old trick. This time, it involves offering you a efund. https://www.bbb.org/en/us/article/news-releases/16553-bbb-tip-tech-support-scams?utm_source=scam-alert&utm_medium=email&utm_campaign=Scam-Ed

****

Hints & Tips plus Security Awareness

Free credit freezes are coming soon
Looking for stronger ways to protect your credit? Thanks to a new federal law, soon you can get free credit freezes and year-long fraud alerts. Here’s what to look forward to when the law takes effect on September 21st: https://www.consumer.ftc.gov/blog/2018/06/free-credit-freezes-are-coming-soon-0?utm_source=govdelivery

Psychological first aid (PFA), or Disaster Psycho-social Support (DPS).
A useful session based and structured on the guide and other materials (freely) available from the World Health Organization. While a good deal of the WHO stuff relates to aid workers in disaster areas, most of it is still going to be applicable to PFA/DPS in your own company BC/DR plan. (Your company BCP *does* cover DPS, doesn't it?)
http://www.who.int/mental_health/publications/guide_field_workers/en/

Ten Best Practices for Outsmarting Ransomware
Almost a year after WannaCry made global news headlines, a number of high-profile organizations have continued to be targeted by this ransomware, some quite recently. It's part of a growing trend that has the potential to impact large numbers of people, and with potentially devastating consequences.
https://www.scmagazine.com/ten-best-practices-for-outsmarting-ransomware/article/767628/?utm_source=newsletter&utm_medium=email&utm_campaign=SCUS_Newswire_20180530&DCMP=EMC-SCUS_Newswire_20180530&email_hash=305F40BE59A0DCB04476BF06C7E07DC9&spMailingID=19651065&spUserID=MjMzMTgxMDAzMgS2&spJobID=1261816263&spReportId=MTI2MTgxNjI2MwS2

27 ways to reduce insider security threats (PDF)
Insider threats can pose even greater risks to company data than those associated with external attacks. This ebook offers a collection of practical strategies that IT pros can follow to identify areas of risk and take steps to mitigate them. http://b2b.cbsimg.net/downloads/Gilbert/TR_EB_insider_threats.pdf

Building Blocks for a Threat Hunting Program
The number and severity of cyberattacks are sending businesses scrambling to figure out their threat intelligence strategies: how to collect threat data, organize it into actionable information, prioritize the most severe threats, and address the biggest problems.
Threat intelligence is among the hottest buzzwords in cybersecurity today, and with good reason. As attacks become more severe, frequent, and complex, businesses struggle to detect and mitigate them with limited resources. New platforms promise artificial intelligence to pick up the slack by processing alerts, freeing up employees for focus on more complex tasks. The problem is there are precious few people who know what to do with threat intelligence once they have it, and they don’t come cheap.
https://www.darkreading.com/analytics/building-blocks-for-a-threat-hunting-program/d/d-id/1331936

What Your Financial Institution Needs to Know About VPNFilter Malware
On May 23rd, the United States Computer Emergency Readiness Team (US-CERT) issued an alert about malware that has been discovered on over 500,000 Internet routers used in homes and small offices. The malware, named VPNFilter, is notable because the initial part of the malware is designed to be persistent and able to survive a reboot (and in some cases a factory reset) of the router.
https://www.bedelsecurity.com/blog/what-your-financial-institution-needs-to-know-about-vpnfilter-malware?utm_campaign=RSS%20Feed&utm_source=hs_email&utm_medium=email&utm_content=63410

395&_hsenc=p2ANqtz-8KTh0wHinBz1pS1WUZAKA3rpywyJluF9XJ_Fga-jufxwWkb9BBw7qWLnONiRh0o54HltgGJ8mzrtR1gVj0EP2bfo6z-w&_hsmi=63410395

6 Enterprise Password Managers That Lighten the Load for Security
EPMs offer the familiar password wallet with more substantial administrative management and multiple deployment models. https://www.darkreading.com/endpoint/6-enterprise-password-managers-that-lighten-the-load-for-security-/d/d-id/1331711?cid=malp&_mc=malp

Special Publication 800-125A Revision 1, Security Recommendations for Virtual Servers
Server Virtualization is now a key component for enterprise IT infrastructure in data centers and cloud services. Virtual servers provide better utilization of hardware resources, reduces physical space required for physical servers, and reduced power consumption as well. The core software used for server virtualization, the Hypervisor, directly provides CPU and memory virtualization.
https://csrc.nist.gov/News/2018/NIST-Publishes-SP-800-125A-Rev-1

Protecting your devices from cryptojacking
Instead of min(d)ing their own business, are scammers using your computer as their virtual ATM? Three years ago, the FTC warned the public and took action against cryptojacking. That's where scammers use your device's processing power to "mine" cryptocurrency, which they can then convert into cold, hard cash.
https://www.consumer.ftc.gov/blog/2018/06/protecting-your-devices-cryptojacking?utm_source=govdelivery

****

News & Views

A Prospective Vendor Either Won't or Can't Provide the Documentation We Need. What Should We Do?
We're doing our due diligence on a new HR software package. We've requested the vendor's financials and a SOC 2 report, but they told us they don't provide financials (they are privately held), and their SOC 2 won't be completed until the end of the year. They do have a SOC 1. What are your thoughts on this?
https://complianceguru.com/2018/05/ask-the-guru-a-prospective-vendor-either-wont-or-cant-provide-the-documentation-we-need-what-should-we-do/?utm_source=hs_email&utm_medium=email&utm_content=63392814

INSIDER THREAT AND THE MALICIOUS INSIDER THREAT – Analyze. Deter. Discover. Prevent. Respond.
Building a quarterly journal that spans broad topical and technical themes can be challenging, and the selection of articles for any one journal intimidating. Over the last five years CSIAC has published special issues on military research laboratories… https://www.csiac.org/wp-content/uploads/2018/04/CSIAC_Journal_V5N4_5.03.18_WEBVERSION.pdf

US says North Korea behind malware attacks
North Korea has been spying on US public infrastructure, aerospace, financial and media companies for nine years using a malware. This was revealed by FBI and DHS who said that North Korea used two pieces of malware to target the key US cyber assets. While this news is important for all US companies, it is surprising that the authorities took nine long years to discover the North Korean malware.
https://www.apnews.com/9fb4327df4994d93a3b5c49ee227b2e0/US-says-North-Korea-behind-malware-attacks

****

"Ctrl -F" for The Board

Why creativity is key to security
Similar to corporate auditors and risk and compliance managers, security teams are often viewed as a hindrance to business growth. They are deemed the killjoys of business innovation by imposing restrictions on access, rules and controls, and responding with “no.” Given this perception, security teams are often times not thought of as innovative or creative. Yet that’s precisely what needs to happen. Mounting pressures forcing change Security teams are under tremendous pressure today. According to…
https://www.helpnetsecurity.com/2018/06/07/creativity-security/

Questions
Contact FIPCO’s Ken Shaurette at 800/722-3498 ext. 251 or email FIPCO IT Services for more information.

"Make Security Part of You and Your Institution's DNA!"

Threat Intelligence Newsletter: June 25, 2018

FIPCO®
IT Audit
Round Table
Discussions

If you would like to host an event, please contact: Becky Schowalter

Upcoming Threat Intelligence Peer Group Discussions
August 16 - Barron

****

Alerts & Warnings

Facebook confirms bug messed with 14 million users' sharing settings
Facebook has admitted that, between May 18 and 27, posts by some 14 million users were automatically set to be shared with the public. "Every time you share something on Facebook, we show you an audience selector so you can decide who gets to see the post. This is based on the people you shared with last time you posted," Erin Egan, the company's Chief Privacy officer explained. "For example, if you choose to share… https://www.helpnetsecurity.com/2018/06/08/facebook-privacy-settings-bug/"

Hackers using Excel IQY files to dodge antivirus and download malware
Security researchers have discovered a new spam email campaign using a novel approach to infect victims. Users tricked into downloading and executing malicious script via Excel. https://www.scmagazine.com/hackers-using-excel-iqy-files-to-dodge-antivirus-and-download-malware/article/772104/?utm_source=newsletter&utm_medium=email&utm_campaign=SCUS_Newswire_20180611&email_hash=305f40be59a0dcb04476bf06c7e07dc9

Work from Home Business Scam Sidelined
Would you be tempted by an online business training program that promises you could earn thousands of dollars a month working from home? I wouldn't blame you if you were. But don't believe the hype. Promises like these are signs of an online business scam.
https://www.consumer.ftc.gov/blog/2018/06/work-home-business-scam-sidelined?utm_source=govdelivery

Securities Regulators Warn of Increasing Promissory Note Scams
The search for high investment returns, especially in this era of historically low (but now rising) interest rates, continues to lure savers and investors into dubious financial schemes. Top of the list for scams in the U.S. are short-term promissory notes, a sort of loan investors can make to businesses.
https://www.scambusters.org/promissorynote.html

Scams and Your Small Business
At the FTC, our mission is to protect consumers, including small business owners. That's why, when we see scammers taking money from small businesses, we step in. Today, the FTC announced Operation Main Street: Stopping Small Business Scams, a coordinated law enforcement and education effort with state and federal partners, as well as the Better Business Bureau (BBB), to stop scams that target small businesses.
https://www.consumer.ftc.gov/blog/2018/06/scams-and-your-small-business?utm_source=govdelivery
BBB New Report – Scams and Your Small Business - https://www.bbb.org/SmallBusiness

This sneaky Windows malware delivers adware – and takes screenshots of your desktop
A newly uncovered form of stealthy and persistent malware is distributing adware to victims across the world while also allowing attackers to take screenshots of infected machines' desktops. Discovered by researchers at Bitdefender, the malware has been named Zacinlo after the name of the final payload that's delivered by the campaign which first appeared in 2012. The vast majority of Zacinlo victims are in the US, with 90 percent of those infected running Microsoft Windows 10. There are also victims in other regions of the world, including Western Europe, China and India. A small percentage of victims are running Windows 7 or Windows 8. https://www.zdnet.com/article/this-sneaky-windows-malware-delivers-adware-and-takes-screenshots-of-your-desktop/

Impostor Scams Now Costing Americans $328 Million a Year
Americans are losing more money to impostors than to any other fraud, according to a recently published report from the Federal Trade Commission (FTC). Scammers pretending to be a friend, relative, police, tax official, tech support, or any one of many other phony roles are now taking more than $328 million out of our pockets every year. https://www.scambusters.org/impostor2.html

Credit card processing "deals" may be scams
If you're in a small business, you probably need a way for people to pay you – and ways to lower your costs. Scammers have been working both of those angles, promising businesses that they can save on leases of credit card processing equipment. They've also been promising that businesses can cancel any time.
https://www.consumer.ftc.gov/blog/2018/06/credit-card-processing-deals-may-be-scams?utm_source=govdelivery

****

Hints & Tips plus Security Awareness

Microsoft: This Azure password-banning tool will help kill off bad 'P@$$w0rd' habits
Admins can now significantly reduce the risk of accounts being compromised by password-spraying attacks. https://www.techrepublic.com/article/microsoft-this-azure-password-banning-tool-will-help-kill-off-bad-pw0rd-habits/?ftag=TREa988f1c&bhid=78480402

Here are the 4 best ways to train employees for better cybersecurity
Email security threats remain a pervasive issue for organizations large and small, according to a recent report from Barracuda (https://www.barracuda.com/campaign/emailsecurityreport). Some 87% of IT security professionals said their company experienced an attempted email-based threat in the past year, while 35% said they have been hit by a ransomware attack, the report found. https://www.techrepublic.com/article/here-are-the-4-best-ways-to-train-employees-for-better-cybersecurity/

Early detection of compromised credentials can greatly reduce impact of attacks
According to Blueliv's credential detection data, since the start of 2018 there has been a 39% increase in the number of compromised credentials detected from Europe and Russia, compared to the same period in 2017 (January-May). In fact, Europe and Russia are now home to half of the world's credential theft victims (49%). In this podcast, Patryk Pilat, Head of Engineering and Cyberthreat Intelligence at Blueliv, talks about the report, and illustrates how these startling… https://www.helpnetsecurity.com/2018/06/19/detect-compromised-credentials/

3 Tips for Driving User Buy-in to Security Policies
IT usage and security policies can be an annoyance for employees who simply see them as draconian roadblocks for their daily activities. With the rise of privacy tools, such as VPNs and privacy-focused web browsers, it's never been easier for users to circumvent organizational controls and, in turn, increase a company's risk profile. Case in point: A 2018 Insider Threat Intelligence Report (https://dtexsystems.com/2018-insider-threat-intelligence-report/) from Dtex found that last year 60% of users surveyed were using anonymous or private browsing to bypass company security policies. https://www.darkreading.com/vulnerabilities---threats/3-tips-for-driving-user-buy-in-to-security-policies/a/d-id/1332053

How to allow users to report suspicious emails with Outlook's Report Message feature
The best defense against phishing attacks for enterprises may be self-reporting employees. Report Message for Outlook provides an easy to use reporting mechanism. https://www.techrepublic.com/article/how-to-allow-users-to-report-suspicious-emails-with-outlooks-report-message-feature/?ftag=TREa988f1c&bhid=78480402

****

News & Views

20-year-old email bug is used to spoof signatures: Here's how to protect yourself
Email encryption tools GnuPG, Enigmail, GPGTools, and python-gnupg have all been updated to patch the critical vulnerability. https://www.techrepublic.com/article/20-year-old-email-bug-is-used-to-spoof-signatures-heres-how-to-protect-yourself/?ftag=TREa988f1c&bhid=78480402

****

"Ctrl -F" for The Board

Mark your calendar: 2018 Governor's Cybersecurity Summit September 10, 2018
2018 Conference Highlights:

- Keynote presentation from innovation keynoter, futurist, and professor Christina "CK" Kerley
- More information coming soon!

https://wigcot.eventsair.com/QuickEventWebsitePortal/cybersecurity18/cybersummit18

Questions
Contact FIPCO’s Ken Shaurette at 800/722-3498 ext. 251 or email FIPCO IT Services for more information.

"Make Security Part of You and Your Institution's DNA!"

Threat Intelligence Newsletter: July 11, 2018

FIPCO®
IT Audit
Round Table
Discussions

If you would like to host an event, please contact: Becky Schowalter

Upcoming Threat Intelligence Peer Group Discussions
August 16 - Barron

****

Alerts & Warnings

MS Office 365 Manipulated In Two Ways To Get Malware To You
Cybercriminals can be very crafty. Within the past couple of months, they have discovered a couple of new ways to fool Microsoft Office 365 Advanced Threat Protection (APT) anti-phishing capabilities. As reported by researchers at Avanan, both involve sending malicious links through email messages or by sending malicious attachments in email. They are very tricky abuses of the features of Office 365 and both should be considered serious…
https://www.sosdailynews.com/news.jspx?&articleid=948E6EE6F1AC25B3D4CCF336B04C9271&sx=79

Hackers use phoney invoice email to trick you into downloading malware
A newly uncovered hacking campaign is targeting industries including shipping and transport for the purpose of cyber espionage — with security researchers pointing to a well-funded and highly capable operation working out of China as the culprit. Attackers have sent thousands of phishing emails loaded with trojan malware — primarily to organisations in India, Saudi Arabia and South-East Asia — with the intention of duping users into installing a malicious payload equipped with the capability to steal credentials and log keystrokes from infected systems. https://www.zdnet.com/article/hackers-use-phoney-invoice-email-to-trick-you-into-downloading-malware/

New Malware Variant Hits With Ransomware or Cryptomining
A long-known ransom Trojan has added new tactics and a new talent, according to research released by Kaspersky Labs. The Trojan-Ransom.Win32.Rakhni family has been around since 2013, but a new variant does a search of files on the victim's system and decides whether to launch ransomware — or simply use the computer to mine cryptocurrency. Researchers identified a new variant of the remote execution

downloader that queries the victim's system on a number of factors, from the existence of Bitcoin storage to the presence of certain virtual machine managers, before deciding which attack to launch. https://www.darkreading.com/attacks-breaches/new-malware-variant-hits-with-ransomware-or-cryptomining/d/d-id/1332221

This password-stealing malware just added a new way to infect your PC
A powerful form of malware which can be used to distribute threats including Trojans, ransomware and malicious cryptocurrency mining software has been updated with a new technique which has rarely been seen in the wild.
Distributed in spam email phishing campaigns, Smoke Loader has been sporadically active since 2011 but has continually evolved. The malware has been particularly busy throughout 2018, with campaigns including the distribution of Smoke Loader via fake patches for the Meltdown and Spectre vulnerabilities which emerged earlier this year. https://threatbrief.com/this-password-stealing-malware-just-added-a-new-way-to-infect-your-pc/

****

Hints & Tips plus Security Awareness

FSB Proposes 'Cyber Lexicon' to Promote Consistency
Financial Stability Board (FSB); To ensure that banks and regulators around the world can cooperate effectively on cybersecurity, the Basel, Switzerland-based Financial Stability Board yesterday issued a proposed "cyber lexicon" to facilitate cross-border understanding and information sharing. The lexicon includes 50 key terms related to cybersecurity and cyber resilience in the financial sector. Comments on the proposed lexicon are due by August 20. http://www.fsb.org/wp-content/uploads/P020718.pdf?utm_campaign=ABA-Newsbytes-070318&utm_medium=email&utm_source=Eloqua

Cyber Defense eMagazine - June 2018 Edition has arrived
We hope you enjoy this month's edition...packed with over 150 pages of excellent content. InfoSec Knowledge is Power. http://www.cyberdefensemagazine.com/newsletters/june-2018/mobile/index.html

4 Basic Principles to Help Keep Hackers Out
Organizations continue to learn the hard way that when it comes to IT security, the simplest things often cause the biggest problems. A network is only as secure as its weakest link, so hackers don't need to spend the time and money it takes to develop advanced persistent threats or zero-day attacks; they just need to focus on finding the easiest ways of getting in. In other words, the most effective hackers keep things simple, something organizations must take into account. https://www.darkreading.com/attacks-breaches/4-basic-principles-to-help-keep-hackers-out/a/d-id/1332197

3 mobile security tips to thwart fraudsters
It's common to see stories about a new hack or malware attack feature stock images of desktop computers or office workers at desks, but the latest quarterly risk report by cybersecurity firm RSA points to a frightening trend that should change that image. Increasingly, the culprit is right in your hand: Cybercriminals are directing their efforts at peoples' mobile devices. As both the RSA and other recents reports show, email phishing remains, by far, the most common way for bad guys to get in. Phishing attempts have grown more sophisticated and realistic, heightening the chances that even savvy users will get duped. https://www.techrepublic.com/article/3-mobile-security-tips-to-thwart-fraudsters/

7 Questions for Evaluating your Security Posture against Insider Threats
Insider threats top the list of the most dangerous cyber risks for organizations worldwide. It doesn't take much effort for insiders to steal your sensitive data, while such activities are hard to discover and impossible to prevent. Unfortunately, lack of visibility into user behavior is one of the key reasons why companies suffer from data breaches that involve either human negligence or malicious intent. To combat insider threats, you need to adopt a holistic approach to data protection. This may be time-consuming and require you to allocate more resources to cyber security. There are various threat detection techniques, but each company is unique and needs a thoughtful approach.
https://www.tripwire.com/state-of-security/risk-based-security-for-executives/connecting-security-to-the-business/7-questions-for-evaluating-your-security-posture-against-insider-threats/

No prizes from the FTC
Recently, someone showed up at the door of the FTC to ask about his prize. He had a mailing saying he'd won $5 million – and the FTC had "certified and verified" it. The letter told him to act immediately to get the money. Otherwise, his millions would be given to somebody else. He'd talked with the so-called officials, who wanted him to pay $500 in fees to claim his (ahem) prize.
https://www.consumer.ftc.gov/blog/2018/06/no-prizes-ftc?utm_source=govdelivery

****

News & Views

How Scammers Use Google for Business Email Compromise
Several companies have made online productivity solutions like G Suite from Google the preferred option for business computing. It's incredibly convenient and usually inexpensive for anyone from solo operations through large enterprises to replace physical machines and all the maintenance that comes with the territory with options like Gmail and other web-based tools. Yet services like Google are regularly exploited by scammers. Google's prominence in the software market as both a SaaS (software as a service) and PaaS (platform as a service) is a kind of double-edged sword – because it's both accessible and familiar, it can be dangerous. https://www.tripwire.com/state-of-security/security-data-protection/cyber-security/how-scammers-use-google-for-business-email-compromise/

****

"Ctrl -F" for The Board

A Seismic Shift: What California's New Privacy Law Means for Cybersecurity
The enactment of the California Consumer Privacy Act of 2018 (CCPA) on June 28 is the latest in a series of new laws and regulations around the world that represent a fundamental shift from the reactionary approach to security governance we've followed since the 1980s. Starting with the European Union's General Data Protection Regulation (GDPR) and continuing with New York's Department of Financial Services (NY DFS) cybersecurity regulations, privacy and security are now inextricably linked in the U.S. https://www.securitymagazine.com/articles/89201-a-seismic-shift-what-californias-new-privacy-law-means-for-cybersecurity

What every SME needs to know about hackers and cyber-security
It seems like not a week goes by at the moment without a new story about a large corporate cyber-security breach. Recent hacks at Ticketmaster, Fortnum & Mason and Dixons Carphone have resulted in customer data being accessed, stolen or potentially compromised. But it's not just large companies that are at risk. Edward Whittingham, founder of online security company Business Fraud Prevention Partnership, believes that it's essential that small and medium-sized enterprises (SMEs) understand that cyber-crime is now a major part of organised crime and they are therefore at risk as well.
https://www.telegraph.co.uk/connect/small-business/what-smes-need-to-know-hackers-cyber-security/

Questions
Contact FIPCO's Ken Shaurette at 800/722-3498 ext. 251 or email FIPCO IT Services for more information.

"Make Security Part of You and Your Institution's DNA!"

Threat Intelligence Newsletter: July 31, 2018

FIPCO®
IT Audit
Round Table
Discussions

If you would like to host an event, please contact: Becky Schowalter

Upcoming Threat Intelligence Peer Group Discussions
August 16 - Barron

****

Alerts & Warnings

Ransomware back in big way, 181.5 million attacks since January
SonicWall announces record numbers for malware volume, ransomware attacks, encrypted threats and chip-based attacks in the mid-year update of the 2018 SonicWall Cyber Threat Report. "Real-time cyber threat intelligence is more critical than ever as cybercriminals continue to find new attack vectors — like encrypted and chip-based attacks," said Chad Sweet, CEO at The Chertoff Group. "To stay protected in the cyber arms race, organizations must use every tool in their security toolbox, particularly technology… https://www.helpnetsecurity.com/2018/07/11/2018-sonicwall-cyber-threat-report/

Widespread Browser Extension Is Collecting Your Data
You have likely heard warnings about installing browser extensions before. Ok, so they can be useful and many of them are fun. In fact, one called Stylish allows a user to customize a website's page to look the way they want it to, rather than them having to see it the way the site's designer intended. That one is so popular that it boasts 1.8 million downloads for both Google Chrome and Firefox. Unfortunately, Stylish also collects data on users' browsing history and sends it back to the developers…
https://www.sosdailynews.com/news.jspx?&articleid=EEDD3E10F0B0CF77D19A2ADEDFFDEEE5&sx=79

Revised Online Banking Malware Creating A Real Mystery For Victims
Researchers from Threat Fabric have found another morphed version of a very dangerous Trojan. LokiBot, which was first seen early in 2017 has already evolved a couple of times, adding new functionality. A previous version uses administrator access that is given when a user is duped into using a fake login screen for various mobile banking apps. It then packed a double punch by being able to lock devices holding them

for ransom. The new one that seems to be using some of the same functionality while "improving" it, targets Android devices; specifically versions 7 and 8.
https://www.sosdailynews.com/news.jspx?&articleid=84532BDB083C50AF334C24100E28218E&sx=79

VMware Tools HGFS out-of-bounds read vulnerability
VMware Tools contains an out-of-bounds read vulnerability in HGFS. Successful exploitation of this issue may lead to information disclosure or may allow attackers to escalate their privileges on guest VMs… https://my.vmware.com/web/vmware/downloads

IC3 Warns of Business Email Compromise Scams
The Internet Crime Complaint Center (IC3) has released an alert on business email compromise scams. This type of scam targets businesses and individuals by using social engineering or computer intrusion to compromise legitimate email accounts and conduct unauthorized fund transfers or obtain personally identifiable information. https://www.ic3.gov/media/2018/180712.aspx

4 exploitable bugs plague Intel Management Engine: Patch now
Some of the flaws require privileged access, but a buffer overflow vulnerability is fairly serious… https://www.techrepublic.com/article/4-exploitable-bugs-plague-intel-management-engine-patch-now/?ftag=TREa988f1c&bhid=78480402

****

Hints & Tips plus Security Awareness

FEMA Releases IS-2900.a Course
The intended audience for this course is the members of the whole community who have a role in providing recovery support – individuals, local, State, tribal, territorial, insular area governments and non-governmental organizations. The revised course is available through the EMI website.
https://training.fema.gov/is/

Cybersecurity Framework What's Up Next
This presentation introduces the audience to the Baldrige Cybersecurity Excellence Builder (BCEB) and provides a brief overview on integrating the BCEB with the Framework for Improving Critical Infrastructure Cybersecurity. https://www.nist.gov/news-events/events/2018/07/cybersecurity-framework-webcast-next

Do You Need a VPN (Virtual Private Network) for Your Internet Safety?
In the clamor for better Internet privacy, people often talk about using a virtual private network, or VPN for short. There's no doubt that a VPN can increase your security, especially when you're on the move and using public networks. But they can also help stop people tracking you when you're using your home network. https://www.scambusters.org/vpn.html

Making Light of the "Dark Web" (and Debunking the FUD)
I'll start this post where I start many of my talks - what does a hacker look like? Or perhaps more specifically, what do people *think* a hacker looks like? It's probably a scary image, one that's a bit mysterious, a shady character lurking in the hidden depths of the internet. People have this image in their mind because that's what they've been conditioned to believe: https://www.troyhunt.com/making-light-of-the-dark-web-and-debunking-the-fud/

No kidnapping, no ransom
Large scale ransomware attacks have been big news over the last few months. Thanks to ever more sophisticated samples — such as the recent variant, Synack —that target victims in almost every country, this has become a global threat. Advice to avoid ransomware: https://www.pandasecurity.com/mediacenter/malware/no-kidnapping-no-ransom/?mc_cid=27ccef52ba&mc_eid=2b2ac7a1bf

Ransomware 101: What Banks Can Do To Mitigate Risk
Ransomware has become one of the most—if not the most—prevalent, effective and successful forms of cybercrime. Ransomware is simple to create and distribute and offers cybercriminals an extremely low-risk, high-reward business model for monetizing malware. Combine this with the fact that most companies and people are unprepared to deal with ransomware, and it's clear why it has become the fastest growing cyber threat to date. https://bankingjournal.aba.com/2018/07/ransomware-101-what-banks-can-do-to-mitigate-risk/?utm_campaign=ABA-Newsbytes-072318&utm_medium=email&utm_source=Eloqua

Exclusive: PwdPwn audits Active Directory DB with 5K passwords in 15-30 seconds
Created by Sydney developer Luke Millanta, the tool is intended for system administrators to conduct audits more regularly and enforce better password rules. Cracking and auditing an Activity Directory database can be a time-consuming process for any admin. But, a new tool called PwdPwn (password pone) from Sydney developer Luke Millanta promises the ability to audit an Active Directory database with more than 5,000 passwords within 15-30 seconds. https://www.techrepublic.com/article/exclusive-pwdpwn-audits-active-directory-db-with-5k-passwords-in-15-30-seconds/?ftag=TREa988f1c&bhid=78480402

****

News & Views

Zero login: Fixing the flaws in authentication
Passwords, birth certificates, national insurance numbers and passports – as well as the various other means of authentication, that we have relied upon for the past century or more to prove who we are to others – can no longer be trusted in today's digital age. That's because the mishandling of these types of personally identifiable information (PII) documents from birth, along with a string of major digital data breaches that have taken place in… https://www.helpnetsecurity.com/2018/07/17/zero-login/

How Scammers Use Google for Business Email Compromise
Several companies have made online productivity solutions like G Suite from Google the preferred option for business computing. It's incredibly convenient and usually inexpensive for anyone from solo operations through large enterprises to replace physical machines and all the maintenance that comes with the territory with options like Gmail and other web-based tools. Yet services like Google are regularly exploited by scammers. Google's prominence in the software market as both a SaaS (software as a service) and PaaS (platform as a service) is a kind of double-edged sword – because it's both accessible and familiar, it can be dangerous. https://www.tripwire.com/state-of-security/security-data-protection/cyber-security/how-scammers-use-google-for-business-email-compromise/

Cyber-Security Professionals Must Rethink Their Strategy Of Beating Cyber-Attacks
It is not a case of "if" a data breach will occur, but "when". Companies would be well advised to shift the emphasis from defending against known external threats and instead focus on identifying attacks as quickly

as possible once they happen – and taking swift action to foil them before they wreak havoc. https://www.informationsecuritybuzz.com/articles/cyber-security-professionals-must-rethink-their-strategy-of-beating-cyber-attacks/

Cybersecurity is Our Shared Responsibility
The Department of Homeland Security and the STOP. THINK. CONNECT.™ Campaign are excited to announce the overarching theme and key messages for the 2018 National Cybersecurity Awareness Month (NCSAM)! https://staysafeonline.org/ncsam/about-ncsam/

Top 5: Ways to protect your privacy
Your privacy is under assault. And I'm not just talking about Facebook. Governments, advertisers, even ISPs want to track you for various reasons from monetization to surveillance.
While laws like Europe's GDPR are trying to give the user more control, you can take matters into your own hands, just to be sure. https://www.techrepublic.com/article/5-ways-to-protect-your-privacy/?ftag=TREa988f1c&bhid=78480402

Emotet creators shift from banking trojan to threat distributor
Symantec researchers predict the firm is presumably taking a cut of the profits made by the threat actors who use its services.
Mealybug, the threat group behind the Emotet banking trojan, has evolved over the years from making its own custom malware to operating as a distributor for other threat groups.
https://www.scmagazine.com/emotet-creators-shift-from-banking-trojan-to-threat-distributor/article/782082/?utm_source=newsletter&utm_medium=email&utm_campaign=SCUS_Newswire_20180723&email_hash=305f40be59a0dcb04476bf06c7e07dc9&hmSubId=XOjrUhr_Swg1

Why Artificial Intelligence Is Not a Silver Bullet for Cybersecurity
Like any technology, AI and machine learning have limitations. Three are detection, power, and people.
https://www.darkreading.com/threat-intelligence/why-artificial-intelligence-is-not-a-silver-bullet-for-cybersecurity/a/d-id/1332336

How to make your small business unattractive to cyberattackers
Cybercriminals perceive small businesses to be lucrative targets. Find out why, and what cybersecurity experts suggest to reduce your digital security risks. https://www.techrepublic.com/article/how-to-make-your-small-business-unattractive-to-cyberattackers/?ftag=TREa988f1c&bhid=78480402

What Are Forensic Artifacts?
"Every contact leaves a trace." These traces are the tiny pieces left behind that we forensic investigators use to help determine in a given situation what happened, where it happened, who it happened to, when it happened, and how it happened, and who did it.
https://www.gillware.com/forensics/blog/articles/favorite-artifacts-part-0-forensic-artifacts/

****

"Ctrl -F" for The Board

How to allocate budget for a well-rounded cybersecurity portfolio
Getting the C-levels to approve an IT security budget is probably one of the most difficult and exasperating tasks that security professionals and IT managers have to do each year. Information security doesn't

contribute directly to the bottom line in most companies and management often views it as a cost. That's why it's essential for infosec professionals and IT managers to allocate the budget they do get as effectively as possible. What should a well-rounded… https://www.helpnetsecurity.com/2018/07/10/cybersecurity-portfolio/

C-Suite Cybersecurity Perspectives
Trends in the Cyberattack Landscape, Security Threats and Business Impacts.
http://images.global.radware.com/Web/Radware/%7Bd53457de-4fad-4941-b6dc-94a12f4c7397%7D_RADWARE_2018_EXECUTIVE_APPLICATION___NETWORK_SECURITY_REPORT.pdf

Here's what US adults actually know about cybersecurity
While cybersecurity attacks are becoming regular occurrences, many Americans have little knowledge of the industry. https://www.techrepublic.com/article/heres-what-us-adults-actually-know-about-cybersecurity/?ftag=TREa988f1c&bhid=78480402

Questions
Contact FIPCO's Ken Shaurette at 800/722-3498 ext. 251 or email FIPCO IT Services for more information.

"Make Security Part of You and Your Institution's DNA!"

Threat Intelligence Newsletter: August 14, 2018

FIPCO®
IT Audit
Round Table
Discussions

If you would like to host an event, please contact: Becky Schowalter

Upcoming Threat Intelligence Peer Group Discussions
To Be Announced

2018 Wisconsin Governor's Cybersecurity Summit
An agenda packed with big names and hot topics. Visit the event website to view the recently updated agenda, featuring sessions on tech megatrends, blockchain in the public sector, current cyber threats, and state-level cybersecurity initiatives. Check out the agenda here; https://wigcot.eventsair.com/QuickEventWebsitePortal/cybersecurity18/cybersummit18. This is one Summit you won't want to miss and to register visit: https://wigcot.eventsair.com/cybersecurity18/registration/Site/Register

****

Alerts & Warnings

Threat Intelligence from the dark web
The reputation of the Dark Web perhaps exceeds its reality. Many think of it as a place where criminals operate. If used by security teams, however, the Dark Web can be ripe with threat intelligence just set for the picking. https://www.scmagazine.com/threat-intelligence-from-the-dark-web/article/780031/?utm_source=newsletter&utm_medium=email&utm_campaign=SCUS_Newswire_20180730&email_hash=305f40be59a0dcb04476bf06c7e07dc9&hmSubId=XOjrUhr_Swg1

Fraudsters Bring Back Old Scams With New Tricks
In an age where the latest technology is available to the everyday consumer, it may be hard to believe people still fall for classic scamming methods. However, fraudsters that utilize scare tactics continue to be highly effective – especially in phone, mail and online scams. https://www.fightingidentitycrimes.com/fraudsters-bring-back-old-scams-with-new-tricks/

LifeLock Data Leak Exposes Customer Emails
On July 25, a flaw was discovered on LifeLock's website that unintentionally leaked millions of customer email addresses. The website vulnerability allowed any Web user to pair unique LifeLock subscriber IDs (randomized numbers attributed to each customer), with customer email addresses – similar to the Panera data leak earlier this year. https://www.fightingidentitycrimes.com/lifelock-data-leak-exposes-customer-emails/

Government imposter scams
You get a text, call, or email from someone who says they're with the government. They may claim to be a U.S. Marshal, saying you must pay a fine for missing jury duty. Or the IRS, saying that you owe thousands in back taxes. Some might threaten legal action, deportation, or arrest if you don't pay up or give them your financial information. https://www.consumer.ftc.gov/blog/2018/07/government-imposter-scams?utm_source=govdelivery

Just Five File Types Make Up 85% of All Spam Malicious Attachments
Spam still reigns supreme as today's main infection vector and the go-to tool of online criminals, according to a report published by Finnish cyber-security firm F-Secure. Experts say that one of the main reasons why spam still works is that users are still having a hard time picking up spam despite spam being more than a 40-year-old trick. This has led to users clicking on spam emails more than ever. F-Secure reports that spam email click rates have gone up from the 13.4% recorded in the second half of 2017 to 14.2% recorded in the first half of the year. https://www.bleepingcomputer.com/news/security/just-five-file-types-make-up-85-percent-of-all-spam-malicious-attachments/

Stolen" Ruse Behind Blocked Phones
Cell phone scammers have hit on a new trick that's costing victims hundreds of dollars and leaves them with a blocked phone they may never be able to use. https://www.scambusters.org/blockedphone.html

Widespread Browser Extension Is Collecting Your Data
You have likely heard warnings about installing browser extensions before. Ok, so they can be useful and many of them are fun. In fact, one called Stylish allows a user to customize a website's page to look the way they want it to, rather than them having to see it the way the site's designer intended. That one is so popular that it boasts 1.8 million downloads for both Google Chrome and Firefox. Unfortunately, Stylish also collects data on users' browsing history and sends it back to the developers…
https://www.sosdailynews.com/news.jspx?&articleid=EEDD3E10F0B0CF77D19A2ADEDFFDEEE5&sx=79

Watch out for card skimming at the gas pump
With the summer travel season in high gear, the FTC is warning drivers about skimming scams at the pump. https://www.consumer.ftc.gov/blog/2018/08/watch-out-card-skimming-gas-pump?utm_source=govdelivery

****

Hints & Tips plus Security Awareness

Stay Safe Online
Helping to make the internet safer and more secure for everyone. https://staysafeonline.org/

As Kids Head Back to School - Internet Safety for Kids
As an educator, (AND WE ALL NEED TO BE) it's important to recognize that children in modern times are surrounded by technology at school. Whether they have a cell phone in their pocket or require a computer to complete in-class assignments, the internet is available everywhere. When you are setting up your classroom for the new year, consider educating your students on how to be safe while exploring the internet. https://www.pandasecurity.com/mediacenter/family-safety/internet-safety-for-kids/?mc_cid=b6398ecf93&mc_eid=2b2ac7a1bf

The ABCs of Detecting and Preventing Phishing
Stay out of cyber criminals' phishing net with these actionable tips
Have you ever considered that you could be a target for phishing attacks? It's not a new issue, but it's a rising threat. Phishing attackers have been constantly growing and improving their techniques. Let's see how you can actually start preventing phishing, since cybercriminal strategies became so convincing that you can barely distinguish them from harmless communications.
https://heimdalsecurity.com/blog/abcs-detecting-preventing-phishing/?utm_source=Heimdal+Security+Newsletter+List&utm_campaign=7404cc1523-EMAIL_CAMPAIGN_2018_07_25_01_44&utm_medium=email&utm_term=0_31fbbb3dbf-7404cc1523-194307777

Six best practices to follow in access control
Finding the right access control for your organization is best done in stages. In this way, you'll be able to foresee costs and activities that you must tackle both on short-term and long-term basis, and keep your staff and business assets consistently safe. Access control best practices include activities where you need to pay attention to how much you will spend upfront for which product, who will be your preferred vendor, how will you set… https://www.helpnetsecurity.com/2018/07/31/access-control-best-practices/

Want to keep your data? Back it up! Protection From Ransomware
We all know it happens – computers crash, malware infects them, or somebody downloads that cool, new program that crashes everything! While there are many tips and tricks of great value for preventing your devices and data from being compromised, it is important to also have a backup of your information in case something goes wrong! https://www.cisecurity.org/newsletter/want-to-keep-your-data-back-it-up/

You've been breached: Eight steps to take within the next 48 hours (PDF)
A slow or mishandled response to a data breach can make a bad situation even worse. As soon as you discover you've been hacked, take these steps to help contain the damage.
http://b2b.cbsimg.net/downloads/Gilbert/TR_EB_data_breach_response.pdf

What does the NCSC think of password managers?
People keep asking the NCSC if it's OK for them to use password managers (sometimes called password vaults). If so, which ones? Who should use them - private citizens, small businesses, massive enterprises? And *how* should people use them? Is it safe to put all your crucial passwords into a password manager, and forget trying to remember any at all? https://www.ncsc.gov.uk/blog-post/what-does-ncsc-think-password-managers

MS Office 365 Manipulated In Two Ways To Get Malware To You
Cybercriminals can be very crafty. Within the past couple of months, they have discovered a couple of new ways to fool Microsoft Office 365 Advanced Threat Protection (APT) anti-phishing capabilities. As reported by researchers at Avanan, both involve sending malicious links through email messages or by sending malicious attachments in email. And both should be considered serious.
https://www.sosdailynews.com/news.jspx?&articleid=948E6EE6F1AC25B3D4CCF336B04C9271&sx=79

Picking up the pieces after a disaster
Dealing with the aftermath of a wildfire, flood, tornado, or other disaster is never easy, but taking stock and developing a recovery plan can give you a sense of hope and purpose. Here are a few tips and links to resources to help make the task less burdensome. https://www.consumer.ftc.gov/blog/2018/08/picking-pieces-after-disaster?utm_source=govdelivery

****

News & Views

Chrome Gets A Malware Catching Boost With Help From Microsoft
Even Microsoft is jumping on the bandwagon to make Google's Chrome browser even better. While Windows does have its own, and arguably safer browser (Edge), Microsoft has also released an extension for Chrome that will help further prevent phishing attacks from becoming successful. And bonus! It works on every operating system, except for Chrome OS.
https://www.stickleyonsecurity.com/news.jspx?articleid=%2016F75C19481C7451C7E29199C42419E0

Cyber fall-out of nation-state conflicts extends beyond politics
Several recent incidents have involved the political relationships of three major nation-states active in the cyber landscape: the United States, Russia and China. The fall-out of their publicly reported conflicts with each other has sometimes affected individuals and companies not involved with politics, such as through the exploitation of Internet of Things (IoT) device users or third-party suppliers. Monitoring the threat landscape and being aware of common tactics, techniques and procedures (TTPs) can help limit a business's exposure to direct or indirect effects of nation-state threat actor attacks.
https://info.digitalshadows.com/rs/457-XEY-671/images/20182707-DSWeeklyIntSum.pdf?mkt_tok=eyJpIjoiWXpVeU5UWXlabUkzTmpkbCIsInQiOiJzZWZNeGx5eUhMXC9YYWRnMjk4N3d6aTYwaHA0bnNrRG9qN2hMSStPWXZBSjlzRUc2cGFVMkREdjErbWMrcHdQTmhLZVM3Y2NVRFpKNWhOdkI2SDVjcExQU2prN1BabWpaNXduSVcrakFJM0JnakkyVmVFRWJEZVhKUEdVSjhyZ0EifQ%3D%3D

How to Build Practical Cross-Training in Infosec
If you're a cybersecurity or technology audit manager, there are some good reasons why you might want to diversify and expand the skill base of the folks on your team. First, we all know that there's a "skills gap" – so those organizations that can best optimize talent (i.e., by making the best use of the resources already in house) have a competitive advantage relative to their peers. https://misti.com/infosec-insider/how-to-build-practical-cross-training-in-infosec

New Wi-Fi attack cracks WPA2 passwords with ease
The common Wi-Fi security standard is no longer as secure as you think.
https://www.zdnet.com/article/new-wi-fi-attack-cracks-wpawpa2-passwords-with-ease/?ftag=TRE-03-10aaa6b&bhid=78480402

FEMA seeks feedback on planning considerations: Evacuation and Shelter-In-Place
FEMA's National Integration Center is seeking feedback on the draft document Planning Considerations: Evacuation and Shelter-in-Place, as part of the continued development of the document. Feedback and recommendations received help ensure the final version of the guide is an effective resource for emergency managers across the nation. https://www.fema.gov/plan.

Cryptocurrency Scammers Trade on Investor Ignorance
Learn how to spot new cryptocurrency swindles: Cryptocurrency investment is the next big money-making opportunity — or so we're told. But plowing your cash into this digital currency market is fraught with dangers, notably the risk of being badly burnt in a fraudulent initial coin offering (ICO). https://www.scambusters.org/cryptocurrency.html

****

"Ctrl -F" for The Board

The weak spot in banks' Cyberinsurance
A clash between a small bank and its insurance company after a cyberattack may have a lot of banks double-checking the fine print of their coverage. https://www.information-management.com/news/the-weak-spot-in-banks-cyberinsurance?utm_campaign=security%20briefing-jul%2031%202018&utm_medium=email&utm_source=newsletter&eid=305f40be59a0dcb04476bf06c7e07dc9

Cyber hygiene: Where do organizations fall behind on basics?
Tripwire released its State of Cyber Hygiene report, which examined how organisations are implementing security controls that the Center for Internet Security (CIS) refers to as cyber hygiene. The survey found that almost two-thirds of the organisations admit they do not use hardening benchmarks, like CIS or Defense Information Systems Agency (DISA) guidelines, to establish a secure baseline. "These industry standards are one way to leverage the broader community, which is important with the resource… https://www.helpnetsecurity.com/2018/08/09/state-of-cyber-hygiene/

Questions
Contact FIPCO's Ken Shaurette at 800/722-3498 ext. 251 or email FIPCO IT Services for more information.

"Make Security Part of You and Your Institution's DNA!"

Threat Intelligence Newsletter: October 1, 2018

FIPCO®
IT Audit
Round Table
Discussions

If you would like to host an event, please contact: Becky Schowalter

Upcoming Threat Intelligence Peer Group Discussions
None available at the current time

Wausau Area Cyber Liaison Officer Training
On November 13, 2018, from 8:30 am to 2:30 pm (registration opens at 8:00am), the Wisconsin Statewide Intelligence Center (WSIC) will be hosting a Cyber Liaison Officer (CLO) training session. The training will be held in Wausau on the campus of Northcentral Technical College at 1000 W Campus Dr. There is room for 50 attendees, and we will cap registrants at 60. Closer to the date, we will send a map and information to registrants. To register for the workshop please go to https://www.surveymonkey.com/r/111318CLO. If you have any questions please contact Josh Maas at maasjr@doj.state.wi.us.

****

Alerts & Warnings

FBI warns companies about hackers increasingly abusing RDP connections
In a new public service announcement, the FBI is warning companies about the dangers of leaving RDP endpoints exposed online. RDP stands for the Remote Desktop Protocol, a proprietary technology that allows a user to log into a remote computer and interact with its OS via a visual interface that includes mouse and keyboard input. RDP access is often turned on for workstations in enterprise networks or for computers located in remote locations, where system administrators need access to, but can't get to in person. https://www.ic3.gov/media/2018/180927.aspx

Your Social Security Number isn't suspended. Ever.
A caller says that he's from the government and your Social Security number (SSN) has been suspended. He sounds very professional. So you should do exactly what he says to fix things…right?
https://www.consumer.ftc.gov/blog/2018/09/your-social-security-number-isnt-suspended-ever?utm_source=govdelivery

Empower yourself against utility scams
You get a call saying your electricity or water will be shut off unless you pay a past due bill. You may not think you have a past due bill. But the caller sounds convincing, and you can't afford to ignore it, especially if you're running a small business. https://www.consumer.ftc.gov/blog/2018/09/empower-yourself-against-utility-scams?utm_source=govdelivery

Dangerous Pegasus Spyware Has Spread to 45 Countries
The infamous Pegasus spyware, which targets iPhones and Android devices, has allegedly infiltrated 45 different countries across the globe — and six of those countries have used surveillance malware in the past to abuse human rights, a group of researchers claim. Researchers from The Citizen Lab scanned the internet in a massive project that took place between 2016 and 2018, sniffing out servers associated with the Pegasus mobile spyware, attributed to Israel-based company NSO Group as an offering for state-level actors around the world. https://threatpost.com/dangerous-pegasus-spyware-has-spread-to-45-countries/137506/

Viborot ransomware comes with a botnet
Researchers discovered a ransomware with Botnet capabilities representing threat actors diversifying attack methods to raise the ante. https://www.scmagazine.com/home/news/viborot-ransomware-comes-with-a-botnet/?utm_source=newsletter&utm_medium=email&utm_campaign=SCUS_Newswire_now&email_hash=&hmSubId=XOjrUhr_Swg1

USB Drives Remain Critical Cyberthreat
USB thumb drives may be used less frequently than before, but they are still commonly used as infection vectors for a wide variety of malware… https://www.darkreading.com/threat-intelligence/usb-drives-remain-critical-cyberthreat/d/d-id/1332894

Adobe discloses bugs in Acrobat and Reader
Description: Adobe released security updates for Acrobat and Reader for Windows and MacOS. Successful exploitation of the critical and important vulnerabilities could lead to arbitrary code execution. https://helpx.adobe.com/security/products/acrobat/apsb18-34.html

****

Hints & Tips plus Security Awareness

Protecting Your Identity One Year After Equifax
A lot can happen in a year. Even a year after the Equifax breach, your personal information may still be at risk. Learn why September 2017 changed the way we think about identity crime, and how to combat the new fraud risks emerging in today's data-driven world. The State of ID Crime in 2018
https://deluxeprovent.ezshield.com/ActivityReport/tabid/10136/Default.aspx?&utm_campaign=Engagement.Identity_Report_C_B_[09-18]&utm_source=EZShield&utm_medium=email

ISACA introduces new credential to build and recognize auditors' cybersecurity knowledge
Auditors are being required to audit cybersecurity processes, policies and tools to provide assurance that their enterprise has appropriate controls in place. To help them acquire and prove these skills, ISACA—creators of the Certified Information Systems Auditor (CISA) certification—has introduced the new

Cybersecurity Audit Certificate Program. The Cybersecurity Audit Certificate Program provides audit/assurance professionals with the knowledge needed to excel in cybersecurity audits. It provides security professionals with an understanding of the audit process, and https://www.helpnetsecurity.com/2018/09/28/isaca-cybersecurity-audit-certificate-program/

10 Tactics For Teaching Cybersecurity Best Practices To Your Whole Company
Smart leaders know that their entire team needs to be well-educated on the importance and best practices of cybersecurity if they hope to protect their data. Unfortunately, this is easier said than done, especially when it comes to training your non-tech employees. Using too much jargon and technical terms will only disengage them, leaving them less prepared and less vigilant. While you don't necessarily need to "dumb down" cybersecurity training for non-techies, you do need to present the information in a way that's relatable and easy to understand. https://www.forbes.com/sites/forbestechcouncil/2018/09/26/10-tactics-for-teaching-cybersecurity-best-practices-to-your-whole-company/#350160817fc3

****

News & Views

(IN)SECURE Magazine issue 59 released
(IN)SECURE Magazine is a free digital security publication discussing some of the hottest information security topics. Issue 59 has been released today. Table of contents The importance of career pathing in the cybersecurity industry Securing healthcare organizations: The challenges CISOs face Fingerprinting HTTP anomalies to dissect malicious operations How to keep cryptominers from opening up your IT container boxes Report: Black Hat USA 2018 Vulnerability research and responsible disclosure: Advice from an industry veteran Managing… https://www.helpnetsecurity.com/dl/insecure/INSECURE-Mag-59.pdf

$505 million in refunds sent to payday loan customers
If you took out an online payday loan from a company affiliated with AMG Services, you may be getting a check in the mail from the FTC. The $505 million the FTC is returning to consumers makes this the largest refund program the agency has ever administered. https://www.consumer.ftc.gov/blog/2018/09/505-million-refunds-sent-payday-loan-customers?utm_source=govdelivery

6 Security Training Hacks to Increase Cyber IQ Org-Wide
Some of security's toughest nuts to crack are the vulnerabilities introduced by the human element. Users are duped by phishers every day. IT operations staff configure infrastructure insecurely over and over again. Developers repeatedly write code in the same insecure fashion. Executives are tricked by business email compromises into wiring large sums of money directly to crooks. And IT security staff is asked to carry out near impossible feats of digital protection because they themselves are poorly trained to set up the tools and practices they need to keep up with attackers. If organizations are going to make a real dent on cyber-risk, they need to start taking security training to the next level.
https://www.darkreading.com/endpoint/6-security-training-hacks-to-increase-cyber-iq-org-wide/d/d-id/1332864

****

"Ctrl -F" for The Board

Five computer security questions you must be able to answer right now
Getting senior managers to take computer security seriously is a struggle within many organisations, despite the frequency of high-profile data breaches and hacking incidents. Now the UK government's computer security agency, the National Cyber Security Centre (NCSC), has put together a list of five questions aimed at starting 'constructive' discussions between executives and their computer security teams. According to the NCSC, two-thirds of boards have received no training to help them deal with a cyber incident, and 10 percent have no plan in place to respond to one. These conversation-starters aim to bridge the gap between executives who don't know about security issues and the IT department that may struggle to make its voice heard. https://www.zdnet.com/article/five-computer-security-questions-you-must-be-able-to-answer-right-now/

2018 Cybercrime Report - 210 Million cyberattacks detected in Q2 2018
The latest edition of the ThreatMetrix Cybercrime Report reveals that attack rates continue to increase and attack vectors are becoming more advanced than ever before. The report is based on actual cybercrime attacks from April 2018 to June 2018 featuring global insights from the ThreatMetrix Digital Identity Network®. https://www.threatmetrix.com/wp-content/uploads/2018/09/q2-2018-cybercrime-report-1536619959.pdf?mkt_tok=eyJpIjoiWlRrek56QmlPRFE1TmprNCIsInQiOiJRdDBDY0VzdG01VG1GSUk1cDdrTFowcjNWdFVmdytmaE9cL2NuK0VTWVdhUkZLWUc5YWJ1WGVxaDVybW5EWjJNSytyRzgwVVNzOHRFS2poVktEWklrMFwvOFI4SnpHZWhxWTJFWTEyMkpmcmRlZTRSQk9PNXJHbzJQYTZQd2JWTzNPIn0%3D

Questions
Contact FIPCO's Ken Shaurette at 800-722-3498 ext. 251 or email FIPCO IT Services for more information.

"Make Security Part of You and Your Institution's DNA!"

Threat Intelligence Newsletter: November 1, 2018

FIPCO®
IT Audit
Round Table
Discussions

If you would like to host an event, please contact: Becky Schowalter

Upcoming Threat Intelligence Peer Group Discussions
None available at the current time

****

Alerts & Warnings

Oregon FBI Tech Tuesday: Building a Digital Defense Against Payroll Phishing Scams
Welcome to the Oregon FBI's Tech Tuesday segment. This week: Building a digital defense against payroll phishing scams. https://www.fbi.gov/contact-us/field-offices/portland/news/press-releases/oregon-fbi-tech-tuesday-building-a-digital-defense-against-payroll-phishing-scams

Zero-days, fileless attacks are now the most dangerous threats to the enterprise
According to a study conducted by the Ponemon Institute and sponsored by Barkly, called the "2018 State of Endpoint Security Risk report," nearly two-thirds of enterprise players have been compromised in the past 12 months by attacks which originated at endpoints, which the organization says is a 20 percent increase year-on-year. Such attacks can prove costly, with the average company enduring a cost of $7.12 million, or $440 per endpoint. The report shows that zero-day vulnerabilities and fileless attacks are now deemed the most dangerous threats to the enterprise… https://www.zdnet.com/article/zero-days-fileless-attacks-are-now-the-most-dangerous-threats-to-the-enterprise/

Password and credit card-stealing Azorult malware adds new tricks
A form of password, credit card details and cryptocurrency-stealing malware has been updated, making it even more potent for cyber criminals. The Azorult malware has been been operating since 2016 and enables crooks to steal credentials including passwords, credit card details, browser histories and contents of cryptocurrency wallets from victims. Now a new version of it is being advertised in an underground forum, as uncovered by researchers at tech security company Check Point, who describe it as "substantially updated". New features include the ability to steal additional forms of crpytocurrency from the wallets of victims – BitcoinGold, electrumG, btcprivate (electrum-btcp), bitcore and Exodus Eden.
https://www.zdnet.com/article/password-and-credit-card-stealing-azorult-malware-adds-new-tricks/

Spread the word about charity fraud
This week, the FTC, the National Association of State Charities Officials (NASCO), and state charity regulators are joining forces with regulators from across the world to participate in the first International Charity Fraud Awareness Week.
https://www.consumer.ftc.gov/blog/2018/10/spread-word-about-charity-fraud?utm_source=govdelivery

Scams against older adults: reporting to Congress
You might have read media stories about older people losing lots of money to scams. It does happen – and FTC data show that when people over 80 report losing money, the amount they lose is a lot higher than the amount younger people lose. But that's not the whole story. In fact, FTC data also show that people 60 and older are great at reporting the fraud they see – and can be great at avoiding it, too. Because, according to the FTC's 2017 data, people 60… https://www.consumer.ftc.gov/blog/2018/10/scams-against-older-adults-reporting-congress?utm_source=govdelivery

FBI Alerts: Cyber Actors Target Banking Credentials and Deploy Ransomware Using Emotet and/or Trickbot Malware
The FBI released two alerts on Oct. 22 regarding cyber criminals' use of the Emotet and/or Trickbot malware to Trojans and malware to target banking credentials and deliver ransomware. Per the alerts, criminals establish persistence on the victim network using the Emotet malware. They then deliver the Trickbot Trojan, which propagates via Server Message Block, and steal banking credentials to conduct high-net-worth transactions on compromised accounts. The FBI also reports that ransomware may also be deployed on the infected network shortly thereafter….
https://www.trendmicro.com/vinfo/in/security/news/cybercrime-and-digital-threats/spam-campaign-delivers-malware-via-wiz-targets-banks Using Emotet…
https://blog.malwarebytes.com/cybercrime/2018/09/emotet-rise-heavy-spam-campaign/

****

Hints & Tips plus Security Awareness

Identify, Protect, Detect, Respond and Recover
The NIST Cybersecurity Framework, https://www.nist.gov/blogs/taking-measure/identify-protect-detect-respond-and-recover-nist-cybersecurity-framework

The Financial Services Sector Cybersecurity Profile, v1.0
1Where can I find the Profile? The latest, free copy of the Profile is available for download on the Financial Services Sector Coordinating Council (FSSCC) website, the NIST Cybersecurity Framework Critical Infrastructure Resources webpage: https://www.nist.gov/cyberframework/critical-infrastructure-resources, and on the websites of supporting trade associations.

New Community Bank Cybersecurity Vignettes from the FDIC
As part of the FDIC's Community Banking Initiative, the agency is adding to its cybersecurity awareness resources for financial institutions. This includes two new vignettes for the Cyber Challenge, which consists of exercises that are intended to encourage discussions of operational risk issues and the potential impact of information technology disruptions on common banking functions.
https://www.fdic.gov/regulations/resources/director/technical/cyber/purpose.html

Virtual Event – Building a Cyber defense for 2019
When it comes to enterprise cybersecurity, the only constant is change. On one side, many organizations are being transformed by technological change, including the rapid movement toward cloud services, digital transformation, and the Internet of Things. On the other side, security teams are rethinking their defense strategies to respond to new threats such as ransomware, crypto mining, and next-generation malware. And as if that isn't enough, major regulatory changes such as GDPR are putting new pressures on enterprise security and privacy. https://events.darkreading.com/cyberdefense/

No-Cost Credit Freezes Step Up Battle to Beat ID Thieves
Hardly a week goes by these days without news of a data breach that's resulted in thousands or even millions of confidential records being stolen by hackers. https://www.scambusters.org/creditfreeze.html

Why we need to bridge the gap between IT operations and IT security
Thycotic released the findings from its 2018 VMworld survey of more than 250 IT operations professionals which looked into their experiences in using cybersecurity tools on a daily basis, including their concerns and preferences. According to the findings, even though IT operations personnel help influence the selection of cybersecurity tools, nearly two out of three say complexity in deployment (30 percent) and complexity in… https://www.helpnetsecurity.com/2018/10/17/it-ops-security-gap/

Will background check errors deny you a home?
A background check can determine if you can get credit, a job, or even a place to live. That's why the law requires businesses that provide these reports have reasonable procedures to ensure the information they collect and share about you is accurate.
https://www.consumer.ftc.gov/blog/2018/10/will-background-check-errors-deny-you-home?utm_source=govdelivery

How to train your employees to avoid online scams: 5 tips
According to Microsoft, online scammers are still tricking people with tech support scams, but there are ways to stay safe. https://www.techrepublic.com/article/how-to-train-your-employees-to-avoid-online-scams-5-tips/?ftag=TREa988f1c&bhid=78480402

Easily Report Phishing and Malware
This is how you can strike back at criminals sending phishing spam - by getting their webpages on blacklists. Blocking their sites helps protect other people and helps researchers trying to stop this. Sites can be blocked within 15 minutes of your report, but you may not immediately see it.
https://decentsecurity.com/malware-web-and-phishing-investigation/

Steering clear of vehicle history report scams
The FTC has been hearing about a new scam targeting people who are selling their cars online. They're getting calls or texts from people who claim to be interested in buying the car – but first want to see a car history report. They ask the seller to get the report from a specific website, where the seller needs to enter some information and pay about $20 by credit card for the report. The seller then sends it to the supposed buyer but never hears back. Weird, huh? Well, it gets weirder…
https://www.consumer.ftc.gov/blog/2018/10/steering-clear-vehicle-history-report-scams?utm_source=govdelivery

****

News & Views

Don’t fall for myths—get the truth about cybersecurity
See which technologies, personnel, and governance practices really make a difference for today’s IT and security professionals. http://watch.bmc.com/watch/bjcatNFiDDT6Ps6JKXz3di

Scams near you, by the numbers
Every day, people across the country are telling the FTC what happened to them. Maybe they lost money to a scam, lost their identity, or just spotted something that looked fishy and wanted somebody to know. All of that information helps FTC and other law enforcement agencies investigate and bring cases against scammers. And, every year, we roll up all that data and give it back to you in an annual data book. Now, though, you don’t have to wait a year to find out what’s happening.
https://www.consumer.ftc.gov/blog/2018/10/scams-near-you-numbers?utm_source=govdelivery

IT and security professionals unprepared for Windows 7 end of life
An Avecto survey of over 500 individuals from Europe, the United Arab Emirates and the United States revealed that, while some organizations have already migrated to Windows 10 and are using the move as a catalyst to improve their security posture, many are lagging behind and don’t understand the potential risks of the migration. Specifically, the survey highlighted global uncertainty about Windows 7 end of life. 31% of respondents believed that it had already occurred,,,,
https://www.helpnetsecurity.com/2018/10/18/windows-7-end-of-life/

What would happen if an attack interrupted a country’s power supply?
When we think about cyberattacks, we tend to imagine the loss of a large chunk of our data, or not being able to work for several hours. In the case of companies, the risk increases considerably, since they can lose confidential information and face serious cybersecurity problems, as well as problems for the running of their business. But what happens when a cyberattack affects a basic service? What if we’re suddenly left without power? https://www.pandasecurity.com/mediacenter/security/attack-power-supply-infrastructures/?mc_cid=71d6ff0309&mc_eid=2b2ac7a1bf

Identity Theft vs. Identity Fraud: What’s the Difference?
Thousands fall victim to identity theft and identity fraud each year. However, few know the difference between the two. https://www.trueidentity.com/identity-theft-resource/identity-theft-vs-identity-fraud?channel=paid&cid=eml:newstid:tidp:news102218tidfrC&utm_source=newstid&utm_medium=email&utm_campaign=news102218tidfrC

Increased dark web activity putting merchants and consumers at risk
Posted on Oct 26, 2018 06:30 am are increasingly targeting retailers and their customers through digital and social channels as retailers leverage new channels for increased revenue opportunities. In a joint report, IntSights scoured the Clear and Dark Web to assess retail data and goods being sold illegally, new cyber scam tactics and how cybercriminals impersonate brands online to trick unknowing consumers. Riskified analyzed the transaction-level results of hundreds of millions of purchases for indicators of fraud to identify trends and... https://www.helpnetsecurity.com/2018/10/26/dark-web-activity/

Cyber Security Assessment
How safe is your business? All business are facing a far higher level of risk than ever before. Find out how prepared you are by taking this short assessment based on the Cyber Security Framework developed by NIST. You will receive a personalised scorecard to see how you measure up against other businesses in your sector. http://cybersec.ifsecglobal.com/assessment

At least 57 negative impacts from cyber-attacks
Cyber-security researchers have identified a total of at least 57 different ways in which cyber-attacks can have a negative impact on individuals, businesses and even nations, ranging from threats to life, causing depression, regulatory fines or disrupting daily activities. The researchers, from Kent's School of Computing and the Department of Computer Science at the University of Oxford, set out to define and codify the different ways in which the various cyber-incidents being witnessed today can have negative outcomes. They also considered how these outcomes, or harms, can spread as time passes. The hope is that this will help to improve the understanding of the multiple harms which cyber-attacks can have, for the public, government, and other academic disciplines.
https://www.sciencedaily.com/releases/2018/10/181024112203.htm

****

"Ctrl -F" for The Board

Inside the Dark Web — AARP
The man who brought organized crime online takes us to a lawless corner of the internet where your personal information can be bought. Brett Johnson, formerly America's most wanted cybercriminal, shows what you can do to protect yourself online. https://www.aarp.org/money/scams-fraud/info-2018/what-is-the-dark-web.html. If you don't have time to read the whole article at least watch this short video: http://videos.aarp.org/detail/video/5827868292001/inside-the-dark-web-%E2%80%94-aarp

Who is to Blame for the Majority of Data Breaches
The risk consulting firm Kroll recently published a report showing that in the United Kingdom the number of security incidents that have led to data breaches has grown by 75% in the last two years. The most affected sector is healthcare, with 1,214 registered security incidents, which represents a 41% growth in the period analyzed. This is followed by service companies, with 362 incidents; education and childcare, with 354; and local public administration, with 328. But, who is responsible for most of these data breaches? Is it always cyber attackers? https://www.pandasecurity.com/mediacenter/security/who-is-to-blame-data-breaches/?mc_cid=71d6ff0309&mc_eid=2b2ac7a1bf

U.S. National Cyber Strategy: What You Need to Know
On September 20, 2018, the White House released a new cybersecurity strategy with several important changes in direction meant to give government agencies and law enforcement partners a greater ability to respond to cybercrime and nation-state attacks. The new U.S. cyber strategy makes one message clear: America will not sit back and watch when attacked in cyberspace. On the contrary, in areas ranging from critical infrastructure to space exploration to intellectual property protection, the USA will respond offensively, as well as defensively in cyberspace. https://www.tripwire.com/state-of-security/government/us-cyber-strategy/

Audits: The Missing Layer in Cybersecurity

There is a broad spectrum of cybersecurity preparedness on the enterprise landscape, but even organizations that are relatively well-resourced and committed to cybersecurity stand to benefit from cybersecurity audits. Recent audit findings revealed gaps in the Washington Metropolitan Area Transit Authority's cybersecurity posture, while deficiencies were similarly pinpointed in an audit of the Michigan Department of Technology, Management and Budget. There is no question that, in many cases, earlier and expanded input from auditors would have helped organizations that have suffered high-profile cyberattacks from sifting through the financial and reputational damage that ensued.
https://www.darkreading.com/endpoint/audits-the-missing-layer-in-cybersecurity-/a/d-id/1333054

National Cybersecurity Awareness Month: A Year-Long Effort

October is National Cybersecurity Awareness Month – a time that is dedicated to showcasing how to stay safe online by providing insight and best practices on how to protect Personally Identifiable Information (PII), financial and sensitive proprietary data. The need for proper cybersecurity within the workplace should be a continuous effort throughout the year. With small businesses feeling the brunt of data breach events, many of which are caused by cyberattacks or other security vulnerabilities, a proactive attitude toward cybersecurity risks in the workplace is now more important than ever.
https://www.fightingidentitycrimes.com/cybersecurity-best-practices-in-out-office/#more-5534

Questions

Contact FIPCO's Ken Shaurette at 800-722-3498 ext. 251 or email FIPCO IT Services for more information.

"Make Security Part of You and Your Institution's DNA!"

Threat Intelligence Newsletter: November 15, 2018

FIPCO®
IT Audit
Round Table
Discussions

If you would like to host an event, please contact: Becky Schowalter

Upcoming Threat Intelligence Peer Group Discussions
None available at the current time

****

Alerts & Warnings

Researcher finds simple way of backdooring Windows PCs and nobody notices for ten months
"RID Hijacking" technique lets hackers assign admin rights to guest and other low-level accounts.
https://www.zdnet.com/article/researcher-finds-simple-way-of-backdooring-windows-pcs-and-nobody-notices-for-ten-months/#ftag=RSSbaffb68

Hang up on spoofed SSA calls
If you get a call that looks like it's from the Social Security Administration (SSA), think twice. Scammers are spoofing SSA's 1-800 customer service number to try to get your personal information. Spoofing means that scammers can call from anywhere, but they make your caller ID show a different number – often one that looks legit. Here are few things you should know about these so-called SSA calls.
https://www.consumer.ftc.gov/blog/2018/10/hang-spoofed-ssa-calls?utm_source=govdelivery

Windows 10 bug lets Microsoft Store apps snoop on all your files without asking
Windows developer Sebastien Lachance discovered that by default Universal Windows Platform apps can access any user-accessible files on a PC's hard drive. https://www.techrepublic.com/article/windows-10-bug-lets-microsoft-store-apps-snoop-on-all-your-data-without-asking/?ftag=TREa988f1c&bhid=78480402

GPlayed Trojan's baby brother is after your bank account
A new member of the GPlayed Trojan has been discovered which has been designed to attack customers of a Russian-owned state bank. Earlier this month, researchers from Cisco Talos revealed GPlayed, an "extremely powerful" Trojan which pretends to be a Google service when infecting Android mobile devices. At the time of discovery, the researchers said they believed the malware was still in development due to clues in the code — but this did not detract from the fact the Trojan was extremely flexible, used

obfuscation, and contained strong destructive and data-stealing capabilities. It has now been found that GPlayed is not the only member of the new Trojan family. Talos said that the malware's "younger brother" has also appeared on the radar. https://www.zdnet.com/article/gplayed-trojans-baby-brother-is-after-your-bank-account/

Spear phishing scammers want more from you
"I'm calling from [pick any bank]. Someone's been using your debit card ending in 2345 at [pick any retailer]. I'll need to verify your Social Security number — which ends in 8190, right? — and full debit card information so we can stop this unauthorized activity..."
https://www.consumer.ftc.gov/blog/2018/10/spear-phishing-scammers-want-more-you?utm_source=govdelivery

Bluetooth Chip Flaws Expose Enterprises to Remote Attacks
Researchers at IoT security company Armis, who in the past discovered the Bluetooth vulnerabilities known as BlueBorne, now claim to have found two serious vulnerabilities in BLE chips made by Texas Instruments. These chips are used in access points and other enterprise networking devices made by Cisco, including Meraki products, and HP-owned Aruba Networks. These vendors provide 70% of wireless access points sold to enterprises annually. The flaws, dubbed BLEEDINGBIT, can allow a remote and unauthenticated attacker to take complete control of impacted devices and gain access to the enterprise networks housing them. Devices used in the healthcare sector, such as insulin pumps and pacemakers, also use the affected BLE chips so they could be vulnerable to BLEEDINGBIT attacks as well.
https://www.securityweek.com/bluetooth-chip-flaws-expose-enterprises-remote-attacks

SMS Phishing + Cardless ATM = Profit
Thieves are combining SMS-based phishing attacks with new "cardless" ATMs to rapidly convert phished bank account credentials into cash. Recent arrests in Ohio shed light on how this scam works.
A number of financial institutions are now offering cardless ATM transactions that allow customers to withdraw cash using nothing more than their mobile phones. But this also creates an avenue of fraud for bad guys, who can leverage phished or stolen account credentials to add a new phone number to the customer's account and then use that added device to siphon cash from hijacked accounts at cardless ATMs. https://krebsonsecurity.com/2018/11/sms-phishing-cardless-atm-profit/

****

Hints & Tips plus Security Awareness

Identify, Protect, Detect, Respond and Recover:
The NIST Cybersecurity Framework, https://www.nist.gov/blogs/taking-measure/identify-protect-detect-respond-and-recover-nist-cybersecurity-framework

You Know The Cyber Threat, Now Do Something About it
We continually capture lessons learned and best practices for reducing digital risk and enhancing cybersecurity and maintain a list you can use to review to ensure you and your team are optimizing defenses. We provide no-nonsense tips on topics like: https://crucialpointllc.com/cybersecurity-best-practices/

Warning – SpyCloud - Interesting Vendor Tool, this is awareness not an endorsement
PROTECT EMPLOYEES AND CUSTOMERS FROM ACCOUNT TAKEOVER, Stamp out fraud, intellectual property theft, and damage to your brand. https://spycloud.com/

Vulnerabilities' CVSS scores soon to be assigned by AI
The National Institute of Standards and Technology (NIST) is planning to use IBM's Watson to evaluate how critical publicly reported computer vulnerabilities are and assign an appropriate severity score. CVSS scores Publicly known information-security vulnerabilities are usually assigned a CVE number to serve as an ID and make it easier for everybody to track, and a Common Vulnerability Scoring System (CVSS) score, to make it easier for companies to prioritize responses and resources according to…
https://www.helpnetsecurity.com/2018/11/05/ai-assigns-cvss-scores/

****

News & Views

FDIC Still Isnt Protecting Its Sensitive Information, Audit Finds
The agency responsible for insuring U.S. bank accounts still isn't meeting federal information security requirements, according to the unclassified summary of an inspector generals' report released Wednesday.
https://www.nextgov.com/cybersecurity/2018/10/fdic-still-isnt-protecting-its-sensitive-information-audit-finds/152465/

5 (more) things we learned by focusing on cybersecurity in October
With National Cybersecurity Awareness Month winding down, we initially reported five things learned from researching and writing about infosec in depth during October.
https://www.healthcareitnews.com/news/5-more-things-we-learned-focusing-cybersecurity-october

Dark Web: A cheat sheet for business professionals
Nefarious profiteers use the encrypted internet to sell stolen data, drugs, and weapons. Facebook and the UN use it to protect dissidents and journalists. This guide shines a light on the Dark Web.
https://www.techrepublic.com/article/dark-web-the-smart-persons-guide/?ftag=TREa988f1c&bhid=78480402

7 places to find threat intel beyond vulnerability databases
The purpose of National Vulnerability Databases (NVDs) is to create a centralized list of security-related software flaws and enable a more automated approach to vulnerability management. The US, China, and Russia all run their own NVDs.
https://www.csoonline.com/article/3315619/security/7-places-to-find-threat-intel-beyond-vulnerability-databases.html

Business Email Phishing Attacks to Reach $9 Billion in 2018
Being duped by a phishing email on your personal account can be devastating enough, but when it happens at work, the risk magnifies many times over. Email phishing targets business with one purpose in mind: Trick unsuspecting employees into opening an email and clicking on its attachments. By now it's no secret those attachments contain malware that steals data, money, and reputations. Hackers know it's proven time and again to work and it sometimes ends with companies hanging up an "Out of Business" sign…
https://www.sosdailynews.com/news.jspx?&articleid=66E564D3B674B62521668AA21587312C&sx=79

Nastiest malware of 2018: Top attack payloads wreaking havoc
Webroot highlights the top cyberattacks of 2018 in its latest nastiest malware list, which showcases the malware and attack payloads that have been most detrimental to organisations and consumers alike. Emotet is this year's nastiest botnet that delivers banking Trojans. It aspires to increase the number of zombies in its spam botnet, with a concentration on credential gathering. Threat actors have recently developed a universal plug and play (UPnP) module that allows Emotet to turn victims' routers into potential proxy nodes for their command-and-control infrastructure.
https://www.helpnetsecurity.com/2018/10/30/nastiest-malware-2018/

****

"Ctrl -F" for The Board

How the FBI weighs cybersecurity risks against other criminal threats
Leo Taddeo, chief information security officer at Cyxtera Technologies, discusses the continuous challenge of balancing incoming cyber threats with CNET's Dan Patterson.
https://www.techrepublic.com/article/how-the-fbi-weighs-cybersecurity-risks-against-other-criminal-threats/?ftag=TREa988f1c&bhid=78480402

CYBER DEFENSE eMAGAZINE
Your personally identifiable information (PII), if stolen, is on sale, right now on the dark web. The same will hold true of your customers PII if it's been lost or stolen. Not only does this make cybercriminals a lot of money on the dark web, it also harms your business. While they profit, if your company is a victim of a breach, you suffer. While it's absolutely not fair, the best thing you can do is learn how to manage and measure risk try using the https://www.fairinstitute.org/ standard and remember that risk is truly measurable, so start measuring your risk right away and take proactive steps to reduce the risk of a breach to your organization. http://www.cyberdefensemagazine.com/newsletters/november-2018/CDM-CYBER-DEFENSE-eMAGAZINE-November-2018.pdf

Questions
Contact FIPCO's Ken Shaurette at 800-722-3498 ext. 251 or email FIPCO IT Services for more information.

"Make Security Part of You and Your Institution's DNA!"

Threat Intelligence Newsletter: November 26, 2018

FIPCO®
IT Audit
Round Table
Discussions

If you would like to host an event, please contact: Becky Schowalter

Upcoming Threat Intelligence Peer Group Discussions
December 20 - Madison

****

Alerts & Warnings

Banking malware added password and browser history stealing to its playbook
The Trickbot banking malware has added yet another tool to its arsenal, allowing crooks to steal passwords as well as steal browser data including web history and usernames. The malware first appeared in 2016, initially focused on stealing banking credentials — but Trickbot is highly customizable and has undergone a series of updates since then. The latest trick — picked up by researchers at both Trend icro and Fortinet — is the addition of a new module designed to steal passwords. This new Trickbot variant first emerged in October. https://www.zdnet.com/article/this-banking-malware-just-added-password-and-browser-history-stealing-to-its-playbook/

Tricky TrickBot Trojan Is Back With A Vengeance
As cybersecurity researchers are reporting, identity theft scams are improving over time. There's a resurgence of different types of hacking schemes from several years ago that fell off the radar while newer scams took their places. The reality is, many tricks of the trade were being improved in the background, only to come back with even more sophisticated tactics.
https://www.sosdailynews.com/news.jspx?&articleid=15C91D7B1FEC722774A00096901A51C1&sx=79

Real estate tricks account for biggest chunk of email compromise scams
Email compromise scams – the term sounds complicated but they're just a nasty way of tricking people into redirecting huge sums of money into to the hands of crooks.
https://www.scambusters.org/emailcompromise.html

Many ATMs Can be Hacked in Minutes
Many ATMs lack adequate security mechanisms and can be compromised in minutes using various methods, according to a new report from vulnerability assessment firm Positive Technologies. https://www.securityweek.com/many-atms-can-be-hacked-minutes-report

Russian hackers are trying out this new malware against US and European targets
A new phishing campaign from a Russian-state backed hacking group targets American and European inboxes. https://www.techrepublic.com/article/russian-hackers-are-trying-out-this-new-malware-against-us-and-european-targets/?ftag=TREa988f1c&bhid=78480402

****

Hints & Tips plus Security Awareness

FSSCC Releases Cybersecurity Profile Tool
Washington, D.C. –The Financial Services Sector Coordinating Council (FSSCC) released the new Cybersecurity Profile. The Profile provides a framework that integrates widely used standards and supervisory expectations to help guide financial institutions in developing and maintaining cybersecurity risk management programs. The Profile is the result of two years' work and collaboration among… https://www.fsscc.org/Financial-Sector-Cybersecurity-Profile

Global Cyber Alliance Launches Email Spoofing Protection Tool
The Global Cyber Alliance has developed an interactive tool to help consumers, businesses and governments evaluate the security and validity of email domains. The tool will use the domain-based Message Authentication, Reporting and Conformance email security protocol —currently containing information on more than 500,000 email domains — to provide intelligence on authenticated domains and help prevent email scammers and criminals from spoofing legitimate email domains... https://www.globalcyberalliance.org/global-cyber-alliance-releases-first-dmarc-leaderboard/?utm_campaign=RiskCyber-20181119&utm_medium=email&utm_source=Eloqua&elqTrackId=d5e5f91d04c64026a3881565e8d62b62&elq=b01b63639315432fb537575911078b72&elqaid=20218&elqat=1&elqCampaignId=5842

Staying Secure While Shopping Online
It is that time of year where so many people prepare to purchase gifts for friends, family, and loved ones. Though it can be convenient to avoid the lines and rush for that latest Black Friday deal by shopping online, this also carries some risk. Cybercriminals are always working to steal your personal and payment information and the holiday shopping season is the perfect opportunity for this to happen. By following a few key practices… https://www.cisecurity.org/newsletter/staying-secure-while-shopping-online/

Warning – SpyCloud - Interesting Vendor Tool, this is awareness not an endorsement
PROTECT EMPLOYEES AND CUSTOMERS FROM ACCOUNT TAKEOVER, Stamp out fraud, intellectual property theft, and damage to your brand. https://spycloud.com/

Best Android antivirus? The top 13 tools
There are plenty of antivirus tools for Android. Here's how the top 13 measure up in protection, usability and features… https://www.csoonline.com/article/3234769/mobile-security/best-android-antivirus-the-top-13-tools.html

****

News & Views

The passwordless web explained

On 20 November 2018, Microsoft announced that its 800 million Microsoft account holders could now log in to services like Outlook, Office, Skype and Xbox Live without using a password. The announcement is part of an apparent acceleration in the march towards a passwordless web, and comes at the end of a year when Mozilla Firefox, Google Chrome and Microsoft Edge all rolled out support for WebAuthn, one of the keystone technologies. Passwordless authentication means ditching usernames and passwords in favour of biometrics, like fingerprints and face recognition, or other forms of authentication compatible with the FIDO2 specification, such as YubiKeys or Titans. In security terms, it's great news, but there's no guarantee that people will embrace it just because it's more secure.
https://nakedsecurity.sophos.com/2018/11/22/the-passwordless-web-explained/

The SEC and Cybersecurity Regulation

American companies are getting hacked, and the Securities and Exchange Commission wants corporate executives to do something about it. According to a White House Council of Economic Advisers reports released earlier this year, malicious cyber activity cost the U.S. economy between $57 billion and $109 billion in 2016. The report acknowledged a widely recognized root of the problem: "[C]yberattacks and cyber theft impost externalities that may lead to rational underinvestment in cybersecurity by the private sector relative to the socially optimal level of investment." http://www.lawfareblog.com/sec-and-cybersecurity-regulation

Vaporworms: New breed of self-propagating fileless malware to emerge in 2019

WatchGuard Technologies' information security predictions for 2019 include the emergence of vaporworms, a new breed of fileless malware with wormlike properties to self-propagate through vulnerable systems, along with a takedown of the internet itself and ransomware targeting utilities and industrial control systems. "Cyber criminals are continuing to reshape the threat landscape as they update their tactics and escalate their attacks against businesses, governments and even the infrastructure of the internet itself," said Corey Nachreiner, CTO at WatchGuard Technologies.
https://www.helpnetsecurity.com/2018/11/16/self-propagating-fileless-malware/

9 cyber security predictions for 2019

Predictions are tough, but even more so in the chaotic world of cyber security. The threat landscape is huge, offensive and defensive technologies are evolving rapidly, and nation-state attacks are increasing in terms of scope and sophistication. This cyber "fog of war" makes it hard to see or assess every trend. Despite this, it is still possible to make some reasonably accurate predictions based on current developments. CSO therefore asked CSO staff and contributors to tell about the biggest events or trends they anticipate for the next 12 months. https://www.csoonline.com/article/3322221/security/9-cyber-security-predictions-for-2019.html

Crooks use cryptojacking to take over PCs for digital currency "mining"

Although it sounds highly technical – and, in a way it is – cryptojacking is actually a dead simple way for crooks to make money using other people's computers. https://www.scambusters.org/cryptojacking.html

****

"Ctrl -F" for The Board

FBI, This Week: The Chief Information Security Officer Academy
Chief information security officers from companies across the country are graduating from an FBI academy designed to teach them how to prevent, counter, and defeat cybercrime. https://www.fbi.gov/audio-repository/ftw-podcast-ciso-academy-102618.mp3/view

Financial Stability Board Publishes New Cyber Lexicon
The Financial Stability Board has published a lexicon of 50 core terms related to cyber security and cyber resilience in the financial sector. The lexicon is intended to create a common understanding of cyber-related terminology to support the collaborative work of the FSB, other standards-setting bodies and industry stakeholders… http://www.fsb.org/wp-content/uploads/P121118-1.pdf?utm_campaign=RiskCyber-20181119&utm_medium=email&utm_source=Eloqua&elqTrackId=6c124d9732534ebd9ae29d78f17ba32a&elq=b01b63639315432fb537575911078b72&elqaid=20218&elqat=1&elqCampaignId=5842

Congress Approves New DHS Cybersecurity Agency
Bill Creating Cybersecurity and Infrastructure Security Agency Awaits President's Signature. The United States will soon officially have a single agency that takes the lead role for cybersecurity. https://www.bankinfosecurity.com/congress-approves-new-dhs-cybersecurity-agency-a-11702

Questions
Contact FIPCO’s Ken Shaurette at 800-722-3498 ext. 251 or email FIPCO IT Services for more information.

"Make Security Part of You and Your Institution's DNA!"

Threat Intelligence Newsletter: December 10, 2018

FIPCO®
IT Audit
Round Table
Discussions

If you would like to host an event, please contact: Becky Schowalter

Upcoming Threat Intelligence Peer Group Discussions
December 20 - Madison

****

Alerts & Warnings

ATM attackers strike again: Are you at risk?
The United States National ATM Council recently released information about a series of ATM attacks using rogue network devices. The criminals opened the upper half of the ATM and installed the device, most likely into the Ethernet switch. The device then intercepted the ATM's network traffic and changed the bank's "withdraw denied" response to "withdraw approved," presumably only for the criminals' cards. For many readers, the attacks' success may… https://www.helpnetsecurity.com/2018/11/27/atm-attackers/

"Free" Trial Offers?
A chance to try something out for free? What have you got to lose?
If you're interested in a particular product or service, trying before you buy might seem like a no-brainer. But what starts as a free trial — or for a very low cost — might end up costing you real money.
https://www.consumer.ftc.gov/articles/0101-free-trial-offers

Cyber-criminals invent a new "no talk" scam to trick you
Telephone scams are nothing new. Almost all of us will have taken a call from someone claiming to be from our bank. Or a helpful representative of Microsoft who needs to help us fix our computers.
https://www.pandasecurity.com/mediacenter/technology/new-no-talk-scam/?mc_cid=3baf3da6bc&mc_eid=2b2ac7a1bf

Hacked Without a Trace: The Threat of Fileless Malware

Understanding Fileless Attacks

Malware. The word alone makes us all cringe as we instantly relate it to something malicious happening on our computers or devices. Gone are the days when we thought the easiest way to protect our computers was to install the latest anti-everything. But today's hackers no longer depend on victims downloading an infected file – they are now leveraging fileless malware…
https://www.fightingidentitycrimes.com/understanding-fileless-malware/

Watch out for this new Social Security call spoofing scam

Call spoofing — a trick scammers use to hide their phone identity and pretend to be someone else – now accounts for around half of all incoming calls, according to some observers. By fooling victims into believing the call is from someone they know or a legitimate organization like a bank or government office, the crooks are out to try to steal confidential information. In the latest call spoofing case, scammers pretend to be from the U.S. Social Security Administration – but you won't lose money if you follow two simple steps, … https://www.scambusters.org/callspoofing.html

Pied Piper phishing scheme infests victims with FlawedAmmyy, RMS RATs

The cybercriminal threat group TA505 is a key suspect in an ongoing phishing campaign that's been attempting to infect victims with the FlawedAmmyy and Remote Manipulator (RMS) remote access trojans. https://www.scmagazine.com/home/security-news/pied-piper-phishing-scheme-infests-victims-with-flawedammyy-rms-rats/?utm_source=newsletter&utm_medium=email&utm_campaign=SCUS_Newswire_20181203&hmSubId=XOjrUhr_Swg1&email_hash=305f40be59a0dcb04476bf06c7e07dc9&mpweb=1325-4164-111266

Printeradvertising.com Spam Service Claims It Can Print Anywhere

In trays of printed paper, a new service called Printeradvertising.com was launched that states that it can print a viral advertising campaign to every connected printer in the world. While this is an overstatement, the service did start out with a bang when Andrew Morris, founder of security company Grey Noise, detected a mass printer spam campaign promoting the service connecting to his company's honeypots. Morris told BleepingComputer that at least sixty distinct Grey Noise honeypot detected connections coming from IP address 194.36.173.50 that were trying to send print jobs. This IP address belongs to a subnet known for malicious activity.
https://www.bleepingcomputer.com/news/security/printeradvertisingcom-spam-service-claims-it-can-print-anywhere/

****

Hints & Tips plus Security Awareness

Why compliance is never enough

THINK ABOUT THAT WHEN YOU FIGURE YOU ARE DONE AT BASELINE!!

Organizations are well aware of the security risks inherent in our hyper-connected world. However, many are making the mistake of focusing their attention on being compliant rather than on ensuring that their security strategy is effective and efficient. As the threat landscape continues to evolve this type of compliance-driven, checkbox mentality is setting many organizations up for a potentially disastrous fall (or breach). Being in compliance does not guarantee that a company has a comprehensive …
https://www.helpnetsecurity.com/2018/11/28/why-compliance-is-never-enough/

Cybersecurity Efforts Get a Boost with New FSSCC profile

Banks face significant operational risk challenges in the current climate, with a mix of cybersecurity threats vying for attention against increasing compliance mandates around risk assessment and mitigation. "We're in a very complex regulatory landscape," says Josh Magri, SVP at BITS, the Bank Policy Institute's technology division. With each of the nine federal financial-sector regulators, along with other agencies at the state level, appropriately focused on cybersecurity, Magri says, "there hasn't been a standardization of the way they talk about it, or issue regulations or develop guidance about it." https://bankingjournal.aba.com/2018/11/cybersecurity-efforts-get-a-boost-with-new-fsscc-profile/?utm_campaign=ABA-Newsbytes-112718&utm_medium=email&utm_source=Eloqua

Half of all Phishing Sites Now Have the Padlock

Maybe you were once advised to "look for the padlock" as a means of telling legitimate e-commerce sites from phishing or malware traps. Unfortunately, this has never been more useless advice. New research indicates that half of all phishing scams are now hosted on Web sites whose Internet address Includes the padlock and begins with "http://". Recent data from anti-phishing company PhishLabs shows that 49 percent of all phishing sites in the third quarter of 2018 bore the padlock security icon next to the phishing site domain name as displayed in a browser address bar. That's up from 25 percent just one year ago, and from 35 percent in the second quarter of 2018. https://krebsonsecurity.com/2018/11/half-of-all-phishing-sites-now-have-the-padlock/

3 ways for your business to spot a spear phishing email during the holidays

Cyberattacks on organizations are predicted to skyrocket during the online holiday shopping season. Here is how to identify possible threats. https://www.techrepublic.com/article/3-ways-for-your-business-to-spot-a-spear-phishing-email-during-the-holidays/?ftag=TREa988f1c&bhid=78480402

Putting cash in the mail

Associate Director, Division of Consumer Response and Operations

We've been warning you about scammers asking you to pay with gift cards or by wiring money. Scammers love getting you to pay that way because they can get your money fast and disappear. It's almost as good as getting you to send cold, hard cash. Which must have occurred to them, too, because some scammers are now going low-tech and asking people to send cash in the mail. Sometimes they even tell people to divide the cash between pages of a magazine. https://www.consumer.ftc.gov/blog/2018/12/putting-cash-mail?utm_source=govdelivery

CSIAC – Webinar; Are Cybersecurity Compliance Based Programs Working?

This presentation provides an overview of two quantitative studies conducted at the Pacific Northwest National Laboratory (PNNL) in 2017. These studies were designed to explore psychological and contextual variables that influence users confronted with cybersecurity challenges and their propensity to comply with policies under those conditions. From these studies, a new, cross-disciplinary approach towards assessing cybersecurity risk began to emerge. Ultimately, these efforts could lead to the development of risk assessment instruments that provide a tailored approach towards understanding organizational risk. https://www.csiac.org/podcast/phishing-for-solutions-are-cybersecurity-compliance-based-programs-working/

Contact lens seller turns a blind eye to the law
Cosmetic contacts lenses – also known as costume or decorative contact lenses – can change the way your eye looks without correcting your vision. While they may seem like just another fashion accessory, the fact is all contacts require a prescription. Anyone who sells you lenses without getting a copy of your prescription or verifying your prescription information with your prescriber is selling them illegally. https://www.consumer.ftc.gov/blog/2018/12/contact-lens-seller-turns-blind-eye-law?utm_source=govdelivery

Snippets issue highlights new gift card, paycheck diversion, Uber and grants scams
We have sneaky tricks galore, including a nasty gift card scam for new employees, in this week's Snippets Issue. https://www.scambusters.org/giftcardscam.html

****

News & Views

The FBI Created a Fake FedEx Website to Unmask a Cybercriminal
The FBI has started deploying its own hacking techniques to identify financially-driven cybercriminals, according to court documents unearthed by Motherboard. The news signals an expansion of the FBI's use of tools usually reserved for cases such as child pornography and bomb threats. But it also ushers in a potential normalization of this technologically-driven approach, as criminal suspects continually cover up their digital trail and law enforcement have to turn to more novel solutions.
https://motherboard.vice.com/en_us/article/d3b3xk/the-fbi-created-a-fake-fedex-website-to-unmask-a-cybercriminal

7 Real-Life Dangers That Threaten Cybersecurity
Cybersecurity tends to focus on dangers that appear on networks or in messages. The attackers may be half a world away, so the threat is the only thing that matters. But what happens when the threat actor is walking through the front door or sitting next to you at an airport coffee shop? Firewall rules and DNSSec can have minimal impact on the thief sliding a company-owned laptop into his backpack and walking out the door. "If we all took our computers, encased them in concrete, and dropped them into the middle of the Atlantic Ocean, nobody would ever steal our data, but it wouldn't matter because our data would be on the bottom of the Atlantic Ocean," says Tim Callan, senior fellow at Sectigo. The challenge, he says, is reconciling physical security with the fact that people need to use their computers and mobile devices for legitimate work. https://www.darkreading.com/risk/7-real-life-dangers-that-threaten-cybersecurity/d/d-id/1333326

Hackers are opening SMB ports on routers so they can infect PCs with NSA malware
Akamai says that over 45,000 routers have been compromised already.
https://www.zdnet.com/article/hackers-are-opening-smb-ports-on-routers-so-they-can-infect-pcs-with-nsa-malware/?ftag=TRE-03-10aaa6b&bhid=78480402

After Microsoft complaints, Indian police arrest tech support scammers
Indian police raid 26 call centers, make 63 arrests. https://www.zdnet.com/article/after-microsoft-complaints-indian-police-arrest-tech-support-scammers-at-26-call-centers/?ftag=TRE-03-10aaa6b&bhid=78480402

Hackers are using leaked NSA hacking tools
More than a year after patches were released to thwart powerful NSA exploits that leaked online, hundreds of thousands of computers are unpatched and vulnerable. First they were used to spread ransomware. Then it was cryptocurrency mining attacks. Now, researchers say that hackers are using the leaked tools to create an even bigger malicious proxy network. New findings from security giant Akamai say that the previously reported UPnProxy vulnerability, which abuses the common Universal Plug and Play network protocol, can now target unpatched computers behind the router's firewall… https://techcrunch.com/2018/11/28/hackers-nsa-eternalblue-exploit-hijack-computers/

Top 4 security threats businesses should expect in 2019
Cybercriminals are developing more sophisticated attacks, while individuals and enterprises need to be more proactive in security practices. https://www.techrepublic.com/article/top-4-security-threats-businesses-should-expect-in-2019/?ftag=TREa988f1c&bhid=78480402

Marriott Data Breach Exposes the Personal Information of 500 Million Guests
On Friday, November 30, 2018, hospitality giant Marriott International announced that hackers had breached its Starwood guest reservation system. Starwood oversees at least 11 hotel brands under the Marriott umbrella, including W Hotels, Regis, Sheraton Hotels & Resorts, and Westin Hotels & Resorts. https://www.fightingidentitycrimes.com/marriott-data-breach/

****

"Ctrl -F" for The Board

How CISOs can tell a better security story to their board
Historically, when CISOs have been called to speak to their organization's board of directors, it was an uncommon event. Just a decade ago, the CISO who presented more than once per year was a rare bird. https://www.scmagazine.com/home/opinions/how-cisos-can-tell-a-better-security-story-to-their-board/?utm_source=newsletter&utm_medium=email&utm_campaign=SCUS_Newswire_20181128&hmSubId=XOjrUhr_Swg1&email_hash=305f40be59a0dcb04476bf06c7e07dc9&mpweb=1325-4050-111266

(IN)SECURE Magazine
(IN)SECURE Magazine is a freely available digital security magazine discussing some of the hottest information security topics. https://www.helpnetsecurity.com/insecuremag/issue-60-december-2018/

Questions
Contact FIPCO's Ken Shaurette at 800-722-3498 ext. 251 or email FIPCO IT Services for more information.

"Make Security Part of You and Your Institution's DNA!"

Threat Intelligence Newsletter: January 3, 2019

FIPCO®
IT Audit
Round Table
Discussions

If you would like to host an event, please contact: Becky Schowalter

Upcoming Threat Intelligence Peer Group Discussions
None available at the current time

****

Alerts & Warnings

Android Trojan steals money from victims' PayPal account
ESET researchers have unearthed a new Android Trojan that tricks users into logging into PayPal, then takes over and mimics the user's clicks to send money to the attacker's PayPal address. The heist won't go unnoticed by the victim if they are looking at the phone screen, but they will also be unable to do anything to stop the transaction from…
https://www.sosdailynews.com/news.jspx?&articleid=A1DAA70D684E81FC8D2013A886F0AD8D&sx=79

Sextortion scams redirecting users to ransomware now
Sextortion emails take a dark turn and are now trying to infect users with the GandCrab ransomware.
https://www.zdnet.com/article/those-annoying-sextortion-scams-are-redirecting-users-to-ransomware-now/

Operation Sharpshooter Takes Aim at Global Critical Assets
Researchers have detected a widespread reconnaissance campaign using a never-before-seen implant framework to infiltrate global defense and critical infrastructure players — including nuclear, defense, energy and financial companies. The campaign, dubbed Operation Sharpshooter, began Oct. 25 when a splay of malicious documents were sent via Dropbox. The campaign's implant has since appeared in 87 organizations worldwide, predominantly in the U.S. and in other English-speaking companies. "Our discovery of a new, high-function implant is another example of how targeted attacks…
https://threatpost.com/sharpshooter-global-critical-assets/139843/

DarkVishnya: Banks attacked through direct connection to local network
While novice attackers, imitating the protagonists of the U.S. drama Mr. Robot, leave USB flash drives lying around parking lots in the hope that an employee from the target company picks one up and plugs it in at the workplace, more experienced cybercriminals prefer not to rely on chance. https://securelist.com/darkvishnya/89169/?utm_campaign=RiskCyber-20181217&utm_medium=email&utm_source=Eloqua

Dozens of companies impersonated in evolving 'Three Questions Quiz' scam
There's no question about it: the "Three Questions Quiz" is a scam, regardless of which legitimate brand it's attempting to imitate. https://www.scmagazine.com/home/security-news/dozens-of-companies-impersonated-in-evolving-three-questions-quiz-scam/?utm_source=newsletter&utm_medium=email&utm_campaign=SCUS_Newswire_20181218&hmSubId=XOjrUhr_Swg1&email_hash=305f40be59a0dcb04476bf06c7e07dc9&mpweb=1325-4567-111266

Remote Firmware Attack Renders Servers Unbootable
Security researchers have found a way to corrupt the firmware of a critical component usually found in servers to turn the systems into an unbootable hardware assembly. The recovery procedure requires physical intervention to replace the malicious firmware. Achieving this is done via regular tools used to keep the baseboard management controller (BMC) up to date.
https://www.bleepingcomputer.com/news/security/remote-firmware-attack-renders-servers-unbootable/

Hackers Bypass Gmail, Yahoo 2FA at Scale
Amnesty International this week released a report detailing how hackers can automatically bypass multifactor authentication (MFA) when the second factor is a text message, and they're using this tactic to break into Gmail and Yahoo accounts at scale. MFA is generally recommended; however, its security varies depending on the chosen factor. Consumers prefer second-factor codes sent via text messages because they're easy to access. Unfortunately for some, cybercriminals like them for the same reason. https://www.darkreading.com/threat-intelligence/hackers-bypass-gmail-yahoo-2fa-at-scale/d/d-id/1333534

Malware Camouflages Itself To Get Business Banking Credentials
Social engineering is a broad term. It can encompass anything from an attacker pretending to be a printer repair person who convinces someone to let him into the office to very specialized targeted methodologies such as cyberstalking. The latter can lead to very effective spear-phishing and appears to be how a recently found malware is deployed. The malware, called…
https://www.sosdailynews.com/news.jspx?&articleid=C8A877A0C58176AF493DE3CEBBCB358F&sx=79

Undetectable Fileless Malware Threatens Businesses and Consumers
Most malware sneaks onto your computer via files you accidentally download -- but watch out now for a growing fileless threat! https://www.scambusters.org/fileless.html or https://searchsecurity.techtarget.com/news/252455018/Malwarebytes-Fileless-ransomware-an-emerging-threat-for-US

This is what a Social Security scam sounds like
Earlier this month, we told you about a growing scam: people pretend to be from the Social Security Administration (SSA) and try to get your Social Security number or your money. That scam is now growing exponentially. Here's what one of those scam calls sound like:
https://www.consumer.ftc.gov/blog/2018/12/what-social-security-scam-sounds?utm_source=govdelivery

****

Hints & Tips plus Security Awareness

What is the FICO® Cyber Risk Score?

The FICO® Cyber Risk Score is an empirical assessment of security risk based on an inventory of Internet-facing network assets, an objective assessment of network condition, observed network management practices and historic evidence of compromise. Third parties such as business partners and cyber insurance underwriters may use the results, represented as a three-digit score, as an important element in their underwriting or contracting decision processes. https://content.fico.com/e/517101/ers-Cyber-Risk-Score-eBook-pdf/4hg4x/321488898?h=AeKu2WYFqKQo8EbmrYHeopgJEbpTn9dr0UoEz8AtIys

Fraud Watch Network

Want to stay safe from cyber criminals and identity thieves during the holidays? The tools, tips and info you need to help protect you and your loved ones are as close as the Fraud Watch Network… https://www.aarp.org/money/scams-fraud/?CMP=EMC-MIM-DIS-OTH-FRD-20181210_Holiday_Fraud_Protection_Indiv_606500_940104-20181210-FraudWatchNetwork_LNK-3423658-&mi_u=43577144&mi_ecmp=20181210_Dec_Holiday_Fraud_Individual_SL2_WINNER_606500_940104&encparam=+ZL+3IZZXuNDJ77xENIwLg

What is the difference between a VPN and a proxy

As you dig into the networking settings on your computer or smartphone, you'll often see options labelled "VPN" or "Proxy". Although they do similar jobs, they are also very different. This article will help you understand what the difference is, and when you might want to use one. https://www.pandasecurity.com/mediacenter/technology/difference-vpn-vs-proxy/?mc_cid=e89fd4233f&mc_eid=2b2ac7a1bf

How to Identify a Business Email Compromise Attack

Business email compromise attacks have skyrocketed over the last few years. Hackers use this strategy to target corporate or publicly available email accounts of executives or high-level employees. The attackers attempt to receive financial gain through phishing attacks or by using keyloggers to perform fraudulent wire transfers. This can result in a significant loss for businesses. https://www.pandasecurity.com/mediacenter/panda-security/business-email-compromise/?mc_cid=e89fd4233f&mc_eid=2b2ac7a1bf

Tips for Securing Your Mobile Devices

Nearly all of us these days have some type of mobile device that is essentially a part of us. It is filled with all kinds of personal information, such as our contacts, our email conversations, and perhaps even our health information. Losing it, having it accessed without permission, or finding out it's… https://www.sosdailynews.com/news.jspx?&articleid=E52F81ACD0E1CA2BE4BFF71F1DDBAE08&sx=79

Common Shopping Scams With A New Twist

This time of year is the busiest for shopping. Considering so many organizations have our payment information stored for quick online purchases, it can be a bit of a shock when you get a notification that purchase was made and you don't have any recollection of making it. The Federal Trade Commission (FTC) is warning of an old scam with a new twist that is hitting consumers hard... https://www.sosdailynews.com/news.jspx?&articleid=37B5E590294916A02250B6D165C152E6&sx=79

Automated Cyber Attacks Are the Next Big Threat. Ever Hear of 'Review Bombing'?
Nonhuman, automated attacks on their own will be able to find and breach even well-protected companies. Nervous? You should be. https://www.entrepreneur.com/article/325142

Doxxing: What It Is How You Can Avoid It
Doxxing means publishing private information about someone online to harass or intimidate them. It has ruined reputations and caused untold distress to hundreds of people. On occasion, doxxing has resulted in injury or even death. Being doxxed can have serious consequences for your safety and privacy. How can you prevent it? https://www.tripwire.com/state-of-security/security-awareness/what-is-doxxing-and-how-can-you-avoid-it/

****

News & Views

Will sophisticated attacks dominate in 2019?
Trend Micro released its 2019 predictions report, warning that attackers will increase the effectiveness of proven attack methods by adding more sophisticated elements to take advantage of the changing technology landscape. As we head into 2019, organizations must understand the security implications of greater cloud adoption, converging IT and OT, and increasing remote working," said Greg Young, vice president of cybersecurity for Trend Micro. "Cybercriminals will continue to follow a winning formula – exploiting existing flaws, social engineering and stolen credentials – to drive profits."
https://www.helpnetsecurity.com/2018/12/12/sophisticated-attacks-dominate/

Microsoft Patch Tuesday includes fix for actively exploited zero-day
Address nearly 40 vulnerabilities including and actively exploited zero-day, in its December 2018 Patch Tuesday release. Several of the issues were rated critical or important and or dealt with remote code execution flaws in Windows including one vulnerability that was actively being exploited in the wild.
https://www.scmagazine.com/home/security-news/microsoft-addressed-nearly-40-

Why Microsoft is fighting to stop a cyber world war
Two days last year finally woke the world up to the dangers of cyberwarfare, according to Microsoft's President Brad Smith: 12 May and 26 June. On 12 May the WannaCry ransomware attack created havoc by encrypting PCs across the world and costing billions to repair the damage. Just over a month later on 16 June the NotPetya malware caused more damage, again costing billions to fix. Western governments have blamed WannaCry on North Korea, and NotPetya on Russia — it probably was designed as an attack on Ukraine which then got out of hand. https://www.zdnet.com/article/why-microsoft-is-fighting-to-stop-a-cyber-world-war/

Imposter Fraud Leads Top Scams Table
Did you get scammed in 2018? We certainly hope not; if you're a regular Scambusters reader we hopefully gave you enough warnings to sidestep the top scams of the year.
https://www.scambusters.org/topscams2018-19.html

****

"Ctrl -F" for The Board

US Couldn’t Handle Catastrophic Cyberattack on Power Grid, Government Warns
Key infrastructures are in the crossfire of cyberwarfare. Growing threats and sophisticated nation-state attacks backed by North Korea, China and Russia jeopardize public safety and national security. Which one is the bigger threat? CHECK OUT THE 2013 National Geographic video…
https://businessinsights.bitdefender.com/us-couldnt-handle-catastrophic-cyberattack-on-power-grid-government-warns?utm_campaign=Weekly%20blog%20notifications&utm_source=hs_email&utm_medium=email&utm_content=68427597&_hsenc=p2ANqtz-8N9HetfyBEdtgb7uMIeZ0ZBo7pkdLtEix3jDosRzty0W7Y04V-ebWObLyJ4vcLwmJVGOqMJ8GVLWz8L4fKA_BiKpKkyA&_hsmi=68427597

Questions
Contact FIPCO’s Ken Shaurette at 800/722-3498 ext. 251 or email FIPCO IT Services for more information.

"Make Security Part of You and Your Institution's DNA!"

Threat Intelligence Newsletter: January 21, 2019

FIPCO®
IT Audit
Round Table
Discussions

If you would like to host an event, please contact: Becky Schowalter

Upcoming Threat Intelligence Peer Group Discussions
None available at the current time

****

Alerts & Warnings

BEC Scammers Go After Employee Paychecks
Cybersecurity experts have noticed an uptick in business email compromise (BEC) scams in which threat actors go after monthly employee paychecks. The scam starts with a threat actor impersonating an employee of a targeted company in an email to the firm's department that is in charge of payroll. The crook will… https://www.oodaloop.com/briefs/2019/01/16/bec-scammers-go-after-employee-paychecks/

The 773 Million Record "Collection #1" Data Breach
Many people will land on this page after learning that their email address has appeared in a data breach I've called "Collection #1". Most of them won't have a tech background or be familiar with the concept of credential stuffing so I'm going to write this post for the masses and link out to more detailed material for those who want to go deeper. https://www.troyhunt.com/the-773-million-record-collection-1-data-reach/

These malicious Android apps will only strike when you move your smartphone
Once again, cybercriminals have managed to sneak malicious apps onto the Google Play Store. Researchers with Trend Micro have found two Android apps on Google Play that serve the Anubis banking Trojan, but only if information from the motion sensors on the targeted device indicate movement. The two apps are Currency… https://www.oodaloop.com/briefs/2019/01/18/these-malicious-android-apps-will-only-strike-when-you-move-your-smartphone/

U.S Secret Service Alert: Man-in-the-Middle Attacks Targeting ATMs
On Dec. 20, the U.S. Secret Service's Global Investigative Operations Center released an alert regarding ATM cash-out activity involving withdrawals on denied transactions through suspected "man-in-the-middle" style attacks targeting Hyosung 5000 CE machines. The U.S. Secret Service urges any institutions witnessing incidents similar to those described in the alert to contact their local field office.

Battling attacks from global criminal networks in the financial sector
Every now and then, banks and financial institutions (and their customers) are targeted by opportunistic hackers, but they are much more worried about those that are smarter, have access to better technologies and knowledge of new techniques, and have considerable funding provided either by organized crime groups or nation-states. "These organised global criminal networks channel their resources into accessing data, executing attacks and laundering the proceeds of these attacks to further fund their agenda," says…
https://www.helpnetsecurity.com/2019/01/09/attacks-financial-sector/

Emotet Malware Gets More Aggressive
Emotet, a nasty botnet and popular malware family, has proven increasingly dangerous over the past year as its operators adopt new tactics. Now armed with the ability to drop additional payloads and arriving via business email compromise (BEC), it's become a major threat to organizations. Security watchers are wary of Emotet, which was among the first botnets to spread banking Trojans laterally within target organizations, making removal difficult. After ramping up in early 2018, Emotet increased again during the holiday season. Through the start of 2019, the malware continued to spread.
https://www.darkreading.com/attacks-breaches/emotet-malware-gets-more-aggressive-/d/d-id/1333584

Apple Phone Phishing Scams Getting Better
A new phone-based phishing scam that spoofs Apple Inc. is likely to fool quite a few people. It starts with an automated call that display's Apple's logo, address and real phone number, warning about a data breach at the company. The scary part is that if the recipient is an iPhone user who then requests a…
https://krebsonsecurity.com/2019/01/apple-phone-phishing-scams-getting-better/

CERT/CC Details Critical Flaws in Microsoft Windows, Server
The CERT Coordination Center (CERT/CC) has published data on vulnerabilities affecting versions of Microsoft Windows and Windows Server. Microsoft had issued an advisory for CVE-2018-8611, a Windows kernel elevation of privilege bug that exists when the Windows kernel fails to properly handle objects in memory. An attacker who exploited this flaw could run arbitrary code in kernel mode. The company also issued CVE-2018-8626 for a Windows DNS server heap overflow vulnerability. A remote code execution flaw exists in Windows DNS servers when they don't properly handle requests, Microsoft explains.
https://www.darkreading.com/vulnerabilities---threats/cert-cc-details-critical-flaws-in-microsoft-windows-server-/d/d-id/1333590

Phishing kit leverages web fonts to obfuscate source code
In an apparent first, researchers last year observed an unusual phishing kit that obfuscates its landing page's source code with web fonts as a means to avoid detection. Attackers recently used the kit as part of a credential harvesting scheme that targeted a major retail bank…
https://www.scmagazine.com/home/security-news/phishing-kit-leverages-web-fonts-to-obfuscate-source-

code/?utm_source=newsletter&utm_medium=email&utm_campaign=SCUS_Newswire_20190108&hmSubId=XOjrUhr_Swg1&email_hash=305f40be59a0dcb04476bf06c7e07dc9&mpweb=1325-4854-111266

This old ransomware is using an unpleasant new trick to try and make you pay up
Researchers at cyber security firm Coveware have uncovered a new ransomware campaign in which threat actors try to manipulate victims into paying ransom to regain access to their files, by claiming the money will be donated to charity. The ransomware used in the campaign is CryptoMix, a relatively unknown file-encrypting… https://www.oodaloop.com/briefs/2019/01/09/this-old-ransomware-is-using-an-unpleasant-new-trick-to-try-and-make-you-pay-up/

Google Search Results Spoofed to Create Fake News
While efforts to increase awareness about fake news and how to spot it, a new technique using Google has emerged that allows users to tamper with Google search results through custom URLs. The tactic reportedly operates by using Knowledge Cards, the boxes on the right-hand side of the screen populated. https://www.oodaloop.com/briefs/2019/01/11/google-search-results-spoofed-to-create-fake-news/

****

Hints & Tips plus Security Awareness

January 28th is National Data Privacy Day - Safeguard your data and your privacy!
In the past year, we saw a significant number of data breaches impacting the privacy of individuals. According to the Privacy Rights Clearinghouse, in 2018, 807 publicly disclosed breaches exposed 1.4 billion records. While this is a decrease from 2017's 2 billion records exposed, the problem remains enormous because so many websites, social media outlets, and devices contain our information.
https://www.cisecurity.org/newsletter/january-28th-is-national-data-privacy-day/?utm_campaign=MS-ISAC&utm_source=hs_email&utm_medium=email&utm_content=69115401&_hsenc=p2ANqtz-9xLX3JzdRs6-sL8dbTEqotYWOwQFjnozv-nL3JGSWAcbHBIY5HkSyMX8VdJmeVcHP4GBDZvSs0qhgb98P4M3UXJrdjxg&_hsmi=69114760

Why Microsoft is leading the march toward a passwordless future
Microsoft rolled out passwordless sign in option for insiders on Windows 10 build 18309. Here's why others will likely follow. https://www.techrepublic.com/article/why-microsoft-is-leading-the-march-toward-a-passwordless-future/?ftag=TREa988f1c&bhid=78480402

NCSC helps American businesses stay safe from nation-state cyberattacks
The United States National Counterintelligence and Security Center (NCSC) has begun to distribute materials to private American companies in order to help protect them from the increasingly severe threat from nation-state actors. Videos, leaflets and other materials will be distributed all across the country as part of the initiative. https://www.bleepingcomputer.com/news/security/ncsc-starts-campaign-to-help-industry-fight-foreign-state-threats/

Incident Response eSummit
On Thursday, February 14, join us for MISTI's Incident Response eSummit, featuring keynote speaker, Mark Butler, CISO for MegaplanIT! We will explore what practitioners are using to probe parts of the operating system, what automation you can apply and how to make your data results useful in the aggregate. Beware Vendor sponsored…. But also these can be very educational.
https://engage.vevent.com/index.jsp?eid=7019&seid=2069

National Counterintelligence and Security Center Launch Campaign Against Cyber Threats
The National Counterintelligence and Security Center recently launched a campaign to help the private sector guard against growing threats from nation state cyber actors. The campaign material includes a host of videos, brochures, flyers and other informative resources aimed at enhancing the private sector's awareness of possible attacks to their networks, proprietary data and supply chains. With this campaign, NCSC plans to equip U.S. companies with the critical information needed to better understand and defend against such attacks… https://www.dni.gov/index.php/ncsc-newsroom/item/1938-national-counterintelligence-and-security-center-launches-campaign-to-help-private-industry-guard-against-threats-from-nation-state-actors?utm_campaign=RiskCyber-20190115&utm_medium=email&utm_source=Eloqua&elqTrackId=9c2295eb4df44e6b820d5969a2d09002&elq=cfe74d4f791540b1956b3961a1eece8c&elqaid=20551&elqat=1&elqCampaignId=6055

Tax Scams: What to Expect in 2019
It used to be that this time of year was the season for tax scams -- during the run-up to Tax Day itself. But no longer. Tax scams are a year-round event with crooks, in the main, either posing as the IRS trying to trick you into sending them money or faking a taxpayer's identity to claim a refund.
https://www.scambusters.org/taxscam2019.html

****

News & Views

Attack Surface Growing Fast
The attack surface is growing faster than it has at any other point in the history of technology
Avast launched its annual Threat Landscape Report, detailing the biggest security trends facing consumers in 2019 as collected by the Avast Threat Labs team. "This year, we celebrated the 30th anniversary of the World Wide Web. Fast forward thirty years and the threat landscape is exponentially more complex, and the available attack surface is growing faster than it has at any other point in the history of technology," commented Ondrej Vlcek, President of Consumer at Avast.
https://www.helpnetsecurity.com/2019/01/07/avast-threat-landscape-report/

Look Out! Nearly 1.5 Million New Phishing Sites Created Every Month
Those tried-and-true lures hackers use for email phishing campaigns keep getting better and more effective. According to the Webroot Threat Report, there are close to 1.5 million new phishing sites every month. For businesses, a Wombat Security study finds that last year, 76% of companies fell victim to phishing attacks. Any way you look at it, there's a boatload of successful phishing going on out there. As such, email phishing continues to proliferate in scope and depth, breaking records year after year…
https://www.sosdailynews.com/news.jspx?&articleid=FF4345205425E2F910196B24DB6763AE&sx=79

Modlishka pen testing tool could be used for real attacks

A Polish cybersecurity researcher has released a tool designed for pen testers that has the ability intercept data in real-time and even swipe 2FA credentials, a move that has some in the industry concerned that it could be used for nefarious purposes. https://www.scmagazine.com/home/security-news/modlishka-pen-testing-tool-could-be-used-for-real-attacks/?utm_source=newsletter&utm_medium=email&utm_campaign=SCUS_Newswire_20190111&hmSubId=XOjrUhr_Swg1&email_hash=305f40be59a0dcb04476bf06c7e07dc9&mpweb=1325-4937-111266

Government cybersecurity at risk as shutdown lingers

Due to the ongoing shutdown, US government agencies are becoming increasingly vulnerable to cyberattacks. Because cybersecurity and IT staff have been furloughed in many government agencies, TLS certificates for government websites are not being renewed, systems aren't being patched and there is no active monitoring of agency networks for performance….
https://www.oodaloop.com/briefs/2019/01/18/government-cybersecurity-at-risk-as-shutdown-lingers/

Facebook Shuts Hundreds of Russia-Linked Pages, Accounts for Disinformation

Helped by a tip from US law enforcement, Facebook has shut down two massive Russian disinformation campaigns comprising hundreds of Facebook groups and pages as well as Facebook and Instagram accounts with hundreds of thousands of followers. One of the campaigns focused on Ukraine, whereas the other targeted countries in Central… https://www.oodaloop.com/briefs/2019/01/18/facebook-shuts-hundreds-of-russia-linked-pages-accounts-for-disinformation/

****

"Ctrl -F" for The Board

Email security predictions: What we can expect in 2019

2018 shed a lot of light on how expensive successful phishing attacks can be, with the FBI reporting in July well over $12B in financial losses due to business email compromise and Anthem reaching a $16M settlement in October due to phishing-driven data breach. Cybercriminals continue to expand their repertoire by iterating on successful attack techniques such as brand impersonations, executive spoofing, and more recently… https://www.helpnetsecurity.com/2019/01/10/email-security-predictions/

Some Thoughts on the Year in Privacy and Data Security Law

Friday, January 4, 2019 As we turn the page on 2018, let's reflect on some of the key privacy and cybersecurity issues that will continue to occupy our hearts and minds in 2019.
https://www.natlawreview.com/article/some-thoughts-year-privacy-and-data-security-law?utm_content=f20a8df1de35f2615e8c93a0dc9d19cb&utm_campaign=1-8-2019Cybersecurity%20Legal%20News&utm_source=Robly.com&utm_medium=email

Four cybersecurity trends every CIO should know
The cybersecurity landscape in 2019 will likely bolster bigger, more complex threats and developments. Given the intricacy of today's cyber security challenges, organizations will need to adopt a security approach that requires digital support and increased collaboration from both IT and security teams. So, what key trends can we expect to see in this new year?
https://www.helpnetsecurity.com/2019/01/11/cio-cybersecurity-trends/

Sizable gap between confidence in security programs and effectiveness
Survey uncovered several challenges and liabilities in security practices that contradict high levels of confidence. https://www.helpnetsecurity.com/2019/01/11/confidence-in-security-programs/

Questions
Contact FIPCO's Ken Shaurette at 800/722-3498 ext. 251 or email FIPCO IT Services for more information.

"Make Security Part of You and Your Institution's DNA!"

Threat Intelligence Newsletter: February 1, 2019

FIPCO® IT Audit Round Table Discussions

If you would like to host an event, please contact: Becky Schowalter

Upcoming Threat Intelligence Peer Group Discussions
None available at the current time

****

Alerts & Warnings

Banking Trojan Sends Spam Attacks Using Your Email Address
If your financial institution was used with DanaBot Trojan as part of its target list, your email address may be causing trouble. Victims who got hooked by the DanaBot lure may have had their email addresses used by hackers to send out email spam to catch other victims. Creators of the DanaBot Trojan recently updated the malware with the ability to gather email addresses from its victims' contacts. This allows them to send countless spam emails to those contacts–including family and friends–using your good name as the sender…
https://www.sosdailynews.com/news.jspx?&articleid=12FA2EDE14343A683E11E64104D8C8D5&sx=79

Trojan malware is back and it's the biggest hacking threat to your business
Old school but effective, hackers are shifting aware from in-your-face ransomware to attacks that are much more subtle. https://www.techrepublic.com/article/trojan-malware-is-back-and-its-the-biggest-hacking-threat-to-your-business/?ftag=TREa988f1c&bhid=78480402

Hackers Use Twitter, Memes, And Hidden Instructions In New Hack
It's the latest and one of the sneakiest social media hacks using Twitter as the conduit. Security researchers recently found a new kind of malware hiding in plain sight. It involves memes sent via Twitter, although the memes themselves aren't infected. They are merely the messengers. It's a roundabout way for hackers to get more information from devices that were already infected with malware sent from the attackers. We know hackers are constantly reinventing themselves and their ways of stealing data.
https://www.sosdailynews.com/news.jspx?&articleid=0713D32DF4BD1F61EEFFC97B5BF359C6&sx=79

Malware Skims Cards At BevMo And Others
Credit and debit card skimming is nothing new to those who follow cybersecurity trends. The most common way we hear it used is with ATM cards. A device is installed on an ATM and as the cardholder inserts the card, information from the magnetic strip and the information entered into the keypad is recorded on the device. Recently, this same technology has been used on retailer sites in a similar way. No hardware is needed, however, and unlike being able to detect a device attached to an ATM, skimming on websites is invisible to the customer…
https://www.sosdailynews.com/news.jspx?&articleid=2DED618EE1CE781D3BAAE6F41A20A962&sx=79

****

Hints & Tips plus Security Awareness

The 'Biggest EVER' Collection of Hacked Passwords Is Not That Bad
If you casually browse tech news today you may come across some scary stuff:
millions and millions of emails and passwords (perhaps even yours!) have been dumped online. Gizmodo called it the "mother of all breaches." Wired said it's a "monster breach." The Daily Mail went with "Biggest EVER collection of breached data." Mashable advised readers to change their password?
https://motherboard.vice.com/en_us/article/evegxw/collection-one-data-breach-password-hack-what-to-do

Hackers impersonate these 10 brands the most in phishing attacks
Phishers often spoof major tech brands in their efforts to gain payments from individuals and businesses, according to a Vade Secure report. https://www.techrepublic.com/article/hackers-impersonate-these-10-brands-the-most-in-phishing-attacks/?ftag=TREa988f1c&bhid=78480402

Trickbot with multiple changes via fake incoming confirmation
Trickbot is back with a vengeance. I have seen a couple of mentions on Twitter earlier this week but haven’t actually been able to find any copies myself. However that all changed last night with several emails to various email addresses on my server. These are targeted at the USA rather than the UK, but I expect the UK targeting to resume very soon. In previous campaigns, I did often see USA appear 1 or 2 days before any UK campaigns. Could this work with any bank name????
https://myonlinesecurity.co.uk/trickbot-with-multiple-changes-via-fake-chase-jp-morgan-incoming-confirmation/

Safeguarding your data from human error and phishing attacks with the cloud
In a world of ransomware attacks, companies should prepare for the worst-case scenario by having smart backup strategies in place to mitigate any potential damage. The public cloud ensures that your information is always backed up and encrypted. Encrypting backup files in the cloud adds an extra layer of protection against unwelcome external parties. This is the third article of a series,
https://www.helpnetsecurity.com/2019/02/01/safeguarding-your-data-from-human-error/
The first article is available at https://www.helpnetsecurity.com/2018/11/30/cybersecurity-hygiene/ and the second one is at https://www.helpnetsecurity.com/2018/12/18/warding-off-security-vulnerabilities/.

In a world of ransomware attacks, companies should prepare for the worst-case scenario by having smart backup strategies in place to mitigate any potential damage. The public cloud ensures that your information is always backed up and encrypted. Encrypting backup files in the cloud adds an extra layer of protection against unwelcome external parties.
https://www.helpnetsecurity.com/2019/02/01/safeguarding-your-data-from-human-error/

****

News & Views

Millions of bank loan and mortgage documents have leaked online
Sheesh. Once again, no password. Why bother hacking when data is left in the open like this? https://techcrunch.com/2019/01/23/financial-files/ The leak gets worse, https://techcrunch.com/2019/01/24/mortgage-loan-leak-gets-worse/.

Should enterprises delay efforts to remediate most vulnerabilities?
Companies today appear to have the resources needed to address all of their high-risk vulnerabilities. The research demonstrates that companies are getting smarter in how they protect themselves from today's cyber threats, improving operational efficiency and resource allocation, while best managing risk. Cybersecurity researchers from Kenna Security and Cyentia Institute analyzed 3 billion vulnerabilities managed across 500+ organizations and 55 sources of external intelligence. They then took a deep dive into the realities of remediation… https://www.helpnetsecurity.com/2019/01/23/delay-patching/

Most out of date applications exposed: Shockwave, VLC and Skype top the list
More than half (55%) of PC applications installed worldwide are out-of-date, making PC users and their personal data vulnerable to security risks. Avast's PC Trends Report 2019 found that users are making themselves vulnerable by not implementing security patches and keeping outdated versions of popular applications on their PCs. The applications where updates are most frequently neglected include Adobe Shockwave (96%), VLC Media Player (94%) and Skype (94%). The report, which uses anonymized and aggregated… https://www.helpnetsecurity.com/2019/01/23/most-out-of-date-applications/

Rushing to patch? Here's how to prioritize your security efforts
When addressing security vulnerabilities, enterprises should focus on those with publicly available exploit code, according to a Kenna Security report. https://www.techrepublic.com/article/rushing-to-patch-heres-how-to-prioritize-your-security-efforts/?ftag=TREa988f1c&bhid=78480402

Hack, Jam, Sense & Shoot: Army Creates 1st Multi-Domain Unit
The U.S. Army has launched its first unit combining long-range targeting, hacking, jamming, and space operations under a single battalion command, bringing together intelligence, information, cyber, electronic warfare, and space (I2CEWS). This first detachment has been designed for counter-China operations, while a second will focus on Europe for counter-Russian operations.
https://breakingdefense.com/2019/01/hack-jam-sense-shoot-army-creates-1st-multi-domain-unit/?utm_source=Sailthru&utm_medium=email&utm_campaign=ebb%2025.01.19&utm_term=Editorial%20-%20Early%20Bird%20Brief

24 million credit and mortgage records exposed on Elasticsearch database

An open Elasticsearch database has again been found this time exposing 24.3 million mortgage and credit reports. https://www.scmagazine.com/home/security-news/data-breach/24-million-credit-and-mortgage-records-exposed-on-elasticsearch-database/?utm_source=newsletter&utm_medium=email&utm_campaign=SCUS_Newswire_20190131&hmSubId=XOjrUhr_Swg1&email_hash=305f40be59a0dcb04476bf06c7e07dc9&mpweb=1325-5370-111266

Digital Forensics Solved a Murder

This mobile forensics case came to us from a nearby local police department in the Summer of 2016. The police department collected an HTC One mobile phone in a homicide investigation in which a 19-year-old girl and her father had been found dead. While it looked like a grisly murder-suicide, the police wanted to completely rule out the presence of a third party. They hoped that the phone found at the scene might hold the information they needed. There was just one problem: the police department's digital forensics lab couldn't get into the phone. Nothing they had tried could bypass or crack the phone's pass code, which kept its contents safe from prying eyes. https://www.gillware.com/digital-forensics/forensic-case-files-htc-one-chip-off/

****

"Ctrl -F" for The Board

Here's What the New U.S. Intelligence Strategy Says About Cyber Threats

The United States intelligence strategy for 2019 has been released, covering seven specific themes. Here's how the United States Intelligence Community will deal with cyber threats: "Despite growing awareness of cyber threats and improving cyber defenses, nearly all information, communication networks, and systems will be at risk for years to…. https://www.oodaloop.com/archive/2019/01/29/heres-what-the-new-u-s-intelligence-strategy-says-about-cyber-threats/

The biggest cybersecurity challenge? Communicating threats internally

IT executives responsible for cybersecurity feel a lack of support from company leaders, and 33 percent feel completely isolated in their role, according to Trend Micro. IT teams are under significant pressure, with some of the challenges cited including prioritizing emerging threats (47 percent) and keeping track of a fractured security environment (43 percent). The survey showed that they are feeling the weight of this responsibility, with many (34 percent) stating that the burden they…
https://www.helpnetsecurity.com/2019/01/30/communicating-threats-internally/

Questions
Contact FIPCO's Ken Shaurette at 800/722-3498 ext. 251 or email FIPCO IT Services for more information.

"Make Security Part of You and Your Institution's DNA!"

Threat Intelligence Newsletter: February 26, 2019

FIPCO®
IT Audit
Round Table
Discussions

If you would like to host an event, please contact: Becky Schowalter

Upcoming Threat Intelligence Peer Group Discussions
None available at the current time

****

Alerts & Warnings

Flaws in Popular RDP Clients Allow Malicious Servers to Reverse Hack PCs
You've always been warned not to share remote access to your computer with any untrusted people for many reasons—it's basic cyber security advice, and common sense, right?
https://thehackernews.com/2019/02/remote-desktop-hacking.html

Trojan malware: The hidden cyber threat to your PC
Trojan malware has evolved into one of the most dangerous malware types. Ignore the threat at your peril.
https://www.zdnet.com/article/trojan-malware-the-hidden-cyber-threat-to-your-pc/?ftag=TRE-03-10aaa6b&bhid=78480402

Phishing Campaign Targets Compliance Officers
A phishing campaign recently targeted anti-money-laundering contacts at banks and credit unions, according to security blogger Brian Krebs. The KrebsOnSecurity post covers the Jan. 30 series of emails that contained malware, addressed contacts by name, and were disguised to look like they came from BSA-AML officers at other financial institutions. The contact information used by fraudsters indicate a possible breach of BSA contact data. https://krebsonsecurity.com/2019/02/phishers-target-anti-money-laundering-officers-at-u-s-credit-unions/

Android WARNING: 'Extremely powerful' malware disguises itself as FAKE Google Play Store
ANDROID fans are being put on alert about an "extremely powerful" piece of malware which disguises itself as a fake Google Play Store app. https://www.express.co.uk/life-style/science-technology/1030707/Android-warning-malware-fake-Google-Play-Store-alert

Your Infant's Identity For Sale On The Dark Web
We never forget about our kids. Right? They are the apples of our eyes, hold the keys to our hearts, and the greatest things since sliced bread, and we always try our best to keep them safe. Don't we? While we are teaching them to safely cross the street, making sure they are fed, clothed, and have roofs over their heads, in this digital world we now live in, there is something else about which we also need to worry…their identities.
https://www.sosdailynews.com/news.jspx?&articleid=B8E9B6520331F4768FAEC704D4A59B77&sx=79

****

Hints & Tips plus Security Awareness

Social Media Gives Hackers Plenty of Ammo
Phishing, smishing and vishing–oh my! All three of these hacking exploits take plenty of cues from social media websites. Information on social media gives hackers the advantage of gleaning personal details about potential victims allowing them to specifically target individuals based on what they've learned about them. Armed with that information, emails, texts, and phone calls are used to pry all kinds of sensitive data from their targets. They use infected attachments, bogus websites, promises of money, threats, and anything else that can motivate a recipient to give up sensitive…
https://www.sosdailynews.com/news.jspx?&articleid=DE75CC03FA255BF01A4574B68B2C2EAA&sx=79

Free Trial Offers That Cost You a Fortune
Have you ever signed up for a product free trial, only to find yourself locked into some sort of payment program you didn't bargain for? https://www.scambusters.org/freetrial.html

Phishing emails imitate North American banks to infect recipients with TrickBot
An spam-based phishing campaign recently targeted North American banking customers with malicious Excel documents designed to infect victims with a new variant of the information-stealing TrickBot banking trojan, researchers reported earlier this week. https://www.scmagazine.com/home/security-news/phishing-emails-imitate-north-american-banks-to-infect-recipients-with-trickbot/?utm_source=newsletter&utm_medium=email&utm_campaign=SCUS_Newswire_20190211&hmSubId=XOjrUhr_Swg1&email_hash=305f40be59a0dcb04476bf06c7e07dc9&mpweb=1325-5652-111266

Smart Home Threats: Securing Your IoT Devices Against Cybercrime and Oversharing
The Internet of Things (IoT) encompasses the billions of devices that are connected to the web all over the world. Smart home devices, like virtual assistants, make our lives more convenient but can also present serious security risks and personal intrusion. With over 7 billion connected IoT devices in use worldwide and growing, there is no better time to secure your home against cybercriminals seeking information that could be used against you or your family, and lock down devices that may be collecting more information than you want to share. https://www.fightingidentitycrimes.com/smart-home-threats/

NIST Cybersecurity Framework: Five years later
Five years after the release of the Framework for Improving Critical Infrastructure Cybersecurity, organizations across all sectors of the economy are creatively deploying this voluntary approach to better management of cybersecurity-related risks. The U.S. Department of Commerce's National Institute of Standards and Technology (NIST) issued what is now widely known simply as the "NIST Cybersecurity Framework" on February 12, 2014. Its development was the result of a year-long collaborative process involving hundreds of organizations and… https://www.nist.gov/news-events/news/2019/02/nist-marks-fifth-anniversary-popular-cybersecurity-framework

****

News & Views

Google Reveals A Big Problem With Passwords On Safer Internet Day
No sooner has Data Privacy Day been and gone, so Safer Internet Day arrives to spread the internet security and privacy education message. Education really is at the heart of Safer Internet Day as it involve… https://www.forbes.com/sites/daveywinder/2019/02/05/google-reveals-a-big-problem-with-passwords-on-safer-internet-day/#3cadc5965e0b

Ransomware Attack Via MSP Locks Customers Out of Systems
Earlier this week, an unidentified threat actor managed to launch a massive ransomware attack resulting in the encryption of between 1,500 to 2,000 endpoint devices belonging to users of a single US managed service provider (MSP). The MSP was subsequently urged to pay a ransom of $2.6 million to have the systems… https://www.darkreading.com/attacks-breaches/ransomware-attack-via-msp-locks-customers-out-of-systems/d/d-id/1333825

Malicious URLs outnumbered attachments in emails 3 to 1 last year
The end of 2018 saw a spike in malicious attachments which businesses need to be wary of, according to a Proofpoint report. https://www.techrepublic.com/article/malicious-urls-outnumbered-attachments-in-emails-3-to-1-last-year/?ftag=TREa988f1c&bhid=78480402

Phone scams remain lucrative, but risks exist: Ex-director of FBI, CIA takes on a phone scammer—and wins
Showcasing some of the common elements of basic phone scams and their surprising successes, a recent case saw a Jamaica-based phone scammer attempt to scam William H. Webster, ex-director of both the FBI and CIA and the only person to have headed both agencies. The case started in 2014 when… https://www.oodaloop.com/briefs/2019/02/14/phone-scams-remain-lucrative-but-risks-exist-ex-director-of-fbi-cia-takes-on-a-phone-scammer-and-wins/

We work to get your money back
The FTC brings lawsuits to stop unfair and deceptive business practices. One way we help right those wrongs is by getting refunds to people who lost money. And from July 2017 to June 2018, people got more than $2.3 billion in refunds from FTC cases. Earlier this week, the FTC released our annual report announcing these results. A new map shows how much money and how many checks the FTC mailed to each state… https://www.consumer.ftc.gov/blog/2019/02/we-work-get-your-money-back?utm_source=govdelivery

****

"Ctrl -F" for The Board

Cyberattacks to watch for in 2019
Consulting company Booz Allen has released a new report outlining eight crucial cyber threats for this year, based on insights from the firm’s top analysts. The research outlines the following threats, while also discussing what companies can do to protect themselves: Information warfare will increasingly target organizations Internet of Things (IoT) devices…
https://www.oodaloop.com/briefs/2019/02/05/cyberattacks-to-watch-for-in-2019/

Governing Cybersecurity Risks - Are you Prepared?
Company boards are recognizing the need for increased independent oversight of cyber risks and managements’ response plans due to increasing exposures. https://www.kralussery.com/ace-files/governing_cybersecurity_risks.pdf

Questions
Contact FIPCO’s Ken Shaurette at 800/722-3498 ext. 251 or email FIPCO IT Services for more information.

"Make Security Part of You and Your Institution's DNA!"

Threat Intelligence Newsletter: March 8, 2019

FIPCO®
IT Audit
Round Table
Discussions

If you would like to host an event, please contact: Becky Schowalter

Upcoming Threat Intelligence Peer Group Discussions
None available at the current time

****

Alerts & Warnings

Security Alert: Malware Hides in Script Injection, Bypassing AV Detection
We all know that cybercriminals never cease to look out for creative methods to launch (more) targeted attacks with a smaller infrastructure to carry out, giving them easy access to users' most valuable data. Security researchers recently observed and analyzed various spam campaigns in which online criminals were trying to infect multiple commercial blogs and insecure Content Management Systems (CMS). https://heimdalsecurity.com/blog/security-alert-malware-script-injection/

Phishing: Don't take the bait
Phishing is when someone uses fake emails or texts – even phone calls – to get you to share valuable personal information, like account numbers, Social Security numbers, or your login IDs and passwords. Scammers use this information to steal your money, your identity, or both. The FTC's new infographic, developed with the American Bankers Association Foundation, offers tips to help you recognize the bait, avoid the hook, and report phishing scams. https://www.consumer.ftc.gov/blog/2019/03/phishing-dont-take-bait?utm_source=govdelivery

Hackers Use Compromised Banks as Starting Points for Phishing Attacks
A new report by Group-IB indicates that cyber attacks on financial institutions can create a domino-effect when threat actors use their foothold on a breached network to infiltrate the systems of connected organizations in other parts of the world. Group-IB has seen various real world instances of these kinds of chain… https://www.bleepingcomputer.com/news/security/hackers-use-compromised-banks-as-starting-points-for-phishing-attacks/

Are Cheap Windows and Office Programs a Scam?
Psst... Looking for cheap Windows or Microsoft Office software? How does a few dollars a pop sound? https://www.scambusters.org/cheapwindows.html

Cybercriminals are Playing Dirty
Online gamers of all ages may not realize the real-life dangers of sharing personal information, leaving them susceptible to vulnerabilities such as fraud, swatting, and identity theft. https://www.fightingidentitycrimes.com/video-game-virtual-vulnerabilities/

Overbiffing: A Wicked Scam That Overcharges People Already in Debt
There's one thing worse than being in debt: Being in debt and not knowing how much you owe -- because then you could become a victim of overbiffing. https://www.scambusters.org/overbiffing.html

****

Hints & Tips plus Security Awareness

Mobile Device Security: Cloud and Hybrid Builds
NIST Cybersecurity Practice Guide SP 1800-4 is now final. The National Institute of Standards and Technology's (NIST's) National Cybersecurity Center of Excellence (NCCoE) security engineers developed an example solution that demonstrates how commercially available technologies can meet your organization's needs to help secure sensitive enterprise data accessed by and/or stored on employees' mobile devices. The example solution can improve security when accessing an organization's sensitive email, contacts, and calendar information from users' mobile devices. These technologies enable users to work inside and outside the corporate network with a security enhanced architecture while minimizing the impact on the user experience. https://www.nccoe.nist.gov/projects/building-blocks/mobile-device-security/cloud-hybrid

Preventing tax identity theft
As if filing your taxes weren't stressful enough, sometimes the process reveals you're a victim of tax identity theft. https://www.trueidentity.com/identity-theft-resource/tax-identity-theft?channel=paid&cid=eml:newstid:tidp:news021819tidmf&utm_source=newstid&utm_medium=email&utm_campaign=news021819tidmf

How to Manage Your Privacy Settings on Social Media
There's a lot of talk in the news about social media privacy and data. The best way you can manage your own privacy is… https://www.experian.com/blogs/ask-experian/how-to-manage-your-privacy-settings-on-social-media/?pc=crm_exp_0&cc=emm_f_m_act_86059_onbeftt_20181025_x_102

It's showtime at the FTC!
Videos from the Federal Trade Commission may not feature a cast of celebrity actors, but they're still entertaining. Produced by the nation's consumer protection agency, these videos offer practical, useful, and memorable messages that can save you money, time, and aggravation. And they're no cost. https://www.consumer.ftc.gov/blog/2019/02/its-showtime-ftc?utm_source=govdelivery

12 Signs Your Identity Might Have Been Stolen
A record 15.4 million Americans were victimized by identity theft last year, with fraudsters netting $16 billion in ill-gotten gains, according to the 2017 Identity Fraud Study by Javelin Strategy & Research. Since 2011, Javelin reports, identity thieves have stolen $107 billion from U.S. consumers. https://www.experian.com/blogs/ask-experian/12-signs-your-identity-might-have-been-stolen/?ty=na&pc=crm_exp_c0003&cc=emm_c_c_act_42985_Blog1_20171218_x_104

About Checking Your Credit Report
When you apply for a new credit card, loan or extension of credit, the potential lender will most likely check your credit report before making a decision. You should too. Check your credit report several weeks or even months prior to making a large credit purchase. https://www.experian.com/blogs/ask-experian/credit-education/report-basics/about-checking-your-credit-report/?ty=na&pc=crm_exp_c0003&cc=emm_c_c_act_42985_Blog1_20171218_x_105

5 ways to avoid top malware threats
Backdoors, cryptomining, fake apps, and banking Trojans increased substantially in the past year, according to McAfee. Here's how to protect your business. https://www.techrepublic.com/article/5-ways-to-avoid-top-malware-threats/?ftag=TREa988f1c&bhid=78480402

Keep your identity safe when filing your taxes
Tax season is already a stressful time for many, and the last thing you need to worry about is tax identity theft. Whether you prepare your own tax returns or hire a professional, learn what you can do to protect yourself. https://www.experian.com/blogs/ask-experian/how-to-file-tax-return-without-getting-burned?ty=mf&pc=crm_exp_0&cc=emm_f_m_act_9991020190226_mktfttFreeCreditRemaining_20190226_x_101&cid=4E5E91F67FAB09C58F189342C8C5C384E825B6B366C5DEE8DC1921BE50E31337

Email Flooding Makes A Comeback With Thousands Of Sent Messages In A Single Blast
Most of us have busy email accounts, especially at work. Clearing an inbox is something we aspire to, but few manage to achieve. Now, imagine opening your work email to find thousands and thousands of emails flooding your inbox... https://www.dugood.org/security-center

****

News & Views

Formjacking is the new get rich quick scheme for cybercriminals
Faced with diminishing returns from ransomware and cryptojacking, cybercriminals are doubling down on alternative methods, such as formjacking, to make money according to Symantec's Internet Security Threat Report (ISTR)… The report analyzes data from Symantec's Global Intelligence Network, which records events from 123 million attack sensors worldwide, blocks 142 million threats daily… https://www.helpnetsecurity.com/2019/02/21/formjacking-get-rich-quick-scheme/

(In)Secure The Magazine – Managing Cyber Risk

- How to know when you're ready for a fractional CISO
- Debunking conventional wisdom to get out of the security and privacy rut
- How accepting that your network will get hacked will help you develop a plan to recover faster
- 5 reasons why asset management is a hot topic in 2019

https://www.helpnetsecurity.com/dl/insecure/INSECURE-Mag-61.pdf

139 US bars, restaurants and coffeeshops infected by credit-card stealing malware
North Country Business Products (NCBP), a provider of point-of-sales systems, has revealed that 139 of their clients have been hit by a malware infection that stole the payment card details of consumers.
https://hotforsecurity.bitdefender.com/blog/139-us-bars-restaurants-and-coffeeshops-infected-by-credit-card-stealing-malware-20871.html#new_tab

The top frauds of 2018
Every year, millions of you tell us – and our partners – about the frauds you spotted. Last year, we heard from 3 million of you, and here's some of what we learned from your reports.
https://www.consumer.ftc.gov/blog/2019/02/top-frauds-2018?utm_source=govdelivery

Microsoft Sees 250% Phishing Increase, Malware Decline by 34%
The 24th volume of Microsoft's Security Intelligence Report shows that phishing surged in 2018. The detected 250% increase in phishing attacks last year confirms similar findings of other recent studies. The research also confirmed that threat actors are moving away from ransomware and malicious software (malware) in general, as malware… https://www.oodaloop.com/briefs/2019/03/05/microsoft-sees-250-phishing-increase-malware-decline-by-34/

****

"Ctrl -F" for The Board

Senior Managers Give Up Credentials To Reschedule Meetings
Attention senior managers, including C-Level executives and board members, and everyone else who attends meetings as a normal part of the day. Researchers at GreatHorn have discovered a phishing attack that specifically targets those in senior level positions, but the reality is that it can apply to anyone and everyone at any time. It involves rescheduling meetings and results in the victims giving up Microsoft Office 365 login credentials and potentially a lot more if you're an executive.
https://www.sosdailynews.com/news.jspx?&articleid=CA1CBF2C07D4BC044B45DFFCB6FAF508&sx=79

3 Top Challenges from the 2019 IT Outlook for Community Banking
For the third consecutive year, we surveyed community banks and credit unions to gain a better understanding of their current IT situation, top IT priorities and challenges, security and compliance issues as well as future technology investments on the horizon. Our third annual report, "2019 IT Outlook for Community Banking," analyzes survey feedback from approximately…
https://www.safesystems.com/blog/2019/02/3-top-challenges-from-the-2019-it-outlook-for-community-banking/?utm_source=hs_email&utm_medium=email&utm_content=70127589

40% of malicious URLs were found on good domains
While tried-and-true attack methods are still going strong, new threats emerge daily, and new vectors are being tested by cybercriminals, according to the 2019 Webroot Threat Report. 40 percent of malicious URLs were found on good domains. Legitimate websites are frequently compromised to host malicious content. To protect users, cybersecurity solutions need URL-level visibility or, when unavailable, domain-level metrics, that accurately represent the dangers. Home user devices are more than twice as likely to get… https://www.helpnetsecurity.com/2019/03/01/malicious-urls-good-domains/

Companies Cautiously Optimistic About Cyber Security
What steps should CISOs and CIOs be taking to ensure a breach doesn't happen at their organizations?
http://docs.media.bitpipe.com/io_12x/io_129069/item_1287903/PYDE%20Survey%20Results.pdf

ABA Foundation, FTC Release Infographic on Phishing Threat
As phishing becomes a top cyber threat—with losses growing to nearly $30 million in 2017 from $8 million in 2015, according to the FBI—ABA and the Federal Trade Commission yesterday released a new infographic highlighting this growing problem... https://www.aba.com/Tools/Infographics/Pages/anti-phishing.aspx?utm_campaign=Newsbytes-20190307&utm_medium=email&utm_source=Eloqua

Questions
Contact FIPCO's Ken Shaurette at 800/722-3498 ext. 251 or email FIPCO IT Services for more information.

"Make Security Part of You and Your Institution's DNA!"

Threat Intelligence Newsletter: March 25, 2019

FIPCO®
IT Audit
Round Table
Discussions

If you would like to host an event, please contact: Becky Schowalter

Upcoming Threat Intelligence Peer Group Discussions
May 15 – Johnston, IA

****

Alerts & Warnings

An Email Marketing Company Left 809 Million Records Exposed Online
Once again, an unsecured database has exposed sensitive data on millions of people and companies This time, "email validation" firm Verifications.io failed to properly secure a MongoDB database containing 809 million marketing-related records. The data included 763 unique email addresses, as well as names, gender, birth dates, phone numbers, physical... https://www.oodaloop.com/briefs/2019/03/08/an-email-marketing-company-left-809-million-records-exposed-online/

Google: Chrome zero-day was used together with a Windows 7 zero-day
Threat actors have been exploiting a recently patched security flaw in Google Chrome by combining the flaw with a vulnerability affecting Windows 7 machines. The combination of vulnerabilities is critical, as it can enable hackers to take over targeted computers. While Windows is working to find a fix for the… https://www.oodaloop.com/briefs/2019/03/08/google-chrome-zero-day-was-used-together-with-a-windows-7-zero-day/

New Tool Gets Around Security Verification
Email phishing has long been the hacker's gold-card of success. One important part of keeping secure is taking additional steps to verify your identity when shopping or banking online, or simply logging in to any online account. One of the most useful tools for an identity check is using 2-Factor Verification (2FA). It's been around a while and is a simple and direct way of taking an additional security precaution–until now. Security researches recently discovered a tool hackers use to get to your of 2FA steps in a way that gives them access to your accounts.
https://www.sosdailynews.com/news.jspx?&articleid=3E1E0F52DEE88B1AAC387B0055C40852&sx=79

Microsoft March Patch Tuesday: 64 Vulnerabilities Patched, 2 Under Attack

As part of Patch Tuesday, Microsoft has released mitigations for 64 security vulnerabilities affecting various products including Microsoft Windows, Microsoft Office, Internet Explorer, Edge and Exchange Server. The patches covered 17 critical flaws and 45 important ones. Two of the vulnerabilities have been actively exploited in the wild. https://www.darkreading.com/threat-intelligence/microsoft-patch-tuesday-64-vulnerabilities-patched-2-under-attack/d/d-id/1334141

US Warns of Sophisticated Cyberattacks From Russia, China

In addition to discussing the US government's new cyber strategy, Department of Defense (DoD) officials on Wednesday elaborated on the growing cyber threat from Russia, China, North Korea and Iran in a hearing of the House Armed Services Subcommittee. According to the officials, the DoD will draw on the positive… https://www.securityweek.com/us-warns-sophisticated-cyberattacks-russia-china

Stolen email credentials being used to pry into cloud accounts

Malicious actors are using the massive supply of previously stolen login credentials to help brute force their way into high-profile cloud-based business systems that cannot easily use two-factor authentication for security. https://www.scmagazine.com/home/email-security/stolen-email-credentials-being-used-to-pry-into-cloud-accounts/?utm_source=newsletter&utm_medium=email&utm_campaign=SCUS_Newswire_20190315&hmSubId=XOjrUhr_Swg1&email_hash=305f40be59a0dcb04476bf06c7e07dc9&mpweb=1325-6506-111266

Scammers Turn to Smishing for ID Theft

Phishing, the scam that involves tricking people into giving away confidential information, is surging via text messaging, posing a greater than ever risk of identity theft. The reason? People trust text messages more than they do email, so they're more likely to fall for the scam.
http://scambusters.org/smishing2.html

Center for Internet Security warns of Trickbot

TrickBot malware targets users financial information and acts as a dropper for other malware and can be leveraged to steal banking information, conduct system and network reconnaissance, harvest credentials and achieve network propagation, according to a security primer released by the Multi-State Information Sharing and Analysis Center (MS-ISAC). https://www.scmagazine.com/home/security-news/the-multi-state-information-sharing-and-analysis-center-ms-isac-released-a-security-primer-on-trickbot-malware/?utm_source=newsletter&utm_medium=email&utm_campaign=SCUS_Newswire_20190319&hmSubId=XOjrUhr_Swg1&email_hash=305f40be59a0dcb04476bf06c7e07dc9&mpweb=1325-6589-111266

Troldesh ransomware emergency kit is available

Businesses are currently being targeted with Troldesh, a ransomware of Russian origin known for adding clever extensions (e.g. .better_call_saul and .heisenberg) to encrypted files.
https://malwarebytes.lookbookhq.com/0319-threat-spotlight-troldesh-na?aliId=eyJpIjoidE16ZkZDekdhOHBENWlsdCIsInQiOiI0TGFLN0E2OU4reTExXC85RXB0KzFJUT09In0%253D

Those (not really) IRS calls

You've probably gotten one of these calls: They say it's the IRS and they're filing a lawsuit against you for back taxes. They may threaten to arrest or deport you. What do you do? Watch this video to learn more:
https://www.consumer.ftc.gov/blog/2019/03/those-not-really-irs-calls?utm_source=govdelivery

****

Hints & Tips plus Security Awareness

What is smishing?
Cybercriminals have created various methods to trick people into downloading viruses or malware onto their laptops, tablets and smartphones. The latest form is smishing. Keep reading to learn more. https://www.experian.com/blogs/ask-experian/what-is-smishing/?ty=mfcor&mkid=C2034F8C-0D2A-5953-9EC0-1DC8471BE72F&pc=crm_exp_0&cc=emm_f_m_act_9890120190312_fttctatm_20190312_x_102

7 emerging data security and risk management trends
Risk appetite statements, governance frameworks and password-less authentication are among the growing trends that will impact security, privacy and risk leaders. https://www.information-management.com/list/7-emerging-data-security-and-risk-management-trends?utm_source=audiencedev&utm_medium=email&utm_content=reengage&utm_campaign=SailthruReengage

Hacker returns and puts 26Mil user records for sale on the Dark Web
A threat actor using the moniker 'Gnosticplayers' has once again uploaded a database containing millions of records to a popular dark web marketplace. Last month, Gnosticplayers put three massive data collections affecting hundreds of millions of users up for sale and promised that more stolen records would be coming soon. https://www.zdnet.com/article/round-4-hacker-returns-and-puts-26mil-user-records-for-sale-on-the-dark-web/

Current phishing defense strategies and execution are not hitting the mark
Few professionals are completely confident in their ability to assess the effectiveness of their phishing awareness efforts. In a new paper, Phishing Defense and Governance, released in partnership with Terranova Security, ISACA outlines key takeaways from this phishing research that reached security, assurance, risk and governance professionals, including: Only a slight majority (63 percent) regularly monitor and report on the effectiveness of their activities. 38 percent of respondents reported that their organizations develop security awareness… https://www.helpnetsecurity.com/2019/03/18/phishing-defense-strategies/

Spring Cleaning for Your Small Business Part 2 of 3: Mobile Device Security Mobile Threats Targeting Your Small Business
Computers aren't the only devices that are at risk for security breaches. Small to midsized business (SMB) owners must be prepared to protect their companies from cyberattacks that target mobile devices, too. With more than 80% of employees using their personal phones, laptops, and tablets for business, the now standard practice of Bring Your Own Device (BYOD) has significantly increased the number of threats to data security. https://www.fightingidentitycrimes.com/spring-cleaning-for-your-small-business-part-2-of-3-mobile-device-security/

Patch Management Best Practices - What is Patch Management?
Patch management is the practice of reviewing, understanding, testing, deploying, and reconciling the deployment state for software product updates. The goal of the updates is to correct problems, close vulnerabilities, and improve product functionality, which is essential to the stability of an IT infrastructure in most environments. By understanding the different kinds of patches and following best practices, an IT service provider can keep client's critical systems free from known vulnerabilities.
https://creatives.techrepublic.com/whitepapers/PatchManagementBestPractices.pdf

****

News & Views

Cybersecurity and Regulatory Changes in 2019
Although financial services companies have been required to abide by cybersecurity laws for many years, such as the SEC’s Identity Theft Red Flag Rule and the Security Rule of the Gramm-Leach-Bliley Act, the developing cybersecurity regulatory landscape is continuing to gain momentum as the number of industries impacted increases.
https://misti.com/internal-audit-insights/cybersecurity-and-regulatory-changes-in-2019?utm_term=Cybersecurity%20and%20Regulatory%20Changes%20in%202019&utm_campaign=AR19-0312&utm_content=email&utm_source=Act-On+Software&utm_medium=email&cm_mmc=Act-On%20Software-_-email-_-The%20Many%20Benefits%20of%20Rotation%20Programs-_-Cybersecurity%20and%20Regulatory%20Changes%20in%202019

10 popular malware campaigns your business should avoid
Coinhive is at the top of the global threat index for the 15th consecutive month.
https://www.techrepublic.com/article/10-popular-malware-campaigns-your-business-should-avoid/?ftag=TREa988f1c&bhid=78480402

Point of sale malware campaign targets hospitality and entertainment businesses
Cybercriminals are targeting small and mid-sized businesses (SMBs) that process a lot of card payments with point-of-sale (POS) malware in order to steal customers’ payment card information, researchers with Flashpoint have found. The malware used in the campaign that mostly targets the hospitality and entertainment industries is dubbed DMSniff. https://www.zdnet.com/article/point-of-sale-malware-campaign-targets-hospitality-and-entertainment-businesses/

Researchers catch whiff of previously unknown POS sniffers and scrapers
3/15, Researchers in the last 48 hours have released a trio of reports, each of which details a newly discovered point-of-sale (POS) malware program that skims or scrapes payment card information from e-commerce websites or in-store checkout terminals. At least two of these three new threats, GMO and DMSniff, have already been observed actively attacking enterprises, while the third, GlitchPOS, has been spotted for sale on multiple dark web forums. https://www.scmagazine.com/home/security-news/researchers-catch-whiff-of-previously-unknown-pos-sniffers-and-scrapers/?utm_source=newsletter&utm_medium=email&utm_campaign=SCUS_Newswire_20190315&hmSubId=XOjrUhr_Swg1&email_hash=305f40be59a0dcb04476bf06c7e07dc9&mpweb=1325-6506-111266

****

"Ctrl -F" for The Board

Debunking Cybersecurity Myths: Part IV—No Target Too Small
Myth #4—Cyber Risk Is a "Big Business" Problem; It's easy to see how this myth developed. After all, when a data breach makes the news it's because it's victimized a large organization like Target or Equifax or Yahoo. You'll never wake up to a news alert on your phone that reads BREAKING NEWS: CORNER DELI HIT WITH RANSOMWARE! https://arcticwolf.com/blog/debunking-cybersecurity-myths-part-iv-no-target-too-small/?utm_source=arcticwolf&utm_medium=nurture&mkt_tok=eyJpIjoiT0RKbU5ERTRNV1F3TTJabSIsInQiOiJOeDc1TzVaaVRcL0lZN0MxSUwwSUFaN3FjTDZFT1dwOTNVMFowUkVLcFFuTmhiRGs0TkVPbm16cHRXWUhCQVVxeHdmQlFuTmhsN3d2N3ZFelljZm5CckpwS0RSZ2Z6UlZtU1lhNlZnemUzMWNuWW5CRmVTOUk3bGtMdzVHSXlpMFoifQ%3D%3D

Questions
Contact FIPCO's Ken Shaurette at 800/722-3498 ext. 251 or email FIPCO IT Services for more information.

"Make Security Part of You and Your Institution's DNA!"

Threat Intelligence Newsletter: April 8, 2019

FIPCO®
IT Audit
Round Table
Discussions

If you would like to host an event, please contact: Becky Schowalter

Upcoming Threat Intelligence Peer Group Discussions
May 15 – Johnston, IA

****

Alerts & Warnings

Spot this New Twist on a Tech Support Scam
Scammers have been duping consumers with a tech support scam that claims your IP address has been compromised. BBB is seeing an increasing number of these cons reported to BBB.org/ScamTracker. There are two versions of this scam you should be ready to spot. https://www.bbb.org/article/news-releases/16553-bbb-tip-tech-support-scams

VMware ESXi, Workstation and Fusion updates address multiple issues
VMware ESXi, Workstation and Fusion out-of-bounds vulnerabilities.
https://www.vmware.com/security/advisories.html

Hundreds of compromised WordPress and Joomla websites
Researchers with Zscaler warn that threat actors are increasingly trying to take advantage of flaws in the immensely popular content management systems (CMSs) WordPress and Joomla in order to get legitimate websites to target users with malicious payloads. In the past month, the researchers detected thousands of attacks, hundreds of... https://www.zdnet.com/article/hundreds-of-compromised-wordpress-and-joomla-websites-are-serving-up-malware-to-visitors/

FTC Proposes to Add Detailed Cybersecurity Requirements to the GLBA Safeguards Rule
On March 5, 2019 the Federal Trade Commission ("FTC") published requests for comment on proposed amendments to two key rules under the Gramm-Leach-Bliley Act ("GLBA").
https://www.ftc.gov/system/files/documents/federal_register_notices/2019/03/p145407_safeguards_rule_fr_notice.pdf. Most significantly, the FTC is proposing to add more detailed requirements to the Safeguards Rule, which governs the information security programs financial institutions must implement to protect customer data. https://www.insideprivacy.com/financial-privacy/ftc-proposes-to-add-detailed-cybersecurity-requirements-to-the-glba-safeguards-rule/

Over 58,000 Android users had stalkerware installed
A new report by Kaspersky Lab highlights the rise of ‘stalkerware’, which is a type of spyware offered by legitimate firms for supposedly benign aims like monitoring children or employees. However, many stalkerware apps do not indicate to users that they are being monitored, even though legitimate solutions should do… https://www.zdnet.com/article/over-58000-android-users-had-stalkerware-installed-on-their-phones-last-year/

****

Hints & Tips plus Security Awareness

Unmasked: What 10 million passwords reveal
A lot is known about passwords. Most are short, simple, and pretty easy to crack. But much less is known about the psychological reasons a person chooses a specific password. We’ve analyzed the password choices of 10 million people, from CEOs to scientists, to find out what they reveal about the things we consider easy to remember and hard to guess. https://wpengine.com/unmasked/

What to do about robocalls
Not another robocall! We’ve all felt that way. Wondering what to do about robocalls? Check out this new video. https://www.consumer.ftc.gov/blog/2019/03/what-do-about-robocalls?utm_source=govdelivery

NIST Usable Cybersecurity
The National Institute of Standards and Technology (NIST) Usable Cybersecurity team brings together experts in diverse disciplines to work on projects aimed at understanding and improving the usability of cybersecurity software, hardware, systems, and processes. Our goal is to provide actionable guidance for policymakers, system engineers and security professionals so that they can make better decisions that enhance the usability of cybersecurity in their organizations. https://csrc.nist.gov/projects/usable-cybersecurity

Is it safe to use Facebook to login on other sites?
Using social-media login credentials to sign into third-party sites can save time and hassle.
But it could also compromise your personal data. https://www.experian.com/blogs/ask-experian/is-it-safe-to-use-facebook-to-login-on-other-sites/?ty=mfcor&mkid=C2034F8C-0D2A-5953-9EC0-1DC8471BE72F&pc=crm_exp_0&cc=emm_f_m_act_9890120190326_fttctatm_20190326_x_102

Emergency Preparedness and Response
Crisis and emergency communication resources… https://emergency.cdc.gov/cerc/index.asp

10 Best Password Manager of 2019
Get the best in security and convenience from our list of the best password managers available on the market today. https://www.consumersadvocate.org/password-manager/a/best-password-manager?pd=true&keyword=password&gca_campaignid=958851270&gca_adgroupid=50782975143&gca_matchtype=p&gca_network=g&gca_device=c&gca_adposition=1t3&gca_loc_interest_ms=&gca_loc_physical_ms=9019312&&pd=true&keyword=password&gca_campaignid=958851270&gca_adgroupid=50782975143&gca_matchtype=p&gca_network=g&gca_device=c&gca_adposition=1t3&gca_loc_interest_ms=&gca_loc_physical_ms=9019312&gclid=Cj0KCQjw7YblBRDFARIsAKkK-dKT5OBB_c42abPVcBTn5S63qIfxVXpVRlY7kfBybLxyBtR2Z1FR_IlaApW_EALw_wcB

How companies are dealing with the security threats of an evolving remote workforce
Multi-factor authentication is a common strategy, while Zero Trust is gaining traction, according to an Okta report. https://www.techrepublic.com/article/how-companies-are-dealing-with-the-security-threats-of-an-evolving-workforce/?ftag=TREa988f1c&bhid=78480402

****

News & Views

8 Million+ Records Exposed in Massive Data Theft
It's not looking good for the public at large in terms of data theft. With a shocking 12,449 more incidents since last year, that translates to a 424% increase in just one year. The latest massive data breach of a data marketing firm exposed roughly 800 million records belonging to U.S. citizens who had no idea their…personally identifiable information (PII) of victims included email addresses, dates of birth, street addresses, phone numbers, and much, much more been…
https://www.sosdailynews.com/news.jspx?&articleid=F91159166C39F52CEA8F3ACE4A75DDF6&sx=79

Global police arrest dozens of people in dark web sting
A collaborate effort by 60 law enforcement experts from the US, Canada as well as 17 European countries and the European organizations Eurojust and Europol, has resulted in the arrests of 61 people believed to have been involved in the exchange of illicit goods and services on dark web market…
https://www.welivesecurity.com/2019/03/27/global-police-arrest-dark-web-sting/

Microsoft takes control of 99 domains operated by Iranian state hackers
Microsoft has confiscated 99 web domains that were used by Iran-linked hackers to launch global spear-phishing campaigns. The domain names resembled those of popular services offered by Microsoft, Yahoo and other companies and could therefore easily be mistaken for legitimate websites by victims of the campaign. The threat actor behind… https://www.zdnet.com/article/microsoft-takes-control-of-99-domains-operated-by-iranian-state-hackers/

Casino Screwup Royale: A tale of "ethical hacking" gone awry
People who find security vulnerabilities commonly run into difficulties when reporting them to the responsible company. But it's less common for such situations to turn into tense trade-show confrontations and competing claims of assault and blackmail. Yet that's what happened when executives at Atrient -- a casino technology firm headquartered in West Bloomfield, Michigan -- stopped responding to two UK-based security researchers who had reported some alleged security flaws.
https://arstechnica.com/information-technology/2019/03/50-shades-of-greyhat-a-study-in-how-not-to-handle-security-disclosures/

Cybersecurity is broken: Here's how we start to fix it
We are building our future on a creaking digital foundation. It's time for that to change.
https://www.zdnet.com/article/cybersecurity-is-broken-heres-how-we-start-to-fix-it/?ftag=TRE-03-10aaa6b&bhid=78480402

Government urges businesses and charities to up cybersecurity
The proportion of UK organizations being hit by cyber attacks and data breaches has dropped in the past year, official statistics show, but government says there is more work to be done and industry experts suggest this should focus on cyber resilience.
https://www.computerweekly.com/news/252461013/Government-urges-businesses-and-charities-to-up-cyber-security

****

"Ctrl -F" for The Board

Addressing the Cyber Threat
Director Discusses FBI Approach at Cybersecurity Conference https://www.fbi.gov/news/stories/director-wray-speaks-at-rsa-cybersecurity-conference-030619

Questions
Contact FIPCO's Ken Shaurette at 800/722-3498 ext. 251 or email FIPCO IT Services for more information.

"Make Security Part of You and Your Institution's DNA!"

Threat Intelligence Newsletter: April 22, 2019

FIPCO®
IT Audit
Round Table
Discussions

If you would like to host an event, please contact: Becky Schowalter

Upcoming Threat Intelligence Peer Group Discussions
May 15 – Johnston, IA

Time Sensitive:

Second Annual Event... CYBER RISK, TRENDS, PREDICTIONS
The mission of the Marquette University Center for Cyber Security Awareness and Cyber Defense includes providing cybersecurity knowledge to the community and the university. To inform the community and the university about current cyber risks and defenses we are hosting the 2nd annual CYBER RISK, TRENDS, PREDICTIONS. https://www.eventbrite.com/e/cyber-risks-trends-predictions-2019-tickets-59949614912?aff=ebdssbdestsearch

****

Alerts & Warnings

Half of online banks allow hackers to steal your money
Recent research indicates that financial institutions are tragically falling short in their responsibility to provide customers with secure solutions for online banking and other digital financial services. While a recent study by Aite Group and Arxan Technologies found major security shortcomings in financial apps, Positive Technologies last week released… https://www.techrepublic.com/article/half-of-online-banks-allow-hackers-to-steal-your-money/

Ask a health professional before popping that pill
When I was young, I wanted the shoes that would make me run faster and jump higher. Now, I wish my brain would run a little faster when I can't remember my account passwords. Unfortunately, some shady outfits have been trying to "help" people like me by making some mind-blowing claims to sell their dietary supplements... https://www.consumer.ftc.gov/blog/2019/04/ask-health-professional-popping-pill?utm_source=govdelivery

Banking Trojan Back With A Vengeance And Sneakier Than Ever!
Since 2007, the highly successful banking Trojan called Ursnif has been making waves. Once found in the popular Gozi banking Trojan, Ursnif has been around in one form or another for over ten years. Researchers recently noticed that over time and with the help of hackers, Ursnif has reinvented itself bigger and sneakier than ever before. This latest version focuses on Microsoft Outlook, Internet Explorer, and Mozilla Thunderbird users and employs new functionality.
https://www.sosdailynews.com/news.jspx?&articleid=4D0C4EAB8AD535FC5C81C87ED6CB6722&sx=79

Your hotel check-in confirmation could be putting you at risk
When your hotel automatically emails you your booking information, there's a good chance that you're not the only person with access to those documents. Symantec, a security company, found flaws on hundreds of hotel websites, which were leaking sensitive information like names, phone numbers, passport numbers and addresses in confirmation emails. Candid Wueest, a threat researcher at Symantec, said he looked at more than 1,500 hotel websites in 54 countries and found the issues among two-thirds of them.
https://www.cnet.com/news/your-hotel-check-in-confirmation-could-be-putting-you-at-risk/

VMware ESXi, Workstation and Fusion multiple vulnerabilities
VMSA-2019-0006 - VMware ESXi, Workstation and Fusion updates address multiple out-of-bounds read vulnerabilities. https://www.vmware.com/security/advisories/VMSA-2019-0006.html

Microsoft web mail services breached
Support agent's credentials are compromised. Hackers reportedly compromised a Microsoft Corp. support agent's credentials, allowing them to gain unauthorized access to the company's various web-based email services, including Outlook, MSN and Hotmail, for at least three months in 2019.
https://www.scmagazine.com/home/security-news/microsoft-web-mail-services-breached-after-support-agents-credentials-are-compromised/?utm_source=newsletter&utm_medium=email&utm_campaign=SCUS_Newswire_20190416&hmSubId=XOjrUhr_Swg1&email_hash=305f40be59a0dcb04476bf06c7e07dc9&mpweb=1325-7263-111266

Not So Good Stuff Heading Our Way On Android
It's not good stuff, it's Gustuff. It's the latest in the Android banking Trojan news and it is full of the bad stuff. This one, according to researchers is joining, if not surpassing the old stand-bys that hold the top spots now including Red Alert, LokiBot, and BankBot. All are pretty serious threats, and all are out to get credentials, but Gustuff holds a unique trick in its pocket to ensure it makes the most out of its efforts. Fortunately, it isn't in the Google Play Store... yet.
https://www.sosdailynews.com/news.jspx?&articleid=4875264C4AD0A4267587C418B6C1257E&sx=79

SSA imposters top IRS in consumer loss reports
Have you gotten calls about supposed problems with your Social Security number from callers pretending they're with the Social Security Administration (SSA)? If so, you're not alone. Our latest Data Spotlight finds that reports about SSA imposters are surging, while reports about IRS imposters have taken a dive.
https://www.consumer.ftc.gov/blog/2019/04/ssa-imposters-top-irs-consumer-loss-reports?utm_source=govdelivery

Threat actors gaining admin rights before ransomware infections
Threat actors are using accounts with admin privileges to install BitPaymer ransomware via PsExec suggesting threat actors are taking a more targeted approach to their distribution of malware. https://www.scmagazine.com/home/security-news/threat-actors-are-taking-a-more-targeted-approach-to-their-distribution-of-malware-gaining-admin-privileges-and-using-custom-notes-with-ransomware/?utm_source=newsletter&utm_medium=email&utm_campaign=SCUS_Newswire_20190416&hmSubId=XOjrUhr_Swg1&email_hash=305f40be59a0dcb04476bf06c7e07dc9&mpweb=1325-7263-111266

Scammers Hide Behind Padlock Security Symbol to Trick Victims
Bad news. For years, we've been advising readers to check for a padlock in their browser address bar as a sign of a website's security. But no more. http://scambusters.org/padlock.html

Adblock Plus Exploit allows threat actors to read Gmail and other Google services
Independent security researcher Armin Sebastian discovered a vulnerability in Adblock Plus which can allow hackers to read a victim's Gmail and look into other Google services. https://www.scmagazine.com/home/security-news/vulnerabilities/independent-security-researcher-armin-sebastian-discovered-a-vulnerability-in-adblock-plus-which-can-allow-hackers-to-read-a-victims-gmail/?utm_source=newsletter&utm_medium=email&utm_campaign=SCUS_Newswire_20190419&hmSubId=XOjrUhr_Swg1&email_hash=305f40be59a0dcb04476bf06c7e07dc9&mpweb=1325-7283-111266

****

Hints & Tips plus Security Awareness

77% of orgs lack a cybersecurity incident response plan
A new study by IBM Security and the Ponemon Institute exposes major shortcomings in cyber resilience among organizations. The report found that more than 3 out of 4 (77%) companies lack a properly and consistently implemented cybersecurity incident response strategy. A majority of firms (54%) do not regularly test their... https://www.helpnetsecurity.com/2019/04/12/cybersecurity-incident-response-plan/
Resources are available to help: https://www.fipco.com/solutions/it-audit-security/cyber-security-resources-links

Refund Denied: What to Do if You're a Victim of Tax Fraud
Now that April 15th has come and gone, it's still critical for you to stay vigilant and to keep a watchful eye for any suspicious activity that may signal tax fraud. Fraudsters have been busy, and may have already been working behind the scenes to steal your refund. The 2018 Consumer Sentinel Network Data Book classifies tax fraud as one of the top three reported types of identity theft submitted to the Federal Trade Commission… https://www.fightingidentitycrimes.com/refund-denied-what-to-do-if-youre-a-victim-of-tax-fraud/

****

News & Views

Nine in 10 CNI Providers Damaged by Cyber-Attacks
A new report by the Ponemon Institute and Tenable highlights the growing cyber threat to critical infrastructure. The survey found that a whopping 90% of critical infrastructure providers suffered a cyberattack resulting in a data breach and/or downtime in the last two years, while 62% experienced multiple attacks. About 1… https://www.infosecurity-magazine.com/news/nine-10-cni-providers-hit-damaging-1/

What is the Dark Web, and why is it so bad if your information is there?
Emily Wilson, vice president of research at Terbium Labs, discusses why consumers and professionals should be concerned if their data is leaked on the Dark Web. https://www.techrepublic.com/article/what-is-the-dark-web-and-why-is-it-so-bad-if-your-information-is-there/?ftag=TREa988f1c&bhid=78480402

Why IT pros fear employee error, not hackers, will cause the most breaches
Security analytics firm Gurucul has released a new report on the growing insider threat to organizations. The survey that was conducted among over 650 IT professionals from various countries indicates that nearly 3 out of 4 organizations are vulnerable to insider threats. Companies consider the biggest insider threats to be... https://www.techrepublic.com/article/why-it-pros-fear-employee-error-not-hackers-will-cause-the-most-breaches/

Why Ransomware Continues to Be an Immensely Profitable Business for Bad Actors
Ransomware, arguably the most efficient malware used by cybercrooks in recent years, continues to wreak havoc on a global scale, affecting everyone and everything, from regular Internet users to enterprises to critical infrastructures. So why do hackers still win? https://businessinsights.bitdefender.com/why-ransomware-continues-to-be-an-immensely-profitable-business-for-bad-actors?utm_campaign=Weekly%20blog%20notifications&utm_source=hs_email&utm_medium=email&utm_content=71803630&_hsenc=p2ANqtz-_PbYWsz_VgC2C9SdbyniqEOvoGZY_BfO1JMklolVmJGjj_YQO7QSsV318m3NavLW5nwREp97VHtTzZH9xmi_tzumjbTw&_hsmi=71803630

Student used 'USB Killer' device to destroy $58, 000 worth of college computers
Could this happen at your institution? A former student of The College of Saint Rose in Albany, New York, has pled guilty to charges that he destroyed tens of thousands of dollars worth of campus computers using a USB device designed to instantly overwhelm and fry their circuitry. The plea was announced Tuesday by the Department of Justice, FBI, and Albany Police Department.
https://www.theverge.com/2019/4/17/18412427/college-saint-rose-student-guilty-usb-killer-destroyed-computers

****

"Ctrl -F" for The Board

Addressing the Cyber Threat
Director Discusses FBI Approach at Cybersecurity Conference https://www.fbi.gov/news/stories/director-wray-speaks-at-rsa-cybersecurity-conference-030619

How to improve cybersecurity for your business: 6 tips
Business cyber risks rates are holding steady for US companies, according to the US Chamber of Commerce and FICO. Here's how to stay safe. https://www.techrepublic.com/article/how-to-improve-cybersecurity-for-your-business-6-tips/?ftag=TREa988f1c&bhid=78480402

Questions
Contact FIPCO's Ken Shaurette at 800/722-3498 ext. 251 or email FIPCO IT Services for more information.

"Make Security Part of You and Your Institution's DNA!"

Threat Intelligence Newsletter: May 7, 2019

FIPCO®
IT Audit
Round Table
Discussions

If you would like to host an event, please contact: Becky Schowalter

Upcoming Threat Intelligence Peer Group Discussions
May 15 – Johnston, IA

****

Alerts & Warnings

Fake Giveaways, Jobs, Followers and More Among Latest Instagram Scams
It's just a coincidence that the name of the photo-sharing social media site Instagram rhymes with "scam" but the link https://scambusters.org/instagramscam.html is certainly appropriate. https://scambusters.org/instagram2.html

Don't Get Caught in a SMiShing Scam - Tripwire
The word SMiShing may sound like gibberish — we think it's a weird one — but... by tapping on a link and entering your information into a look-alike website. While cyber scams and identity theft attacks are one of the fastest... https://www.tripwire.com/state-of-security/security-awareness/caught-smishing-scam/

Scam Alert: Medical Equipment Scam Targets Seniors
Seniors are less likely to fall for scams overall, according to the BBB Scam Tracker Risk Report (BBB.org/RiskReport). But here is one scam that's aimed right at seniors: free medical equipment. The Better Business Bureau is hearing from consumers – more than 200 since the first of the year – who have been targeted by scammers for "free" back braces. https://www.bbb.org/article/news-releases/16916-bbb-tip-healthcare-scams

Disruptions from cyber attacks increasing, taking longer to fix
Cyber attack disruptions are increasing, and it's taking organizations longer to fix the underlying issues, according to a new report. https://www.information-management.com/news/disruptions-from-cyber-attacks-increasing-taking-longer-to-fix?utm_campaign=security%20briefing-apr%2030%202019&utm_medium=email&utm_source=newsletter&eid=305f40be59a0dcb04476bf06c7e07dc9

Return to Sender: A Technical Analysis of a Paypal Phishing Scam
Everyone gets phishing emails, but who knows how they actually work? This technical breakdown takes a look under the hood of one phishing email method to see what is really going on.
https://www.sentinelone.com/blog/technical-analysis-paypal-phishing-scam/?utm_campaign=Newsletter&utm_source=hs_email&utm_medium=email&utm_content=72237986&_hsenc=p2ANqtz-_Wo5VcbypsnrkZCKOmG1dqURxdfWVV1P62mWt9puAYl_bpveFfKPHvAEqiZmgKqX7KVfCtyCMpkgHH9eqXYO3UbNho7A&_hsmi=72237986

Mystery Data Breach Exposes 80 Million U.S. Households
The 24GB folder was discovered unprotected on a Microsoft cloud servicer — meaning that anyone who knew where to look could access and steal the data within. Microsoft has since taken the database offline, but these records had been available since February 2019 and the damage may have already been done.
https://www.fightingidentitycrimes.com/mystery-data-breach-exposes-80-million/

Encrypted Email Clients Vulnerable to Signature Spoofing:
After testing more than two dozen popular encrypted email clients, researchers found that the majority are vulnerable to one or more signature spoofing attacks… https://www.securityweek.com/majority-encrypted-email-clients-vulnerable-signature-spoofing

Crooks Learn How to Clone Latest Chipcards
One of the great things we were told about the replacement of magnetic strips with smart chips (chipcards) on our debit and credit cards was that it would significantly improve security.
http://scambusters.org/chipcards2.html

Malware from illegal video streaming apps: What to know
The popularity of video streaming services has taken off in the past few years. It's become easier to stream video through smart TVs, streaming boxes that connect to your not-so-smart TV, and even streaming sticks. These devices let you stream video through popular apps like Hulu, Netflix, SlingTV, Amazon Prime Video, and YouTube TV. Unfortunately, there are other apps that let you watch illegal pirated content. And hackers are using those apps to spread malware. Here's what you need to know.
https://www.consumer.ftc.gov/blog/2019/05/malware-illegal-video-streaming-apps-what-know?utm_source=govdelivery

Consumers Pay Shipping for Nonexistent "Free" Products
For years now, scammers have been tricking consumers out of their money using "free trial" scams. Recently, consumers have been reporting a new twist on this scam on the BBB.org/ScamTracker, one that involves offering consumers a variety of products at no charge. https://www.bbb.org/article/tips/14040-bbb-tip-smart-shopping-online

****

Hints & Tips plus Security Awareness

Identity Theft vs. Identity Fraud: What's the Difference?
Thousands fall victim to identity theft and identity fraud each year. However, few know the difference between the two. While they may seem similar, identity theft and identity fraud are two different crimes that have different effects on your finances and credit depending on their severity. Understanding these differences may help you better protect yourself and prepare you to fight back...
https://www.trueidentity.com/identity-theft-resource/identity-theft-vs-identity-fraud?channel=paid&cid=eml:newstid:tidp:news042219tidmf&utm_source=newstid&utm_medium=email&utm_campaign=news042219tidmf

COPPA: A few tips to keep your child safe online
Online games and websites for kids are everywhere these days – to the point that it's commonplace to see toddlers playing with them, too. And while the internet has positive ways for kids to explore and learn, privacy concerns are lurking. To help protect children's privacy, the FTC enforces the Children's Online Privacy Protection Act (COPPA), which requires websites and online services to get consent from parents before collecting personal information from kids younger than 13…
https://www.consumer.ftc.gov/blog/2019/04/coppa-few-tips-keep-your-child-safe-online?utm_source=govdelivery

How to Avoid Getting Insta-Scammed on Instagram
When cruising the gram for cute dog pics and great looks, make sure you watch out for stock photos or questionable giveaways—and never give out your personal info or location data.
https://www.opploans.com/blog/how-to-avoid-getting-insta-scammed-on-instagram/

****

News & Views

Nearly half of firms suffer data breaches at hands of vendors
Almost one in two (44%) companies has experienced a disruptive data breach as the result of a third-party vendor getting compromised, recent research by eSentire and Spiceworks shows. 26% of the breaches were the result of human error and stolen passwords, while about half involved malware. Even though third-party agreements… https://www.oodaloop.com/briefs/2019/04/24/nearly-half-of-firms-suffer-data-breaches-at-hands-of-vendors/

Hackers Had Access to Citrix Network for Five Months
Citrix said hackers had access to its network for five months and they may have stolen names, SSNs and financial information relating to current and former employees. https://www.securityweek.com/hackers-had-access-citrix-network-five-months

Microsoft Knows Password-Expiration Policies are Useless
Microsoft isn't doing away with its password-expiration policies across the board, but the blog post makes the company's stance clear: expiring passwords does little good.
https://www.engadget.com/2019/04/24/microsoft-password-expiration-security/

Fake Followers; Real Problems
Fake followers and fake likes have spread throughout social media in recent years. Social media platforms such as Facebook and Instagram have announced that they are cracking down on so-called “inauthentic activity,” but the practice remains prevalent. For brands advertising on social media, paying for fake followers and likes is… https://www.natlawreview.com/article/fake-followers-real-problems?utm_content=864d04010b852c515354968356c7f23d&utm_campaign=5-1-2019Cybersecurity%20Legal%20News&utm_source=Robly.com&utm_medium=email

A Hacker or Your Cloud Provider. Who Presents the Greatest Risk to Your Data?
It’s your worst nightmare. All of your most important and sensitive data, the thing your business values most, the thing your company cannot operate without, the thing your regulators require you to protect, has been taken hostage. Your business grinds to a halt. Your customers and business partners are livid. Your regulators are demanding an explanation as to how something like this could happen.
https://www.natlawreview.com/article/hacker-or-your-cloud-provider-who-presents-greatest-risk-to-your-data?utm_content=864d04010b852c515354968356c7f23d&utm_campaign=5-1-2019Cybersecurity%20Legal%20News&utm_source=Robly.com&utm_medium=email

****

"Ctrl -F" for The Board

Just Released: Discussion Draft of the NIST Privacy Framework
Just released a discussion draft of the NIST Privacy Framework: An Enterprise Risk Management Tool! The discussion draft reflects stakeholder input we’ve received throughout the development process. Now, we want your feedback: check out the discussion draft and related documents here: https://www.nist.gov/privacy-framework/working-drafts.

Questions
Contact FIPCO’s Ken Shaurette at 800/722-3498 ext. 251 or email FIPCO IT Services for more information.

"Make Security Part of You and Your Institution's DNA!"

Threat Intelligence Newsletter: May 22, 2019

FIPCO®
IT Audit
Round Table
Discussions

If you would like to host an event, please contact: Becky Schowalter

Upcoming Threat Intelligence Peer Group Discussions
June 27 – New Berlin (registration coming soon)

****

Alerts & Warnings

AR19-133A: Microsoft Office 365 Security Observations
As the number of organizations migrating email services to Microsoft Office 365 (O365) and other cloud services increases, the use of third-party companies that move organizations to the cloud is also increasing. Organizations and their third-party partners need to be aware of the risks involved in transitioning to O365 and other cloud services. https://www.us-cert.gov/ncas/analysis-reports/AR19-133A

'Mirrorthief' card-skimming attack steals card data from online college stores
A total of 201 online college stores in the U.S. and Canada have fallen victim to a Magecart-style card-skimming attack that appears to be the work of a new cybercrime group with no clear ties to past Magecart activity. https://www.scmagazine.com/home/security-news/mirrorthief-card-skimming-attack-steals-card-data-from-online-college-stores/?utm_source=newsletter&utm_medium=email&utm_campaign=SCUS_Newswire_20190507&hmSubId=XOjrUhr_Swg1&email_hash=305f40be59a0dcb04476bf06c7e07dc9&mpweb=1325-7746-111266

Scammers phish promising 'Avengers: Endgame' download
Scammers are promising full movie downloads for the Marvel blockbuster "Avengers: Endgame."
https://www.scmagazine.com/home/security-news/phishing/scammers-are-promising-full-movie-downloads-for-the-marvel-blockbuster-avengers-endgame/?utm_source=newsletter&utm_medium=email&utm_campaign=SCUS_Newswire_20190507&hmSubId=XOjrUhr_Swg1&email_hash=305f40be59a0dcb04476bf06c7e07dc9&mpweb=1325-7746-111266

SCAM Phone Call – Don’t Call Back

A while back, we warned you about the “one ring” scam. That’s when you get a phone call from a number you don’t know, and the call stops after just one ring. The scammer is hoping you’ll call back, because it’s really an international toll number and will appear as a charge on your phone bill — with most of the money going to the scammer. Well, the scam is back with a vengeance, and the FCC just issued a new advisory about it. Read the FCC’s advisory for more detail, but the advice from both agencies remains the same if you get one of these calls: https://www.consumer.ftc.gov/blog/2019/05/get-one-ring-call-dont-call-back

Class Action Lawsuits: The Rules and the Scams

Sometimes, victims get even with the people and organizations that deceive them, thanks to a class action lawsuit. https://scambusters.org/classaction.html

WhatsApp Vulnerability Exploited to Place Spyware on Phones

A vulnerability in WhatsApp is being actively exploited to install spyware on mobile phones. The attackers infected targeted devices by calling them; users did not even have to answer the call. A WhatsApp representative said that the flaw, a buffer overflow vulnerability in the WhatsApp VOIP stack, was addresses in a server-side update on Friday, May 10. A fix for end-users was released on Monday, May 13. https://arstechnica.com/information-technology/2019/05/whatsapp-vulnerability-exploited-to-infect-phones-with-israeli-spyware/

Email Phishing Uses Fake Adobe Files To Steal Company Data

True to form, hackers are using tactics they know worked best in the past and improve on them. In a recent hack, the tried-and-true tactic is email phishing. One reason for the incredible success behind email phishing is that it gives cybercriminals direct access to their most reliably vulnerable assets–the users themselves. This time, the improved malware called Separ uses email phishing to target businesses in North America and countries worldwide.
https://www.sosdailynews.com/news.jspx?&articleid=42FCF58AE601D883A956FCC508499348&sx=79

Watch Out for Camera Theft and Other Common Travel Scams

Have you ever been struggling to arrange a photo while on vacation? Maybe there's just you and your partner and you're not that good at selfies or you're using a real camera. Or there's a group and you realize one of you will have to take the photo and therefore not be in the shot.
https://scambusters.org/travelscams2019.html

Intel CPUs Impacted By New Class of Spectre-Like Attacks

Once again, security researchers have discovered critical vulnerabilities in CPU chips that allow attackers to use a technique called speculative execution in order to get CPUs to leak sensitive information. The January 2018 disclosure of a previous set of such flaws, called Meltdown and Spectre, sent shock waves through the… https://threatpost.com/intel-cpus-impacted-by-new-class-of-spectre-like-attacks/144728/

Critical Microsoft Remote Desktop Vulnerability

An Alert is used to raise awareness of a recently disclosed Remote Code Execution vulnerability in the Microsoft Remote Desktop Services platform… https://cyber.gc.ca/en/alerts/critical-microsoft-remote-desktop-vulnerability

****

Hints & Tips plus Security Awareness

Security Monitoring Framework – Use Cases
The MaGMa Use Case Framework (UCF) is a framework and tool for use case management and administration that helps organizations to operationalize their security monitoring strategy.
https://www.betaalvereniging.nl/en/safety/magma/

FS-ISAC Cyber-Attack Against Payment Systems Exercise
The FS-ISAC will host its Cyber-Attack Against Payment Systems (CAPS) exercise for financial institutions in North America on October 1-2 and October 8-9. These virtual, two-day tabletop exercises simulate an attack on payment systems and processes and allows participants to challenge their institution's incident response team's ability to mobilize quickly, critically apprise information, as it is available, connect the "cyberdots" to defend against an attack. FS-ISAC membership is not required to participate in these free exercises. For more information, view the FS-ISAC's CAPS 2019 FAQs https://fs22.formsite.com/FS-ISAC/2019_CAPS_NA/index.html?utm_campaign=RiskCyber-20190514&utm_medium=email&utm_source=Eloqua

How to Recognize a Robocall
Listen for these key phrases related to insurance, jury duty and Social Security
https://www.aarp.org/money/scams-fraud/info-2019/recognize-a-robocall.html?cmp=EMC-DSO-NLC-MONY-FRD--MCTRL-051419-F1-3761604&ET_CID=3761604&ET_RID=43577144&mi_u=43577144&mi_ecmp=20190514_Money_M_CTRL_Winner_654400_963209&encparam=a2kbABDTs8aki3KrMaMg9C%2f8GD2Ftx%2bE8fs%2fPojRO%2bU%3d

What to do if you think you're a victim of fraud
Experian® suggests that you follow a 4-step process if you notice something unfamiliar or suspicious on one of your accounts. See the 4 steps so you know what to do. https://www.experian.com/blogs/ask-experian/credit-education/preventing-fraud/victim-assistance/?ty=mfcor&mkid=C2034F8C-0D2A-5953-9EC0-1DC8471BE72F&pc=crm_exp_0&cc=emm_f_m_act_9890120190514_fttctatm_20190514_x_102

****

News & Views

What differentiates the strongest cybersecurity programs from the rest
New research by Deloitte and the Financial Services Information Sharing and Analysis Center (FS-ISAC) highlights three key traits of successful cybersecurity programs, namely: Support and involvement of executives and the board. Treating cybersecurity and IT as separate departments of equal standing. Tying cyber risk management strategy to business strategy. The…
https://www.helpnetsecurity.com/2019/05/06/strongest-cybersecurity-programs/

National Cybersecurity Career Awareness Week
National Cybersecurity Career Awareness Week focuses local, regional, and national interest to inspire, educate, and engage citizens to pursue careers in cybersecurity. National Cybersecurity Career Awareness Week takes place during November's National Career Development Month.
https://www.ncda.org/aws/NCDA/pt/sp/ncdmonth

Disruptions from cyber attacks increasing, taking longer to fix
Cyber attack disruptions are increasing, and it's taking organizations longer to fix the underlying issues, according to a new report. https://www.information-management.com/news/disruptions-from-cyber-attacks-increasing-taking-longer-to-fix?utm_campaign=security%20briefing-apr%2030%202019&utm_medium=email&utm_source=newsletter&eid=305f40be59a0dcb04476bf06c7e07dc9

Two years after WannaCry, a million computers remain at risk
"Two years ago today, WannaCry impacted hundreds of thousands of computers in over 150 countries. It was one of the first large instances of ransomware and today as many as 1.7 million internet-connected endpoints are still vulnerable to the exploits, according to the latest data." It also raises many questions...
https://www.zdnet.com/article/hackers-are-collecting-payment-details-user-passwords-from-4600-sites/

Dark Web Deals: Your Child's Identity for Sale
Did you know a child's identity is twice as likely to be compromised as an adult's? More than 1 million children under the age of 18 in the U.S. were identity theft victims in a single year, according to the most recent study on Child Identity Fraud by Javelin Strategy & Research. Two-thirds of those young victims are under the age of eight. Cyber thieves seek out the untapped identities of children to open credit cards, commit tax fraud, qualify for government benefits, or apply for work or a place to live – and by doing so, this compromise of personal information can go undetected for years, at least until your child has a need to open a credit card account or apply for a loan. https://www.fightingidentitycrimes.com/dark-web-deals-your-childs-identity-for-sale/

Password Log-Ins Are Under Fire
The world moved a step closer this week to killing off a much maligned element of digital life, the password... https://it.toolbox.com/article/password-log-ins-under-fire-but-microsoft-google-face-resistance-to-killing-them?utm_medium=email&utm_source=digest

****

"Ctrl -F" for The Board

ABA Free Cybersecurity Webinar: FSSCC Cybersecurity Profile for Midsize Banks: A NIST-Based Approach to Cybersecurity Assessments
On Thursday, May 23 at 1 PM ET, ABA is hosting a free 60 minute webinar on the FSSCC Cybersecurity Profile for Midsize Banks with Fulton Financial's CISO, Barth Bailey. The Profile is a NIST-based Cybersecurity Assessment that many banks are finding a robust alternative approach for cybersecurity and IT exams. To learn more about the Profile, visit: www.fsscc.org or www.aba.com/cyberprofile.

Questions
Contact FIPCO's Ken Shaurette at 800/722-3498 ext. 251 or email FIPCO IT Services for more information.

"Make Security Part of You and Your Institution's DNA!"

Threat Intelligence Newsletter: June 4, 2019

FIPCO®
IT Audit
Round Table
Discussions

If you would like to host an event, please contact: Becky Schowalter

Upcoming Threat Intelligence Peer Group Discussions
June 27 – New Berlin

FTC Comment Period Extended – Recommended Amendments to GLBA Section 501b
March 5, 2019 the Federal Trade Commission has put forth quite prescriptive recommendations as an amendment to GLBA Section 501b – the Safeguards Rule. You may as well prepare for enhanced security practices if you haven't already or are not audited by FIPCO you may not have had some of these suggestions: https://www.federalregister.gov/documents/2019/04/04/2019-04981/standards-for-safeguarding-customer-information

FS-ISAC Cyber-Attack Against Payment Systems Exercise
The FS-ISAC will host its Cyber-Attack Against Payment Systems (CAPS) exercise for financial institutions in North America on October 1-2 and October 8-9. These virtual, two-day tabletop exercises simulate an attack on payment systems and processes and allows participants to challenge their institution's incident response team's ability to mobilize quickly, critically apprise information, as it is available, connect the "cyberdots" to defend against an attack. FS-ISAC membership is not required to participate in these free exercises. For more information, view the FS-ISAC's CAPS 2019 FAQs. Register - https://fs22.formsite.com/FS-ISAC/2019_CAPS_NA/index.html?utm_campaign=RiskCyber-20190520&utm_medium=email&utm_source=Eloqua

****

Alerts & Warnings

This ransomware sneakily infects victims by disguising itself with anti-virus software
This file-locking malware family has evolved a new tactic which abuses trust to create new ransomware victim… https://www.zdnet.com/article/this-ransomware-sneakily-infects-victims-by-disguising-itself-with-anti-virus-software/?ftag=TRE-03-10aaa6b&bhid=78480402

Millions of Instagram influencers had their private contact data scraped and exposed
A security researcher recently found an unsecured Amazon Web Services server exposing the personal information of over 49 million prominent Instagram users including so-called “influencers,” celebrities and brands accounts. The leaky database consisted of scraped data. In addition to account information available to all followers, such as the account name… Should I be worried?
https://www.fightingidentitycrimes.com/nearly-50-million-instagram-records-exposed-in-data-leak/

How You May Help "Cookie Stuffing" Scammers
Are you helping website crooks earn income without knowing it, merely by visiting their page -- encountering a trick known as cookie stuffing or affiliate marketing fraud? Let's start by explaining what affiliate marketing is. It's a way of earning income from a website by directing visitors to another website that pays for these leads. https://www.scambusters.org/cookiestuffing.html

Intense scanning activity detected for BlueKeep RDP flaw
Threat actors are actively scanning the web looking for Remote Desktop Protocol (RDP) services that are affected by the highly critical BlueKeep security flaw. The vulnerability, tracked as CVE-2019-0708, impacts RDP implementations on Windows XP, Windows 7, Windows Server 2003, Windows Server 2008 and other older Windows operating systems. While… https://www.zdnet.com/article/intense-scanning-activity-detected-for-bluekeep-rdp-flaw/

Reward Risks: Hackers are Targeting Your Loyalty Points
Loyalty programs are big business for retailers and fraudsters alike. From airline miles to hotel stays to free coffee, consumers are extremely willing to share personal information with their favorite stores for rewards. Fraudsters are increasingly targeting these loyalty programs because consumers often don’t treat it like real money. https://www.fightingidentitycrimes.com/reward-risks-hackers-are-targeting-your-loyalty-points/

****

Hints & Tips plus Security Awareness

Business Email Compromise (BEC) exercise at the Federal Reserve Bank of Chicago on July 25, 2019
As in previous years, FS-ISAC partnered with ManTech – a large, experienced provider of cyber range exercises – to build the network environment and facilitate a realistic, live-fire cyber-attack against a financial institution. Experts will be on-site to answer questions and explain the scenario. You or your institution’s security analysts may participate in person or remotely from your home or office. https://fsisac.myabsorb.com/#/purchase/category/ac5d57a5-8314-4ecf-bf8e-48ce2ab8b441

Make it a scam-free vacation
It’s almost summer! Right now, you probably have beaches on the brain or you’re thinking about that long-planned trip abroad. Before you head out, take steps to help keep your dream vacation from becoming a nightmare: https://www.consumer.ftc.gov/blog/2019/05/make-it-scam-free-vacation?utm_source=govdelivery

Your right to post honest reviews

You probably read customer reviews to learn what people say about their experiences with a business or product. The Consumer Review Fairness Act (CRFA) protects people's ability to share their truthful experiences and opinions. The FTC enforces the CRFA, and recently sued three businesses (and two of their owners) for violating that law… https://www.consumer.ftc.gov/blog/2019/05/your-right-post-honest-reviews?utm_source=govdelivery

Keys to Keeping Your Business Safe When Your Employees' are Away on Summer Vacation

Nearly half of small businesses experienced at least one cyberattack last year, losing an average of over $30,000 per security incident. From phishing scams to delinquent utilities and office supply scams, fraudsters are trying to infiltrate your business for financial gain. Summer is a prime season for vulnerability, as your employees' vacation time results in fewer resources to thwart these attacks. Plan ahead to defend your company against fraud. https://www.fightingidentitycrimes.com/keys-to-keeping-your-business-safe-when-your-employees-are-away-on-summer-vacation/

UNWANTED CALLS?

Just last week, an AARP-endorsed bill known as the TRACED Act passed in the Senate to help deter criminal robocall violations. Learn about the bill and several tips, services and apps to help slow down unwanted calls. https://www.aarp.org/money/scams-fraud/info-2019/how-to-stop-robocalls.html?cmp=EMC-DSO-NLC-RSS-FRD--CTRL-052919-P1-3792902&ET_CID=3792902&ET_RID=43577144&mi_u=43577144&mi_ecmp=20190529_DailyBulletin_Control_247401_320001&encparam=a2kbABDTs8aki3KrMaMg9C%2f8GD2Ftx%2bE8fs%2fPojRO%2bU%3d

****

News & Views

Social Media's Rules Just Changed. Here's How To Keep Up

RIP, "town square." Hello, "living room." In case you missed it, in a single blog post earlier this year, Mark Zuckerberg quietly upended the world of social media. Gone (or nearly so) is the quaint idea of social media as a public broadcast channel — a way for anyone to reach a mass audience, start a dialogue and change the world. It was an inspiring vision, to be sure, but one undone by…
https://www.linkedin.com/pulse/social-medias-rules-just-changed-heres-how-keep-up-ryan-holmes/?trk=eml-email_feed_ecosystem_digest_01-recommended_articles-5-Unknown&midToken=AQHHgQ6LBzJodQ&fromEmail=fromEmail&ut=3VnDEsapUNo8M1

Cyber Attacks Remain a High Risk, and More Enterprises are Buying Insurance for Protection

The Society of Actuaries (SOA), the world's largest actuarial professional organization, recently released its annual survey of emerging risks in conjunction with other partner organizations. The good news for security programs is that cyber risk for the first time in five years was not ranked at the top of the list. The bad news is that cyber security is still a formidable challenge for organizations.
https://securityboulevard.com/2019/05/cyber-attacks-remain-a-high-risk-and-more-enterprises-are-buying-insurance-for-protection/

First American Financial Exposed Millions of Sensitive Documents
Financial services giant First American Financial exposed hundreds of millions of customer mortgage documents containing sensitive information… https://www.securityweek.com/first-american-financial-exposed-millions-sensitive-documents

Snapchat workers snooped on users with internal tool
Snapchat's 186 million users may be in for a rude awakening today after revelation that multiple employees of the social media giant were able to abuse their power and snoop on members. https://hotforsecurity.bitdefender.com/blog/snapchat-workers-snooped-on-users-with-internal-tool-21266.html#new_tab

****

"Ctrl -F" for The Board

Proposed Revisions to the Safeguards Rule's Information Security Program Requirements – Comments due by August
March 5, 2019 the Federal Trade Commission has put forth quite prescriptive recommendations as an amendment to the GLBA Section 501b – the Safeguards Rule. https://www.federalregister.gov/documents/2019/04/04/2019-04981/standards-for-safeguarding-customer-information

Internet crime now costing Americans $2.7 billion a year
Every day, almost a thousand Americans complain to the FBI that they've fallen victim to Internet crime. http://scambusters.org/internetcrime2018.html

Questions
Contact FIPCO's Ken Shaurette at 800/722-3498 ext. 251 or email FIPCO IT Services for more information.

"Make Security Part of You and Your Institution's DNA!"

Threat Intelligence Newsletter: June 17, 2019

FIPCO® IT Audit Round Table Discussions

If you would like to host an event, please contact: Becky Schowalter

Upcoming Threat Intelligence Peer Group Discussions
June 27 – New Berlin

****

Alerts & Warnings

Fake RFP Emails Steal Real Business Names
If you are a small business owner, you always have an eye out for your next contract. Receiving an RFP (request for proposal) could be a way to win a new client. Unfortunately, it may also be a scam. Scammers are sending RFP emails that use the names and info of real companies in hopes of fooling business owners. https://www.bbb.org/council/news-events/bbb-scam-alerts/2017/05/scam-alert-phony-proposal-emails-target-small-business-owners/

Threat actors host malware, C2 servers on Microsoft Azure
Cybercriminals are storing malicious content, including malware and C2 servers, on Microsoft's Azure cloud services. https://www.scmagazine.com/home/security-news/malware/cyber-criminals-are-storing-malicious-content-including-malware-and-c2-servers-on-microsofts-azure-cloud-services/?utm_source=newsletter&utm_medium=email&utm_campaign=SCUS_Newswire_20190604&hmSubId=XOjrUhr_Swg1&email_hash=305f40be59a0dcb04476bf06c7e07dc9&mpweb=1325-8398-111266

Even the NSA is urging Windows users to patch BlueKeep (CVE-2019-0708)
In the wake of Microsoft's second alert regarding the highly critical BlueKeep security flaw (CVE-2019-0708) that impacts Remote Desktop Protocol (RDP) implementations on older Windows operating systems, the National Security Agency (NSA) has now issued a similar warning. https://ooda.us1.list-manage.com/track/click?u=f16e84831246ee66e1d9f6eab&id=d62c62f1ec&e=def73aba0a

BlackSquid malware wants to wrap its tentacles around web servers and drives
Researchers have discovered a new malware family that uses a set of eight exploits to compromise web servers, network drives and removable drives. https://www.scmagazine.com/home/security-news/malware/blacksquid-malware-wants-to-wrap-its-tentacles-around-web-servers-and-drives/?utm_source=newsletter&utm_medium=email&utm_campaign=SCUS_Newswire_20190605&hmSubId=XOjrUhr_Swg1&email_hash=305f40be59a0dcb04476bf06c7e07dc9&mpweb=1325-8439-111266

New RCE vulnerability impacts nearly half of the internet's email servers
Exim vulnerability lets attackers run commands as root on remote email servers.
https://www.zdnet.com/article/new-rce-vulnerability-impacts-nearly-half-of-the-internets-email-servers/?ftag=TRE-03-10aaa6b&bhid=78480402

BlueKeep, the Global Cyber Security Threat We Can Still Prevent
This blog post will continue to update as events around BlueKeep continue. The goal is to proactively reduce the impact of a vulnerability that could impact at a global scale.
https://www.ivanti.com/blog/bluekeep-the-global-cyber-security-threat-we-can-still-prevent?mkt_tok=eyJpIjoiTWpRMU9UUXpOR0ZsTjJGbCIsInQiOiJ2Mlk3OXoyT1hvQThvVnNLSGxCYmVpR2FkR091NCtcL0xXRTZLT2UwczI2Z2tTbFY0cXNIM0VVdXVadHIzMmw1XC8ybndZeVwvcGtmTXFQMkRQNHIzS0xKMFlrUWkweW94WjI1ZWJpUGdqSGhZdnVuNldyT1czZ3ZJWThyQ2JnK3o5eiJ9

BBB Tip: Travel and Vacation Scams
Taking a vacation this summer? If you book your airfare through a third-party website, be sure to use caution. BBB Scam Tracker is receiving reports of scammers pretending to be online airline ticket brokers. They cancel your airline ticket reservations, but not before charging you.
https://www.bbb.org/article/news-releases/16913-bbb-tip-travel-and-vacation-scams

IRS Warns of New Tax Scams
The Internal Revenue Service (IRS) has issued a reminder urging consumers to look out for two new variations of tax-related phone and email scams. The phone scam involves pre-recorded messages threatening to suspend or cancel a victim's Social Security number, and the email phishing scam involves a fake agency—the "Bureau of Tax Enforcement"—claiming that the victim owes past due taxes.
https://www.irs.gov/newsroom/irs-reminder-tax-scams-continue-year-round

IC3 Issues Alert on HTTPS Phishing
The Internet Crime Complaint Center (IC3) has released an alert on Hypertext Transfer Protocol Secure (HTTPS) phishing—a scheme which lures email recipients into visiting malicious websites that look legitimate and secure… https://www.ic3.gov/media/2019/190610.aspx

Zero-Day Exploit Bears Its Teeth On Windows 10 And Server 2019
Windows users, bear with us! There's a new zero-day exploit on Windows 10 and Windows Server 2019. This means there is no patch available for it and that could mean trouble! A security researcher, who has found several zero-day vulnerabilities…
https://www.sosdailynews.com/news.jspx?&articleid=2128D1C4450E6633934EDD7F2DC2BAA4&sx=79

Critical Microsoft NTLM vulnerabilities allow remote code execution on any Windows machine
The Preempt research team found two critical Microsoft vulnerabilities that consist of three logical flaws in NTLM, the company's proprietary authentication protocol.
https://www.helpnetsecurity.com/2019/06/11/microsoft-ntlm-vulnerabilities/

Latest YouTube Scams Involve Extortion, Phishing Tricks
Supposing you post an item on the video sharing site, YouTube. More and more of us are doing just that. In some cases, people post so many; they set up their own channels, which enables viewers to "follow" the channel just like following a person or organization on any other social media service.
https://scambusters.org/youtube2.html

****

Hints & Tips plus Security Awareness

Should Failing Phish Tests Be a Fireable Offense?
Would your average Internet user be any more vigilant against phishing scams if he or she faced the real possibility of losing their job after falling for one too many of these emails? Recently, I met someone at a conference who said his employer had in fact terminated employees for such repeated infractions.
https://krebsonsecurity.com/2019/05/should-failing-phish-tests-be-a-fireable-offense/

What To Do When Hackers Attack
It's happened. You've uncovered a major cyber breach of your organization's systems and data, and it's your job to limit the damage. What are the first steps you should take? How can you determine the cause and effects of the breach? REGISTER NOW
http://app.reg.techweb.com/e/er?elq_mid=90747&elq_cid=27291187&s=2150&lid=138889&elqTrackId=1DD0A473E2FDC8332DA91475F7106A91&keycode=DRVE19_DORG_EM5&elq=1d74c0d92124403b83af50ea7f632ae8&elqaid=90747&elqat=1

Avoiding mortgage closing scams
The CFPB has posted an article and video explaining ways consumers can protect themselves from mortgage closing scams involving fraudulent last-minute instructions to alter wire-transfer routing…
https://www.consumerfinance.gov/about-us/blog/mortgage-closing-scams-how-protect-yourself-and-your-closing-funds/

Making Customers Feel Protected from Cyber Risk
Banks don't have it easy, balancing ever-changing consumer demands with the need for ironclad security and privacy. They're responsible for managing more data than ever, across more devices—all while driving innovation and striving to exceed expectations. It's certainly a tall order.
https://bankingjournal.aba.com/2019/06/making-customers-feel-protected-from-cyber-risk/?utm_campaign=Newsbytes-20190617&utm_medium=email&utm_source=Eloqua

5 reasons why you should use a password manager
Need a reason to use a password manager? How about five? https://www.techrepublic.com/article/5-reasons-why-you-should-use-a-password-manager/?ftag=TREa988f1c&bhid=78480402

Malicious Apps Consume Your Android Screens
It may be a new year, but cybercriminals are up to old tricks. Google recently removed at least 85 fake apps from the official Google Play store after discovering they included adware that actually displayed full-screen ads every 15 minutes. These apps were, of course, the type that are attractive to a wide range of consumer such as TV and remote control simulators and games. Trend Micro researchers said they found malicious adware apps that had been downloaded around 9 million times.
https://www.sosdailynews.com/news.jspx?&articleid=5BAE5BCAAA174346296D8447623E28AC&sx=79

What is angler phishing and how can you avoid it?
Angler phishing is the practice of masquerading as a customer service account on social media, hoping to reach a disgruntled consumer. https://www.experian.com/blogs/ask-experian/what-is-angler-phishing-and-how-can-you-avoid-it/?ty=mfcor&mkid=C2034F8C-0D2A-5953-9EC0-1DC8471BE72F&pc=crm_exp_0&cc=emm_f_m_act_9890120190611_fttctatm_20190611_x_102

What to Do When Hackers Attack? Online eConference
The only thing worse than discovering a compromise of your critical IT systems is not knowing the extent of the damage. How many systems are at risk? How much data was compromised? How long was the attacker inside the perimeter, and are they still there? These are crucial questions to answer in the first hours following an online attack.
https://events.darkreading.com/virtualsummit/?elq_mid=90750&elq_cid=27291187&keycode=DRVE19_DORG_EM6#tour

****

News & Views

Sheltered Harbor Overview Webinar This Month
Recently, ICBA President and CEO Rebeca Romero Rainey sent a letter to community bank CEOs urging them to join Sheltered Harbor, a not-for-profit industry initiative to protect against natural disasters and cybercrime. Since then, there's been a flurry of interest around the initiative, so Sheltered Harbor is holding a webinar at 1 p.m. (Eastern time) on Wednesday, June 19 for interested parties to…
https://shelteredharbor.webex.com/mw3300/mywebex/default.do?nomenu=true&siteurl=shelteredharbor&service=6&rnd=0.1585185693214336&main_url=https%3A%2F%2Fshelteredharbor.webex.com%2Fec3300%2Feventcenter%2Fevent%2FeventAction.do%3FtheAction%3Ddetail%26%26%26EMK%3D4832534b00000004438693543092a22ae2fa080d89d1f1ef63c5f7fe0358af583cb58ba7a2efe70a%26siteurl%3Dshelteredharbor%26confViewID%3D128892163994975588%26encryptTicket%3DSDJTSwAAAAR6FYUcJQJLr4e1UZXeIGYUO1qrVO19N1TzgC8B2EFs1g2%26email%3Delizabeth.heathfield%2540shelteredharbor.org

Cybercrime: An Inside View from Ex-Hacker Brett Johnson
It’s not often that you get the insider’s view of the cybercrime world from a convicted cybercriminal. Recently, cybersecurity vendor Looking Glass Solutions sponsored an event featuring Brett Johnson, who the FBI Field Office in Columbia, South Carolina, called “The Original Internet Godfather.”
https://incyberdefense.com/featured/cybercrime-inside-view-brett-johnson/?utm_source=NXTsoft+Risk+Management&utm_campaign=4be53d0ed9-CYBERBYTES+APR+2_COPY_01&utm_medium=email&utm_term=0_e91de0e00a-4be53d0ed9-124358533

Unpatched Vulnerabilities Cause Breaches in 27% of Orgs, Finds Study
Tripwire partnered with Dimensional Research to survey 340 information security professionals about trends in vulnerability management. The study revealed that many organizations could be doing more to manage their vulnerabilities. https://www.tripwire.com/state-of-security/vulnerability-management/unpatched-vulnerabilities-breaches/?utm_source=The+State+of+Security+Newsletter&utm_campaign=7f3a3b38e9-EMAIL_CAMPAIGN_2019_06_03_01_49&utm_medium=email&utm_term=0_a2892d69fb-7f3a3b38e9-271420573

Quest Diagnostics Breach Leaks Personal Information for Nearly 12 Million Patients
On Monday, June 3rd, 2019, Quest Diagnostics, one of the largest clinical testing networks in the U.S., disclosed a data breach that impacted the personal information of approximately 11.9 million patients. The breach exposed credit card and bank account numbers, Social Security numbers, and medical information of Quest Diagnostics labs patients. The statement came after one of Quest Diagnostics' vendors, American Medical Collection Agency (AMCA), notified the laboratory that an unauthorized third-party had accessed its systems and took control of its payments page between August 1st, 2018 and March 30th, 2019… https://www.fightingidentitycrimes.com/quest-diagnostics-data-breach/

The ultimate list of 2018's worst scams
What a year it was—in 2018 there were 47,567 scams added to the Better Business Bureau (BBB) Scam Tracker. That's an increase from 2017, which had a reported 45,401 scams.
https://www.experian.com/blogs/ask-experian/the-ultimate-list-of-the-years-worst-scams/

CBP Says Thousands of Traveler Photos Stolen in 'Malicious Cyber-Attack
United States Customs and Border Protection (CBP) was the targeted of a "a malicious cyber-attack" resulting in the theft of data belonging to thousands of travelers entering and exiting the US. The attackers obtained the data by breaching a CBP subcontractor that had put the data at risk by failing… https://www.nextgov.com/cybersecurity/2019/06/cbp-says-traveler-license-plate-pictures-stolen-malicious-cyber-attack/157616/

****

"Ctrl -F" for The Board

ICBA to Agencies: Stress Voluntary Nature of Cyber Tool
ICBA called on federal banking regulators to stress that use of their Cybersecurity Assessment Tool is voluntary and that banks may use one or more recognized technology frameworks. In a comment letter, ICBA also asked regulators to provide banks an automated or interactive document to input information for the CAT… https://www.icba.org/docs/default-source/icba/advocacy-documents/letters-to-regulators/19-06-04_catltr.pdf?sfvrsn=8f395c17_0&utm_source=Informz&utm_medium=email&utm_campaign=Informz&_zs=mESjU&_zl=Om5e1

You're probably over-confident about your defenses or under-prepared for a breach
Many Internet users seem over-confident when it comes to their ability to protect themselves from cybercriminals, a new report by Palo Alto Networks and YouGov shows. More than two out of three (68%) respondents said they are doing everything possible to stay safe online. This confidence was shared by three… https://www.zdnet.com/article/cybersecurity-youre-probably-over-confident-about-your-defences-or-under-prepared-for-a-breach/

Zero trust: Trust no one, verify everything
Tried-and-true security solutions like URL filtering, anti-phishing software, firewalls, and other detection and signature-based solutions are able to mitigate most cybersecurity attacks. But they operate on…. . https://www.scmagazine.com/home/opinion/executive-insight/zero-trust-trust-no-one-verify-everything/?utm_source=newsletter&utm_medium=email&utm_campaign=SCUS_Newswire_20190604&hmSubId=XOjrUhr_Swg1&email_hash=305f40be59a0dcb04476bf06c7e07dc9&mpweb=1325-8398-111266

Cyber Risks to Exceed Natural Disasters for Insurers

Cyber risks will soon become bigger risks than natural catastrophes for the insurance sector, Scor Chairman and Chief Executive Officer Denis Kessler said, recommending the industry build a comprehensive, common global scale to assess cyber-related incidents.
https://www.bloomberg.com/news/articles/2019-05-10/cyber-risks-to-exceed-natural-disasters-for-insurers-scor-ceo?srnd=cybersecurity&utm_source=NXTsoft+Risk+Management&utm_campaign=4be53d0ed9-CYBERBYTES+APR+2_COPY_01&utm_medium=email&utm_term=0_e91de0e00a-4be53d0ed9-124358533

Questions
Contact FIPCO’s Ken Shaurette at 800/722-3498 ext. 251 or email FIPCO IT Services for more information.

"Make Security Part of You and Your Institution's DNA!"

Threat Intelligence Newsletter: June 28, 2019

FIPCO®
IT Audit
Round Table
Discussions

If you would like to host an event, please contact: Becky Schowalter

Upcoming Threat Intelligence Peer Group Discussions
None available at the current time

7th Annual Wisconsin Governor's Cybersecurity Summit – Registration OPEN
Save the Date and register early; September 23, 2019. https://wigcot.eventsair.com/2019-wisconsin-governors-cybersecurity-summit/attendee/Site/Register

****

Alerts & Warnings

Yubico to replace vulnerable YubiKey FIPS security keys
Yubico said today it plans to replace certain hardware security keys because of a firmware flaw that reduces the randomness of cryptographic keys generated by its devices. Affected products include models part of the YubiKey FIPS Series, a line of YubiKey authentication keys certified for use on US government networks (and others) according to the US government's Federal Information Processing Standards (FIPS).
https://www.zdnet.com/article/yubico-to-replace-vulnerable-yubikey-fips-security-keys/

New Twist on Job Scams: Text Messages
Employment scams are nothing new but they are on the rise. In 2018, employment scams were the riskiest, according to the *BBB Scam Tracker Risk Report* (BBB.org/RiskReport). As technology changes, so do scammers' tactics. In this new twist on a long-time scam, con artists use text messages and Google Hangouts to convince people to hand over money in exchange for a job that doesn't exist.
https://www.bbb.org/article/tips/12261-bbb-tip-employment-scams

Triton Attackers Seen Scanning US Power Grid Networks
New research by Dragos indicates that the threat actors behind the 2017 Triton (aka Trisis) malware attack that shut down a petrochemical plant in Saudi Arabia, started to scan power grids in the US and Asia-Pacific regions at the end of last year. Because of this, analysts are worried that… https://www.darkreading.com/perimeter/triton-attackers-seen-scanning-us-power-grid-networks/d/d-id/1334968

DHS Email Phishing Scam
The Cybersecurity and Infrastructure Security Agency (CISA) is aware of an email phishing scam that tricks users into clicking on malicious attachments that look like legitimate Department of Homeland Security (DHS) notifications. The email campaign uses a spoofed email address to appear like a National Cyber Awareness System (NCAS) alert and lure targeted recipients into downloading malware through a malicious attachment. https://www.us-cert.gov/ncas/current-activity/2019/06/18/DHS-Email-Phishing-Scam

Millions of Dell PCs Vulnerable to Attack: Patch Now
A new report by SafeBreach warns that millions of Dell computers are at risk of being remotely compromised by threat actors due to a critical vulnerability in SupportAssist, a hardware-diagnostics tool that comes preinstalled on all Dell machines. The flaw affects a SupportAssist component made by PC-Doctor. As many as 100… https://www.tomsguide.com/us/dell-supportassist-flaw,news-30414.html

Riltok banking trojan begins targeting Europe
The Riltok banking trojan has set its sights for the European Market after a few modifications. The Riltok banking trojan, originally intended to target Russians, has, after a few modifications, set its sights on the European market. https://www.scmagazine.com/home/security-news/malware/the-riltok-banking-trojan-has-set-its-sights-for-the-european-market-after-a-few-modifications/?utm_source=newsletter&utm_medium=email&utm_campaign=SCUS_Newswire_20190626&hmSubId=XOjrUhr_Swg1&email_hash=305f40be59a0dcb04476bf06c7e07dc9&mpweb=1325-8904-111266

Scammers Turn to a New Platform: WhatsApp
For years, scammers have been contacting strangers via telephone, email and, more recently, text message and Facebook Messenger. Now scammers are turning to a new platform: WhatsApp. WhatsApp is a free messaging app many people use to contact friends and family. But as with any communication platform, always exercise caution… https://www.bbb.org/article/news-releases/20246-scam-alert-scammers-target-new-victims-using-whatsapp

CISA Statement on Iranian Cybersecurity Threats
WASHINGTON -- In response to reports of an increase in cybersecurity threats, the Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency (CISA) Director Christopher C. Krebs issued a statement… https://www.infosecnews.org/cisa-statement-on-iranian-cybersecurity-threats/

"Cash For Your House" Ads Could be a Scam
"We pay cash for your house" – you've probably seen those signs posted on streetlights, planted on empty lots and, increasingly, on social media sites. https://scambusters.org/cashforyourhouse.html

****

Hints & Tips plus Security Awareness

5 Ways to Spot a Phishing Email
System breaches, hacking successes and ransomware attacks are common items in the news today. Computer systems are under constant threat. IT specialists are often stretched beyond capacity to protect and maintain their systems. NXTsoft is here to help, by providing useful tools and assistance to your IT crew, and education for both your employees and customers. https://www.nxtsoft.com/posts/5-ways-to-spot-a-phishing-email?utm_source=NXTsoft+Risk+Management&utm_campaign=1392f4bcee-CYBERBYTES+JUN+19+2&utm_medium=email&utm_term=0_e91de0e00a-1392f4bcee-124334541

What should I do if my driver's license number is stolen?
A driver's license number is an ID thief's paradise because it can give them your birthdate, address, and even your height, eye color and signature. Plus, it's connected to your vehicle registration, insurance policies, DMV records and more. Here is what you should do if your driver's license number is stolen…
https://www.experian.com/blogs/ask-experian/what-should-i-do-if-my-drivers-license-number-is-stolen/?ty=mfcor&mkid=C2034F8C-0D2A-5953-9EC0-1DC8471BE72F&pc=crm_exp_0&cc=emm_f_m_act_9890120190618_fttctatm_20190618_x_102

Harmonization of the NIST framework for risk, security and privacy
Amidst rising concern around consumer data privacy, NIST is currently developing a data privacy framework that is similar in spirit to the popular Cybersecurity Framework (CSF). Like the CSF, the upcoming privacy Framework will be… https://www.scmagazine.com/home/opinion/executive-insight/harmonization-of-the-nist-framework-for-risk-security-and-privacy/?utm_source=newsletter&utm_medium=email&utm_campaign=SCUS_Newswire_20190621&hmSubId=XOjrUhr_Swg1&email_hash=305f40be59a0dcb04476bf06c7e07dc9&mpweb=1325-8812-111266

2019 Q1 Threat Intelligence Vendor Whitepaper
eSentire's Threat Intelligence team observed a significant reduction in hostile traffic on the eSentire threat detection surface in the first quarter of 2019 (Figure 1) including malware, phishing and remote exploit attempts (abbreviated exploits). Leading this contraction was a drop in opportunistic campaigns targeting Microsoft IIS, ThinkPHP, GPON and D-Link.
https://www.esentire.com/assets/resources/13592a7a89/q1-2019-quarterly-threat-report-esentire.pdf

There are no "quick fixes" to clean up your credit
If you're trying to clean up your credit, you'll come across plenty of companies offering an easy fix. But any company promising instant results for a price is likely a scam.
https://www.consumer.ftc.gov/blog/2019/06/there-are-no-quick-fixes-clean-your-credit-0?utm_source=govdelivery

****

News & Views

What You Need to Know About Zero Trust Security
The zero trust model might be the answer to a world in which perimeters are made to be breached. Is it right for your organization? While the concept behind the zero trust model is…
https://www.darkreading.com/vulnerabilities---threats/what-you-need-to-know-about-zero-trust-security/d/d-id/1334751?cid=malp&_mc=malp

Evernote Security Flaw Leaves 4.6 Million Users Vulnerable
What Happened? On Wednesday, June 12th, 2019, a flaw within Evernote's Google Chrome extension code was reported, which created a security vulnerability impacting 4.6 million consumers and companies. The organizational software app's extension defect, discovered by security company Guardio, opened the door to potential harvesting of user data by bad actors, including authentication data, financial information, private social media conversations, emails, and more…
https://www.fightingidentitycrimes.com/evernote-web-clipper-security-flaw/

Malicious URL attacks using HTTPS surge across the enterprise
The latest Email Threat report by FireEye shows that threat actors are increasingly using HTTPS in order to make malicious URLs to seem legitimate. Between Q4 of 2018 and Q1 of this year, the number of malicious HTTPS links increased by 26%. Malicious email attachments are becoming less common. Phishing…
https://www.zdnet.com/article/social-engineering-attacks-surge-across-the-enterprise/

The Dirty Dozen: 12 Top Cloud Security Threats
Cloud computing is on the rise and as more data and applications move to the cloud unique infosecurity challenges are created. Based on our experience, we weren't surprised to see data breaches and account hijacking make the top 12.
https://www.csoonline.com/article/3043030/the-dirty-dozen-12-top-cloud-security-threats.html?utm_campaign=Newsletter&utm_source=hs_email&utm_medium=email&utm_content=74141610&_hsenc=p2ANqtz-_iG5Hq5m_QTzFIYHUpE91nlMMWCRFwArWRkAWqaFYvtbgrof2Cw5sSLvqHK6mal-Pvv7z3r068mSXQohriLKyXpb_OaQ&_hsmi=74141610

****

"Ctrl -F" for The Board

Sun Prairie, Wis. warns of data breach after intruder accesses employee email accounts
For nearly two months this year, an unauthorized party had illegitimate access to the email accounts of certain employees working for the city of Sun Prairie, Wisconsin. These accounts contained sensitive data such as Social Security numbers, account logins and passwords, drivers' licenses, state identification numbers, bank and financial account numbers, medical information and payment card information.
https://www.scmagazine.com/home/security-news/sun-prairie-wisc-warns-of-data-breach-after-intruder-accesses-employee-email-accounts/?utm_source=newsletter&utm_medium=email&utm_campaign=SCUS_Newswire_20190628&hmSubId=XOjrUhr_Swg1&email_hash=305f40be59a0dcb04476bf06c7e07dc9&mpweb=1325-8930-111266

The CEO Cybersecurity Challenge
Security experts will instantly see the simple genius of this social engineering tactic. In just 10 words you get… https://www.davidfroud.com/the-ceo-cybersecurity-challenge/

Questions
Contact FIPCO's Ken Shaurette at 800/722-3498 ext. 251 or email FIPCO IT Services for more information.

"Make Security Part of You and Your Institution's DNA!"

Threat Intelligence Newsletter: July 15, 2019

FIPCO®
IT Audit
Round Table
Discussions

If you would like to host an event, please contact: Becky Schowalter

Upcoming Threat Intelligence Peer Group Discussions
None available at the current time

****

Alerts & Warnings

Warn All Your Customers – This is REAL!!
Can you be fooled, hope you don't get tested… https://www.nbcnews.com/nightly-news/video/beware-of-growing-social-security-phone-scam-63492165977

BBB Tip: Tech Support Scams
A tech support rep calls you at home and offers to fix a computer bug that you haven't even noticed, or a popup warning appears on your screen instructing you to dial a number for help. In this con, scammers pose as tech support employees of well-known computer companies and hassle victims into paying for their "support." https://www.bbb.org/article/news-releases/16553-bbb-tip-tech-support-scams

One Billion Instagram Users Face New Phishing Scam
There are one billion monthly Instagram users and they are finding out a recent email phishing campaign aimed at them is working. It's designed to steal user credentials with fake copyright infringement email notices, as strange as that may sound. After all, how many Instagram users are even aware of copyright infringement, much less being told they have done so? Not many, that's why it's working. Hackers have been sending Instagram users emails appearing to be directly from Instagram, and they do look very legitimate.
https://www.sosdailynews.com/news.jspx?&articleid=D259CEAAF4077848853047C28D29068D&sx=79

USCYBERCOM discovers active malicious use of CVE-2017-11774
Recommends immediate patching... CVE-2017-11774 is a vulnerability in how Microsoft Outlook handles objects in memory. Successful exploitation of the vulnerability may allow a malicious actor to execute arbitrary commands. This vulnerability exists in Microsoft Outlook 2010, 2013 and 2016. Microsoft patched

the vulnerability in October 2017. Details regarding the vulnerability and the patches can be found here: https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-11774. The WSIC strongly urges our readers to ensure their systems are patched against this vulnerability. https://www.virustotal.com/gui/user/CYBERCOM_Malware_Alert/.

Who's pretending to be the government now?
You've gotten the calls: from Social Security. Or the IRS. Or Medicare. Or any number of other agencies. Except: as soon as the caller threatens you or demands that you pay them with a gift card or by wiring money, you know. It's a scam. Even if caller ID tells you otherwise – that's not the government calling. https://www.consumer.ftc.gov/blog/2019/07/whos-pretending-be-government-now?utm_source=govdelivery

WannaLocker ransomware found combined with RAT and banking trojan
Researchers are warning that a new version of WannaLocker – essentially a mobile derivative of WannaCry ransomware – has been enhanced with spyware, remote access trojan and banking trojan capabilities. https://www.scmagazine.com/home/security-news/ransomware/wannalocker-ransomware-found-combined-with-rat-and-banking-trojan/?utm_source=newsletter&utm_medium=email&utm_campaign=SCUS_Newswire_20190703&hmSubId=XOjrUhr_Swg1&email_hash=305f40be59a0dcb04476bf06c7e07dc9&mpweb=1325-9072-111266

As Package Deliveries Increase, So Do Scams
With so many people shopping online, package deliveries are on the rise… doubling since 2010. Scammers, never missing a beat, are taking advantage of this to fool consumers into giving out their personal information. https://www.bbb.org/ScamTips, If you've been the victim of a package delivery scam, report it on the https://www.bbb.org/scamtracker/us.

Anubis Android banking malware returns with extensive financial app hit list
Thousands of new samples are targeting 188 banking and finance-related apps. https://www.zdnet.com/article/anubis-android-banking-malware-returns-with-a-bang/?ftag=TRE-03-10aaa6b&bhid=78480402

A fileless campaign is dropping the Astaroth info-stealer
Attackers are delivering the Astaroth info-stealing backdoor by leveraging a combination of fileless malware and "living off the land" techniques, Microsoft's security team warns. https://www.helpnetsecurity.com/2019/07/09/astaroth-fileless-malware/

Two Windows Privilege Escalation Vulnerabilities Exploited in Attacks
Microsoft's July 2019 Patch Tuesday updates fix nearly 80 vulnerabilities, including two Windows zero-day flaws and six issues whose details were previously made public. One of the zero-day vulnerabilities is CVE-2019-0880, which Microsoft describes as a local privilege escalation issue related to how the splwow64.exe component in Windows handles certain calls. https://www.securityweek.com/two-windows-privilege-escalation-vulnerabilities-exploited-attacks

New ShadowGate Ransomware Installs Immediately
A new version of ransomware is aggressively infecting websites and not even bothering to lurk around in the shadows hiding from you. As soon as a user visits a website infected with this ransomware, files are immediately locked up, an unpleasant notification pops up letting you know about it, and those files are held for ransom to the tune of hundreds of Bitcoin. These days, that's in the tens of thousands of Dollars. Whatever can you do?
https://www.sosdailynews.com/news.jspx?&articleid=AF3E594A62D422EA54E3B0682E34D5F1&sx=79

****

Hints & Tips plus Security Awareness

The 2019 State of the Phish Report
Analyzes data from tens of millions of simulated phishing attacks sent over a 12-month period, as well as examines an extensive survey of domestic and international infosec professionals. It includes cybersecurity insights into end-user security awareness and behavior around phishing, ransomware and more. https://training.misti.com/acton/attachment/10465/f-bebf1676-2db2-432c-ab7e-2ab79ecfba0f/1/-/-/-/-/pfpt-us-tr-state-of-the-phish-2019%20%28final%29.pdf?utm_term=pfpt-us-tr-state-of-the-phish-2019%20%28final%29.pdf&utm_campaign=State%20of%20the%20Phish%202019%20Report&utm_content=landing+page&utm_source=Act-On+Software&utm_medium=landing+page&cm_mmc=Act-On%20Software-_-Landing%20Page-_-State%20of%20the%20Phish%202019%20Report-_-pfpt-us-tr-state-of-the-phish-2019%20%28final%29.pdf&sid=TV2:iGdpVjqCE

VMSA-2019-0011 - ESXi patches
These will address partial denial of service vulnerability in hosted process (CVE-2019-5528) See the advisory here: https://www.vmware.com/security/advisories/VMSA-2019-0011.html

How to protect your network just like a bank ATM
A report out from Talos on the state of ATM malware contains lots of tips on protecting these machines from malware, and they're just as applicable to other industries. https://www.techrepublic.com/article/how-to-protect-your-network-just-like-a-bank-atm/?ftag=TREa988f1c&bhid=78480402

Social Security scams have become an epidemic, government says
Pretending to be from the IRS is getting tougher for scammers — so they've switched their attention to Social Security. In fact, Social Security impersonations have moved into the top slots among impostor scams. https://www.scambusters.org/socialsecurity4.html

****

News & Views

Trust dimensions in zero trust security
The increasing sophistication of cyberattacks and subsequent costs associated with containment and remediation has brought about an evolution in the security industry. Enterprises are now beginning to realize that trust is a precious commodity and one of the best ways to preserve it is by taking a zero trust approach. https://www.helpnetsecurity.com/2019/07/03/dimensions-zero-trust-security/

How financial services companies can protect against mobile threats
Financial services organizations face a variety of cyber threats. But mobile risks represent a major Achilles' heel for the industry, says a new report from Wandera. https://www.techrepublic.com/article/how-financial-services-companies-can-protect-against-mobile-threats/?ftag=TREa988f1c&bhid=78480402

From zero to one hundred: Why 'Zero-Trust' is taking off in the enterprise
Businesses are readily adopting a "zero trust" security architecture thanks to sophisticated cybersecurity threats and evolving regulations, Technologies such as encryption, multifactor authentication… https://it.toolbox.com/guest-article/from-zero-to-one-hundred-why-zero-trust-is-taking-off-in-the-enterprise?utm_medium=email&utm_source=digest

Passwords Aren't Enough: Exploring Multi-factor Authentication As A Part of Your Cybersecurity Strategy
In the early days of the internet, all you needed to log into an account or website was a username and a short, simple password. https://www.nxtsoft.com/posts/passwords-aren-t-enought-exploring-multi-factor-authentication-as-a-part-of-your?utm_source=NXTsoft+Risk+Management&utm_campaign=86eb68cdbd-CYBERBYTES+16&utm_medium=email&utm_term=0_e91de0e00a-86eb68cdbd-124334541

Persistent Threats Can Last Inside SMB Networks for Years
Persistent threats can compromise the networks of small and midsize businesses (SMBs) for years on end according to a new report by Infocyte. The study, which focused on organizations with a headcount between 99-5,000 and no more than $1 billion in annual revenue, found that persistent threats excluding ransomware… https://www.darkreading.com/threat-intelligence/persistent-threats-can-last-inside-smb-networks-for-years/d/d-id/1335207

****

"Ctrl -F" for The Board

What can financial institutions do to improve email security?
Financial institutions are in a fully-fledged war against data breaches. And rightly so – the finance sector is a frequent target of ransomware, phishing, and other malicious attacks. Sensitive communications are particularly vulnerable, with thousands getting leaked every year.
https://www.helpnetsecurity.com/2019/07/09/financial-institutions-email-security/

Inside the NIST team working to make cybersecurity more user-friendly
Cybersecurity is usually not a user's primary duty, yet they suffer an increasing burden to respond to security warnings, maintain many complex passwords, and make security decisions for which they are not equipped. https://www.helpnetsecurity.com/2019/07/11/nist-cybersecurity/

Questions
Contact FIPCO's Ken Shaurette at 800/722-3498 ext. 251 or email FIPCO IT Services for more information.

"Make Security Part of You and Your Institution's DNA!"

Threat Intelligence Newsletter: July 30, 2019

FIPCO®
IT Audit
Round Table
Discussions

If you would like to host an event, please contact: Becky Schowalter

Upcoming Threat Intelligence Peer Group Discussions
None available at the current time

Nationwide Suspicious Activity Reporting Initiative (NSA) and WiWATCH Training
The WSIC Fusion Center website, https://wifusion.org, offers a SAR reporting platform with an interface for mobile devices. This feature supports WSIC's goal of maximizing its ability to detect, prevent, investigate, and respond to criminal and terrorist activity. (WSIC = Wisconsin State Information Center)

****

Alerts & Warnings

This strange new phishing attack uses a surprise bill to trick you into clicking
Researchers uncover a campaign which uses SHTML files - commonly associated with web servers - to direct users to malicious, credential-stealing websites. https://www.zdnet.com/article/this-strange-new-phishing-attack-uses-a-surprise-bill-to-trick-you-into-clicking/?ftag=TRE-03-10aaa6b&bhid=78480402

Are your passwords among the 100,000 most breached ones?
Year after year, the list of most often used passwords changes but a little: the latest one, compiled by infosec researcher Troy Hunt and published by the UK National Cyber Security Centre (NCSC), puts "123456", "123456789", "qwerty", "password" and "111111" on the top five spots.
https://www.helpnetsecurity.com/2019/04/23/most-often-used-passwords/

Scams use false alerts to target Office 365 users, admins
Malicious actors have recently been targeting Microsoft Office 365 users in two separate scams – one that distributes the TrickBot information-stealing trojan via a fake website and a phishing campaign that sends fake alerts with the intent to take over the accounts of email domain administrators.
https://www.scmagazine.com/home/security-news/cybercrime/scams-use-false-alerts-to-target-office-365-users-admins/?utm_source=newsletter&utm_medium=email&utm_campaign=SCUS_Newswire_20190723&hmSubId=XOjrUhr_Swg1&email_hash=305f40be59a0dcb04476bf06c7e07dc9&mpweb=1325-9325-111266

Thwart the pressing threat of RDP password attacks
How long does it takes for Internet-facing, RDP-enabled computers to come under attack? In some cases, a few minutes. In most, less than 24 hours… https://www.helpnetsecurity.com/2019/07/23/thwart-rdp-password-attacks/

Flaws in widely used corporate VPNs put company secrets at risk
Researchers have found several security flaws in popular corporate VPNs, said the flaws found in the three corporate VPN providers Palo Alto Networks, Pulse Secure and Fortinet are easy to remotely exploit.
https://techcrunch.com/2019/07/23/corporate-vpn-flaws-risk/

VMware Security Advisories
VMSA-2019-0010.1 - Updated security advisory with remediation information for the vCenter 6.7 and AppDefense 2.x release lines and removed Horizon from affected products as it was incorrectly listed.
https://www.vmware.com/security/advisories/VMSA-2019-0010.html

Phishers targeting Office 365 admins have a new trick up their sleeve
Phishers targeting Office 365 admins have a new trick up their sleeve: they are checking the credentials entered into the spoofed login page in real-time and, if they are valid, the victims are redirected to their real Office 365 inbox. https://www.helpnetsecurity.com/2019/07/24/phishers-targeting-office-365-admins/

Linux Botnet Adding BlueKeep-Flawed Windows RDP Servers to Its Target List
Cybersecurity researchers have discovered a new variant of WatchBog, a Linux-based cryptocurrency mining malware botnet, which now also includes a module to scan the Internet for Windows RDP servers vulnerable to the Bluekeep flaw. https://thehackernews.com/2019/07/linux-malware-windows-bluekeep.html

Spread The Word About Social Security Scams
Getting calls saying your Social Security number is suspended because of suspicious activity? It's a scam. The Social Security Administration (SSA) is not calling you, no matter what your caller ID says.
https://www.identitytheft.gov/ssa?utm_source=govdelivery

Threat Spotlight: Sodinokibi ransomware attempts to fill GandCrab void
Sodinokibi ransomware, also known as Sodin and REvil, is hardly three months old, yet it has quickly become a topic of discussion among cybersecurity professionals because of its apparent connection with the infamous-but-now-defunct GandCrab ransomware. https://blog.malwarebytes.com/threat-spotlight/2019/07/threat-spotlight-sodinokibi-ransomware-attempts-to-fill-gandcrab-void/?machine-id=70c7587888dbcfda54e3d89bd6720e45beb4909c&lang=en

****

Hints & Tips plus Security Awareness

Typosquatting Is Quickly Rising, How To Protect Yourself
Have you ever opened your web browser, typed in a website URL, and when the page came up, you were not at the website that you thought you were going to land on? In most cases, a simple check of the URL that you typed will reveal that you have a typo and accidentally hit the wrong letter when entering the URL. For example, instead of typing in www.netflix.com, you type in www.netflxi.com by accidentally typing the "X" before the "I" at the end of the domain name.
https://www.sosdailynews.com/news.jspx?&articleid=F154B01155AFF572D218E6301EBFEAF1&sx=79

Medicare does not give out DNA kits
Here's one that goes to show just how creative scammers can be. The FTC is getting reports that callers claiming to be from Medicare are asking people for their Medicare numbers, Social Security numbers, and other personal information…in exchange for DNA testing kits. The callers might say the test is a free way to get early diagnoses for diseases like cancer, or just that it's a free test, so why not take it? But the truth is, Medicare does not market DNA testing kits to the general public.
https://www.consumer.ftc.gov/blog/2019/07/medicare-does-not-give-out-dna-kits?utm_source=govdelivery

Caught in a Browser Mousetrap? Here's How to Escape!
Have you ever landed on a web page and discovered you can't leave? You feel like you're caught in a mousetrap and there's no escape. It's a trick many scammers (and even some legitimate organizations) use to hold your attention. Not surprisingly, the tactic is called mousetrapping.
https://scambusters.org/mousetrap.html

Summer Film Series: Family emergency scams
Welcome to the Summer Film Series! Each week, we'll highlight one of the FTC's many videos on topics such as avoiding scams, recovering from fraud, and managing your money. Grab a blanket and some popcorn and enjoy. https://www.consumer.ftc.gov/blog/2019/07/summer-film-series-family-emergency-scams?utm_source=govdelivery

****

News & Views

True passwordless authentication is still quite a while away
The password has been one of the great inventions in the history of computing: a solution that allowed simple and effective identity and access management when the need arose for it.
https://www.helpnetsecurity.com/2019/07/18/true-passwordless-authentication/

German banks are moving away from SMS one-time passcodes
New EU legislation might help kill SMS 2FA / 2SV / OTP. https://www.zdnet.com/article/german-banks-are-moving-away-from-sms-one-time-passcodes/

How Safe are Fingerprint and Facial Recognition Sign-ons?
Will fingerprints and other biometrics replace passwords? Is security that's based on your fingerprint or your facial features safer than using a password? Yes and no, say the experts.
https://scambusters.org/fingerprint.html

Researchers Easily Trick Cylance's AI-Based Antivirus Into Thinking Malware Is 'Goodware'
Security researchers with Skylight Cyber have found a surprisingly easy way to let malware bypass Cylance's AI-based anti-malware solution. The research shows that while artificial intelligence holds great potential for cybersecurity, AI-driven security offerings can be far from bulletproof. In order to deceive Cylance's algorithm, all the researchers had to… https://www.vice.com/en_us/article/9kxp83/researchers-easily-trick-cylances-ai-based-antivirus-into-thinking-malware-is-goodware

****

"Ctrl -F" for The Board

Webinar: What Are Phishing, Vishing and Smishing and How Can I Protect My Small Business?
On August 13, the National Cyber Security Alliance and Infosec will host a webinar on how businesses can protect against phishing and other threats like smishing and vishing. Presenters will break down these terms and outline steps organizations can take to protect themselves from cyber criminals.
https://staysafeonline.org/event/csmb-webinar-aug19/

National Cybersecurity Awareness Month 2019
CISA, in partnership with the National Cyber Security Alliance (NCSA), is observing its 16th annual National Cybersecurity Awareness Month (NCSAM) this October. Businesses and organizations are invited to participate as CISA and NCSA take strides towards positive user behavior change and broader awareness across the nation. Under the overarching theme of 'Own IT. Secure IT. Protect IT.,' NCSAM 2019 is focused on digital privacy, cybersecurity careers, and encouraging personal accountability and proactive behavior in security best practices. https://staysafeonline.org/ncsam/themes/

Questions
Contact FIPCO's Ken Shaurette at 800/722-3498 ext. 251 or email FIPCO IT Services for more information.

"Make Security Part of You and Your Institution's DNA!"

Threat Intelligence Newsletter: August 26, 2019

FIPCO®
IT Audit
Round Table
Discussions

If you would like to host an event, please contact: Becky Schowalter

Upcoming Threat Intelligence Peer Group Discussions
None available at the current time

****

Alerts & Warnings

The Hotel Hackers Are Hiding in the Remote Control Curtains
Back doors to your personal data can be found in everything from smart fish tanks to Wi-Fi pineapples. https://www.bloomberg.com/news/features/2019-06-26/the-hotel-hackers-are-hiding-in-the-remote-control-curtains?utm_source=NXTsoft+Risk+Management&utm_campaign=1d51c9cac3-CYBERBYTES+JULY+ROUNDUP&utm_medium=email&utm_term=0_e91de0e00a-1d51c9cac3-124334541

Summer Film Series: Unwanted calls to your mobile phone
Ring, ring! The film series is back, this time with help to stop unwanted calls to your mobile phone. Unwanted calls are annoying. They interrupt your day, and many are meant to scam you. But what can you do about these calls? Today's video gives you some ways to stop unwanted calls on your mobile phone, so take a look. https://www.consumer.ftc.gov/blog/2019/08/summer-film-series-unwanted-calls-your-mobile-phone?utm_campaign=unwanted-calls&utm_medium=email&utm_source=govdelivery

Fake News, Videos and More Launch Year of 2020 Election Scams
Although we won't be voting for about a year for our President and other elected representatives, election scams are already rife. And we can expect them to get worse. The closer we get to November 3, 2020, the more we're likely to be targeted by online scammers. https://scambusters.org/electionscam2.html

****

Hints & Tips plus Security Awareness

How to limit the impact of data breaches
IBM offers advice about how to defend against and respond to data breaches.
https://www.techrepublic.com/article/how-to-limit-the-impact-of-data-breaches/?ftag=TREa988f1c&bhid=78480402

How to protect your corporate bank account after the Capital One breach: 10 tips
A Capital One data breach put the data of 106 million people at risk, including social security numbers and banking information…. https://www.techrepublic.com/article/how-to-protect-your-corporate-bank-account-after-the-capital-one-breach-10-tips/?ftag=TREa988f1c&bhid=78480402

DHS Cybersecurity and Infrastructure Security Agency Issues Guidelines for O365 Migrations
The U.S. Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) has issued a set of guidelines and best practices to help organizations migrate to Microsoft Office 365 and avoid introducing vulnerabilities that could make it easier for cybercriminals to conduct attacks and gain access to Office 365 accounts. https://www.netsec.news/dhs-cybersecurity-and-infrastructure-security-agency-issues-guidelines-for-o365-migrations/

****

News & Views

CyberRisk Alliance acquires Cybersecurity Collaborative establishing its Peer Council Business Platform
CyberRisk Alliance ("CRA"), a business intelligence company serving the cybersecurity and information risk management marketplace, has acquired Cybersecurity Collaborative, a peer council platform for Chief Information Security Officers (CISOs) and other senior-level security executives from Stuart Cohen, the company's founder and CEO. Stuart will continue to lead the business as its chief executive.
https://www.scmagazine.com/home/sc-corporate-news/cyberrisk-alliance-acquires-cybersecurity-collaborative-establishing-its-peer-council-business-platform/?utm_source=newsletter&utm_medium=email&utm_campaign=SCUS_Newswire_20190820&hmSubId=XOjrUhr_Swg1&email_hash=305f40be59a0dcb04476bf06c7e07dc9&mpweb=1325-9770-111266

Employee Error Behind Half of Industrial Network Incidents
A new report by Kaspersky shows that employee mistakes are the leading cause of industrial cybersecurity incidents. Last year, 52% of such incidents were the result of human error. Despite growing cyber threats, only 57% of industrial firms have a dedicated cybersecurity budget for operational technology (OT) / industrial control… https://www.infosecurity-magazine.com/news/employee-error-half-industrial/

****

"Ctrl -F" for The Board

Crime is 4,000 times easier today
In part one of TechRepublic's four-part series "Mastermind con man behind Catch Me If You Can talks cybersecurity" TechRepublic's Karen Roby sat down with Frank Abagnale, the famous con man turned FBI Academy instructor, who inspired the Leonardo DiCaprio character in the movie Catch Me if You Can to discuss his work at the FBI's law enforcement training and research center and what C-suite executives need to know regarding cybersecurity. https://www.techrepublic.com/article/famous-con-man-frank-abagnale-crime-is-4000-times-easier-today/?ftag=TREa988f1c&bhid=78480402

Who Has My Data & How Did They Get It?
Technology is now integrated into every aspect of daily life. We use the internet for knowledge, shopping, communication, business, convenience, and much more. Although technology has become increasingly invasive over the past few decades, many users are just beginning to understand and question the data collection practices of vendors used every day. https://www.nxtsoft.com/posts/who-has-my-data-how-did-they-get-it?utm_source=NXTsoft+Risk+Management&utm_campaign=47a927971d-CYBERBYTES+19&utm_medium=email&utm_term=0_e91de0e00a-47a927971d-124334541

Questions
Contact FIPCO’s Ken Shaurette at 800/722-3498 ext. 251 or email FIPCO IT Services for more information.

"Make Security Part of You and Your Institution's DNA!"

Threat Intelligence Newsletter: September 12, 2019

FIPCO®
IT Audit
Round Table
Discussions

If you would like to host an event, please contact: Becky Schowalter

Upcoming Threat Intelligence Peer Group Discussions
None available at the current time

****

Alerts & Warnings

Where is your online search leading you?
Dishonest companies set up websites that look like legitimate places to get information on finding a job, joining the military, or getting government benefits. But they might not help you with any of those things. Instead, they'll take your personal information and sell it to other companies. The companies that buy those "leads" then try to pitch you products or services you didn't ask for.
https://www.consumer.ftc.gov/blog/2019/08/where-your-online-search-leading-you?utm_source=govdelivery

Instagram phishing scam uses fake 2FA code to appear trustworthy
Researchers recently spotted a sneaky phishing scam that uses a phony two-factor authentication request to trick email recipients into entering their Instagram login credentials.
https://www.scmagazine.com/home/security-news/cybercrime/instagram-phishing-scam-uses-fake-2fa-code-to-appear-trustworthy/?utm_source=newsletter&utm_medium=email&utm_campaign=SCUS_Newswire_20190828&hmSubId=XOjrUhr_Swg1&email_hash=305f40be59a0dcb04476bf06c7e07dc9&mpweb=1325-9906-111266

Malicious websites were used to secretly hack into iPhones for years, says Google
Threat actors may have hacked into thousands of iPhones via an "indiscriminate" attack involving a number of malicious websites, new research by Google shows. The websites were visited by thousands of users per week and according to Ian Beer of Google, "simply visiting the hacked site was enough for the… https://techcrunch.com/2019/08/29/google-iphone-secretly-hacked/

The biggest cybersecurity risks in the financial services industry
Ransomware, SQL injection attacks, and cross-site scripting are also serious cybersecurity risks for banks and brokerage firms, according to a new study. https://www.techrepublic.com/article/the-biggest-cybersecurity-risks-in-the-financial-services-industry/?ftag=TREa988f1c&bhid=78480402

WordPress Plugins Exploited in Ongoing Attack, Researchers Warn
Researchers are warning of an ongoing campaign exploiting vulnerabilities in a slew of WordPress plugins. The campaign is redirecting traffic from victims' websites to a number of potentially harmful locations. https://threatpost.com/wordpress-plugins-exploited-in-ongoing-attack-researchers-warn/147671/

Forget email: Scammers use CEO voice 'deepfakes' to con workers into wiring cash
AI-generated audio was used to trick a CEO into wiring $243,000 to a scammer's bank account. https://www.zdnet.com/article/forget-email-scammers-use-ceo-voice-deepfakes-to-con-workers-into-wiring-cash/?ftag=TRE-03-10aaa6b&bhid=78480402

Security hole opens a billion Android users to advanced SMS phishing attacks
Check Point Research has revealed a security flaw in Samsung, Huawei, LG, Sony and other Android-based phones that leaves users vulnerable to advanced phishing attacks.
https://www.helpnetsecurity.com/2019/09/04/android-advanced-phishing-attacks/

Warshipping – A new Attack type to Hack into Corporate or Personal Networks
Warshipping is a new form of attack that counters the limitations with wardialing and wardriving techniques and improves the accuracy dramatically.
https://brica.de/alerts/alert/public/1271045/warshipping-a-new-attack-type-to-hack-into-corporate-or-personal-networks/ also https://gbhackers.com/warshipping-attack-type/

Free trials and tribulations
As you browse online, you probably see offers to try out cool products or services for free. This can be tempting and, many times, it's okay to check them out. But some dishonest companies will bury the terms of their "free trial" offers in fine print or not disclose them at all. Their real goal is to rob you blind.
https://www.consumer.ftc.gov/blog/2019/09/free-trials-and-tribulations?utm_source=govdelivery

****

Hints & Tips plus Security Awareness

Cell Phone Fraud Soars — Here's How to Beat It
7 things you can do to defeat the cell phone fraudsters; Cell phone fraud is rising fast, but some service providers aren't well enough prepared to stop it from costing their customers a fortune.
https://scambusters.org/cellphonefraud.html

Curious Characters Create Devious URL's For Phishing Attacks
There's a word for it…homographic hack, and cyberthieves love to use them. Homographic attacks happen when hackers register a domain name using characters from other, non-Latin languages that look almost exactly like some characters used in the English language. The reason they do it is to trick users into following URL's that have been created to look like the real deal. Once a user goes to a web address using homographs, all bets are off. The web page is designed to look exactly like what a user expects from their online site, only it's anything but. Users hand over their account numbers, passwords, and other PII (Personally Identifiable Information) without the slightest idea they are in the wrong place–a very wrong place.
https://www.sosdailynews.com/news.jspx?&articleid=610F05E0753B77C2A3CDAD20F4A727A5&sx=79

Windows 7 end of life: Months from patch cut-off
Nearly half of all PCs used in small businesses are running Windows 7 despite Microsoft's January 2020 deadline. https://www.zdnet.com/article/windows-7-end-of-life-months-from-patch-cut-off-millions-still-havent-upgraded/?ftag=TRE-03-10aaa6b&bhid=78480402

Losing her phone to a thief was just the beginning of her problems
One of the 200+ people who had their phones stolen at Lollapalooza has reached out to *CWBChicago* with a cautionary tale. It's a head's up that everyone needs to be aware of in case their phone goes missing. For her, the misery didn't end with losing her phone to a thief. http://www.cwbchicago.com/2019/08/losing-her-phone-to-thief-was-just.html

How to prevent a Corporate Account Takeover
Corporate accounts are the crown jewels to hackers. Learn how to stop hackers from business identity theft. https://www.techrepublic.com/article/how-to-prevent-a-corporate-account-takeover/?ftag=TREa988f1c&bhid=78480402

****

News & Views

Small Businesses Must Demand More from their Banking Relationship
Many Small to Medium-Sized Businesses (SMBs) rely on their bank for all their checking and credit needs. But could they be doing more? A recent study by J.D. Power discovered only 37% of small business banking customers believe their bank appreciates their business, and 32% say their bank understands their business. A strong relationship is one built with... https://www.fightingidentitycrimes.com/small-businesses-must-demand-more-from-their-banking-relationship/

WannaCry Remains No. 1 Ransomware Weapon
Over two years after the global WannaCry infection, the infamous worm continues to be the most detected ransomware variant out there, a new Trend Micro study shows. In the first six months of this year, WannaCry was detected around 10 times more frequently than the combined total for all other…
https://www.darkreading.com/endpoint/wannacry-remains-no-1-ransomware-weapon/d/d-id/1335659

A ransomware revival leads to 2.2 billion stolen credentials on the dark web in Q1
In a new report, McAfee Labs said cybercriminals were focusing in on attacking weak IoT devices and extracting huge troves of data from large companies. https://www.techrepublic.com/article/a-ransomware-revival-leads-to-2-2-billion-stolen-credentials-on-the-dark-web-in-q1/?ftag=TREa988f1c&bhid=78480402

Equifax data breach: Pick free credit monitoring
Assistant Director, Division of Privacy and Identity Protection
Just last week, the FTC and others reached a settlement with Equifax about its September 2017 data breach that exposed personal information of 147 million people. We've told you to go to ftc.gov/Equifax, where you can find out if your information was exposed and learn how to file a claim with the company in charge of the claims process… https://www.consumer.ftc.gov/blog/2019/07/equifax-data-breach-pick-free-credit-monitoring?utm_source=govdelivery

The Risk of Weak Online Banking Passwords
If you bank online and choose weak or re-used passwords, there's a decent chance your account could be pilfered by cyberthieves — even if your bank offers multi-factor authentication as part of its login process. This story is about how crooks increasingly are abusing third-party financial aggregation services like Mint, Plaid, Yodlee, YNAB and others to surveil and drain consumer accounts online.
https://krebsonsecurity.com/2019/08/the-risk-of-weak-online-banking-passwords/

Over Half Of Americans Don't Know If They Were Caught Up In A Data Breach
At this point in time, it seems unlikely an average American consumer remains unscathed by one of countless mega data breaches. Yet, a survey by Lexington Law shows 56% of Americans failed to use the many options available to verify their involvement in a data breach. Considering some of the mega data breaches over the past few years. Yet data shows most consumers don't know how to follow-up after a data breach, leaving them with fingers crossed and hoping for the best…
https://www.sosdailynews.com/news.jspx?&articleid=0C2CCC14EE83C165DB94FC8C9E7A2F91&sx=79

Revisiting Social Security Numbers As Identification
Since 1936, the U.S. Government has provided a Social Security Number (SSN) for every citizen. In a world that's radically different than it was over 80 years ago, cybersecurity professionals question the assistance SSN's now provide to identity theft. In past years, over 400 million SSN's have been exposed in massive data breaches and hacking events. That presents a huge problem, as these compromised SSN's are often the gateway to identity theft. So, why do we still use them for identification and should we stop?
https://www.sosdailynews.com/news.jspx?&articleid=03B77BD5222CD50B351D21FF6CE29553&sx=79

****

"Ctrl -F" for The Board

DOJ Guidance on Compliance Programs & Cooperation Credit
In recent months, the US Department of Justice (DOJ) has issued new guidance on two distinct topics: how to evaluate corporate compliance programs[1], and how to award "cooperation credit" to defendants that co-operate during a False Claims Act (FCA) investigation. https://www.natlawreview.com/article/doj-guidance-compliance-programs-cooperation-credit?utm_content=aba0ce15c66b190dedc5bf62212333b9&utm_campaign=2019-8-29SEC%20%26%20Corporate%20Legal%20News&utm_source=Robly.com&utm_medium=email

New ransomware grows 118% as cybercriminals adopt fresh tactics and code innovations
The number of new ransomware samples more than doubled in the first quarter of this year, a new study by McAfee Labs shows. New ransomware increased by 118%, while the most prevalent strains were Dharma (aka Crysis), GandCrab and Ryuk. McAfee detected 504 threats per minute.
https://www.helpnetsecurity.com/2019/08/29/new-ransomware/

BEC overtakes ransomware and data breaches in cyber-insurance claims
Business email compromise (BEC) has become the most common reason for organizations to file cyber-insurance claims, a new AiG study[pdf] covering the EMEA (Europe, the Middle East, and Asia) region shows. Last year, 23% of all cyber-insurance claims were related to BEC. Ransomware accounted for 18% of claims, followed by data… https://www.zdnet.com/article/bec-overtakes-ransomware-and-data-breaches-in-cyber-insurance-claims/

Questions
Contact FIPCO's Ken Shaurette at 800/722-3498 ext. 251 or email FIPCO IT Services for more information.

"Make Security Part of You and Your Institution's DNA!"

Threat Intelligence Newsletter: September 24, 2019

FIPCO®
IT Audit
Round Table
Discussions

If you would like to host an event, please contact: Becky Schowalter

Upcoming Threat Intelligence Peer Group Discussions
November 7 – Eau Claire

Get ready for National Cybersecurity Awareness Month
National Cybersecurity Awareness Month is less than a month away! Use our free NCSAM toolkit to engage employees in cybersecurity this October. https://www2.infosecinstitute.com/l/12882/2019-08-27/frbczp

****

Alerts & Warnings

Holy cybercrime, Batman! Joker malware commits ad fraud, data theft
Two dozen apps that collectively generated over 472,000 downloads from the Google Play store were found to be infected with a new Android malware called Joker, which delivers a payload that perpetrates both ad fraud and data theft, a research firm has reported. https://www.scmagazine.com/home/security-news/holy-cybercrime-batman-joker-malware-commits-ad-fraud-data-theft/?utm_source=newsletter&utm_medium=email&utm_campaign=SCUS_Newswire_20190909&hmSubId=XOjrUhr_Swg1&email_hash=305f40be59a0dcb04476bf06c7e07dc9&mpweb=1325-10067-111266

Simjacker vulnerability actively exploited to track, spy on mobile phone owners
Threat actors are actively exploiting a security weakness in SIM cards in order to covertly collect the location information of thousands of users, new research by AdaptiveMobile Security shows. The firm warns that the Simjacker attack, which involves sending malicious SMS messages to vulnerable devices, may put over 1 billion… https://www.helpnetsecurity.com/2019/09/12/simjacker/

Emotet back in action
The Emotet botnet is back from a four-month vacation with a new spam campaign that began early on September 16. https://www.scmagazine.com/home/security-news/malware/emotet-back-in-action/?utm_source=newsletter&utm_medium=email&utm_campaign=SCUS_Newswire_20190918&hmSubId=XOjrUhr_Swg1&email_hash=305f40be59a0dcb04476bf06c7e07dc9&mpweb=1325-10246-111266

Browser Extenstions Send Off Data Of Millions Of Users Without Permission
Browser extensions can be our friends. They can help us find bargains, help us keep track of information, add to our security, or do something that's simply fun such as the ones that let you distort photos into funny images. They can also do harm, as is the case with a recent find by a security researcher involving several extensions (or add-ons) used with Firefox and Chrome. They collected data from millions of users every time a page was clicked.
https://www.sosdailynews.com/news.jspx?&articleid=BC716A1883E1C3F0C9012C06F6923D0E&sx=79

Phony Social Media Ads Pull at Heart Strings
Social media advertising is an effective way for small business to get the word out about their products. Unfortunately, the same goes for scams. BBB Scam Tracker (BBB.org/ScamTracker) is getting reports of Facebook and Instagram ads that take advantage of shoppers' goodwill by claiming to give proceeds to charity. https://www.bbb.org/article/tips/14040-bbb-tip-smart-shopping-online

Ryuk-like malware targeting law, military and finance groups
A new malware containing some similarities to Ryuk ransomware, but which acts as an information stealer targeting military, law and financial institutions has been uncovered by MalwareHunterTeam.
https://www.scmagazine.com/home/security-news/ransomware/ryuk-like-malware-targeting-law-military-and-finance-groups/?utm_source=newsletter&utm_medium=email&utm_campaign=SCUS_Newswire_20190916&hmSubId=XOjrUhr_Swg1&email_hash=305f40be59a0dcb04476bf06c7e07dc9&mpweb=1325-10198-111266

LastPass bug leaks credentials from previous sit
Password manager LastPass has released an update last week to fix a security bug that exposes credentials entered on a previously visited site. https://www.zdnet.com/article/lastpass-bug-leaks-credentials-from-previous-site/?ftag=TRE-03-10aaa6b&bhid=78480402

Filed for a Tax Extension? You're Still at Risk of Fraud
If you are one of the millions of taxpayers who have filed for a tax extension in 2019, the October 15th deadline is just around the corner. Fraudsters may have attempted to steal your identity and tax information throughout the year using a number of IRS tax fraud scams, and filing for an extension leaves you vulnerable to tax fraud for an extended amount of time. Keep an eye out for signs you are a victim of tax identity theft and take the appropriate steps to protect your tax information.
https://www.fightingidentitycrimes.com/filed-for-a-tax-extension-youre-still-at-risk-of-fraud/

Social Security is not trying to take your benefits
We've seen a new twist on the Social Security Administration (SSA) scam recently. Check out this SSA imposter robocall, which says your benefits will end. (That's not true, by the way.)
https://www.consumer.ftc.gov/blog/2019/09/social-security-not-trying-take-your-benefits?utm_source=govdelivery

Microsoft Phishing Page Sends Stolen Logins Using JavaScript
A new landing page for a Microsoft account phishing scam has been discovered that utilizes the SmtpJS service to send stolen credentials via email to the attacker. There is nothing special about the appearance of the Microsoft account phishing page shown below that was discovered by MalwareHunterTeam.
https://www.bleepingcomputer.com/news/security/microsoft-phishing-page-sends-stolen-logins-using-javascript/

****

Hints & Tips plus Security Awareness

VMSA-2019-0013 - VMware ESXi and vCenter Server updates
injection and information disclosure vulnerabilities. (CVE-2017-16544, CVE-2019-5531, CVE-2019-5532, CVE-2019-5534) https://www.vmware.com/security/advisories/VMSA-2019-0013.html, https://www.scmagazine.com/home/security-news/vulnerabilities/patches-issued-for-vmwares-vsphere-esxi-vmware-vcenter-server/?utm_source=newsletter&utm_medium=email&utm_campaign=SCUS_Newswire_20190919&hmSubId=XOjrUhr_Swg1&email_hash=305f40be59a0dcb04476bf06c7e07dc9&mpweb=1325-10272-111266

In cybersecurity speed kills, but faster saves
The 2019 Verizon Data Breach Investigations Report (DBIR) came out not long ago. There are a lot of incremental change in the 78 pages of charts and graphs, which is normal for a report of this kind. The DBIR isn't rocking anyone's boat with blockbuster findings; instead, it reveals…
https://www.scmagazine.com/home/opinion/executive-insight/in-cybersecurity-speed-kills-but-faster-saves/?utm_source=newsletter&utm_medium=email&utm_campaign=SCUS_Newswire_20190918&hmSubId=XOjrUhr_Swg1&email_hash=305f40be59a0dcb04476bf06c7e07dc9&mpweb=1325-10246-111266

Credential Stuffing: Hackers Make the Most of a Data Breach
If a data breach is big enough to make the evening news, pay attention–especially if you have an account with the breached company. Never the type to sit back after a data breach, hackers have found a new way to maximize the damage from a data theft. It's called credential stuffing and they're not afraid to use it. A California mother of a toddler found out security cameras in her home were overtaken by a hacker and she soon learned that as a result, her data had been "stuffed."
https://www.sosdailynews.com/news.jspx?&articleid=9B828E4C749A85F115CA0495FB90003E&sx=79

VMWare Updates
VMSA-2019-0013 - VMware ESXi and vCenter Server updates address command
injection and information disclosure vulnerabilities. (CVE-2017-16544, CVE-2019-5531, CVE-2019-5532, CVE-2019-5534) https://www.vmware.com/security/advisories/VMSA-2019-0013.html VMSA-2019-0014 - VMware ESXi, Workstation, Fusion, VMRC and Horizon Client updates address use-after-free and denial of service vulnerabilities. (CVE-2019-5527, CVE-2019-5535)
https://www.vmware.com/security/advisories/VMSA-2019-0014.html

Incident Response Guide
Download incident response guide and checklist available from CMU.
https://carnegieendowment.org/specialprojects/fincyber/guides/incidence-response

****

News & Views

Preliminary Draft of the NIST Privacy Framework
We've just released the Preliminary Draft of the NIST Privacy Framework: A Tool for Improving Privacy through Enterprise Risk Management for public comment! https://www.nist.gov/privacy-framework/working-drafts

FFIEC Supports Industry-Developed Cybersecurity Profile
The Federal Financial Institutions Examination Council last month highlighted a number of available standardized tools institutions can take advantage of to assess and improve their level of cybersecurity preparedness. Among the tools referenced was the Financial Services Sector Coordinating Council's Cybersecurity Profile, which was developed by ABA and other trades under the direction of the FSSCC. https://www.ffiec.gov/press/pr082819.htm?utm_campaign=RiskCyber-%2020190917s&utm_medium=email&utm_source=Eloqua

Are you aware of the Cyber Readiness Institute?
The Cyber Readiness Institute is an initiative that convenes business leaders from across sectors and geographic regions to share resources and knowledge that inform the development of free cybersecurity tools for small and medium-sized businesses. Advancing the cyber readiness of small and medium-sized businesses improves the security of global value chains. https://www.cyberreadinessinstitute.org/

How Big is your Password Haystack… and how well hidden is YOUR needle?
This is not a password strength tester, but it does a good job of explaining length vs complexity. Too often we get caught up in making the password complex. This leads to writing it down, and slow typing (allowing people to watch). https://www.grc.com/haystack.htm

****

"Ctrl -F" for The Board

More than 99% of attacks in the past year relied on human error to gain access
A new Proofpoint report underscores the need for organizations to address the human factor in their cybersecurity programs. According to the study, over 99% of cyberattacks last year relied on user interaction. In other words, the attacks could only succeed because someone did something they shouldn't have done, such as… https://www.techrepublic.com/article/more-than-99-of-attacks-in-the-past-year-relied-on-human-error-to-gain-access/

Microsoft: Cyberattacks now the top risk, say businesses
The risk of cyberattacks far outranks other threats to businesses in a new report[pdf] by Microsoft and Marsh. 79% of survey respondents stated that cyberattacks are either the top concern (22%) or a top 5 risk (57%) to their firm. In 2017 only 62% of companies mentioned cyber threats as…
https://www.zdnet.com/article/microsoft-cyberattacks-now-the-top-risk-say-businesses/

Questions
Contact FIPCO's Ken Shaurette at 800/722-3498 ext. 251 or email FIPCO IT Services for more information.

"Make Security Part of You and Your Institution's DNA!"

Threat Intelligence Newsletter: October 4, 2019

FIPCO®
IT Audit
Round Table
Discussions

If you would like to host an event, please contact: Becky Schowalter

Upcoming Threat Intelligence Peer Group Discussions
November 7 – Eau Claire

****

Alerts & Warnings

Exobot Banking Trojan Loves Botnets And Your Money
Last year, the Android banking malware called Exobot was released to the public domain. It targets banking apps with one goal in mind: Stealing money. Exobot is an Android malware first seen in 2016, and for three years and counting, hackers can easily get their mitts on its code. You can bet that during this time, Exobot has seen many upgrades that improve its stealth-like capabilities. But unlike other banking malware, Exobot uses a bot network (botnet) to spread quickly.
https://www.sosdailynews.com/news.jspx?&articleid=09C7DB2C08D89610A86B576D6D0C7BAA&sx=79

What do we know about the big, scary, exploited, IE security hole CVE-2019-1367?
Microsoft set the patching world on its ear on Monday when it released an "out of band" patch to fix a vulnerability known as CVE-2019-1367. Susan Bradley raised the alarm immediately. I chimed in a few hours later with more details. https://www.computerworld.com/article/3440523/what-do-we-know-about-the-big-scary-exploited-emergency-patched-ie-security-hole-cve-2019-1367.html

Video games, loot boxes, and your money
Play video games, or have kids who do? For most of us, that's a yes, according to a recent industry survey. It also means you might have… https://www.consumer.ftc.gov/blog/2019/09/video-games-loot-boxes-and-your-money?utm_source=govdelivery

Social Security Scams on the Rise
You may think that Social Security number (SSN) phone scams are a thing of the past, and that fraudsters have moved on to more creative ways to con individuals out of their money or steal their personal information. In fact, some scams remain more common than others because they continuously return results, and the phone call remains one of the favorite vehicles for identity thieves. It's an inexpensive way for criminals to reach out and snag someone unaware, getting them to hand over their Personally Identifiable Information (PII) without realizing who is actually on the other end of the line.
https://www.fightingidentitycrimes.com/social-security-scams-on-the-rise/

PDFex attacks can exfiltrate content from encrypted PDF documents
Researchers from Ruhr University Bochum and Münster University of Applied Sciences have devised new attacks allowing them (and potential attackers) to recover the plaintext content of encrypted PDF documents. https://www.helpnetsecurity.com/2019/10/02/content-exfiltration-encrypted-pdf/

Google Android Alert: Millions Of Phones Are Vulnerable To Hack By Israeli Surveillance Dealers
Google is warning that hundreds of millions of Android devices are vulnerable to an attack developed by NSO Group, an Israeli spyware vendor. No patch has been released for the flaw, which affects many popular phones including the Google Pixel 2, Huawei P20, Xiaomi Redmi 5A, Xiaomi Redmi Note 5…
https://www.forbes.com/sites/thomasbrewster/2019/10/04/google-android-alert-millions-of-phones-are-vulnerable-to-hack-created-by-israeli-surveillance-dealers/#44ebbdfbcca3

****

Hints & Tips plus Security Awareness

Microsoft releases out-of-band security update to fix IE zero-day & Defender bug
Microsoft publishes rare out-of-band security update to address CVE-2019-1367 and CVE-2019-1255.
https://www.zdnet.com/article/microsoft-releases-out-of-band-security-update-to-fix-ie-zero-day-defender-bug/?ftag=TRE-03-10aaa6b&bhid=78480402

Draft Special Publication (SP) 800-207, Zero Trust Architecture
Discusses the core logical components that make up a zero trust architecture (ZTA) network strategy. Zero trust refers to an evolving set of network security paradigms that narrows defenses from wide network perimeters to individuals or small groups of resources. Its focus on protecting resources rather than network segments is a response to enterprise trends that include remote users and cloud-based assets that are not located within an enterprise-owned network boundary…
https://csrc.nist.gov/publications/detail/sp/800-207/draft

Examining the Financial Consequences of a Data Breach
The likelihood of a company, big or small, facing a security incident has increased, and an estimated one in three organizations will fall victim in the next two years. As long as cybercriminals can make a profit from consumer and business data on the Dark Web, organizations will continue to be targeted by hackers. Businesses must be empowered to better protect and prepare their organization against a data breach. The consequences are costly, but the good news is the damages, and the expense, can be mitigated.
https://www.fightingidentitycrimes.com/examining-the-financial-consequences-of-a-data-breach/#more-5880

Eavesdropping smartphones: Fact or fiction?
It’s an oft-repeated tale: Someone talks with a friend about a certain thing, and then, bang, an ad for it appears on the smartphone screen. https://www.kaspersky.com/blog/smartphones-eavesdropping/27817/?utm_source=NXTsoft+Risk+Management&utm_campaign=ae7a0a864d-CYBERBYTES+SEP+ROUNDUP&utm_medium=email&utm_term=0_e91de0e00a-ae7a0a864d-124334541

New SIM card attack disclosed, similar to Simjacker
Security researchers from Ginno Security Labs have uncovered a new SMS-based attack that can be abused by cyber espionage actors to track users’ devices. The WIBattack takes advantage of vulnerabilities in the Wireless Internet Browser (WIB) app that runs on SIM cards. Earlier this month, research by AdaptiveMobile Security described… https://www.zdnet.com/article/new-sim-card-attack-disclosed-similar-to-simjacker/

New info on Facebook scams, danger texts, robocalls and podcasts
Some scams just won’t die because they’re too easy to use to dupe victims.
https://scambusters.org/facebookgold.html

Self-defense against scams
To everyone who hangs up on unwanted calls, learns about the latest scams, and checks with friends about suspicious offers: good news! People who did all those things were less likely to lose money to a scam than people who didn’t, according to Exposed to Scams: What Separates Victims from Non-Victims?, a report from the FINRA Investor Education Foundation, the BBB Institute for Marketplace Trust, and the Stanford Center on Longevity. https://www.consumer.ftc.gov/blog/2019/09/self-defense-against-scams-0?utm_source=govdelivery

How to defend your organization against browser-hijacking malware and ransomware
Network attacks more than doubled this past quarter versus the prior quarter, according to a new report from security provider WatchGuard. https://www.techrepublic.com/article/how-to-defend-your-organization-against-browser-hijacking-malware-and-ransomware/?ftag=TREa988f1c&bhid=78480402

Two-Factor Security Check Is Not Enough -- This is What You Need
One password is not enough for your safety. We already told you that. To increase security, especially on sites that have our confidential information, it's common to have to answer a secret question.
https://www.scambusters.org/twofactor.html

Top 5 tips to prevent ransomware
Ransomware continues to present a real cybersecurity threat. Tom Merritt offers five ways you can prevent it from affecting your business. https://www.techrepublic.com/article/top-5-tips-to-prevent-ransomware/?ftag=TREa988f1c&bhid=78480402

Windows out-of-band update: Microsoft's mandatory security patch is for all versions
Microsoft finally releases IE 0-day patch via Windows Update, also solving printing issues caused by original fix. https://www.zdnet.com/article/windows-out-of-band-patch-microsofts-mandatory-security-update-is-for-all-versions/?ftag=TRE-03-10aaa6b&bhid=78480402

Bought a New Gadget? Watch Out for This Con

A favorite tactic of scammers is to convince consumers to pay for services that would otherwise be free. BBB Scam Tracker (BBB.org/ScamTracker) is getting reports of a con where scam artists charge activation fees for devices that are, in fact, completely free to set up. For more ways to avoid tech support scams, see BBB.org/TechSupport. You can also find tips to help you stay alert to scammers' tactics at BBB.org/AvoidScams. For a more detailed analysis of this problem, see our full report on tech support scams: BBB.org/ScamStudies

****

News & Views

Updated National Emergency Communications Plan Release

the Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) released the updated National Emergency Communications Plan (NECP) – the Nation's roadmap to ensuring emergency communications interoperability at all levels of government. The NECP was updated to… https://www.cisa.gov/necp

Clever Ways Cybercriminals Plant Malicious Links

Are you ready for another article preaching about the risks associated with emails? Well, I will make you a deal with you. I will only talk about the stuff you probably already know for just one second and then I'll spend the rest of the time talking about some crazy new ways on how criminals are having success with malicious links in emails. I know, I know, phishing scams are old news and only your grandparents and Millennials are still falling victim, but you have to remember, criminals are not known for giving up.
https://www.sosdailynews.com/news.jspx?&articleid=8348140570CF8F6E27F14DA845603867&sx=79

Responding to email-based attacks takes over three hours, on average

Companies need 212 minutes on average to remediate a single email-based cyberattack, and 11% of firms need more than 6 hours to achieve this, a recent study by Barracuda Networks found. Since the average firm responds to about five email attacks every day, security teams spend over 17 hours each…
https://www.techrepublic.com/article/responding-to-email-based-attacks-takes-over-three-hours-on-average/

Ransomware: To pay or not to pay

The crudely written ransom notes in movies 20-30 years ago may have been replaced by more modern, digital missives – like a texted photo a la Liam Neeson's "Taken" – but the message remains the same: Pay up or else. https://www.scmagazine.com/home/security-news/ransomware/ransomware-to-pay-or-not-to-pay/?utm_source=newsletter&utm_medium=email&utm_campaign=SCUS_Newswire_20191001&hmSubId=XOjrUhr_Swg1&email_hash=305f40be59a0dcb04476bf06c7e07dc9&mpweb=1325-10478-111266

Millennials and fraud: What's the story?

Lots of people fall for scams. Is it any different for Millennials? That's what the FTC explores in its new Data Spotlight, Not what you think: Millennials and fraud.
https://www.consumer.ftc.gov/blog/2019/10/millennials-and-fraud-whats-story?utm_source=govdelivery

****

"Ctrl -F" for The Board

Moving Your Digital Security Strategy Into the 21st Century
As the author of the autobiographical book-turned-film "Catch Me If You Can," Frank W. Abagnale knows a thing or two about theft. Once a con man, he now works as a security consultant and has written multiple books on the subject. We asked him about the biggest trends in the world of digital security. https://www.futureofbusinessandtech.com/digital-security/moving-your-digital-security-strategy-into-the-21st-century/?utm_source=NXTsoft+Risk+Management&utm_campaign=ae7a0a864d-CYBERBYTES+SEP+ROUNDUP&utm_medium=email&utm_term=0_e91de0e00a-ae7a0a864d-124334541#

Weaponized Data Can Lead To Identity Theft
We get a lot of mail, even these days when so much of our communication is done electronically. Granted, most of it is not of interest to most of us and it goes directly into the trusty "File 13." However, those pre-approved credit card applications, loan re-finance offers, bank statements, and the like are all valuable to would-be cybercriminals. While perhaps none of this data on its own is of much value, it can be collated and put into a neat and tidy package. At that point… https://www.sosdailynews.com/news.jspx?&articleid=1C7B7C0E315813FF960C043735AF4168&sx=79

Business Email Scams Cost Businesses Billions
No matter the size of your office -- or whether it's a business, government, or nonprofit -- be on the lookout for phishing scams that appear to be routine emails from colleagues or the boss. A new Better Business Bureau study (BBB.org/BECStudy) reports that business email scams have cost businesses and other organizations more than $3 billion since 2016. https://www.bbb.org/globalassets/local-bbbs/council-113/media/bbb-explosion-of-bec-scams.pdf

Employee negligence can be a leading contributor to data breaches
More than two in three (68%) organizations suffered one or more data breaches in the past year, a new Ponemon report found. In over two-thirds (69%) of those breaches, paper documents or electronic devices storing sensitive data were either lost or stolen. 65% of managers fear that their company may… https://www.helpnetsecurity.com/2019/10/01/workplace-data-breaches-risk/

Questions
Contact FIPCO's Ken Shaurette at 800/722-3498 ext. 251 or email FIPCO IT Services for more information.

"Make Security Part of You and Your Institution's DNA!"

Threat Intelligence Newsletter: October 24, 2019

FIPCO® IT Audit Round Table Discussions

If you would like to host an event, please contact: Becky Schowalter

Upcoming Threat Intelligence Peer Group Discussions
November 7 – Eau Claire

****

Alerts & Warnings

IC3 Issues Alert on Ransomware
The Internet Crime Complaint Center (IC3) has released an alert on ransomware threats to U.S. businesses and organizations. Ransomware is a type of malware designed to deny access to a computer system or data until a ransom is paid. https://www.us-cert.gov/ncas/current-activity/2019/10/04/ic3-issues-alert-ransomware

Microsoft revises and re-releases patch for exploited Internet Explorer bug
Microsoft Corp. yesterday re-released a security update for CVE-2019-1367, a critical remote execution bug in Internet Explorer that has been actively exploited. The new release expands upon the previous emergency out-of-band update, which took place Sept. 23. https://www.scmagazine.com/home/network-security/microsoft-revises-and-re-releases-patch-for-exploited-internet-explorer-bug/?utm_source=newsletter&utm_medium=email&utm_campaign=SCUS_Newswire_20191007&hmSubId=XOjrUhr_Swg1&email_hash=305f40be59a0dcb04476bf06c7e07dc9&mpweb=1325-10586-111266

Vulnerabilities Exploited in Multiple VPN Applications
Cyber Security Centre released an alert on advanced persistent threat actors exploiting vulnerabilities in Virtual Private Network products from various vendors to take control of an affected system. Per the alert, vulnerabilities exist in several SSL VPN products from Pulse secure, Palo Alto and Fortinet that… https://www.ncsc.gov.uk/news/alert-vpn-vulnerabilities

Robocalls annually scam one in 10 Americans, to a loss of $9.5 billion
Computerized auto dialers deliver pre-recorded phone calls with 60 billion expected in 2019 alone. Here's how to handle robocalls... https://www.techrepublic.com/article/robocalls-annually-scam-one-in-10-americans-to-a-loss-of-9-5-billion/?ftag=TREa988f1c&bhid=78480402

Real estate investment scheme
These days, it seems like everyone wants to make money by flipping houses. There are companies out there promising to tell you how, but not all those promises are real. The most recent example is Zurixx, a real estate investment company sued by the FTC and the Utah Division of Consumer Protection (DCP). https://www.consumer.ftc.gov/blog/2019/10/zurixxs-real-estate-investment-scheme?utm_source=govdelivery

How Deepfakes Can Ruin Your Business
For those of you who are not familiar with the mechanism yet, deepfakes are an emerging technology which can credibly paste people’s faces over an existing video. The future can quickly become a scary place. Here’s why. https://heimdalsecurity.com/blog/deepfakes-can-ruin-your-business/

Flaw in iTunes for Windows Abused for Ransomware Attacks
Security researchers with Morphisec are warning the BitPaymer ransomware actors have been exploiting a security flaw in the Bonjour updater for the Windows version of Apple iTunes in order to avoid detection by anti-malware solutions on targeted systems. Bonjour contains an “unquoted path vulnerability,” that can enable threat actors to... https://www.pcmag.com/news/371261/flaw-in-itunes-for-windows-abused-for-ransomware-attacks

Scam Tempts Victims with Promises of Free Cash
Free cash you didn’t know you had? It sounds like a dream come true, but it’s actually a trick many consumers have reported to BBB.org/ScamTracker. In this scheme, con artists use the false promise of unclaimed rewards to fool consumers into giving up their credit card information.
https://www.usa.gov/unclaimed-money?utm_source=newsletter&utm_medium=email&utm_content=USA.gov/unclaimed-money&utm_campaign=scam-alert

Virtual Hard Disk Images Containing Malware Are Ignored by Windows and Antivirus Engines
This disturbing find by a CERT researcher demonstrates how attackers can encode malicious files within a Virtual Hard Disk (VHD) image that acts in the same way as a ZIP archive.
https://www.digitalmunition.me/virtual-hard-disk-images-containing-malware-are-ignored-by-windows-and-antivirus-engines/

WAV audio files are now being used to hide malicious code
Steganography malware trend moving from PNG and JPG to WAV files.
https://www.zdnet.com/article/wav-audio-files-are-now-being-used-to-hide-malicious-code/?ftag=TRE-03-10aaa6b&bhid=78480402

Millions of Fake Listings Found on Google Maps
Why defeating and removing scammers is an ongoing problem for Google Maps. Google Maps (and other mapping software) have changed our lives for the better and made shopping easier and, often, cheaper. But not always. https://scambusters.org/googlemaps.html

****

Hints & Tips plus Security Awareness

Google Adds New Password Checker to Chrome
Google will soon alert Chrome browser users of weak or compromised passwords. The checks will be in real time as Chrome users visit a password protected website. Bad passwords will trigger a red dialogue box alerting users to take action to better protect their account. https://threatpost.com/google-adds-password-checkup-feature-to-chrome-browser/148838/

What are the NIST Password Guidelines, Anyway?
Glad you asked. We put together a whitepaper dedicated entirely to helping you better understand the details behind the National Institute of Standards and Technology (NIST) password guidelines and what they mean for your institution…
https://cdn2.hubspot.net/hubfs/3791228/SpyCloud_Understanding_Latest_NIST_Guidelines.pdf?__hssc=188594551.1.1570447253104&__hstc=188594551.45cfd991c75e4894339dd5a8d7074dc7.1568746590180.1568746590180.1570447253104.2&__hsfp=472682775&hsCtaTracking=aba34f73-6b9f-416a-879a-5bbc5cd971c3%7C513947f6-fd06-42a8-bb57-7ff6c7e4be64

7 Big Factors Putting Small Businesses At Risk
Small organizations still face a long list of security threats. These threats and vulnerabilities should be top of mind. Here, we outline the attacks SMBs should be aware of and the vulnerabilities putting them at risk. https://www.darkreading.com/risk/7-big-factors-putting-small-businesses-at-risk/d/d-id/1335581?cid=em_x_dr_edt_tsnr_dr_x_x-20190716-emnurture-em1&_mc=em_x_dr_edt_tsnr_dr_x_x-20190716-emnurture-em1&elq_mid=91766&elq_cid=27291187

How to stop robocalls
Tired of interruptions? How often do you find yourself at your desk in the middle of a critical, time-sensitive project only to have your concentration shattered by the ear-piercing ring of your mobile phone?
https://store.hp.com/app/tech-takes/how-to-stop-robocalls?utm_content=S2R2C1%20mod1&jumpid=em_com_nc_ns&aoid=200936840&utm_medium=em&utm_source=sf&rid=C863DF491CF5200405D8FABC71B90538&test=&jobid=2009368&emailid=105034

****

News & Views

Cryptocurrency Users and Investors Face New Wave of Scams
Cryptocurrency scams now cost $1 billion a year, Cryptocurrency — virtual cash you can use but never see — is increasingly common both as a payment method and investment vehicle.
https://scambusters.org/cryptocurrency2.html

Let’s talk Emotet malware – Its returning Beware
You may have heard about Emotet in the news. What is it: Ancient Egyptian king, your teenage sister’s favorite emo band? We’re afraid not. https://www.malwarebytes.com/emotet/

Microsoft and NIST Team Up on Patching Guide
Microsoft and the US National Institute of Standards and Technology (NIST) have joined forces in order to create a new guide to help enterprises streamline to challenging patch management process. The initiative follows close cooperation from Microsoft with other US partners, including the Center for Internet Security, the Department of… https://www.infosecurity-magazine.com/news/microsoft-and-nist-team-up-on/

Renting a car: Factoring in the fees
Whether you're planning a weekend getaway or a cross-country road trip, a rental car may be in your future. Comparing prices online can save you a bundle, but make sure you compare the total cost — not just the advertised rate. Added fees can increase the base price dramatically.
https://www.consumer.ftc.gov/blog/2019/10/renting-car-factoring-fees?utm_source=govdelivery

What Do Not Call complaints are telling us
Have you gotten a call from an imposter, maybe someone pretending to be with the Social Security Administration, IRS, or a tech support company, this year? If so, you're not alone. Calls from imposters were the most-reported topic of unwanted calls to the FTC over the past year (FY2019). You can see our annual report on Do Not Call complaints, with state-specific data. But here are some key takeaways.
https://www.consumer.ftc.gov/blog/2019/10/what-do-not-call-complaints-are-telling-us?utm_source=govdelivery

****

"Ctrl -F" for The Board

A data breach could be game over for a brand
81% of consumers will turn away from a brand after a data breach, and 55% say they are even more likely to do this when an organization shares their private information without their consent, a new Ping Identity survey shows. Just under half (49%) of respondents said they are more…
https://www.helpnetsecurity.com/2019/10/23/data-breach-game-over/

Questions
Contact FIPCO's Ken Shaurette at 800/722-3498 ext. 251 or email FIPCO IT Services for more information.

"Make Security Part of You and Your Institution's DNA!"

Threat Intelligence Newsletter: November 5, 2019

FIPCO®
IT Audit
Round Table
Discussions

If you would like to host an event, please contact: Becky Schowalter

Upcoming Threat Intelligence Peer Group Discussions
November 7 – Eau Claire

****

Alerts & Warnings

‘Absolute scam’: Complaints about credit monitoring plans flood CFPB
Regulators have long warned the credit bureaus about deceptive marketing that causes consumers to sign up unwittingly for paid monitoring services. But the practice has persisted, according to complaint data. https://www.americanbanker.com/news/absolute-scam-complaints-about-credit-monitoring-plans-flood-cfpb?position=editorial_1&campaignname=AB_Daily_DailyBriefing_MobileTest_SplitC-10212019&utm_source=newsletter&utm_medium=email&utm_campaign=AB_Daily_DailyBriefing_MobileTest_SplitC%2B%27-%27%2B10212019&bt_ee=coETfx6ucXceNctcuxSiPlrpzhpZQ43OIkhViC8zZA9sP53JXVnlx86Yu5DLibrz&bt_ts=1571651622429

Avast breached by hackers who wanted to compromise CCleaner again
Czech security software maker Avast has suffered another malicious intrusion into their networks, but the attackers didn’t accomplish what they apparently wanted: compromise releases of the popular CCleaner utility. https://www.helpnetsecurity.com/2019/10/21/avast-breach-2019/

Beware Encrypted OneDrive Message. Don’t Be Phish Food
One of the latest email phishing campaigns is preying on the human curiosity factor. Microsoft’s OneDrive customers are receiving cryptic alerts pretending to be from their email server. It’s all about receiving an encrypted message. Humans…
https://www.sosdailynews.com/news.jspx?&articleid=13F0A6DD38B434A3E13708C0977B89E0&sx=79

SIM Swap Scams: How to Protect Yourself
If your cell phone is your go-to device for checking your email, paying your bills, or posting to social media, you're not alone. So imagine that your cell phone suddenly stops working: no data, no text messages, no phone calls. Then picture getting an unexpected notification from your cellular provider that your SIM card has been activated on a new device. What's going on? These could be signs that a scammer has pulled a SIM card swap to hijack your cell phone number. Find out how scammers pull off a SIM card swap like this and what you can do to protect yourself from a SIM card swap attack.
https://www.consumer.ftc.gov/blog/2019/10/sim-swap-scams-how-protect-yourself?utm_campaign=online-safety&utm_content=consumer-alerts&utm_medium=email&utm_source=govdelivery

Beware of Stalking Apps
The Federal Trade Commission (FTC) has released an article warning consumers of "stalking apps"—spyware that secretly monitors smartphones. These apps can… https://www.us-cert.gov/ncas/current-activity/2019/10/23/beware-stalking-apps

Fake followers: A social media hoax
Influencers, celebrities and other people with strong online followings can be, well, influential. When considering whether you want to buy something or use a service – especially when you're buying online – you might look at a person's or company's social media. A bigger following might mean something to you, maybe telling you something about their legitimacy or how good their product or service is.
https://www.consumer.ftc.gov/blog/2019/10/fake-followers-social-media-hoax?utm_source=govdelivery

Trick or Treat: Your Information Lurks in the Dark Web
This is the time of year that makes it even more fun to step away from the hustle and bustle of daily life. Scary movies, costumes, haunted houses and hayrides, trick-or-treating with family, and dreaming about all things ghosts and ghouls. If only our biggest worry was to not run out of candy on Hallows' eve!
https://www.fightingidentitycrimes.com/trick-or-treat-your-information-lurks-in-the-dark-web/

Malware Scare with Halloween Emails
If it happened at Halloween you can expect it for future holidays as well… The Emotet Trojan is celebrating Halloween by pushing out new spam templates that want to invite you to a neighborhood party. While these emails promise you a treat, in reality Emotet is tricking you into installing an infection. For those not familiar with Emotet, it is a malware infection that is spread through spam emails containing malicious documents. These documents install the Emotet Trojan on the victim's computer, which then installs other malware and uses the victim's computer to send out more spam.
https://www.bleepingcomputer.com/news/security/emotet-trojan-brings-a-malware-scare-with-halloween-emails/

Office 365 users targeted with fake voicemail alerts in suspected whaling campaign
Office 365 users at high-profile companies in a wide variety of industries are being targeted with voicemail-themed phishing emails, McAfee researchers have found.
https://www.helpnetsecurity.com/2019/10/31/office-365-voicemail-phishing/

Chinese Hackers Compromise Telecom Servers to Spy on SMS Messages
A group of Chinese hackers carrying out political espionage for Beijing has been found targeting telecommunications companies with a new piece of malware designed to spy on text messages sent or received by highly targeted individuals. Dubbed "MessageTap," the backdoor malware is a 64-bit ELF data... https://thehackernews.com/2019/10/sms-spying-malware.html?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+TheHackersNews+%28The+Hackers+News+-+Cyber+Security+Blog%29&_m=3n.009a.2104.aa0ao086k1.1b7w

****

Hints & Tips plus Security Awareness

'These 9 biggest password mistakes will get you in trouble,' warns fraud expert and ex-con artist
We think our passwords keep us safe, but that's just a fantasy. They don't protect us from hackers or maintain the privacy of our online information… https://www.cnbc.com/2019/09/24/dont-make-these-9-biggest-password-mistakes-warns-fraud-expert-and-ex-con-artist.html?utm_source=NXTsoft+Risk+Management&utm_campaign=98b0e5a936-CYBERBYTES+OCT+ROUNDUP&utm_medium=email&utm_term=0_e91de0e00a-98b0e5a936-124334541

FBI Releases Article on Defending Against E-Skimming
The Federal Bureau of Investigation (FBI) has released an article to raise awareness on e-skimming threats. E-skimming occurs when an attacker injects malicious code onto a website to capture credit or debit card data or personally identifiable information (PII). https://www.us-cert.gov/ncas/current-activity/2019/10/23/fbi-releases-article-defending-against-e-skimming

How to remove human error from the cyber risk equation
In attempting to fortify the enterprise's cyber assets, we have turned much of our attention to human error. After all, the vast majority of hackers rely upon their exploitation of employees to break through corporate defenses, anticipating that these employees will fail to "see" a threat that is hidden inside a seemingly harmless web link, email or on-screen message.
https://www.helpnetsecurity.com/2019/10/23/mitigate-human-error/

Instagram introduces new tool to help prevent phishing attacks
Sorting the genuine from the fake emails… https://www.theverge.com/2019/10/8/20904233/instagram-anti-phishing-feature-emails-security

Chrome and Firefox will now alert you about data breaches involving your accounts
Mozilla has launched Firefox 70 for Windows, Mac, and Linux with new features such as social tracking protection, a Privacy Protections report, and a native data breach notification service for your saved logins. The company — which began offering granular control over third-party tracking last October with Enhanced Tracking Protection — has now added social media… https://ctovision.com/chrome-and-firefox-will-now-alert-you-about-data-breaches-involving-your-accounts/

VMSA-2019-0019 – VMware ESXi, Workstation VMSA-2019-0018 - VMware vCenter
VMware ESXi, Workstation and Fusion updates address a denial-of-service vulnerability (CVE-2019-5536) advisory here: https://www.vmware.com/security/advisories/VMSA-2019-0019.html VMSA-2019-0018 - VMware vCenter Server Appliance updates address sensitive information disclosure vulnerability in backup and restore functions (CVE-2019-5537, CVE-2019-5538) advisory here:
https://www.vmware.com/security/advisories/VMSA-2019-0018.html

Publishers Clearing House Imposters Are Back, Again
You've won – a new car! Millions of dollars! Cash for life! The crazy thing is you don't even recall entering the contest. Con artists pose as Publishers Clearing House and play on our desire to "get rich quick."
https://info.pch.com/category/fraud/?utm_source=newsletter&utm_medium=email&utm_content=website%E2%80%99s%20fraud%20information%20center&utm_campaign=scam-alert

Free electronic credit monitoring coming soon to the military
Starting October 31, many members of the military will have access to a free tool to help spot identity theft. The nationwide credit reporting agencies – Equifax, Experian, and TransUnion – have confirmed that they will provide free electronic credit monitoring services to active duty servicemembers and National Guard members. https://www.consumer.ftc.gov/blog/2019/10/free-electronic-credit-monitoring-coming-soon-military?utm_source=govdelivery

What you can do to fend off hackers
Your personal information is valuable. That's why hackers try to steal it. This year, for National Cyber Security Awareness Month, we've got tips to help you keep your personal information from ending up in the hands of a hacker. https://www.consumer.ftc.gov/blog/2019/10/what-you-can-do-fend-hackers?utm_campaign=online-safety&utm_medium=email&utm_source=govdelivery

****

News & Views

Air Force finally retires 8-inch floppies from missile launch control system
"Solid state storage" replaces IBM Series/1's floppy drive. For that younger generation that have never seen one, there are pictures… https://arstechnica.com/information-technology/2019/10/air-force-finally-retires-8-inch-floppies-from-missile-launch-control-system/

NIST Cybersecurity Framework
The United States National Institute of Standards and Technology (NIST) has created a framework for improving critical infrastructure cybersecurity, referred to as the NIST Cybersecurity Framework. The main objective of this framework is to offer… https://blog.sucuri.net/2019/10/nist-cybersecurity-framework.html?utm_campaign=Blog%20RSS&utm_source=hs_email&utm_medium=email&utm_content=78451541&_hsenc=p2ANqtz--YowS8xWSkAL6AtWIgskvfpJ_adeZXPExLVIAHK2QwlK_Qp6RrKaTBQJKbS8NEjUGIorVfir7faer9u8sxn3egP6hiiw&_hsmi=78451541

Time for Password Expiration to Die
Password expiration is a dying concept. Essentially, it's when an organization requires their workforce to change their passwords every 60, 90 or XX number of days. And while there are several reasons behind the password expiration policy, most at this point seem obsolete… https://www.sans.org/security-awareness-training/blog/time-password-expiration-die

Scams and older consumers: Looking at the data
The FTC just sent a report to Congress called Protecting Older Consumers 2018-2019. The report suggests steps to take to help protect older consumers from fraud. But the evidence also shows a thing or two everyone else can learn from them. Check out the sometimes surprising findings in this year's report… https://www.consumer.ftc.gov/blog/2019/10/scams-and-older-consumers-looking-data?utm_source=govdelivery

Bed Bath & Beyond declares data incident
Home goods retailer Bed Bath & Beyond yesterday disclosed in a Securities & Exchange Commission 8-K filing that an unauthorized third party illegally accessed one percent of its online customers' accounts. https://www.scmagazine.com/home/security-news/cybercrime/bed-bath-beyond-declares-data-incident/?utm_source=newsletter&utm_medium=email&utm_campaign=SCUS_Newswire_20191031&hmSubId=XOjrUhr_Swg1&email_hash=305f40be59a0dcb04476bf06c7e07dc9&mpweb=1325-11018-111266

Leading domain name registrars suffered data breach
Web technology company Web.com and its subsidiaries – domain name registrars Register.com and Network Solutions – have suffered a data breach. https://www.helpnetsecurity.com/2019/10/31/domain-name-registrars-breach/

CyberDefense Magazine
https://www.yumpu.com/en/document/read/62898512/cyber-defense-emagazine-november-2019

****

"Ctrl -F" for The Board

The FBI Understands if You Pay Ransom to Cyber Hackers, But Isn't Too Pleased About It
While the FBI won't be impressed if you pay ransomware demands in order to get your systems or data back after a cyber attack, its updated ransomware guidance contemplates that this might just be the outcome of an attack anyway. The FBI's softening in this regard takes into account the reality of a cyber attack – of course businesses aren't keen to pay the criminals who caused the crisis in the first place, but without an ability to quickly and cheaply restore from backup, the business has ground to a halt...
https://www.natlawreview.com/article/fbi-understands-if-you-pay-ransom-to-cyber-hackers-isn-t-too-pleased-about-it?utm_content=f09ff0e1751817325f50c4b6371d19cc&utm_campaign=2019-10-30Cybersecurity%20Legal%20News&utm_source=Robly.com&utm_medium=email

2020 is the Year Data Gets Weaponized
A new Forrester report projects how the cyber threat landscape is likely to evolve in the coming years. The picture it paints of the near future is grim, to say the least. The researchers project that it might not be long before "evil can adopt artificial intelligence and machine learning…
https://www.nextgov.com/cybersecurity/2019/10/report-2020-year-data-gets-weaponized/160984/

Questions
Contact FIPCO's Ken Shaurette at 800/722-3498 ext. 251 or email FIPCO IT Services for more information.

"Make Security Part of You and Your Institution's DNA!"

Threat Intelligence Newsletter: November 18, 2019

FIPCO®
IT Audit
Round Table
Discussions

If you would like to host an event, please contact: Becky Schowalter

Upcoming Threat Intelligence Peer Group Discussions
None available at the current time

ABA LAUNCHES PEER GROUP FOR COMMUNITY AND MIDSIZE BANK USERS OF FSSCC CYBER PROFILE
On October 16, ABA hosted the first call of the FSSCC Cybersecurity Profile for community and midsize banks. The FSSCC Cybersecurity Profile is a NIST-based approach for IT exams and cybersecurity assessments that was developed by the financial services industry over 3 years in cooperation with the federal banking agencies and the conference of State Bank Supervisors (CSBS). The Profile is tailored to an institution's individual risk, and most community banks only complete 136 assessment questions – an assessment that is 79% shorter than the often used FFIEC CAT. To learn more about the FSSCC Cybersecurity Profile, visit https://www.aba.com/banking-topics/technology/cybersecurity/cybersecurity-profile?utm_campaign=SBA-Alliance-Newsletter-20191106.html&utm_medium=email&utm_source=Eloqua&elqTrackId=e7432a5bbce740689dd6846c6a446f74&elq=faa7fbc4d6a64578930b9724ec0f28d2&elqaid=22410&elqat=1&elqCampaignId=7036

****

Alerts & Warnings

New GlitchPOS credit card stealer malware found for sale
An experienced malware developer is hawking a new POS malware strain called GlitchPOS on crimeware forums, and even created and posted a marketing video promoting its ease of use to potential buyers. https://www.scmagazine.com/home/security-news/new-glitchpos-credit-card-stealer-malware-found-for-sale/?utm_source=newsletter&utm_medium=email&utm_campaign=SCUS_Newswire_20191104&hmSubId=XOjrUhr_Swg1&email_hash=305f40be59a0dcb04476bf06c7e07dc9&mpweb=1325-10995-111266

Sneaky purchases being made by Android keyboard app

The Android version of the popular virtual keyboard app ai.type has attempted to make over 14 million unauthorized transactions that could have cost the users US$18 million in unwanted charges, reads a report from mobile technology firm Upstream. https://www.welivesecurity.com/2019/11/05/android-keyboard-app-caught-redhanded-sneaky-purchases/

MegaCortex ransomware variant threatens data breach, alters credentials

A newly discovered variant of MegaCortex ransomware goes well beyond just encrypting victims' files — it also changes their Windows passwords and threatens to publish their stolen data if they fail to pay. https://www.scmagazine.com/home/security-news/ransomware/megacortex-ransomware-variant-threatens-data-breach-alters-credentials/?utm_source=newsletter&utm_medium=email&utm_campaign=SCUS_Newswire_20191108&hmSubId=XOjrUhr_Swg1&email_hash=305f40be59a0dcb04476bf06c7e07dc9&mpweb=1325-11143-111266

Microsoft Warns of More Harmful Windows BlueKeep Attacks, Patch Now

Research by Microsoft shows that the new campaign in which attackers exploit RDP instances vulnerable to the BlueKeep vulnerability in order to install cryptojacking malware, is likely tied to a cryptojacking campaign observed in September of this year. BlueKeep is a critical remote code execution flaw affecting RDP services on… https://www.bleepingcomputer.com/news/security/microsoft-warns-of-more-harmful-windows-bluekeep-attacks-patch-now/

Construction Companies and Vendors Targeted for BEC Fraud

The FBI last week released a Private Industry Notification warning of cyber criminals' use of subscription-based commercial databases to gather information on businesses involved in construction projects, including key contact information, and target them for business email compromise fraud. The BEC actors use the information to register domains similar to construction companies engaged in ongoing projects and email victim companies direct deposit forms and instructions that direct payments to accounts they control. For more information, including recommendations for preventing and reporting BEC fraud, https://www.aba.com/-/media/documents/cybersecurity-reports/pin/fbi-pin-110719.pdf?rev=63e175812ad74614b587f04b97f9bd61&hash=7100A54CFBD314708DA108F283E5D99B&utm_campaign=RiskCyber-%2020191111s&utm_medium=email&utm_source=Eloqua

Multiple Vulnerabilities in VMware Products Could Allow for Remote Code Execution

Multiple vulnerabilities have been discovered in VMWare Workstation, Fusion and ESXi, the most severe of which could allow for remote code execution. Successful exploitation of the most severe of these vulnerabilities could result in an attacker gaining the same privileges given to the host machine. Depending on the privileges ran with VMWare Workstation or Fusion, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than those who operate with administrative user rights. https://www.vmware.com/security/advisories/VMSA-2019-0020.html; https://www.vmware.com/security/advisories/VMSA-2019-0021.html

Small Firms Lose Thousands to Business Website Fraudsters

If you're self-employed, you probably either have a business website or have been convinced that you need one to help promote your service or product. https://scambusters.org/businesswebsite.html

Newer Intel Chips Vulnerable to Variant of ZombieLoad Attack
A new variant of the attack dubbed ZombieLoad impacts Intel CPUs that were not affected by the previously disclosed ZombieLoad method https://www.securityweek.com/newer-intel-cpus-vulnerable-variant-2-zombieload-attack

New phishing email campaign impersonates US postal service to deliver malware
A report published on Thursday by Proofpoint states that a phishing campaign that has been targeting Europe has now been attacking the United States with the goal of spreading Trojan malware onto computers. The latest phishing attacks impersonate the US Postal Service and contain a Word document that, when opened, https://www.techrepublic.com/article/new-phishing-email-campaign-impersonates-us-postal-service-to-deliver-malware/

Over 100,000 Fake Domains With Valid TLS Certificates Target Major Retailers
Venafi has uncovered over 100,000 fake domains with valid TLS certificates that mimic the domains of 20 major retailers in the US, UK, Australia, Germany and France. https://www.securityweek.com/over-100000-fake-domains-valid-tls-certificates-target-major-retailers

****

Hints & Tips plus Security Awareness

Easier Cybersecurity Assessments - Update to Cyber Security Evaluation Tool
The Cybersecurity and Infrastructure Security Agency (CISA) has released version 9.2 of its Cyber Security Evaluation Tool (CSET). CSET is a desktop software tool that guides asset owners and operators through a consistent process for evaluating control system networks as part of a comprehensive cybersecurity assessment that uses recognized government and industry standards and recommendations.
https://www.us-cert.gov/ncas/current-activity/2019/11/04/cset-version-92-now-available

Cyber Essentials
Your success depends on cyber readiness. Both depend on you. CISA's Cyber Essentials is a guide for leaders of small businesses as well as leaders of small and local government agencies to develop an actionable understanding of where to start implementing organizational cybersecurity practices. Consistent with the NIST Cybersecurity Framework and other standards, the Cyber Essentials are the starting point to cyber readiness. https://www.cisa.gov/publication/cisa-cyber-essentials

About Identifying Whether an E-mail, Phone Call, or Webpage is from Amazon
If you receive a suspicious (sometimes called phishing) correspondence, here are some tips to determine if it's an email, phone call, or webpage from Amazon.com.
https://www.amazon.com/gp/help/customer/display.html?nodeId=15835501

Experts: Don't reboot your computer after you've been infected with ransomware
Users who fall victim to ransomware should not to reboot their computers because this could make the infection worse under some conditions, Coveware CEO & Co-Founder Bill Siegel warns. Siegel explained that during the process of locating and encrypting data on an infected system, the ransomware executable sometimes "trips, or… https://www.zdnet.com/article/experts-dont-reboot-your-computer-after-youve-been-infected-with-ransomware/

10 Best Practices for a Phishing Simulations Program
Wondering how to effectively protect your organization against phishing attempts? Follow these best practices to transform your employees' behavior and build organizational resilience…
https://cybeready.com/wp-content/uploads/PhishingSimulationsPlaybook.pdf

Top 5 additional ways to fend off ransomware
In 2019, 23 city governments in Texas experienced a coordinated ransomware attack. Tom Merritt explains how they defended themselves and ways you can protect your own business.
https://www.techrepublic.com/article/top-5-additional-ways-to-fend-off-ransomware/?ftag=TREa988f1c&bhid=78480402

FS-ISAC Releases All-Hazards Framework
The FS-ISAC last week released two documents intended to guide industry response to crises and during exercises: FS-ISAC All-Hazards Framework. https://www.aba.com/-/media/documents/cybersecurity-reports/tlp-white-fsisac-all-haz-framework-101519.pdf?utm_campaign=RiskCyber-%2020191105s&utm_medium=email&utm_source=Eloqua

CISA Launches Cyber Essentials Effort
The Cybersecurity and Infrastructure Security Agency released an infographic that identifies six actions that organizations can take to reduce cyber risks:
https://www.cisa.gov/sites/default/files/publications/19_1105_cisa_CISA-Cyber-Essentials.pdf?utm_campaign=RiskCyber-%2020191111s&utm_medium=email&utm_source=Eloqua

****

News & Views

How Chat Rooms, Fake Customer Reps and Phony Surveys Steal Your Info
Remember chat rooms? At one time, they were all the rage -- online meeting places where users with similar interests could virtually gather to ask questions and discuss topics.
https://www.scambusters.org/chatroom.html

New, improved Microsoft 365 security and compliance features
Microsoft has announced a number of enhancements to help its business and enterprises customers improve security and compliance efforts. https://www.helpnetsecurity.com/2019/11/06/microsoft-365-security-and-compliance-features/

CypherCon 5.0 (2020) returns downtown Milwaukee Glitch - The threat is real
25+ security industry presentations from beginners to experts. A new challenging electronic badge created by the famous tymkrs Conference-wide gamification with groundbreaking challenges Wireless capture the flag Networking with local hackers. Specialties: Hacking 101, Industrial Control Systems, Hardware Hacking, Secure DevOps, Artificial Intelligence, Bio-hacking, Lock-picking, Safe-cracking, Vintage Computer Systems, Game Hacking, Cypher Cracking, Password Cracking, Internet of Things, Espionage secrets, Consciousness altering virtual reality, and more to be revealed. April 2/3, 2020! https://register.cyphercon.com/tickets Save $10 with code: 10off.

Twitter & Trend Micro become Victim to Malicious Insiders
The companies are the latest on a long and growing list of organizations that have fallen victim to users with legitimate access to enterprise systems and data. Two separate incidents reported this week have once again highlighted how insiders with legitimate access to systems and data can be far more dangerous to enterprise security than external attackers. https://www.darkreading.com/attacks-breaches/twitter-and-trend-micro-fall-victim-to-malicious-insiders/d/d-id/1336301

IBM Social Engineer Hacks CBS Reporters – Investigative Report
How an IBM social engineer hacked two CBS reporters--and then revealed the tricks behind her phishing and spoofing attacks. Dan Patterson, CNET and CBS News Senior Producer, and Graham Kates, CBS Investigative Reporter, volunteered to have their information hacked for research purposes. For three weeks, Stephanie "Snow" Carruthers, who is a Global Social Engineering Expert on IBM's X-Force Red team, hacked Patterson and Kates. Earlier this year, all three of them sat down in a CBS News studio to discuss the information Carruthers gathered about the two CBS reporters, which included passwords and personal details.
https://static.cbsileads.com/direct/whitepapers/IBM_social_engineer_hacked_two_CBS_reporters.pdf

Microsoft to honor California's digital privacy law all through the U.S.
In the absence of a federal digital privacy law, Microsoft has decided to comply with the requirements of California's Consumer Privacy Act (CCPA) throughout the U.S.
https://www.helpnetsecurity.com/2019/11/13/microsoft-ccpa/

****

"Ctrl -F" for The Board

EDR: The Future of Cybersecurity and Incident Response
A data breach responder can be a lot like a high-tech plumber. Just like a plumber does when a house's basement floods, data breach responders toil to identify the cause of the breach; combine forces to contain its damage; and collaborate on remediation. But unfortunately, the basement-flood/data breach analogy stops there… http://www.cybersecuritydocket.com/2015/05/08/edr-the-future-of-cybersecurity-and-incident-response/

Financial Industry – DoomsDay Cybersecurity Exercise
The financial industry just finished its annual 'doomsday' cybersecurity exercise -- here's what they imagined would happen… https://www.cnbc.com/2019/11/07/quantum-dawn-v-sifma-cyber-doomsday-exercise-adds-global-scope.html

Fighting Identity Crimes
Breach Tables keep you on top of all the data breaches tracked each month. Learn about which companies were breached, how many were affected and much more!
https://www.fightingidentitycrimes.com/breach-news-summary/?utm_campaign=Engagement.Identity_Report_C_[11-19]&utm_source=EZShield&utm_medium=email

Questions
Contact FIPCO's Ken Shaurette at 800/722-3498 ext. 251 or email FIPCO IT Services for more information.

"Make Security Part of You and Your Institution's DNA!"

Threat Intelligence Newsletter: December 4, 2019

FIPCO®
IT Audit
Round Table
Discussions

If you would like to host an event, please contact: Becky Schowalter

Upcoming Threat Intelligence Peer Group Discussions
None available at the current time

****

Alerts & Warnings

Android camera apps could be hijacked to spy on users
A vulnerability in the Google Camera app may have allowed attackers to surreptitiously take pictures and record videos even if the phone is locked or the screen is off, Checkmarx researchers have discovered.
https://www.helpnetsecurity.com/2019/11/19/android-camera-spy/

Millions of Sites Exposed by Flaw in Jetpack WordPress Plugin
WordPress website admins and owners are encouraged to immediately apply the Jetpack 7.9.1 critical security update. Vulnerabilities in Jetpack that could leave websites subject to attack have existed since Jetpack 5.1. Jetpack is a popular WordPress plugin that features security, performance and site management services including malware scanning and brute-force…
https://www.bleepingcomputer.com/news/security/millions-of-sites-exposed-by-flaw-in-jetpack-wordpress-plugin/

More Than 1300 Android Apps Steal User Data Without Permission
Data collection is big business, and the latest research findings show it's going on despite user objections. The International Computer Science Institute reports finding over 1,300 apps in Google Play Store are hiding on mobile Android devices. The apps are secretly stealing data even after being denied permission by the user. In a world where data collection is aggressive and pervasive, those who choose to deny access to their data are finding it's happening anyway…
https://www.sosdailynews.com/news.jspx?&articleid=1FDDB8CF1DEB6122A80F3E7702E6FFF9&sx=79

Celebrity Names Deliver a Nasty, Costly Shock
Do you play the celebrity name game? You know, where you follow the activities and posts of famous people. Millions of us do. If so, you must be on your guard against a possible scam. https://scambusters.org/celebrityname.html

1.2 Billion Records Found Exposed Online in a Single Server
In October of this year, security researcher Vinny Troia stumbled upon an unsecured server that was leaking a stupendous amount of personal data —1.2 billion records with a combined size of 4 terabytes. The data includes information from hundreds of millions of Facebook, Twitter, LinkedIn, Github and other social media… https://www.wired.com/story/billion-records-exposed-online/

Skimming operation creates fake 3rd-party payment processing page to phish victims
Cybercriminals have devised a card-skimming scheme that involves creating a phishing page that impersonates a retailer's third-party payment service platform (PSP).
https://www.scmagazine.com/home/security-news/cybercrime/skimming-operation-creates-fake-3rd-party-payment-processing-page-to-phish-victims/?utm_source=newsletter&utm_medium=email&utm_campaign=SCUS_Newswire_20191126&hmSubId=XOjrUhr_Swg1&email_hash=305f40be59a0dcb04476bf06c7e07dc9&mpweb=1325-11441-111266

Scams telling you to pay with Bitcoin on the rise
At first, scammers tried to get you to wire them money. Then, they demanded payment with gift cards. Now, scammers are luring people into paying them with Bitcoin – a type of digital money or cryptocurrency. Read on to learn how to spot and avoid some of the top ways scammers are trying to get you to pay with Bitcoin… https://www.consumer.ftc.gov/blog/2019/11/scams-telling-you-pay-bitcoin-rise?utm_source=govdelivery

Fake Emergency Alerts Spark Danger and Panic
What kind of emergency would make you run out of your home, perhaps without giving much thought to what you're leaving behind, maybe not even locking the door? https://scambusters.org/emergency.html

****

Hints & Tips plus Security Awareness

"Pass it On" at the holidays
Holidays often mean time with family and friends. If you're looking for conversation starters that avoid tricky topics – like who should've won the World Series – why not chat about scams? Pass it On, an FTC education campaign, gives you new ways to talk about scams and how to prevent them.
https://www.consumer.ftc.gov/blog/2019/11/pass-it-holidays?utm_source=govdelivery

Truth from Fiction: How Synthetics Will Continue to Evolve in 2020 WEBINAR from Vendor
Synthetic identities are the fastest-growing and hardest-to-detect type of financial crime in the United States. The known disparities in synthetic fraud behavior and lack of a universal tagging system for synthetic identities make it difficult for enterprises to quantify the severity of the problem, let alone solve it… https://www.brighttalk.com/webcast/16991/374852/truth-from-fiction-how-synthetics-will-continue-to-evolve-in-2020

Third-party risk management essentials
Vendor Galvanize eBook Third-party risk management essentials review at anytime with the link provided: http://www.wegalvanize.com/assets/u/ebook-third-party-risk-management-man.pdf?_ga=2.233255838.1876073821.1574873032-972627204.1574873032

Privilege Escalation - How Attackers Level Up: Dec 10 Webinar (Vendor)
Learn to detect adversaries who use privilege escalation to access sensitive systems and information… https://redcanary.com/resources/webinars/privilege-escalation/?utm_source=carbonblack&utm_medium=email&utm_term=securityweek

CIS Benchmarks Demo
Ever wonder how the CIS Benchmarks configuration guidelines can help your organization start secure and stay secure? Every month our team holds two webinars that will provide a deep-dive into the CIS Benchmarks resources. Bring your questions for one of our CIS-CAT developers and join us at one of the upcoming demos: https://www.cisecurity.org/webinar/cis-benchmarks-demo/?utm_campaign=CIS%20SecureSuite&utm_source=hs_email&utm_medium=email&utm_content=79882041&_hsenc=p2ANqtz-_acbV464mNkCg72t_gBvWIAOjt2u3arxYf3h3JStk5fpeebm0qPVPLb2qnmFMpMxnxs1sPA5vYeJsw1AaEA2mdbobtCQ&_hsmi=79884128

What Internal Auditors Need to Know About BlockChain
Companies are rapidly finding applications for blockchain technology, meaning internal auditors will need to assess those applications. To do so will require some foundational knowledge of how blockchain works and the risks associated with its use. In this week's featured article, Joseph McCafferty provides an overview of what you need to know about blockchain. https://misti.com/internal-audit-insights/what-internal-auditors-need-to-know-about-blockchain?utm_term=what%20you%20need%20to%20know%20about%20blockchain.&utm_campaign=AR_1126&utm_content=email&utm_source=Act-On+Software&utm_medium=email&cm_mmc=Act-On%20Software-_-email-_-What%20Internal%20Auditors%20Need%20to%20Know%20About%20Blockchain-_-what%20you%20need%20to%20know%20about%20blockchain

Threat Intelligence Handbook in eBook format
The brand new second edition of “The Threat Intelligence Handbook” explains how integrating intelligence across your existing security programs can empower better decisions and faster actions. https://go.recordedfuture.com/hubfs/ebooks/threat-intelligence-handbook-second-edition.pdf?utm_campaign=THR-EBO-1019&utm_source=hs_automation&utm_medium=email&utm_content=78663535&_hsenc=p2ANqtz-_4gSCJoeRaacS1dtmu8GT3g2qNaMIgtJB3XDnUfpevAH_tlxBLvibV9tbstSCj5atH0BHbQsbbZERLaEgLdxpgbEcdGQ&_hsmi=78663535

Actionable Ways to Protect Your Data and IT Systems
eGuide: "Cyber Security - Actionable Ways to Protect Your Data and IT Systems", a new vendor “Purch” sponsored publication.
https://thehackernews.tradepub.com/?p=w_pura08&w=d&email=kshaurette@fipco.com&key=yQpyYVF8rmf6PfoGhGpU&ts=76062&u=0710870891091572886476&e=a3NoYXVyZXR0ZUBmaXBjby5jb20=&secure=1&_afn=0

Privilege Escalation - How Attackers Level Up – Vendor Sponsored
Learn to detect adversaries who use privilege escalation to access sensitive systems and information.
https://redcanary.com/resources/webinars/privilege-escalation/?utm_source=carbonblack&utm_medium=email&utm_term=securityweek

****

News & Views

Ongoing Research Project Examines Application of AI to Cybersecurity:
Project Blackfin is a multi-year research effort aimed at investigating how to apply artificial intelligence (AI) innovations to cybersecurity. https://www.securityweek.com/ongoing-research-project-examines-application-ai-cybersecurity

Do third-party users follow security best practices and policies?
Many organizations across the globe fall short of effectively managing access for third-party users, exposing them to significant vulnerabilities, breaches and other security risks, One Identity reveals.
https://www.helpnetsecurity.com/2019/11/21/third-party-users-follow-security-best-practices/

Are Printers Vulnerable to Security Risks?
The topic of security has received a lot of attention lately due to the recent hacks of several high-profile companies. It seems like we can't turn on the news anymore without hearing about a recent hack of our personal or private data. Hacking attacks are on the rise these days, and criminals are looking at just about any entry point they can exploit to gain access to networks with sensitive information.
https://www.imageoneway.com/blog/printers-pose-security-risks

Cyberattack Warning As Dangerous Issues Found On Popular Office Printers: Report
It turns out that the networked printers in businesses large and small could represent a much greater danger than paper jams and extortionate ink prices. The research reported "remote vulnerabilities" in all printers tested against "various attack vectors—uncovering a large number of zero-day vulnerabilities." What that means, in short, is that those innocuous devices could be the easiest entry point for cyberattackers into small businesses, enterprises and government departments.
https://www.forbes.com/sites/zakdoffman/2019/08/09/warning-as-dangerous-cybersecurity-risks-found-in-mainstream-office-printers-report/#40ed3351140d

Fake Mobile Banking Apps Triple In Number
The mobile apps we've come to know, and love are getting riskier to use. Fake mobile apps are on the rise in a big way, especially those apps we use for banking. There's no doubt financial fraud is on the rise, and RSA's Fraud and Risk Intelligence (FRI) team discovered financial malware is up 80% between the last six months of 2018 and the first six months of 2019. The average cost of each fraudulent transaction is…
https://www.sosdailynews.com/news.jspx?&articleid=6D5A14F6EF9A4C64545906E30D1CE377&sx=79

Most Organizations Have Incomplete Vulnerability Information
A new report by Risk Based Security shows that organizations need to get their vulnerability information from more sources than just the Common Vulnerabilities and Exposures (CVE) and National Vulnerability Database (NVD) systems if they want to identify all flaws in their environment. This year alone, researchers with the firm… https://www.darkreading.com/vulnerabilities---threats/most-organizations-have-incomplete-vulnerability-information/d/d-id/1336460

Suspect Can't be Compelled to Reveal "64-character" Password, Court Rules
The Fifth Amendment to the US Constitution bars people from being forced to turn over personal passwords to police, the Pennsylvania Supreme Court ruled this week. https://arstechnica.com/tech-policy/2019/11/police-cant-force-child-porn-suspect-to-reveal-his-password-court-rules/

What Did You Say? Popular Voice Assistants Used for Fraud and Other Hacks
Siri and Alexa don't mean you any harm, but the cybercriminals who hack them certainly do. As smart devices are becoming more common in homes and workplaces, so too grow the opportunities for hackers to take advantage of them. As convenient as the Internet of Things (IoT) can be, as more devices get connected, the more options there are for bad actors to exploit them. In particular…
https://www.sosdailynews.com/news.jspx?articleid=%209423FCC0D6F3146B908C785AD0B35C8B

Hackers hold Milwaukee-based tech company's data for ransom; nursing homes affected
Russian hackers are holding hostage data from a Milwaukee-based company that provides technology services to more than 100 nursing homes across the country after the company couldn't afford a $14 million ransom demand. https://www.jsonline.com/story/news/local/2019/11/23/milwaukee-firm-falls-victim-hackers-100-plus-nursing-homes-affected/4285213002/

****

"Ctrl -F" for The Board

DO YOU KNOW CISO? (eBook)
Everything You Need to Know for a CISO to be Successful, https://secure-anchor.com/wp-content/uploads/2018/07/Secure-Anchor-ebook_Do-You-Know-CISO.pdf

The overlooked part of an infosec strategy: Cyber insurance underwriting
When a data breach or cyber attack hits the headlines one of the last things businesses are likely to consider is how cyber insurance could helped. Outside of a general awareness that cyber insurance is an easy to purchase , some companies struggle to effectively manage their processes and , security to ensure they qualify for the protection that is just as important to keeping their business operating and with a strong reputation. https://www.helpnetsecurity.com/2019/11/26/cyber-insurance-underwriting/

Questions
Contact FIPCO's Ken Shaurette at 800/722-3498 ext. 251 or email FIPCO IT Services for more information.

"Make Security Part of You and Your Institution's DNA!"

Threat Intelligence Newsletter: December 13, 2019

FIPCO®
IT Audit
Round Table
Discussions

If you would like to host an event, please contact: Becky Schowalter

Upcoming Threat Intelligence Peer Group Discussions
None available at the current time

****

Alerts & Warnings

How credential stuffing attacks work, and how to prevent them
Credential stuffing attacks pose a significant risk to consumers and businesses. Learn how they work and what you can do about them. https://www.techrepublic.com/article/how-credential-stuffing-attacks-work-and-how-to-prevent-them/?ftag=TREa988f1c&bhid=78480402

FBI Wars - Securing Smart TVs
FBI points out that "Beyond the risk that your TV manufacturer and app developers may be listening and watching you, that television can also be a gateway for hackers to come into your home". (…) "In a worst-case scenario, they can turn on your bedroom TV's camera and microphone and silently cyberstalk you." https://www.fbi.gov/contact-us/field-offices/portland/news/press-releases/tech-tuesdaysmart-tvs/?=portland-field-office

Crooks are exploiting unpatched Android flaw to drain users' bank accounts
Hackers are taking advantage of StrandHogg, a recently publicized Android vulnerability, to steal banking credentials and empty accounts. European security company Wultra warns that several banks in the Czech Republic have reported money disappearing from customer accounts. All versions of Android are affected by the vulnerability, as well as all… https://www.helpnetsecurity.com/2019/12/03/strandhogg-vulnerability/

Scammers pretend to be the FTC
Did you recently get an official FTC letter from "me"? That's in quotes because it wasn't actually from me. And the letter wasn't official, or even from the FTC at all. In fact, scammers have been faking official-looking letterhead to write scary messages to people, threatening them. But, again: it's not real. https://www.consumer.ftc.gov/blog/2019/12/scammers-pretend-be-ftc?utm_source=govdelivery

FakeUpdates hackers are back to spread ransomware

Hackers have restarted a campaign to spread ransomware in a bid to extort millions of pounds from victims with Dridex and NetSupport used to drop BitPaymer or DoppelPaymer ransomware… https://www.scmagazineuk.com/fakeupdates-hackers-back-spread-ransomware/article/1661275

2020 Census Scams Have Already Started

Simple rules that will help you spot a Census scam: https://scambusters.org/census.html

Shopping Online? Beware of This Delivery Trick

This holiday season, BBB Scam Tracker has received many reports of a new trick scammers are using to steal from online shoppers. The con artists are exploiting a PayPal policy and deceiving online shoppers into paying for goods that don't exist. https://www.bbb.org/article/scams/21097-scam-alert-tracking-code-trick-costs-holiday-shoppers?utm_source=newsletter&utm_medium=email&utm_content=Shopping%20Online%3F%20Beware%20of%20This%20Delivery%20Trick&utm_campaign=scam-alert

For more information also visit…

- Spotting PayPal Fraud: https://www.paypal.com/us/smarthelp/article/how-do-i-report-potential-fraud,-spoof-or-unauthorized-transactions-to-paypal-faq2422?utm_source=newsletter&utm_medium=email&utm_content=spotting%20and%20reporting%20PayPal%20fraud&utm_campaign=scam-alert,
- FedEx Fraud: https://www.fedex.com/en-us/trust-center/report-fraud.html?utm_source=newsletter&utm_medium=email&utm_content=FedEx%27s%20website&utm_campaign=scam-alert,
- UPS Fraud: https://www.ups.com/us/en/help-center/legal-terms-conditions/fight-fraud.page?utm_source=newsletter&utm_medium=email&utm_content=UPS%27s%20online%20resource%20center&utm_campaign=scam-alert

Snatch Team Steals Data and Hammers Orgs with Ransomware

Snatch, a ransomware variant, has been discovered in campaigns that force Windows machines to reboot into Safe Mode before beginning the encryption process. Snatch is one of multiple components of a malware constellation that is emerging in carefully orchestrated and sophisticated attacks that can feature rampant and high-risk data collection. https://threatpost.com/snatch-team-infiltrates-steals-data-ransomware/150974/

****

Hints & Tips plus Security Awareness

Battling ATO Risks Without Compromising User Experience

In a competitive marketplace in which too much customer friction can lead to brand abandonment, you have one shot to get it right. https://www.securitymagazine.com/articles/91037-battling-account-takeover-risks-without-compromising-user-experience?utm_source=hs_automation&utm_medium=email&utm_content=80219542&_hsenc=p2ANqtz-9HfG7rJgdAw7hbo3G_zk3lGoDSpncBnsASKDrtEOGtPZdDsNXv9sUAci-e5ojcor7hvJxleUiVFUe78KSP-1fSZtYOyA&_hsmi=80219542

Top tips for avoiding scams at the holidays
Now that the holiday shopping season is in full swing, scammers are shopping too, looking for people to separate from their money. We already gave you some of the FTC’s tips for happy holiday shopping, but here are some tips to help you outsmart those bah-humbug scammers and donate safely…
https://www.consumer.ftc.gov/blog/2019/12/top-tips-avoiding-scams-holidays?utm_source=govdelivery

Visa Finds New And Improved Skimming Attack Ahead Of Holiday Shopping Season
Visa recently released a security alert about a new type of skimming attack on their payment cards. Customers using Visa for online shopping found their account number, expiration date, CVV, and name and address were now in the hands of bad actors. Visa’s Payment Fraud Disruption detected the JavaScript skimmer, called Pipka, has affected at least 16 e-commerce merchants to date. Card holders need to be aware of the current risk using their Visa cards for online shopping.
https://www.sosdailynews.com/news.jspx?articleid=CA2279F12731EB8AFCD10D450EBEEDED

Don’t Wait To Update! 90.4% Of iOS Phones Ripe For Hacking
Using a personal device for work presents its own set of security challenges. Whether a smartphone, laptop or tablet, devices used in a mobile environment typically don’t have the same level of protection as those connected in an office space. Internal devices are usually overseen by an IT department that updates devices when security patches and operating system updates are available. Apple iPhone business enterprise users are now finding this out the hard way.
https://www.sosdailynews.com/news.jspx?&articleid=CA2279F12731EB8AFCD10D450EBEEDED&sx=79

Secure Your Identity This Holiday Season 2019
Identity Thieves LOVE the Holidays, The holiday season is an exciting time for consumers, and even more exciting for identity thieves. Criminals know that good cybersecurity practices are often put on the back burner when consumers are shopping for the perfect holiday gift.
https://www.fightingidentitycrimes.com/secure-your-identity-holiday-2019/?utm_source=EZShield&utm_medium=email&utm_campaign=Engagement.Fraud_Newsletter_C_[12-19]

Ransomware: How to Defend Your Companies Data
2019 has been characterized by an unprecedented series of high-profile cyberattacks in the US. City governments like Baltimore and Atlanta, and a number of smaller municipalities throughout the country fell prey to hackers . These attacks, employing ransomware, were simply a variation of, the now too common, consumer data breaches. https://www.nxtsoft.com/posts/ransomware-how-to-defend-your-company-s-vital-data-byline-luis-simonet-chief-inf?utm_campaign=Data%20Analytics%20Newsletter&utm_source=hs_email&utm_medium=email&utm_content=80266496&_hsenc=p2ANqtz-_CwIgUBxwNLD67Z0meLahRnK-h-yhi8mK7ujDVgGJF-YE2KDhJvMclwsOjJzmppjz8zWxUQb3VK6UStmUPKPdPbBJBMQ&_hsmi=80266496

Cookie Consent in CCPA
Cookies got you confused? Learn how you need to manage cookie consent prior to the CCPA 2020 deadline. In this webinar series we will cover: https://www.onetrust.com/ccpa-compliance/masterclass/cookie-consent-in-ccpa/?utm_campaign=20191205_Cookie_Webinar_Series&utm_medium=email&utm_source=Eloqua

Webinar: Understanding NIST 800-171 and 800 53r4 v r5
NIST has updated 800-53r4 to r5. to meet the information security needs of and be more generally applicable to all types of businesses including public and private sectors. The revision also addresses a broader scope of systems including industrial control systems, IoT devices, and other physical cyber devices and systems. https://zoom.us/webinar/register/WN_bsaLGzFoTZmQpOLgSrcM4g

10 Tips to Securely Configure Your New Devices
The holiday season is upon us, which means shopping for the latest gadget is in full swing. With the massive number of discounts that are available this year, it makes sense for you to buy that latest smart device, right? However, as impressive as the latest iPhone or gaming computer might be, ensuring you're able to properly secure these devices is more important than ever! Any device that connects to the internet is potentially vulnerable and could become compromised.
https://www.cisecurity.org/newsletter/10-tips-to-securely-configure-your-new-devices/

Tips for holiday gift card shopping
Gift cards are one quick way to get through your last-minute holiday shopping list. But before you give (and get) gift cards, here are a few things you need to know.
https://www.consumer.ftc.gov/blog/2019/12/tips-holiday-gift-card-shopping?utm_source=govdelivery

Security 101: What Is a Man-in-the-Middle Attack?
Specific numbers are hard to pin down on man-in-the-middle (MitM) attacks, but according to IBM's X-Force Threat Intelligence Index 2018, more than one-third of exploitation of inadvertent weaknesses involved MitM attacks. Exactly how do these hacks play out? How do criminals get in and steal information – and how are their techniques evolving? Here's a closer… https://ctovision.com/security-101-what-is-a-man-in-the-middle-attack/

****

News & Views

Hackers Target Major Brands: Disney and Macy's Breached
Fraudsters are warming up for the holidays, targeting household names through e-commerce site hacking and credential stuffing attacks. On November 19, 2019, news broke that was infiltrated by a third party, embedding malicious code into Macy's online checkout page.
https://www.fightingidentitycrimes.com/disney-macys-targeted-by-hackers/

Don't Wait To Update! 90.4% Of iOS Phones Ripe For Hacking
Using a personal device for work presents its own set of security challenges. Whether a smartphone, laptop or tablet, devices used in a mobile environment typically don't have the same level of protection as those connected in an office space. Internal devices are usually overseen by an IT department that updates devices when security patches and operating system updates are available. Apple iPhone business enterprise users are now finding this out the hard way.
https://www.sosdailynews.com/news.jspx?&articleid=B693937E2FEA1DB1EC002DE1F319282A&sx=79

Feds Crack Down on Money Mules, Warn of BEC Scams
The Justice Department stated earlier this week that it is cracking down on money mules, or middlemen who provide assistance in fraud schemes, claiming that it has stopped over 600 money mules this year. Money mules refer to people who receive money from victims and forward the proceeds to foreign…
https://threatpost.com/feds-crack-down-on-money-mules-warn-of-bec-scams/150900/

Key Steps in Satisfying Your CCPA and Other Privacy Obligations
Millions of businesses worldwide will be subject to the CCPA. Those subject to the law will be any company that has information about California residents and generates at least $25 million in annual revenue, those that have personal data on at least 50,000 California consumers, or any organization that generates more than 50 percent of its revenues from the sale of personal data.The CCPA may be more far-reaching than other privacy regulations like the GDPR and will require a different, albeit overlapping, set of capabilities to address properly… https://www.businesswire.com/news/home/20191120005130/en/New-Report-Reveals-Businesses-Prepared-Comply-California

Compromised passwords used on 44 million Microsoft accounts
44 million Microsoft Azure AD and Microsoft Services accounts were vulnerable to account hijacking due to use of compromised passwords, Microsoft has shared.
https://www.helpnetsecurity.com/2019/12/09/compromised-passwords-microsoft-accounts/

FBI Classifies FaceApp as Counterintelligence Threat, Citing Ties to Russian Intelligence - The Hill
The FBI has classified FaceApp as a counterintelligence threat due to its ties to Russia, with the FBI emphasizing that it will take action if it assesses the face-editing app is involved in election interference efforts. https://thehill.com/policy/cybersecurity/472678-fbi-classifies-faceapp-as-counterintelligence-threat-citing-ties-to

Microsoft details the most clever phishing techniques it saw in 2019
This year's most clever phishing tricks include hijacking Google search results and abusing 404 error pages.
https://www.zdnet.com/article/microsoft-details-the-most-clever-phishing-techniques-it-saw-in-2019/?ftag=TRE-03-10aaa6b&bhid=78480402

****

"Ctrl -F" for The Board

"The Changing Role of the CISO"
The expanding cybersecurity threat landscape has dramatically changed the role and impact of the CISO. This role was traditionally seen as a security enforcer; today they need to be engaged with all C-Level and the Board. Historically this role was viewed as a tech solution leader and today they need to be seen as part of the business leadership team helping to drive business outcomes, not block them.
https://zoom.us/webinar/register/WN_GBQ9kgcBRuiJmxf8Z9RgXA

Cost of data breaches in 2019: The 4 worst hits on the corporate wallet
Read Taylor Armerding list four worst data breaches of 2019 on Security Boulevard : Corporations that don’t keep their data secure may soon long for the good old days when the “only” expenses they had to worry about from a data breach were recovery costs, brand damage, lawyers’ fees, and potential class-action lawsuits. Because soon… https://ctovision.com/cost-of-data-breaches-in-2019-the-4-worst-hits-on-the-corporate-wallet/

Questions
Contact FIPCO’s Ken Shaurette at 800/722-3498 ext. 251 or email FIPCO IT Services for more information.

"Make Security Part of You and Your Institution's DNA!"

Threat Intelligence Newsletter: January 2, 2020

FIPCO®
IT Audit
Round Table
Discussions

If you would like to host an event, please contact: Becky Schowalter

Upcoming Threat Intelligence Peer Group Discussions
None available at the current time

****

Alerts & Warnings

VISA Warns of Ongoing Cyber Attacks on Gas Pump PoS Systems
VISA recently published a security alert addressing the ongoing threat of attacks on North American fuel dispenser merchants by coordinated cybercrime groups. According to the Visa Payment Fraud Disruption, three attacks on fuel dispenser merchants were observed over the summer of 2019, each with the end goal of scraping credit… https://www.bleepingcomputer.com/news/security/visa-warns-of-ongoing-cyber-attacks-on-gas-pump-pos-systems/

Getting bombarded by scam calls? You're not alone
The Social Security Administration (SSA) scam is the number one scam reported to the FTC right now. As soon as a caller threatens you, or demands you pay them with a gift card or by wiring money. It's a scam. Even if the caller ID tells you otherwise. https://www.consumer.ftc.gov/blog/2019/12/getting-bombarded-scam-calls-youre-not-alone?utm_source=govdelivery

Free Child Safety Kits May Be ID Theft Trick
Scammers have thought up a new con involving "free child safety kits." According to recent BBB Scam Tracker reports, scammers are offering these free "kits" as a way to get their hands on sensitive information that can be used to steal a child's identity. https://www.wsmv.com/news/police-warn-about-possible-child-safety-kit-scam/article_57b34a58-76a0-11e9-802c-4b8f24c8330a.html?utm_source=newsletter&utm_medium=email&utm_content=warning%20about%20the%20scam&utm_campaign=scam-alert

1 Billion Android Smartphones Can Be Infected By Watching Videos

Android mobile users with OS 7.0 through OS 9.0 running on their device need to beware of using them to watch video files. This advice comes from researchers who discovered that watching innocent videos can expose an Android OS to a hacking vulnerability. Strangely enough, a cute kitten video sent in an email or grabbed off the internet can compromise a mobile device. A device can be hacked with an innocuous, but infected video as the bait.
https://www.sosdailynews.com/news.jspx?&articleid=C2D6DBB3D6A1D9264BC0F243804FA101&sx=79

Serious Updates Released From Adobe And Microsoft-Install Patches Now

Adobe released a bunch of patches this week for several products, including Adobe Acrobat. When we say “a bunch,” we do mean many and no less than 17 of them are considered security critical and need to be addressed right away. Other products included are Photoshop, Reader, Brackets, and ColdFusion. Fourteen affect Adobe Acrobat and Reader. Not to be outdone, Microsoft also released a gaggle of patches that need to be installed right away.
https://www.sosdailynews.com/news.jspx?&articleid=25631654F5FC87B19DCF758BDF29E17A&sx=79

It’s a trap! Cybercriminals use Star Wars: Rise of Skywalker as bait

Star Wars: The Rise of Skywalker is just being released into theaters today but cybercriminals were already assembling fake websites and social media profiles to deliver malware to fans, instead of something useful like the Death Star’s plans. https://www.scmagazine.com/home/security-news/malware/its-a-trap-cybercriminals-use-star-wars-rise-of-skywalker-as-bait/?utm_source=newsletter&utm_medium=email&utm_campaign=SCUS_Newswire_20191220&hmSubId=XOjrUhr_Swg1&email_hash=305f40be59a0dcb04476bf06c7e07dc9&mpweb=1325-11699-111266

New malware dropper is a “hornet’s nest” of dangerous software

A new malware dropper, dubbed the Legion Loader, has emerged. Deep Instinct researchers discovered the malware, and have since been referring to it as a “hornet’s nest” of malware due to its ability to infect computers and install additional malware on them. Although this is common among droppers, which are…
https://www.techrepublic.com/article/new-malware-dropper-is-a-hornets-nest-of-dangerous-software/

On Guard! Top Scams Point to Need to Monitor Your Card Accounts

As we move into the third decade of the 21st century, it's a sad fact that Internet scams have become a part of everyday life. https://www.scambusters.org/topscams2019-20.html

USB Charger Scams – Beware

Travelers should avoid using public USB power charging stations in airports, hotels and other locations because they may contain dangerous malware. http://da.lacounty.gov/about/inside-LADA/juice-jacking-criminals-use-public-usb-chargers-steal-data-ff?utm_source=newsletter&utm_medium=email&utm_content=full%20alert%20from%20LA%20County%E2%80%99s%20District%20Attorney&utm_campaign=scam-alert

Scammers Send Fake FTC Letters

Scammers love to impersonate government officials. We’ve warned about con artists claiming to be from the IRS, Medicare, and even the Social Security Administration. Now, add another government agency to that list: the Federal Trade Commission. https://www.consumer.ftc.gov/blog/2019/12/scammers-pretend-be-ftc?utm_source=newsletter&utm_medium=email&utm_content=FTC%E2%80%99s%20new%20alert%20about%20this%20impersonation%20scam&utm_campaign=scam-alert

****

Hints & Tips plus Security Awareness

Implementing the NIST Framework”
Webinar with Dr. Ron Ross & Chuck Brooks. If you have any questions though, please feel free to respond to this email, follow us on social media for the latest updates, or reach out to us on the organization’s website at Cybersecurity Collaborative (https://cyberleadersunite.com/) To see the slides from the presentation visit: https://cdn2.hubspot.net/hubfs/5035658/NIST%20Webinar%20.pdf?utm_campaign=Implementing%20NIST%20Framework&utm_source=hs_email&utm_medium=email&utm_content=80760149&_hsenc=p2ANqtz-8VFOfo2iM-Z54Ot1JFuAg4w_aOnTU0Pb19nq4wEAycibhgVKFHGBGFELiECSiyHdw0kwPZ3CG7XTF9D3ofZSoSBcY4HA&_hsmi=80760149

Cyber Security Evaluation Tool 9.2 released
The Cybersecurity and Infrastructure Security Agency (CISA) has released version 9.2 of its Cyber Security Evaluation Tool (CSET). https://www.helpnetsecurity.com/2019/11/05/cyber-security-evaluation-tool-9-2/

Single Sign-On and Authentication for Beginners (Vendor whitepaper)
Combat threats without threatening productivity… https://resources.jamf.com/documents/white-papers/single-sign-on-and-authentication-for-beginners.pdf

****

News & Views

New brochure for social media influencers
Chances are you know an influencer – a person who works with a brand to recommend or endorse a product in social media. Maybe you work at a company that uses influencers or perhaps that describes you, a friend, or a family member. Then you should read a new FTC brochure: Disclosures 101 for Social Media Influencers. https://www.consumer.ftc.gov/blog/2019/11/new-brochure-social-media-influencers?utm_source=govdelivery

30 years of ransomware: How one bizarre attack laid the foundations for the malware taking over the world
In December 1989 the world was introduced to the first ever ransomware - and 30 years later ransomware attacks are now at crisis levels. https://www.zdnet.com/article/30-years-of-ransomware-how-one-bizarre-attack-laid-the-foundations-for-the-malware-taking-over-the-world/?ftag=TRE-03-10aaa6b&bhid=78480402

Open dark web database exposes info on 267 million Facebook
An unsecured database on the dark web left the personal information of more than 267 million Facebook users, mostly in the U.S., exposed. https://www.comparitech.com/blog/information-security/267-million-phone-numbers-exposed-online/

Chinese hacker group caught bypassing 2FA
Chinese state-sponsored group APT20 has been busy hacking government entities and managed service providers. https://www.zdnet.com/article/chinese-hacker-group-caught-bypassing-2fa/?ftag=TRE-03-10aaa6b&bhid=78480402

Canadian Banks Targeted in Massive Phishing Campaign
https://siliconangle.com/2019/12/23/canadian-bank-customers-targeted-newly-discovered-phishing-campaign/

Do you have data from NY Residents?
The SHIELD Act requires employers in possession of New York residents' private information to "develop, implement, and maintain reasonable safeguards to protect the security, confidentiality and integrity of the private information." ... Designating an employee or employees to coordinate the data security program. https://www.shrm.org/resourcesandtools/legal-and-compliance/state-and-local-updates/pages/new-york-shield-act.aspx

****

"Ctrl -F" for The Board

"The Changing Role of the CISO"
The expanding cybersecurity threat landscape has dramatically changed the role and impact of the CISO. This role was traditionally seen as a security enforcer; today they need to be engaged with all C-Level and the Board. Historically this role was viewed as a tech solution leader and today they need to be seen as part of the business leadership team helping to drive business outcomes, not block them.
https://zoom.us/webinar/register/WN_GBQ9kgcBRuiJmxf8Z9RgXA

Cost of data breaches in 2019: The 4 worst hits on the corporate wallet
Read Taylor Armerding list four worst data breaches of 2019 on Security Boulevard : Corporations that don’t keep their data secure may soon long for the good old days when the “only” expenses they had to worry about from a data breach were recovery costs, brand damage, lawyers’ fees, and potential class-action lawsuits. Because soon… https://ctovision.com/cost-of-data-breaches-in-2019-the-4-worst-hits-on-the-corporate-wallet/

Questions
Contact FIPCO’s Ken Shaurette at 800/722-3498 ext. 251 or email FIPCO IT Services for more information.

"Make Security Part of You and Your Institution's DNA!"

Threat Intelligence Newsletter: January 15, 2020

FIPCO®
IT Audit
Round Table
Discussions

If you would like to host an event, please contact: Becky Schowalter

Upcoming Threat Intelligence Peer Group Discussions
None available at the current time

ABA Launches Cybersecurity Profile Peer Groups for Banks of All Sizes
Inspired by the success of the Federal Services Sector Coordinating Council's Cybersecurity Profile for risk management and examination assessments, ABA is hosting bimonthly peer groups for banks of all sizes. Whether banks are in the initial stages of reviewing the profile for adoption, have fully implemented the profile or are somewhere in between, they are invited to join a peer group.

Keyed to the National Institute for Standards and Technology's Cybersecurity Framework, the profile harmonizes more than 23,000 regulations, issuances and elements of guidance, including the FFIEC IT Handbook and New York Department of Financial Services' cybersecurity rule. It was developed by the financial services industry with input from more than 150 institutions and 300 banking experts. The profile uses a 9-question survey to identify an institution's risk tier (ranging from 1 to 4) offering a customized risk-based cybersecurity assessment for each tier group. The average community bank would complete 136 assessment questions as a Tier 4 institution; a nationwide or globally active bank would complete 277 assessment questions as a Tier 1 institution. https://www.aba.com/banking-topics/technology/cybersecurity/cybersecurity-profile?utm_campaign=NEWSBYTES-20200107&utm_medium=email&utm_source=Eloqua

****

Alerts & Warnings

VISA Warns of Ongoing Cyber Attacks on Gas Pump PoS Systems

VISA recently published a security alert addressing the ongoing threat of attacks on North American fuel dispenser merchants by coordinated cybercrime groups. According to the Visa Payment Fraud Disruption, three attacks on fuel dispenser merchants were observed over the summer of 2019, each with the end goal of scraping credit… https://www.bleepingcomputer.com/news/security/visa-warns-of-ongoing-cyber-attacks-on-gas-pump-pos-systems/

Scammers Send Fake FTC Letters

Scammers love to impersonate government officials. We've warned about con artists claiming to be from the IRS, Medicare, and even the Social Security Administration. Now, add another government agency to that list: the Federal Trade Commission.
https://www.consumer.ftc.gov/blog/2019/12/scammers-pretend-be-ftc?utm_source=newsletter&utm_medium=email&utm_content=FTC%E2%80%99s%20new%20alert%20about%20this%20impersonation%20scam&utm_campaign=scam-alert

Soleimani killing will likely result in reprisal cyberattacks by Iran

The U.S. drone strike that killed Iranian General Qasem Soleimani in Baghdad is expected to generate kinetic reprisal strikes from Iran, but cyber experts say cyberattacks are also likely.
https://www.scmagazine.com/home/security-news/government-and-defense/soleimani-killing-will-likely-result-in-reprisal-cyberattacks-by-iran/?utm_source=newsletter&utm_medium=email&utm_campaign=SCUS_Newswire_20200106&hmSubId=XOjrUhr_Swg1&email_hash=305f40be59a0dcb04476bf06c7e07dc9&mpweb=1325-11768-111266

First Suleimani Attack By 'Iranian' Hackers Hits U.S., Exposing 'Noisy' New Threat

Over the weekend, threat actors defaced the website of the US Federal Depository Library Program (FDLP), in what could be the first Iranian state-sponsored cyberattack in retaliation for the US drone strike that killed Iranian military commander Maj. Gen. Qassim Suleimani at Baghdad airport last Friday. In the wake of… https://www.washingtonpost.com/nation/2020/01/06/american-government-website-defaced-iran-hackers-bloodied-trump/

Snake ransomware tries to slither its way into enterprise networks

Add yet another malicious encryption program to the expanding ranks of ransomware programs that target large enterprise networks in hopes of scoring big financial payoffs.
https://www.scmagazine.com/home/security-news/ransomware/snake-ransomware-tries-to-slither-its-way-into-enterprise-networks/?utm_source=newsletter&utm_medium=email&utm_campaign=SCUS_Newswire_20200109&hmSubId=XOjrUhr_Swg1&email_hash=305f40be59a0dcb04476bf06c7e07dc9&mpweb=1325-11833-111266

Scam Alert: You Missed Jury Duty!? Long-Running Scam Preys on Fears

Some scams just don't quit! Despite running for years, this con still successfully uses threatening calls and intimidating emails to scare people into paying up. Jury duty scams have staying power because they prey on a fear of law enforcement. https://www.bbb.org/article/scams/21259-scam-alert-you-missed-jury-duty-long-running-scam-preys-on-fears?utm_source=newsletter&utm_medium=email&utm_content=Jury%20Duty%20Scam%20Preys%20on%20Law%20Enforcement%20Fears&utm_campaign=scam-alert

****

Hints & Tips plus Security Awareness

Backing Up The Fight Against Ransomware
Organizations are facing drastic increases in ransomware attacks. A report by Malwarebytes finds a 90% increase in such attacks since 2016–that's almost ten times the amount of attacks since 2016. Many of these attacks are aimed at businesses, but this report also shows a 12% increase for consumers as well. Ransomware is very difficult to fight, as data is encrypted and locked by hackers, who then demand a ransom to restore the data. The increased ransomware attacks show one thing for sure– ransomware attacks are highly effective and profitable for hackers.
https://www.sosdailynews.com/news.jspx?&articleid=F1C853608B72A2B669AEDA6523E7E986&sx=79

ID Protection: How to Hide Yourself on the Internet
If you're like most people, you didn't realize how vulnerable you were to identity theft and how important ID protection was until it was a bit too late. https://scambusters.org/idprotection.html

Protected Voices: Social Engineering
The FBI's Protected Voices initiative provides cybersecurity recommendations to political campaigns on multiple topics, including social engineering, to help mitigate the risk of cyber influence operations targeting U.S. elections. https://www.fbi.gov/video-repository/protected-voices-social-engineering-083018.mp4/view

Protecting small business from imposters
Opening a business requires planning, elbow grease, and probably some paperwork to register your new company with your state or local government. And that's where some not-so-honest outfits may try to confuse you into thinking they're from the government and that you need to pay money to complete your registration. Their mailings look like an official bill for documents to complete your registration – and may even include what looks like a government seal. To convince you it's legit, the mailer may include your business identification number. To get you to pay, the mailer claims that you need to hurry up and pay or you could be in legal hot water. https://www.consumer.ftc.gov/blog/2020/01/protecting-small-business-imposters?utm_source=govdelivery

One simple step will help you avoid bank fraud
Bank fraud costs the financial industry billions of dollars every year, but it also impacts consumers' wallets as well as their credit record… https://scambusters.org/bankfraud.html

****

News & Views

DHS: Iran maintains a robust cyber program and can execute cyber-attacks against the US
The US Department of Home Security (DHS) on Saturday issued a rare National Terrorism Advisory System (NTAS) alert warning about possible Iranian terror and cyber campaigns in retaliation for the US drone strike that killed Iranian military commander Maj. Gen. Qassim Suleimani at Baghdad airport last Friday. Suleimani was the… https://www.zdnet.com/article/dhs-iran-maintains-a-robust-cyber-program-and-can-execute-cyber-attacks-against-the-us/

PCs still running Windows 7 will soon be significantly more at risk of ransomware
PCs still running when Windows 7 reaches end of life on the 14th of January will be significantly more at risk of ransomware, Veritas Technologies has warned. According to experts, 26% of PCs are expected to still be running the Microsoft software after support for patches and bug fixes end.
https://www.helpnetsecurity.com/2020/01/07/windows-7-ransomware/

****

"Ctrl -F" for The Board

2020 cybersecurity predictions
Cybersecurity experts take a look ahead at the threat landscape and offer predictions.
https://www.scmagazine.com/home/security-news/2020-cybersecurity-predictions/?utm_source=newsletter&utm_medium=email&utm_campaign=SCUS_Newswire_20191230&hmSubId=XOjrUhr_Swg1&email_hash=305f40be59a0dcb04476bf06c7e07dc9&mpweb=1325-11743-111266

Questions
Contact FIPCO's Ken Shaurette at 800/722-3498 ext. 251 or email FIPCO IT Services for more information.

"Make Security Part of You and Your Institution's DNA!"

Threat Intelligence Newsletter: January 29, 2020

FIPCO®
IT Audit
Round Table
Discussions

If you would like to host an event, please contact: Becky Schowalter

Upcoming Threat Intelligence Peer Group Discussions
None available at the current time

****

Alerts & Warnings

Scam Alert: Is That Really the Census Person at Your Door?
Census Bureau scams are hard to spot and easy to fall for. We all want to do our duty and participate, BUT with so many impersonators, how can you know who to trust? https://www.bbb.org/article/news-releases/19617-census-bureau-scams-count-me-out

Office 365 users: Beware of phishing emails pointing to an Office App
One of phishers' preferred methods for fooling both targets and email filters is to use legitimate services to host phishing pages. The latest example of this involves Office 365 users being directed to phishing and malicious pages hosted on Office Sway, a web application for content creation that's part of Microsoft Office. https://www.helpnetsecurity.com/2020/01/10/phishing-office-sway/

Free cruise? Try illegal robocall with an upsell.
The recorded message made it sound easy — take a phone survey and get two free tickets to go on a cruise. But, you guessed it, it wasn't that simple. The call was an illegal robocall. And those free tickets came with a catch. https://www.consumer.ftc.gov/blog/2020/01/free-cruise-try-illegal-robocall-upsell?utm_source=govdelivery

Cable Haunt' Bug Plagues Millions of Home Modems
Multiple cable modems used to provide broadband into homes have been compromised due to a critical vulnerability in their makeup that allows an attacker full remote control of the device in question. The vulnerability, named "Cable Haunt" by researchers, has been found in vendors including COMPAL, Netgear, Arris, Technicolor, and… https://threatpost.com/cable-haunt-remote-code-execution/151756/

Nemty ransomware makers may be latest to adopt data leak strategy
Following in the footsteps of Maze and Sodinokibi, it appears the makers another malicious encryption program plans to adopt the tactic of publishing data that’s been exfiltrated from targets.
https://www.scmagazine.com/home/security-news/ransomware/nemty-ransomware-makers-may-be-latest-to-adopt-data-leak-strategy/?utm_source=newsletter&utm_medium=email&utm_campaign=SCUS_Newswire_{{%27now%27|date:%27%Y%m%d%27}}&hmSubId={{contact.cms_id_encrypted}}&email_hash={{contact.email|md5}}

FTC says “Success By Health” is a pyramid scheme
Earn UNLIMITED income! Quit your job! Change your life!
Do we have your attention? Good! Are you rolling your eyes? Even better. That means you’ve heard warnings about illegal pyramid schemes that masquerade as legitimate multi-level marketing (MLM) businesses and promise life-changing income, but take your money instead.
https://www.consumer.ftc.gov/blog/2020/01/ftc-says-success-health-pyramid-scheme?utm_source=govdelivery

Beware of this sneaky phishing technique now being used in more attacks
Security company researchers warn of a large increase in conversation-hijacking attacks. Here's what they are and how to spot them. https://www.zdnet.com/article/beware-of-this-sneaky-phishing-technique-now-being-used-in-more-attacks/?ftag=TRE-03-10aaa6b&bhid=7848040

Critical WordPress Bug Leaves 320,000 Sites Open to Attack
Infinite Client and WP Time Capsule, two WordPress plugins, contain vulnerabilities that leave sites open to attack. The bug is a critical authorization complication that allows adversaries access to the backend of a site without a password. The attacker only needs the admin username for the WordPress plugins. Both of…
https://threatpost.com/wordpress-bug-leaves-sites-open-to-attack/151911/

Scammers Use Microsoft's Announcement to Trick Windows Users
Microsoft announced that they are no longer providing technical assistance, software updates, or bug fixes for Windows 7. It’s big news for users of the popular operating system. The announcement is giving scammers an opportunity to confuse Windows users into paying to update their “expiring Windows license” – whether they need to or not, according to recent BBB Scam Tracker reports.
https://www.bbb.org/article/scams/21310-scam-alert-windows-upgrade-scams-take-consumers-by-surprise?utm_source=newsletter&utm_medium=email&utm_content=Scammers%20Use%20Microsoft%27s%20Announcement%20to%20Trick%C2%A0%20Windows%20Users&utm_campaign=scam-alert

Threat Advisory: HG Updates on Citrix vulnerability - CVE-2019-19781
Over the past month, Herjavec Group has been supporting clients impacted by the vulnerability (CVE-2019-19781) impacting multiple versions of Citrix Application Delivery Controller (ADC), Citrix Gateway, and Citrix SD-WAN WANOP…
https://support.citrix.com/article/CTX267027?mkt_tok=eyJpIjoiTVRGaFpHRmpZemt4WXpGaylsInQiOiI4R1l2WVlnRnp5SEZiamZiTndUUTJCZ1M0d3hlWHhNTmhCNXZiNmJZazVHTDJhbmlGcXk4WGxiYStjaHdsY2QyaTdwNXlmZ1ZjNVAxc24zNW81UFgralQzenRWOGI4VSt1R1J0VkhsME9CdThkWjROeWFVSjRMdnViYTJ3bVZSMyJ9

Internet-enabled dash cams that allow anyone to track your GPS location in real-time
Watch out car drivers. If you have have installed a BlackVue dash cam into your vehicle you might have unwittingly made available your real-time GPS location. https://www.grahamcluley.com/blackvue-dash-cam-gps-tracking/

Android Users Beware: These Top Camera Apps May Secretly Be Spying On You
The latest warning issued to consumers downloading apps that require camera access off of the Play Store has come from the research team at CyberNews. The reports exp… https://www.forbes.com/sites/zakdoffman/2020/01/19/android-users-beware-these-top-camera-apps-may-secretly-be-spying-on-you/?ss=cybersecurity#6bc7a98d58a0

Hacker Leaks More Than 500K Telnet Credentials for IoT Devices
A hacker has published credentials for more than 500,000 servers, home routers, and other devices. The leak is being advertised as the biggest leak of Telnet passwords to date. The leak also demonstrates the lack of security protocol upheld by Telnet as well as highlights persistent vulnerabilities in their networks. https://threatpost.com/hacker-leaks-more-than-500k-telnet-credentials-for-iot-devices/152015/

FBI Warns Job Applicants of Scams Using Spoofed Company Sites
The FBI's Internet Crime Complaint Center issued a public service announcement warning Americans about scammers setting up spoofed company websites with fake job listings to target applicants. The announcement was released yesterday and states that since early 2019, victims have reported numerous examples of the type of scam to the… https://www.bleepingcomputer.com/news/security/fbi-warns-job-applicants-of-scams-using-spoofed-company-sites/

****

Hints & Tips plus Security Awareness

New year, new credit blog series
With the start of a new year, many of us want to get our finances in order. We often think about budgeting, but what about credit? To help you get a handle on credit, we've put together a four-part blog series: (1) why does your credit matter; (2) getting your credit report; (3) reading your credit report; and (4) fixing your credit report. https://www.consumer.ftc.gov/blog/2020/01/new-year-new-credit-blog-series?utm_source=govdelivery

Reading your credit report
You're getting your financial life in order in 2020. Yesterday, we explained how to get your credit report. Now that you have it, you want to know what it means. Here's where to start. https://www.consumer.ftc.gov/blog/2020/01/reading-your-credit-report?utm_source=govdelivery

Microsoft January 2020 Patch Tuesday fixes 49 security bugs
Today's patches also fix a major vulnerability in Windows' cryptographic library. https://www.zdnet.com/article/microsoft-january-2020-patch-tuesday-fixes-49-security-bugs/?ftag=TRE-03-10aaa6b&bhid=78480402

Credit repair: Fixing mistakes on your credit report
If you've been reading our new year, new credit series, then you have your credit report and learned how to read it. But what if you see mistakes? Maybe it's an account that you didn't open, an error in your name or address, or a bankruptcy that doesn't really belong to you. Here are tips on fixing your credit, while avoiding scams. https://www.consumer.ftc.gov/blog/2020/01/credit-repair-fixing-mistakes-your-credit-report?utm_source=govdelivery

What is formjacking and how can you prevent it?
Formjacking — the hijacking of online forms with malicious code — is the latest scam technique for stealing people's personal information. https://scambusters.org/formjacking.html

Don't Wait To Update; Serious Window 10 Vulnerability Could Allow Man-In-The-Middle Attack
Indeed, Microsoft "Patch Tuesday" has come and gone this month, but don't just brush it aside as business as usual. This week, that group of fixes contains a solution to a vulnerability in Windows 10 that could allow someone to exploit it and perform "man-in-the-middle" attacks. It was reported to Microsoft by the National Security Agency (NSA) that has been given kudos for reporting it to Microsoft rather than creating its own exploit using it.
https://www.sosdailynews.com/news.jspx?&articleid=97DE655029C85C802952B589956D92F9&sx=79

Micropatch simulates workaround for recent zero-day IE flaw, removes negative side effects
ACROS Security has released a micropatch that implements the workaround for a recently revealed actively exploited zero-day RCE flaw affecting Internet Explorer (CVE-2020-0674).
https://www.helpnetsecurity.com/2020/01/21/micropatch-cve-2020-0674/

****

News & Views

Companies increasingly reporting attacks attributed to foreign governments (Does your Cyber insurance cover acts of war or terrorism?)
More than one in four security managers attribute attacks against their organization to cyberwarfare or nation-state activity, according to Radware. https://www.helpnetsecurity.com/2020/01/15/attacks-attributed-to-foreign-governments/

FBI: Nation-state actors have breached two US municipalities
The SharePoint CVE-2019-0604 vulnerability has been one of the most targeted security flaws.
https://www.zdnet.com/article/fbi-nation-state-actors-have-breached-two-us-municipalities/?ftag=TRE-03-10aaa6b&bhid=78480402

Why 2019 Was Actually A Secret Success For Blockchain In Financial Services
Now, as most of the 2020 blockchain predictions have settled in and the year is near its end, let's review the highlights in the enterprise blockchain and digital assets space, esp…
https://www.forbes.com/sites/biserdimitrov/2020/12/30/why-2019-was-actually-a-secret-success-for-blockchain-in-financial-services/#428cf9d21280

Have you ordered your NCPW materials yet?
March is right around the corner, and you know what that means….it's almost time for National Consumer Protection Week (NCPW)! This year, NCPW is March 1-7, 2020. That's just over a month away, so now's the time to jump into planning. https://www.consumer.ftc.gov/blog/2020/01/have-you-ordered-your-ncpw-materials-yet?utm_source=govdelivery

Phishing campaign leads to UPS Store data breach
In a data breach notification letter to customers, The UPS Store has disclosed that an unauthorized party successfully devised a phishing scheme to gain entry into the email accounts of numerous store locations.
https://www.scmagazine.com/home/security-news/data-breach/phishing-campaign-leads-to-ups-store-data-breach/?utm_source=newsletter&utm_medium=email&utm_campaign=SCUS_Newswire_{{%27now%27|date:%27%Y%m%d%27}}&hmSubId={{contact.cms_id_encrypted}}&email_hash={{contact.email|md5}}

****

"Ctrl -F" for The Board

The top frauds of 2019
Each year, the FTC takes a hard look at the number of reports people make to our Consumer Sentinel Network. In fact, during 2019, we got more than 3.2 million reports to the FTC from you. We've read what you've said, and crunched the numbers. Here's what you told us in 2019…
https://www.consumer.ftc.gov/blog/2020/01/top-frauds-2019?utm_source=govdelivery

Questions
Contact FIPCO's Ken Shaurette at 800/722-3498 ext. 251 or email FIPCO IT Services for more information.

"Make Security Part of You and Your Institution's DNA!"

Threat Intelligence Newsletter: February 7, 2020

FIPCO®
IT Audit
Round Table
Discussions

If you would like to host an event, please contact: [Becky Schowalter]

Upcoming Threat Intelligence Peer Group Discussions
None available at the current time

****

Alerts & Warnings

Scam Alert: Is That Really the Census Person at Your Door?
Census Bureau scams are hard to spot and easy to fall for. We all want to do our duty and participate, BUT with so many impersonators, how can you know who to trust? https://www.bbb.org/article/news-releases/19617-census-bureau-scams-count-me-out

The Chrome Web Store is currently facing a wave of fraudulent transactions
The Google security team has indefinitely blocked the publishing of any commercial Chrome extensions due to a recent surge in the number of paid extensions engaging in fraudulent transactions through the Chrome Web Store. The transactions began to spike earlier this month, and Google engineers described the influx as happening… https://www.zdnet.com/article/the-chrome-web-store-is-currently-facing-a-wave-of-fraudulent-transactions/

Slow Browser? It May Have Been Hijacked By Malware
Before calling your internet provider to complain about a slow browser think about this: It's no secret malware loves to hide in all kinds of things like adware, spyware, scareware, and fake browser updates. Finding your browser is not only slow, but also acting strangely is a sign something isn't quite right. If after going through the internet provider's standard toolbox for troubleshooting doesn't help, it's time to think about malware… https://www.komando.com/privacy/popups-blocking-videos-it-could-be-a-nasty-malware/480920/

Cyberattacks against endpoints rising, reaching $9 million per attack in 2019
Attacks against endpoints have become more costly, up more than $2 million since 2018. https://www.techrepublic.com/article/cyberattacks-against-endpoints-rising-reaching-9-million-per-attack-in-2019/

Windows update message installs ransomware on victims' PCs
Microsoft never sends out email notifications of a Windows update so, if you get one, you can be sure it's a fake. https://scambusters.org/windowsupdate.html

U.S. Finance Sector Hit with Targeted Backdoor Campaign
The United States's financial sector experienced an increase in cyberattacks last month, the majority of which delivered a powerful backdoor named Minebridge. Minebridge gives cyberattackers advantage over a victim's machine, allowing them to have full access to all functions. The attack chain employed in the US financial services sector included… https://threatpost.com/us-finance-sector-targeted-backdoor-campaign/152634/

Making mobile payments? Protect yourself from scams.
Using mobile payment apps like CashApp, Venmo, or Zelle can be a convenient way to get quick cash to your family and friends. But remember the first rule of sending money, whether you're using an app or money wiring service: Be sure you know who's on the receiving end. Otherwise, you might lose the money you sent — and then some. https://www.consumer.ftc.gov/blog/2020/02/making-mobile-payments-protect-yourself-scams?utm_campaign=online-safety&utm_content=mobile-payment-apps&utm_medium=email&utm_source=govdelivery

New ransomware doesn't just encrypt data. It also meddles with critical infrastructure
Ekans represents a "new and deeply concerning" evolution in malware targeting control systems. https://arstechnica.com/information-technology/2020/02/new-ransomware-intentionally-meddles-with-critical-infrastructure/

Scam Alert: Watch Out for Tax ID Theft
BY BETTER BUSINESS BUREAU – It is the Season to be more aware!!
The U.S. tax season is here, and so are the scammers. Con artists are using the Social Security numbers of unsuspecting Americans to file phony tax returns and steal their refunds. In honor of the Federal Trade Commission's Tax Identity Theft Awareness Week, be on the lookout for this and other tax season scams. https://www.bbb.org/article/news-releases/16949-bbb-tip-tax-identity-theft

****

Hints & Tips plus Security Awareness

Bots vs. Bad actors: How to spot the difference and protect yourself
Hackers. Bots. Trolls. Cybercriminals. We've all heard these terms used – sometimes interchangeably – to describe alleged perpetrators of cyberattacks and other…
https://www.scmagazine.com/home/opinion/executive-insight/bots-vs-bad-actors-how-to-spot-the-difference-and-protect-yourself/?utm_source=newsletter&utm_medium=email&utm_campaign=SCUS_Newswire_{{%27now%27|date:%27%Y%m%d%27}}&hmSubId={{contact.cms_id_encrypted}}&email_hash={{contact.email|md5}}&oly_enc_id=5134E7768601H7Z

Intel Is Patching the Patch for the Patch for Its 'Zombieload' Flaw
Over the past few years, security researchers have found hundreds of vulnerabilities that allow a hacker to trick Intel's microprocessors into unauthorized data access. As the flaws have been exposed, employees have rushed to release patches for them. However, Intel has failed to patch the underlying problem behind a serious… https://www.wired.com/story/intel-zombieload-third-patch-speculative-execution/

What to do when you can't cancel a subscription
If you haven't fallen victim to an online subscription scam, you're either lucky or you know how to steer clear of the crooks behind them. https://scambusters.org/subscription.html

FTC videos: Rated "P" for People
Videos from the Federal Trade Commission offer practical, useful, and memorable messages that can save you money, time, and aggravation. And they're free. And now, for your viewing pleasure... a selection of the FTC's top releases. https://www.consumer.ftc.gov/blog/2020/02/ftc-videos-rated-p-people?utm_source=govdelivery

****

News & Views

In Financial Services
Now, as most of the 2020 blockchain predictions have settled in and the year is near its end, let's review the highlights in the enterprise blockchain and digital assets space, esp…
https://www.forbes.com/sites/biserdimitrov/2020/12/30/why-2019-was-actually-a-secret-success-for-blockchain-in-financial-services/#428cf9d21280

Coronavirus Campaigns Spread Emotet, Malware
Hackers are capitalizing on the public fear of the coronavirus, using headlines related to the global health emergency to spread malicious files, including the notorious Emotet malware. The botnet driven emails are using the coronavirus as a theme to target populations, luring victims into clicking on bad links. The emails… https://threatpost.com/coronavirus-propagate-emotet/152404/

LendEDU deceptively promoted financial products
Online comparison sites can be great ways to check out products you want to try or buy. But are those reviews and rankings objective, accurate, and unbiased? It's a question to always ask, and here's why: Some online product reviews and rankings might be influenced by advertiser payments.
https://www.consumer.ftc.gov/blog/2020/02/lendedu-deceptively-promoted-financial-products?utm_source=govdelivery

Cyber Defense Magazine
Learn from the experts, cybersecurity best practices, Find out about upcoming information security related conferences, expos and trade shows. https://www.yumpu.com/en/document/read/63055792/cyber-defense-emagazine-february-2020-edition

****

"Ctrl -F" for The Board

2020 SonicWall Cyber Threat Report | Cyber Threat Intelligence
Cyber threat data and intelligence that unmasks the threats that target global enterprises, businesses, governments a... https://www.sonicwall.com/resources/2020-cyber-threat-report-pdf/

Questions
Contact FIPCO's Ken Shaurette at 800/722-3498 ext. 251 or email FIPCO IT Services for more information.

"Make Security Part of You and Your Institution's DNA!"

Threat Intelligence Newsletter: March 6, 2020

FIPCO®
IT Audit
Round Table
Discussions

If you would like to host an event, please contact: Becky Schowalter

Upcoming Threat Intelligence Peer Group Discussions
None available at the current time

****

Alerts & Warnings

FTC: The bottom-line on fake checks scams
If someone you don't know sends you a check and asks for money back, that's a scam. Over the last several years, the number of fake check scams reported to the FTC has steadily increased, and so have the dollars lost. https://www.consumer.ftc.gov/blog/2020/02/ftc-bottom-line-fake-checks-scams?utm_source=govdelivery

Coronavirus: Scammers follow the headlines
Scammers are taking advantage of fears surrounding the Coronavirus. They're setting up websites to sell bogus products, and using fake emails, texts, and social media posts as a ruse to take your money and get your personal information. Here are some tips to help you keep the scammers at bay. https://www.consumer.ftc.gov/blog/2020/02/coronavirus-scammers-follow-headlines?utm_source=govdelivery

Exposing Tax Scams
The beginning of a new year marks the beginning of tax season. For most people, this is a mad scramble of W-2s, W-4s, 1098s, 1099s and more. For employees and business owners alike, tax season can be stressful and time-consuming. Criminals are ver…. https://blog.nxtsoft.com/exposing-tax-scams?utm_campaign=Data%20Security%20Newsletter&utm_source=hs_email&utm_medium=email&utm_content=83199455&_hsenc=p2ANqtz--T9HY0lCua9cnD3BpzSEEHUhS5FaYQ0J8-qGmBFSDVyst_YjJZjRWBeFJk6GyeTUhu8mTzvNcwSUWUVL5Los49yDKOIQ&_hsmi=83199456

Emotet Now Hacks Nearby Wi-Fi Networks to Spread Like a Worm
Cybersecurity experts have recently discovered a new Emotet malware sample that has the ability to spread to insecure WiFi networks located nearby to an infected device. The malware then attempts to infect the devices connected to these WiFi networks, resulting in a rapid escalation of Emotet's spread. This new development… https://threatpost.com/emotet-now-hacks-nearby-wi-fi-networks-to-spread-like-a-worm/152725/

Emotet: Crimeware you need to be aware of
According to the U.S. Department of Homeland Security, Emotet continues to be among the most costly and destructive malware threats affecting state, local, and territorial governments and its impact is felt across both the private and public sectors. https://www.helpnetsecurity.com/2020/02/12/emotet-malware/

Bogus advertisement offers target small businesses
Lots of small businesses need to advertise locally. So, if someone told your business that it could advertise through well-known local firms or organizations, that might interest you. But unfortunately, sometimes the results are not as promised. https://www.consumer.ftc.gov/blog/2020/02/bogus-advertisement-offers-target-small-businesses?utm_source=govdelivery

Feds expose North Korean hacking campaign
Federal law enforcement identified a North Korean hacking campaign targeting financial institutions, among other private-sector industries. https://www.us-cert.gov/northkorea

Spear-Phishing Attacks Targeting Office 365 Users, SaaS Applications
Over the course of the last 15 years, cyber threats have gone from urban myths and corporate ghost stories to as mainstream as carjackings and burglaries. There isn't a business owner of a small restaurant chain or a CEO of a Fortune 500 company who doesn't think about the fallout of being breached.
https://blog.sonicwall.com/en-us/2020/01/spear-phishing-attacks-targeting-office-365-users-saas-applications/

Nasty Android malware reinfects
Android malware known as xHelper reinfects devices even after factory resets. The malware dropper Trojan was first noticed last spring. Theories that the reinfections came from pre-installed malware or from the Google Play store were disproven. Researchers at Malwarebytes, along with a savvy Android user, discovered that the reinfection came from folders that were not removed even after a factory reset. Malwarebytes has instructions for removing the folders.
https://arstechnica.com/information-technology/2020/02/researcher-says-nasty-android-infection-survived-a-factory-reset/?_cldee=a3NoYXVyZXR0ZUBmaXBjby5jb20%3d&recipientid=contact-32b1bfff1f65e511810cc4346bb588f0-8720cbc21eec46ea8666c7d73e1f2492&utm_source=ClickDimensions&utm_medium=email&utm_campaign=WipfliSecurity%20Weekly&esid=a5318144-6352-ea11-a812-000d3a579c34

Android Ad Blocker Bombards Users With Ads
Does anyone really like ads popping-up on their devices? For those of us who don't like them, beware: The Android app that is supposed to block such ads, called "Ads Blocker" is on the loose. Rather than blocking pesky ads, it actually makes them even more frequent. Those who download the app to reduce advertising find themselves on the wrong end of the very thing they wanted to stop. And it's not just full screen ads that show up that will drive you nuts…
https://www.sosdailynews.com/news.jspx?&articleid=779CC0F2553E73D1FCC37AC5C907B018&sx=79

SMS Phishing Campaign Targets Mobile Bank App Users in North America
A dozen North American banks have been targeted in a mobile phishing campaign that has already victimized 4,000 victims through deploying an automated SMS tool. The tool sends out fraudulent security text messages to mobile phone users and has targeted customers of banks like Chase, TD Bank, and Royal Bank… https://threatpost.com/sms-phishing-bank-app-north-america/152896/

Is that text message about your FedEx package really a scam?
You may be skeptical when someone you don't know sends you a text message you didn't expect and it tells you to click on a link. Maybe that little voice in your head starts talking to you. I know mine does. It says, "Hmm, this could be a scam. Maybe someone wants to steal my personal information. Or get me to pay for something." I guess that's why scammers come up with new stories all the time, like a FedEx package tracking scam we're hearing about. Here's how it works…
https://www.consumer.ftc.gov/blog/2020/02/text-message-about-your-fedex-package-really-scam?utm_campaign=online-safety&utm_content=package-tracking&utm_medium=email&utm_source=govdelivery

How Your Car Stickers Can Land You in Trouble
Car stickers can play a role in identity theft, Car stickers seem innocent enough, don't they?, But they may not be, if they give others information about you or your kids… https://scambusters.org/carsticker.html

****

Hints & Tips plus Security Awareness

Microsoft Addresses Active Attacks, Air-Gap Danger with 99 Patches
There are 12 critical and five previously disclosed bugs in the February 2020 Patch Tuesday Update. Microsoft has issued one of its largest Patch Tuesday updates for the shortest month of the year, addressing 99 security vulnerabilities across a range of products. Twelve of the bugs are listed as critical – and the rest are rated as being important. https://threatpost.com/microsoft-active-attacks-air-gap-99-patches/152807/

Adobe release updates for Reader, Flash Player and more
Description: Adobe disclosed 42 new vulnerabilities this week as part of its monthly security update, 35 of which are considered critical. These updates include Acrobat Reader, Flash Player and other Adobe products. Most notable are two bugs in Flash Player and Adobe Framemaker that could allow an attacker to execute arbitrary code on the victim machine. https://threatpost.com/adobe-security-update-critical-flash-framemaker-flaws/152782/

Find Out if You're a Tax Identity Theft Victim
How to avoid or respond to tax identity theft. https://scambusters.org/taxidentitytheft.html

Stay Informed on the Coronavirus 2019-nCoV
The centers for Disease controls is strongly encouraging communities to stay alert. www.cdc.gov/ncov

It's easier to spot an impostor if you know what you're looking for
Impostor scams start innocently enough, as an email or call from a familiar name such as a government agency, well-known company, or even a family member. They count on your trust to help them steal your money and personal information. https://www.bbb.org/scamtracker/us/
https://www.aarp.org/money/scams-fraud/tracking-map/?CMP=EMC-MIM-DIS-OTH-FRAUD-Impostor_ACE_Light_C1-861101-1267801-02172020_Map_BTN-4375872-&encparam=a2kbABDTs8aki3KrMaMg9C/8GD2Ftx+E8fs/PojRO+U=

NIST Cyber Security Framework Explained
Presentation on the NIST CSF…
https://www.rsaconference.com/writable/files/rsac_cforum_webinar_v5_ps.pdf

****

News & Views

1/5 3rd Bank Slammed for "Vague and Deceptive" Breach Disclosure
American bank Fifth Third has come under fire for sending customers a cryptic breach disclosure letter judged to be "vague and deceptive" by a consumer group. https://www.infosecurity-magazine.com/news/us-bank-slammed-for-breach/

It's Not Just Celebrities Who Should Worry About Their Social Media Accounts Getting Hacked
The fame, the fortune, the accolades–all are part of celebrity status. But the price tag of stardom sometimes includes unwanted attention from critics, stalkers, and now social media hackers. Public attacks on Twitter, Facebook, and other social media sites have also…
https://www.sosdailynews.com/news.jspx?&articleid=2A497977AEC8AE6B0D53E928222D6224&sx=79

Apple joins FIDO Alliance, commits to getting rid of passwords
Apple announced that it plans to join the FIDO Alliance in an effort to kill off passwords. Passwords have long been a weak link in the cybersecurity industry, with 81% of all hacking based security breaches traced back to poor passwords. FIDO Alliance aims to replace password-only logins with secure
https://www.zdnet.com/article/apple-joins-fido-alliance-commits-to-getting-rid-of-passwords/

90% of UK Data Breaches Due to Human Error in 2019
Human error caused 90% of cyber data breaches in 2019, according to a CybSafe analysis of data from the UK Information Commissioner's Office (ICO). According to the cybersecurity awareness and data analysis firm, nine out of 10 of the 2376 cyber-breaches reported to the ICO last year were caused by mistakes made by end-users. This marked… https://www.infosecurity-magazine.com/news/90-data-breaches-human-error/

500 Malicious Chrome Extensions Impact Millions of Users
Duo Security released an analysis on Thursday claiming that over 500 malicious Chrome extensions were secretly collecting browser data and redirecting users to websites containing malware. Researchers at Duo Security stated that the extensions have since been removed from Google's Chrome Web Store, but that they were previously downloaded millions. https://threatpost.com/500-malicious-chrome-extensions-millions/152918/

****

"Ctrl -F" for The Board

(In)Secure Magazine
Security for 2020 and Beyond; Hardware hacks: The next generation of cybercrime
https://img2.helpnetsecurity.com/dl/insecure/INSECURE-Mag-65.pdf

Questions
Contact FIPCO’s Ken Shaurette at 800/722-3498 ext. 251 or email FIPCO IT Services for more information.

"Make Security Part of You and Your Institution's DNA!"

Threat Intelligence Newsletter: March 17, 2020

FIPCO®
IT Audit
Round Table
Discussions

If you would like to host an event, please contact: Becky Schowalter

Upcoming Threat Intelligence Peer Group Discussions
None available at the current time

As Outbreak Worsens, Don't Fall for Face Mask Cons
NOTE: BBB continues to monitor changes in the marketplace in reaction to COVID-19 (coronavirus). Please go to https://www.bbb.org/council/coronavirus/ for the latest information.

****

Alerts & Warnings

Attackers look around for Microsoft Exchange servers vulnerable to CVE-2020-0688
Just a day after the publication of technical details about the vulnerability, adversaries began to actively scan the Internet in search of vulnerable Microsoft Exchange Servers. CVE-2020-0688 is a remote code execution flaw, and the latest Microsoft Patch Tuesday… https://www.peerlyst.com/posts/attackers-look-around-for-microsoft-exchange-servers-vulnerable-to-cve-2020-0688-soc-prime?trk=search_page_search_result&utm_source=hs_email&utm_medium=email&utm_content=84034689&_hsenc=p2ANqtz-82Js6WJRf0uQnV6hkPMf3ro7ynJLn2Fex47AJ4JwoTsHjR1X2SEzO9l9edIfpuJB6v9Nhf8MF5OcZFDpgfuU4UyLHAVw&_hsmi=84034689

Android banking trojan steals Google two-factor authentication codes
New version of Cerberus is not yet for sale on hacking forums...
https://www.techradar.com/news/android-banking-trojan-steals-google-two-factor-authentication-codes?utm_source=hs_email&utm_medium=email&utm_content=84034689&_hsenc=p2ANqtz-82Js6WJRf0uQnV6hkPMf3ro7ynJLn2Fex47AJ4JwoTsHjR1X2SEzO9l9edIfpuJB6v9Nhf8MF5OcZFDpgfuU4UyLHAVw&_hsmi=84034689

Billions of Devices Open to Wi-Fi Eavesdropping Attacks
A serious vulnerability in Wi-Fi chips manufactured by Broadcom and Cypress has been discovered. The flaw reveals communications from devices from Amazon, Google, Samsung, and others, allowing attackers to eavesdrop on Wi-Fi communications. The bug breaks the WPA2-Personal and WPA-2 Enterprise security protocols as it stems from the use of… https://threatpost.com/billions-of-devices-wifi-encryption-hack/153267/

TrickBot Adds ActiveX Control, Hides Dropper in Images
The TrickBot banking trojan has recently increased its capabilities, adding Windows 10 ActiveX control. This new feature gives the banking trojan the ability to execute malicious macros that are hidden in documents. A researcher at Morphisec Labs stated that in the past few weeks, two dozen documents have emerged that https://threatpost.com/trickbot-activex-control-dropper/153370/

'Malware-free' attacks now most popular tactic amongst cybercriminals
Malware-free or fileless techniques accounted for 51% of attacks last year, compared to 40% the year before, as hackers turn to stolen credentials to breach corporate networks, reveals CrowdStrike's latest threat report. https://www.zdnet.com/article/malware-free-attacks-now-most-popular-tactic-amongst-cybercriminals/

Vulnerability allows attackers to register malicious lookalikes of legitimate web domains
Cybercriminals were able to register malicious generic top-level domains (gTLDs) and subdomains imitating legitimate, prominent sites due to Verisign and several IaaS services allow…
https://www.helpnetsecurity.com/2020/03/05/register-malicious-domains/

FFIEC Press Release Alert
Pandemic Preparedness Guidance, https://www.ffiec.gov/press/pr030620.htm

Hackers are getting hacked via trojanized hacking tools
Someone has been trojanizing a wide variety of hacking tools to compromise the machines of hackers who want to use the tools for free, Cybereason researcher Amit Serper has revealed.
https://www.helpnetsecurity.com/2020/03/10/trojanized-hacking-tools/

Don't Get Hooked Updating That Security Certificate
As if it isn't difficult enough to determine if a website is legitimate or not, a new phishing technique is going to be keeping us all on our toes now while watching for this new hook. Cybercriminals are trying to trick website visitors into believing a security certificate for a site needs to be updated before going forward with viewing the site contents. What's behind that click could Instead be a nasty surprise waiting--one of two malware variants that leave a door open on your device.
https://www.sosdailynews.com/news.jspx?&articleid=DE5FA20C3F277547AD0EE063DEF1066E&sx=79

Tricky RIPlace Ransomware Evades AV Efforts
Since its discovery last year, the ransomware called RIPlace has been getting away with the goods and not getting caught. To date, the biggest targets for the ransomware are Microsoft Windows 10 and a number of other security software providers. It took a while for RIPlace to get the attention it's getting now, and anyone running Windows XP and newer can catch the malware infection. A recent survey by Spiceworks finds that 33% of businesses are still using Windows XP on at least one computer…
https://www.sosdailynews.com/news.jspx?&articleid=D5CC6FD871ABBC3F9E5104D360FBB1C0&sx=79

Intricate Phishing Scam Uses Support Chatbot to 'Assist' Victims
A recent phishing scam is targeting consumers by utilizing a malicious customer service chatbot function that steals victims' information by prompting them to fill out various forms including credit card numbers and bank account information. The campaign was discovered by MalwareHunterTeam and is targeting Russian citizens. The threat actors are… https://www.bleepingcomputer.com/news/security/intricate-phishing-scam-uses-support-chatbot-to-assist-victims/

Cookiethief: a cookie-stealing Trojan for Android
We recently discovered a new strain of Android malware. The Trojan (detected as: Trojan-Spy.AndroidOS.Cookiethief) turned out to be quite simple. Its main task was to… https://securelist.com/cookiethief/96332/

State-sponsored hackers are now using coronavirus lures to infect their targets
Chinese, North Korean, and Russian government cyberspies caught using COVID-19-themed emails to infect victims with malware. https://www.zdnet.com/article/state-sponsored-hackers-are-now-using-coronavirus-lures-to-infect-their-targets/?ftag=TRE-03-10aaa6b&bhid=78480402

Malware Campaign Feeds on Coronavirus Fears
Criminals are leveraging the COVID-19 epidemic to spread malware through a "Coronavirus Map" app that actually delivers a strain of the data stealing malware AZORult.
https://blog.reasonsecurity.com/2020/03/09/covid-19-info-stealer-the-map-of-threats-threat-analysis-report/

****

Hints & Tips plus Security Awareness

Ransomware Victims Can Get Files Back Without Paying a Ransom!
Who doesn't love getting something for free? Well, now victims of ransomware attacks are thrilled to know they can get their encrypted and ransomed files back from cybercriminals–without having to pay a ransom demand. Even better, they can decrypt the files themselves and do it entirely for free! Thanks to The No More Ransom Project, an effort by cybersecurity and law enforcement professionals to combat ransomware, many victims now have the tools they need to decrypt their ransomed files.
https://www.sosdailynews.com/news.jspx?&articleid=34F16A3F3401AB5E3887B56D12D7F601&sx=79

FBI Says $140+ Million Paid to Ransomware, Offers Defense Tips
The FBI stated that after analyzing collected ransomware bitcoin wallets and ransom notes, they have determined that ransomware operators have received roughly $140 million in payments over the last six years. At the RSA security conference earlier this week, an FBI agent explained how he analyzed the collected data to… https://www.bleepingcomputer.com/news/security/fbi-says-140-million-paid-to-ransomware-offers-defense-tips/

Agility Recovery Coronavirus kit
Included a table top exercise: https://www.agilityrecovery.com/coronavirus-preparedness-business-continuity/?utm_source=pardot&utm_medium=email&utm_campaign=Coronavirus

Additional information on COVID-19
Commonly referred to as the Coronavirus. As such, we are providing the links below, as these resources will assist with questions you may have regarding the Coronavirus.

> Centers for Disease Control and Prevention (CDC) – Coronavirus Disease 2019 (COVID-19)
> https://www.cdc.gov/coronavirus/2019-nCoV/index.html
> World Health Organization (WHO) – Q&A on coronaviruses (COVID-19)
> https://www.who.int/news-room/q-a-detail/q-a-coronaviruses
> Overseas Security Advisory Council (OSAC) – COVID-19 (Coronavirus) Outbreak Resources
> https://www.osac.gov/Content/Announcement/fee23fa6-8c30-44ae-985f-180e3ce9635e

5 steps to avoid coronavirus cure scams and other pandemic con tricks
If you recently read about a coronavirus cure, we hope you didn't act on it. Because there isn't one — so far at least. https://scambusters.org/coronaviruscure.html

NXTsoft Pandemic Plan from Business Continuity Plan
The most frequently asked question related to the pandemic threat is:
https://cdn2.hubspot.net/hubfs/6544150/NXTsoft%20Pandemic%20Plan%20Page%20-%20For%20BCP.pdf?utm_source=hs_email&utm_medium=email&utm_content=84377179&_hsenc=p2ANqtz--k6cNg_jW-u7CsevwBUmgoGdjRqd8J9qyz9J2St_hSzrw_HJb1Bo_0NSPtL0AzZW6ugPXcGvcGKK7GHSX90-yURSaxWw&_hsmi=84377179

FFIEC Highlights Pandemic Preparedness Guidance
The Federal Financial Institutions Examination Council (FFIEC) today updated guidance identifying actions...
https://www.ffiec.gov/press/PDF/FFIEC%20Statement%20on%20Pandemic%20Planning.pdf

On-Demand Webinar: Preparing for a Pandemic
Warning vendor sponsored by Quantivate, registration required except to download the slides:
https://go.quantivate.com/l/824713/2020-03-05/cln1

Seasonal Influenza Preparedness Checklist (vendor sponsored by Agility)
Every year, seasonal influenza affects millions of businesses. In fact, 5% to 20% of the U.S. population gets the flu every year, resulting in 31.4 million outpatient visits. According to the Centers for Disease Control and Prevention… https://www.agilityrecovery.com/resources/seasonal-influenza-preparedness-checklist/

Coronavirus Preparedness: Business Continuity Planning and Leading Practices
The presentation deck and webinar recording are now available. You'll find these and additional resources to help your institution prepare and respond to the evolving situation at https://www.aba.com/banking-topics/risk-management/incident-response/coronavirus?utm_source=abawom&utm_medium=vanity&utm_campaign=resources&utm_content=coronavirus.

Work From Home Best Practices
Tips For Working From Home Effectively https://blogs.cisco.com/collaboration/work-from-home-best-practices

****

News & Views

Third Party Data Breaches: An Unavoidable Threat for All Businesses
Some of the largest data breaches, scams, and threats come from third party relationships. Discover what you can do to protect your small business. https://www.fightingidentitycrimes.com/third-party-data-breaches/?utm_source=EZShield&utm_medium=email&utm_campaign=Engagement.Fraud_Newsletter_C_[03-20]

Evaluating Security Incident Management Programs
The dynamic operational landscape that is created as businesses drive competitive advantage through technology renders a static risk management program ineffective. As enterprises innovate, information technology groups are challenged with revisiting the suitability of architecture, security platforms and/or software deployment to meet business-driven changes. In keeping…
https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2020/evaluating-security-incident-management-programs

FTC: Detox tea claims are hard to swallow
Looking to improve your health or lose a few pounds? Maybe detox teas promoted by celebrities on social media have caught your eye. Before you pay up and down a cup, listen to what the FTC has to say about one purveyor of such potions. https://www.consumer.ftc.gov/blog/2020/03/ftc-detox-tea-claims-are-hard-swallow?utm_source=govdelivery

Is That Charity Really What it Seems?
In the past few months, https://www.bbb.org/scamtracker/us has gotten more than a dozen reports of a nonprofit organization using what consumers think are shady tactics to solicit donations. Potential donors beware! If an organization isn't a charity, then contributions are not "donations" and cannot be deducted from your taxes. https://www.bbb.org/article/news-releases/21666-scam-alert-donors-beware-charity-not-what-it-seems

FTC to Host Workshop Examining Issues Related to Proposed Amendments to the Safeguards Rule
The Federal Trade Commission will hold a public workshop on May 13, 2020 seeking research, testimony, and other input on the proposed changes to the Safeguards Rule under the Gramm-Leach-Bliley Act.
https://www.ftc.gov/news-events/press-releases/2020/03/ftc-host-workshop-examining-issues-related-proposed-amendments

Why Fake News is a Bigger Threat Than Ever
Five years ago, most of us had never heard of fake news. Or, if we did, it was a term to trick us into clicking links that loaded malware onto our computers. https://scambusters.org/fakenews2.html

Hacking has become a viable career, according to HackerOne
HackerOne announced findings from the 2020 Hacker Report, which reveals that the concept of hacking as a viable career has become a reality, with 18% describing themselves as full-time ha…
https://www.helpnetsecurity.com/2020/02/28/hacking-career/

****

"Ctrl -F" for The Board

Nemty Ransomware Punishes Victims by Posting Their Stolen Data
The latest cybercrime operation involving Nemty Ransomware has been stealing victim's files before encrypting computers and publicly posting the files if the victim does not agree to pay ransom demands. The newest campaign uses a data leak site to punish victims who refuse to pay, and the information released has… https://www.bleepingcomputer.com/news/security/nemty-ransomware-punishes-victims-by-posting-their-stolen-data/

My Business Has a Credit Score?
It's critical for your business' health and reputation to keep track of your business credit score with regular monitoring. https://www.fightingidentitycrimes.com/my-business-has-a-credit-score/?utm_source=EZShield&utm_medium=email&utm_campaign=Engagement.Fraud_Newsletter_C_[03-20]

What Is Tax Identity Theft? And How to Prevent It
No one enjoys filing taxes, but the annual, unavoidable task can become infinitely less fun if you become the victim of tax identity theft. https://www.northwesternmutual.com/life-and-money/what-is-tax-identity-theft-and-how-to-prevent-it/

US Cyberspace Solarium Commission
75 recommendations that range from upping the number of military personnel trained for cyber operations to using government resources to protect "systemically important" critical infrastructure owned by the private sector to promoting the use of paper-based voting systems as widely as possible.
https://drive.google.com/file/d/1ryMCIL_dZ30QyjFqFkkf10MxIXJGT4yv/view

Questions
Contact FIPCO's Ken Shaurette at 800/722-3498 ext. 251 or email FIPCO IT Services for more information.

"Make Security Part of You and Your Institution's DNA!"

Threat Intelligence Newsletter: March 27, 2020

If you would like to host an event, please contact: Becky Schowalter

Upcoming Threat Intelligence Peer Group Discussions
None available at the current time

Evasive malware increasing, evading signature-based antivirus solutions
Evasive malware has grown to record high levels, with over two-thirds of malware detected in Q4 2019 evading signature-based antivirus solutions. https://www.helpnetsecurity.com/2020/03/26/evasive-malware-increasing/ If you'd like to consider an alternative to your traditional antivirus solutions contact FIPCO for a demonstration on a managed solution that we believe you will want to consider to prevent incidents like the recent Finastra and CUNA malicious code activities that caused outages.

****

Alerts & Warnings

Researchers Uncover a Nigerian Hacker's Pursuit of his Million Dollar Dream
Social engineering-driven malware threats continue to be a big threat, but new research details how cybercriminals profit off such schemes to launder hundreds of thousands of dollars from stolen credit cards of unsuspecting victims. Cybersecurity firm Check Point Research, in a report shared with...
https://thehackernews.com/2020/03/nigerian-hacker-million-dollars.html?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+TheHackersNews+%28The+Hackers+News+-+Cyber+Security+Blog%29&_m=3n.009a.2186.aa0ao086k1.1d9i

Malicious Memes Running Wild On Twitter
The level of false information on the internet is legendary. Not getting caught up in it is getting more difficult as technology evolves. Fake memes and videos are popping up everywhere, but nowhere more than on social media. Hackers are behind many of the postings, hoping to get responses, then clicks that can install malware and steal your personal information. The effects fake memes have on us can be harmful, but in general they are intended to be funny. Some nuisance memes can go away with a click and some can install malware and take down an entire corporate network.
https://www.sosdailynews.com/news.jspx?&articleid=F040366ED0C6E274775E46CDE8464821&sx=79

Hackers Scanning for Vulnerable Microsoft Exchange Servers, Patch Now!
Attackers are actively scanning the Internet for Microsoft Exchange Servers vulnerable to the CVE-2020-0688 remote code execution vulnerability patched…
https://www.bleepingcomputer.com/news/security/hackers-scanning-for-vulnerable-microsoft-exchange-servers-patch-now/

Some commercial password managers vulnerable to attack by fake apps
Security experts recommend using a complex, random and unique password for every online account, but remembering them all would be a challenging task. That's where password managers come in handy.
https://www.helpnetsecurity.com/2020/03/18/password-managers-vulnerable/

FTC: Coronavirus scams, Part 2
Last month, we alerted you to Coronavirus scams we were seeing at the time. Earlier this month, we sent warning letters to seven sellers of scam Coronavirus treatments. So far, all of the companies have made big changes to their advertising to remove unsupported claims. But scammers don't take a break. Here's an update on more scams we're seeing, and steps you can take to protect yourself, your personal information, and your wallet. https://www.consumer.ftc.gov/blog/2020/03/ftc-coronavirus-scams-part-2?utm_campaign=coronavirus&utm_content=scams_2&utm_medium=email&utm_source=govdelivery

Now more than ever, spot the scams with #FTCScamBingo
During the Coronavirus outbreak, many people are working from home — and maybe even, for the first time in a long time, answering calls from unfamiliar phone numbers. It might be your colleague's cell phone…or it might be a robocaller or scammer. So here's a way you can spot some of those scam calls you might be getting. And it's a way to spread the word to help protect others in your community.
https://www.consumer.ftc.gov/blog/2020/03/now-more-ever-spot-scams-ftcscambingo?utm_source=govdelivery, scam bingo
https://www.consumer.ftc.gov/sites/www.consumer.ftc.gov/files/scam-bingo-v4.pdf

Malware Found Hidden in Android Utility Apps, Children's Games
Researchers have discovered a new malware family operating in 56 different apps previously available on Google's Play Store. The applications have already been collectively downloaded almost a million times. The new malware, called Tekya, tries to commit mobile ad fraud by imitating user actions to click on malicious advertisements... https://www.darkreading.com/application-security/malware-found-hidden-in-android-utility-apps-childrens-games/d/d-id/1337396

New Windows 10 bug hits home working: Outlook, Office 365, Teams can't access internet
Microsoft is rushing to release an out-of-band fix in early April for a Windows 10 connectivity bug.
https://www.zdnet.com/article/new-windows-10-bug-hits-home-working-outlook-o365-teams-cant-access-internet/

****

Hints & Tips plus Security Awareness

NIST Telework Security Basics
Your employer has unexpectedly directed you to telework—and you are feeling overwhelmed. With many changes happening at once, telework security could be an afterthought or completely overlooked. This could put you and your organization at increased risk from attackers, who…
https://www.nist.gov/blogs/cybersecurity-insights/telework-security-basics

The cybersecurity implications of working remotely
Having a sizable amount of employees suddenly working remotely can be a major change for organizations and presents numerous problems with regard to cybersecurity.
https://www.helpnetsecurity.com/2020/03/20/cybersecurity-working-remotely/

Artificial intelligence for fraud detection is bound to save billions
Fraud mitigation is one of the most sought-after artificial intelligence (AI) services because it can provide an immediate return on investm... https://www.zmescience.com/science/ai-fraud-detection-0942323/

US Commerce Dept Shares Tips On Securing Virtual Meetings
Yesterday, the US National Institute of Standards and Technology shared measures that corporations should take to secure virtual meetings between remote workers…
https://www.bleepingcomputer.com/news/security/us-commerce-dept-shares-tips-on-securing-virtual-meetings/

Pausing the Pandemic Panic: Ideas and Solutions for Financial Institutions in These Uncertain Times
Webinar schedule for several informational sessions…
https://info.nxtsoft.com/webinars?utm_campaign=Financial%20Institution%20Newsletter&utm_source=hs_email&utm_medium=email&utm_content=84910806&_hsenc=p2ANqtz--At-6pdl_apmYBoxwPigMtsxOJ6JexUcYoJo_zaeHIufgAUWJB36C5-jwocUVzqDzsYQLL28baENP33lFCvmYb6ZmK7g&_hsmi=84910806

How to evaluate a password management solution for business
Password managers are one of the most powerful defenses against breaches, which can cause massive damage and be incredibly expensive to mitigate. https://www.helpnetsecurity.com/2019/08/26/business-password-management/

Online security tips for working from home
Teleworking during the Coronavirus outbreak? While working from home can help slow the spread of the virus, it brings new challenges: juggling work while kids are home from school; learning new software and conferencing programs; and managing paper files at home. As you're getting your work-at-home systems set up, here are some tips for protecting your devices and personal information.
https://www.consumer.ftc.gov/blog/2020/03/online-security-tips-working-home?utm_source=govdelivery

Webinar Series to Assist Financial Institutions During The COVID-19 Pandemic
The educational webinar series titled Pausing the Pandemic Panic: Ideas and Solutions for Financial Institutions in these Uncertain Times is specifically designed for NXTsoft bank and credit union customers but will also be available to any financial institution personnel who wants to attend. After each webinarNXTsoft will compile written answers to any questions asked during the webinar and will distribute an FAQ document on their website and via email to all attendees.
https://blog.nxtsoft.com/pandemicwebinarseries?utm_campaign=Financial%20Institution%20Newsletter&utm_source=hs_email&utm_medium=email&utm_content=84910806&_hsenc=p2ANqtz--At-6pdl_apmYBoxwPigMtsxOJ6JexUcYoJo_zaeHIufgAUWJB36C5-jwocUVzqDzsYQLL28baENP33lFCvmYb6ZmK7g&_hsmi=84910806

Continuity Innovations Pandemic Planning Tool
We have quickly developed a FREE simple Pandemic Planning Tool to help organizations around the world develop a Pandemic Plan. Our Pandemic Planning Tool will guide you through a wizard to easily capture key planning components such as, a pandemic team, key staff, critical vendors, action items, key stakeholders, and more! https://continuityinnovations.com/pandemicplanningtool/

How to Check a Business Reputation
When it comes to buying and selling products or services, seller reputations are everything. Well, almost. Value has a role to play too. https://www.scambusters.org/reputation.html

****

News & Views

Password vulnerability at Fortune 1000 companies
Despite often repeated advice of using unique passwords for online accounts – or at least the most critical ones – password reuse continues to be rampant. And, according to breach discovery firm SpyCloud, employees of the Fortune 1000 are just as bad about reusing passwords as the rest of us. https://www.helpnetsecurity.com/2020/03/25/password-reuse-companies/

Legal industry at great risk from insider data breaches
A staggering 96% of IT leaders in the legal sector say insider breach risk is a significant concern… https://www.helpnetsecurity.com/2020/03/25/legal-industry-breaches/

667% spike in email phishing attacks due to coronavirus fears
Amid the coronavirus pandemic, attackers are capitalizing on public fear and taking advantage of heightened emotions by targeting victims in email phishing attacks related to COVID-19. The number of email attacks related to COVID-19 has been increasing since January according to data collected by cybersecurity firm Barracuda Networks… https://www.techrepublic.com/article/667-spike-in-email-phishing-attacks-due-to-coronavirus-fears/

****

"Ctrl -F" for The Board

Nemty Ransomware Punishes Victims by Posting Their Stolen Data
The latest cybercrime operation involving Nemty Ransomware has been stealing victim's files before encrypting computers and publicly posting the files if the victim does not agree to pay ransom demands. The newest campaign uses a data leak site to punish victims who refuse to pay, and the information released has… https://www.bleepingcomputer.com/news/security/nemty-ransomware-punishes-victims-by-posting-their-stolen-data/

How to Prioritize Your Mental Health While Self-Isolating
As local governments and health authorities look to curb the spread of COVID-19, more and more people throughout the U.S. are being told to stay home and practice social distancing. Likewise, those who are sick or have tested positive for COVID-19 are further limiting their social contact through… https://onemedical.com/blog/live-well/mental-health-self-isolation

Data allegedly stolen in ransomware attack on cybersecurity insurance provider Chubb
Cybersecurity insurance provider Chubb Group Holdings Inc. is allegedly the latest victim of a ransomware attack. https://siliconangle.com/2020/03/26/data-allegedly-stolen-ransomware-attack-cybersecurity-insurance-provider-chubb/

Thinking critically about Coronavirus news and information

It's dizzying, the amount of information out there about the Coronavirus. You're dealing with story after story online and through social media, television, radio, and in newspapers and magazines — each with its own take — at all hours of the day and night, from all around the world. So how can we sort out what's real and what's not? https://www.consumer.ftc.gov/blog/2020/03/thinking-critically-about-coronavirus-news-and-information?utm_campaign=coronavirus&utm_content=news_and_info&utm_medium=email&utm_source=govdelivery

Questions

Contact FIPCO's Ken Shaurette at 800/722-3498 ext. 251 or email FIPCO IT Services for more information.

"Make Security Part of You and Your Institution's DNA!"

Threat Intelligence Newsletter: April 10, 2020

FIPCO®
IT Audit
Round Table
Discussions

If you would like to host an event, please contact: Becky Schowalter

Upcoming Threat Intelligence Peer Group Discussions
None available at the current time

****

Alerts & Warnings

Threat Advisory: Phishing Campaigns Using the Zoom Video Conferencing Platform
With the global situation around COVID-19 shifting organizations to remote work, the number of users utilizing audio/video conferencing tools has greatly increased. Given this increase in usage, Zoom, a popular video conferencing platform, is being targeted to execute conference hijacking attacks and is being utili… https://www.herjavecgroup.com/phishing-campaigns-using-zoom-platform/?mkt_tok=eyJpIjoiWXpFNFlqQmhObU5rWVRobSIsInQiOiJJMlwvMyt1UlFsVmMra1RTZ1p0aGlOOTEwWlpoTkhJZmxtNldmMnRSQ3VFQUhRb0x0TkREc1BPakkrdEh0enpSQk96ZFE4eG1IaGNxZUxSRlwvNGtVQ2hmREdheVFcL3czUHFlZ2wyc3Vja0NISHh4ZE12U2Q1bzJDYTZybVhXaDQ5TCJ9

Ginp Banking Trojan Sends Fake Texts to Android Phones
A banking Trojan with an odd name isn't amusing Android smartphone users. In fact, the banking malware called Ginp is wreaking havoc by sending fake SMS text messages and push notifications to its victims. First detected only last year, Ginp is rapidly evolving into a highly successful banking-spoof Trojan. Using SMS and push notifications, the malware warns users that they need to verify account information with their bank or credit card. The handy link provided in the text takes users to their bank or credit card websites where they can input their information, including account numbers and passwords. But wait, there's more…
https://www.sosdailynews.com/news.jspx?&articleid=4CDA986FD3247AF54C2A8318E05DCBC6&sx=79

Look Out for Phony SBA Grant Offer
Small business owners are getting hit with a lot of information and making tough decisions on how to survive the COVID-19 crisis. With all of these messages flooding their inbox, social media, and phone, it's easy to mistake a scam for a real offer.
https://www.bbb.org/council/coronavirus/?utm_source=newsletter&utm_medium=email&utm_content=BBB.org/Coronavirus&utm_campaign=scam-alert Resources to help:
https://www.bbb.org/globalassets/local-bbbs/council-113/coronavirus/bbb-coronavirus-report-us.pdf

Critical WordPress Plugin Bug Lets Hackers Turn Users Into Admins
A vulnerability has been found in the WordPress SEO Plugin that allows attackers to give admin privileges to any registered users on sites run by WordPress. This leaves 200,000 sites with active installations vulnerable to attack if left unpatched. The plugin, called Rank math, allows website owners to perform search… https://www.bleepingcomputer.com/news/security/critical-wordpress-plugin-bug-lets-hackers-turn-users-into-admins/

Zeus Sphinx Banking Trojan Arises Amid COVID-19
After three years, the Zeus Sphinx banking trojan has returned to the cybersecurity scene amid the global pandemic, aiming to capitalize on government relief efforts. According to two researchers at IBM X-Force, Amir Gandler and Limor Kessem, the trojan began resurfacing in December, however, there has been a significant increase… https://threatpost.com/zeus-sphinx-banking-trojan-covid-19/154274/

Two Zoom Zero-Day Flaws Uncovered
Patrick Wardle, a security researcher with Jamf, has uncovered two zero-day flaws in the Zoom macOS client version. The telecom and online class platform vulnerabilities have the potential to give local attackers root privileges, which subsequently allow the attackers to access the victims' microphone and camera. The two flaws have… https://threatpost.com/two-zoom-zero-day-flaws-uncovered/154337/

FBI Warns of Attacks on Video Meetings
Yesterday, the US Federal Bureau of Investigation (FBI) warned of what has been deemed "Zoom bombing," in which people hijack Zoom video conferences currently popular for telecommuting and online classes. The goal of these hijackers is to disrupt those meetings electronically over the platform or pulling pranks that are later… https://www.bleepingcomputer.com/news/security/fbi-warns-of-ongoing-zoom-bombing-attacks-on-video-meetings/

COVID-19 malware that will wipe your PC and rewrite your MBR
Cybercriminals have emerged with a new malware that destroys an infected system by either wiping files or rewriting the computer's master boot record (MBR). The information security community has identified at least five new strains (some in the wild and others as tests) that operate this way amid the COVID-19… https://www.zdnet.com/article/theres-now-covid-19-malware-that-will-wipe-your-pc-and-rewrite-your-mbr/

Want to get your Coronavirus relief check? Scammers do too.
You've probably heard the news by now – the government is sending out relief checks as part of the federal response to the Coronavirus. Scammers heard the same thing, and they're hoping to cash in on yours. https://www.consumer.ftc.gov/blog/2020/04/want-get-your-coronavirus-relief-check-scammers-do-too?utm_source=govdelivery

FBI warns again of BEC scammers exploiting cloud email services
The FBI issued a warning to the public yesterday, stating that its Internet Crime Complaint Center (IC3) has received numerous reports of cybercriminals abusing could based email services in Business Email Compromise (BEC) attacks. This marks the second time within the past month that the FBI has warned of BEC... https://www.bleepingcomputer.com/news/security/fbi-warns-again-of-bec-scammers-exploiting-cloud-email-services/

Avoiding SSA scams during COVID-19
While some of you are home, practicing social distancing and frequent hand washing to avoid the Coronavirus, remember that scammers are still busy trying to take advantage of people. Some scammers are pretending to be from the Social Security Administration (SSA) and trying to get your Social Security number or your money. https://www.consumer.ftc.gov/blog/2020/04/avoiding-ssa-scams-during-covid-19?utm_source=govdelivery

Cisco 'Critical Update' Phishing Attack Steals Webex Credentials
Emails purporting to be a Cisco "critical security advisory" are actually part of a phishing campaign trying to steal victims' Webex credentials. https://threatpost.com/cisco-critical-update-phishing-webex/154585/

****

Hints & Tips plus Security Awareness

How to prevent Zoom bombing: 5 simple tips
Internet trolls are crashing Zoom video conferences and flooding them with inappropriate content. Here are easy ways to protect your meetings from Zoom bombers. https://www.techrepublic.com/article/how-to-prevent-zoom-bombing-5-simple-tips/?ftag=TREa988f1c&bhid=78480402&mid=12778097

Socially distancing from COVID-19 robocall scams
Scammers – and scammy companies – are using illegal robocalls to profit from Coronavirus-related fears. Listen to some of the latest scammy robocall pitches, so you can be on the lookout and know how to respond. (Here's a hint: hang up!) https://www.consumer.ftc.gov/blog/2020/03/socially-distancing-covid-19-robocall-scams?utm_source=govdelivery

Webinar – Getting Inside the Mind of an Attacker: TLS Attacks and Pitfalls
Transport Layer Security (TLS) is a common cybersecurity protocol that is frequently seen in email, web browsers, messaging, and other communication…
https://www.helpnetsecurity.com/2020/03/31/webinar-tls-attacks/

While you're at home, spot the scams
Many of us are at home, trying to protect our communities from the Coronavirus. (Thanks to those who are still working outside the home. Be safe.) If you have a minute to spare, it could be a good time for a refresher on spotting some common scams. Especially now that you might be home to get all those robocalls – and especially since the scammers are doubling down on ways to scam you. With that in mind, this is the first in a series of blog posts to help you spot some common scams.
https://www.consumer.ftc.gov/blog/2020/04/while-youre-home-spot-scams?utm_source=govdelivery

Avoid scams while finding help during quarantine
Older adults may be hard hit by the coronavirus – and scammers prey on that. If you or someone you know must stay at home and needs help with errands, you'll want to know about this latest scam. https://www.consumer.ftc.gov/blog/2020/04/avoid-scams-while-finding-help-during-quarantine?utm_source=govdelivery

No and Low Cost Online Cybersecurity Learning Content
During this unusual time in our lives, many of us find we want to improve our knowledge, skills or even prepare for new career opportunities. If you are interested in cybersecurity careers, there are numerous online education providers to choose from. Many online courses are available from your local community college, four-year universities, even the prestigious Centers of Academic Excellence programs – please review all options. https://www.nist.gov/itl/applied-cybersecurity/nice/resources/online-learning-content

Hang up on tech support calls
It can be frustrating to have problems with your computer, especially now that so many people are working from home. But if you get a call from someone claiming to be a Microsoft technician, saying there are viruses on your system, hang up the phone. It's a scam.
https://www.consumer.ftc.gov/blog/2020/04/hang-tech-support-calls?utm_source=govdelivery

****

News & Views

Debunking vulnerability management myths for a safer enterprise
Cybersecurity is one of the most daunting challenges enterprises will face in 2020. According to IBM's 2019 Cost of a Data Breach report,… https://www.helpnetsecurity.com/2020/03/30/vulnerability-management-myths/

Remote learning and children's privacy
"Social distancing," "shelter-in-place," "virtual happy hour" – these are some of the new expressions on everyone's lips the past few weeks. For many kids, parents, and teachers, add "remote learning" or "distance learning" to the list. Because of Coronavirus-related school closures, millions of students are now learning from home. For parents who are concerned about the privacy and security of their children's personal data while they're learning online, here are some things to know.
https://www.consumer.ftc.gov/blog/2020/04/remote-learning-and-childrens-privacy?utm_source=govdelivery

Video conferencing for teams and consumers: What is the right choice for you?
Though some claim that this forced "work from home" situation has shown that many of the discussions that previously required office meetings can actually be expedited simply by exchanging a few emails, there's no doubt that, for some tasks, face-to-face meetings – even if over the internet – are a must.
https://www.helpnetsecurity.com/2020/04/09/video-conferencing-teams/

Password Expiration Costs
Forced password resets are estimated to cost companies $420 per employee in lost productivity per year. How do the costs add up? Who is impacted by these policies? And is it costing your organization more than you realize? https://www.enzoic.com/cost-password-expiration-policies/?utm_source=hs_automation&utm_medium=email&utm_content=85738505&_hsenc=p2ANqtz-8Ug4qWdVami_tQV-icHRkKawnl-enPdQXnvwfvGxaaoj-MLp0OCpHXlvLyyMxhoSpPI4Y1EK-2RLzEvOra7to92KH07Q&_hsmi=85738505

****

"Ctrl -F" for The Board

Cyber Hygiene Critical for Your Business Now Than Ever Before – Here's Why
Given the rising threat of cybercrime, organizations should build their security programs with the understanding that no matter how many firewalls or network controls they have in place, the risk of insider threat will always be present. https://www.herjavecgroup.com/cyber-hygiene-critical-business/?mkt_tok=eyJpIjoiWkRsa05qUTBNR013TkRNMCIsInQiOiJuODdwd0FEK0F3aEVMXC96Y0FDcE1uNERuR0FOTkFhNFZvRDc1dkthSW8yYkI2aEh5WUNtOU56dWJkcXVuZU1WakZBZEdsbWYrTmNwTDdRUjVxTnVkeW52ZnNBN2o4QzVtSTNnNDI2TkhJZk9JdWdHTUdUR1RmXC9PVHFKWEJsTVNmIn0%3D

Questions
Contact FIPCO's Ken Shaurette at 800/722-3498 ext. 251 or email FIPCO IT Services for more information.

"Make Security Part of You and Your Institution's DNA!"

Threat Intelligence Newsletter: April 20, 2020

FIPCO®
IT Audit
Round Table
Discussions

If you would like to host an event, please contact: Becky Schowalter

Upcoming Threat Intelligence Peer Group Discussions
None available at the current time

****

Alerts & Warnings

Looking for work after Coronavirus layoffs?
Have you been laid off due to the Coronavirus? Or maybe your small business shut down? Today, the FTC kicks off a series of blogs with tips about handling the financial impact of the Coronavirus. These days, many people start by looking for ways to make money working from home. If you're eyeing a work-at-home gig, here are some things to keep in mind… https://www.consumer.ftc.gov/blog/2020/04/looking-work-after-coronavirus-layoffs?utm_source=govdelivery

Critical VMware Bug Opens Up Corporate Treasure to Hackers
The bug — rated 10 in severity — potentially affects large numbers of corporate VMs and hosts.
https://threatpost.com/critical-vmware-bug-corporate-treasure-hackers/154682/

Overlay Malware Leverages Chrome Browser, Targets Banks and Heads to Spain
On Monday, IBM's X-Force researchers posted an analysis of a malware that leverages a fake Chrome browser plugin, subsequently targeting the accounts of banking customers in Spain. The banking malware, called Grandoreiro, also uses a remote overlay to display a full-screen overlay image when a target accesses their online banking… https://threatpost.com/overlay-malware-exploits-chrome-browser-targets-banks-and-heads-to-spain/154713/

Over 700 Malicious Typosquatted Libraries Found On RubyGems Repository
As developers increasingly embrace off-the-shelf software components into their apps and services, threat actors are abusing open-source repositories such as RubyGems to distribute malicious packages, intended to compromise their computers or backdoor software projects they work on. In the latest...
https://thehackernews.com/2020/04/rubygem-typosquatting-malware.html

Isoprex misleads seniors
"Isoprex Slashes Pain in 5 Days – Naturally!" "Walking without a Cane!" "Clinically Proven!" "Relieves painful swelling in 100% of even the worst cases." These claims are false or misleading, according to the FTC's complaint against Isoprex's distributor, Renaissance Health Publishing, Inc.
https://www.consumer.ftc.gov/blog/2020/04/isoprex-misleads-seniors?utm_source=govdelivery

Loan Relief Scam
This quick video with Jeff Rossen and Jim Stickley outlines how incredibly vulnerable many if not most businesses are to a simple phone scam:
https://www.youtube.com/watch?time_continue=32&v=AALA24tcybI or visit
https://www.doverfcu.com/resources/tools/security-center

****

Hints & Tips plus Security Awareness

VMware plugs critical flaw in vCenter Server, patch ASAP!
VMware has fixed a critical vulnerability (CVE-2020-3952) affecting vCenter Server, which can be exploited to extract highly sensitive information that could be used to compromise vCenter Server or other services which depend on the VMware Directory Service (vmdir) for authentication.
https://www.helpnetsecurity.com/2020/04/14/cve-2020-3952/

April Patch Tuesday: Microsoft Battles 4 Bugs Under Active Exploit
April's Patch Tuesday consisted of 113 patches, which was most likely difficult for IT staff under WFH security concerns. This patch Tuesday includes 19 critical vulnerabilities and 94 that are classified as important. Four of the critical vulnerabilities are being exploited in the wild, however, two have previously been publicly… https://threatpost.com/april-patch-tuesday-microsoft-active-exploit/154794/

Stay safe while video conferencing
Have you been video conferencing in these days of social distancing? It's pretty cool to see several people at once on the screen and be able to have a conversation as if everyone was in the same room. But we don't want strangers in our meetings — and we'd all probably rather keep our information to ourselves. So let's review some basic safety tips: https://www.consumer.ftc.gov/blog/2020/04/stay-safe-while-video-conferencing?utm_source=govdelivery

7 actions you can take to avoid check washing crooks
New Coronavirus scams are appearing virtually every day, and the latest one is targeting people who get Social Security payments. Meanwhile, an old favorite scam is back on the crime scene — check washing.
https://scambusters.org/checkwashing.html

****

News & Views

GDPR, CCPA and beyond: How synthetic data can reduce the scope of stringent regulations
As many organizations are still discovering, compliance is complicated. Stringent regulations, like the GDPR and the CCPA, require multiple steps from numerous department…
https://www.helpnetsecurity.com/2020/04/14/synthetic-data/

How Zoom Is Attempting to Fix Security 'Missteps'
Thanks largely to the COVID-19 pandemic, Zoom's number of worldwide users has surpassed the 200 million mark, a spectacular rise after market analyst Apptopia reported it served a mere 12.9 million users on Jan. 1. https://www.eweek.com/mobile/how-zoom-is-attempting-to-fix-security-missteps?utm_medium=email&utm_campaign=B2B_NL_DYE_20200415_AR1&mkt_tok=eyJpIjoiWldSa05qUXdZVEkwWVdSaSIsInQiOiJEcFJFMHpBVENMXC94UzBoM0J2UzRORit6T25rUVByVnNoTVU2VnFia3FuakR2bzhpSVpOZ25UZ25Od05nKzVMaGszR3pPVzhyRVFNQ0NGUWlRdTJiVUZocUZwWVMrTDhjc1RPOEU4RFVyKzBwZkpaXC9KcTlMTWxBSzVNc2E3Q0tRIn0%3D

Phishing kits: The new bestsellers on the underground market
Phishing kits are the new bestsellers of the underground market, with the number of phishing kit ads on underground forums and their sellers having doubled in 2019 compared to the previous year, Group-IB reveals. https://www.helpnetsecurity.com/2020/04/16/phishing-kits-market/

****

"Ctrl -F" for The Board

On my mind: Transitioning to third-party cloud services
During this extended period of social distancing filled with increased online activity, I can’t help but reflect on all the user data that has been created, stored, hacked, exposed, bought, shared and sold over the last 10 years. What’s known as the black market is built on this immeasura…
https://www.helpnetsecurity.com/2020/04/16/third-party-cloud-services/

Questions
Contact FIPCO’s Ken Shaurette at 800/722-3498 ext. 251 or email FIPCO IT Services for more information.

"Make Security Part of You and Your Institution's DNA!"

Threat Intelligence Newsletter: April 27, 2020

FIPCO®
IT Audit
Round Table
Discussions

If you would like to host an event, please contact: Becky Schowalter

Upcoming Threat Intelligence Peer Group Discussions
None available at the current time

****

Alerts & Warnings

Office printers: The ticking IT time bomb hiding in plain sight
Office printers don't have to be security threats: with foresight and maintenance they're very easily threat-proofed. The problem is that system administrators rarely give the humble printer (or scanner, or multifunction printer) much attention. https://www.helpnetsecurity.com/2020/04/17/unprotected-printers/

Looking for work after Coronavirus layoffs?
Have you been laid off due to the Coronavirus? Or https://www.doverfcu.com/resources/tools/security-center

Phishers exploiting employees' layoff, payroll concerns
Two new phishing campaigns that aim to obtain Zoom and WebEx credentials have emerged, capitalizing on fears of layoffs and payroll changes. The phishing emails deliver fake information with "Zoom meeting about termination" in the headline, scaring recipients into clicking malicious links that then harvest Zoom passwords. Abnormal Security discovered… https://www.helpnetsecurity.com/2020/04/23/fake-termination-emails/

Oil and Gas Companies Targeted
Recent spearphishing campaigns have targeted the oil and gas industry, using the so-called Agent Tesla spyware Trojan. According to security firm Bitdefender, attackers impersonated an Egyptian state oil company called Enppi, (Engineering for Petroleum and Process Industries) to launch attacks against organizations in several countries including Malaysia, the US, Iran,… https://www.securityweek.com/oil-and-gas-companies-targeted-agent-tesla-malware

****

Hints & Tips plus Security Awareness

Managing your bills during COVID-19

COVID-19 has thrown the economy into a tailspin. Many people have been laid off, furloughed, or are working fewer hours. And as wages dry up, bills can pile up. Debt can be tricky – especially when you have more month than money. Here are some ideas about how you can manage your debts and start regaining your financial footing. https://www.consumer.ftc.gov/blog/2020/04/managing-your-bills-during-covid-19?utm_source=govdelivery

COVID-19 Scams Raise Security Concerns for Businesses

Over the past weeks, the novel coronavirus (COVID-19) pandemic has caused a shift in our working conditions, our social interactions, and our work/life balance in general. Many organizations have instituted work-from-home policies to adhere to the social distancing requirements in every state, and over one-third of employers say the recommendations to limit social contact have triggered a work from home policy for the first time. https://www.fightingidentitycrimes.com/coronavirus-business-security-risk/

****

News & Views

Reports confirm that US Power Grid is not prepared for Cyber Attacks

Security Researchers at the US Power Grid have confirmed media reports that the government's critical infrastructure is not at all prepared to withstand cyber attacks. Known as the largest interconnected machine, the US electricity Grid is having more than… https://www.cybersecurity-insiders.com/reports-confirm-that-us-power-grid-is-not-prepared-for-cyber-attacks/

267 Million Facebook Profile Records for Sale on The Dark Web

What Happened? On April 20, 2020, more than 267 million Facebook profiles were found listed for sale on the Dark Web — for only $600. Reports link these profiles back to the Facebook data leak discovered in December 2019, and possibly others. Researchers are still uncertain how…
https://www.fightingidentitycrimes.com/267-million-facebook-profiles-sold-dark-web/#more-6008

Ransomware is now the biggest online menace you need to worry about - here's why

Ransomware attacks have become more commonplace than payment card theft incidents for the first time, as cyber criminals alter how they go about their malicious operations in an effort to gain the biggest financial reward for the least amount of effort. Analysis of more than a trillion security events over the past year and hundreds of breach investigations by researchers at cybersecurity company Trustwave found that ransomware attacks have become the most common security incident. The number of ransomware incidents quadrupled when compared with the previous year and it now means that ransomware attacks are more common that payment card and financial data breaches for the first time. Incidents involving stolen bank account details and credit card information accounted for 17% of incidents during 2019.
https://www.zdnet.com/article/ransomware-is-now-the-biggest-online-menace-you-need-to-worry-about/

APT41 – The Spy Who Encrypted Me

This case study is based on our most recent investigation into one of APT41’s operations against a major global nonprofit organization. Our client contacted us at the end of March 2020 after discovering the ransom notes... https://lifars.com/knowledge-center/the-spy-who-encrypted-me/?utm_source=LIFARS&utm_campaign=3883da0b52-linktrackCyber_Security_Newsletter-04-24-20&utm_medium=email&utm_term=0_20a0f45127-3883da0b52-343178117&ct=t(ClickTaleCyber_Security_Newsletter-04-24-20)&goal=0_20a0f45127-3883da0b52-343178117&mc_cid=3883da0b52&mc_eid=35555732e3

****

"Ctrl -F" for The Board

CISOs: Quantifying cybersecurity for the board of directors

Only 9% of security teams feel as if they are highly effective in communicating security risks to the board and to other C-suite executives, according to a recent survey conducted by the Ponemon Institute.
https://www.helpnetsecurity.com/2020/04/21/quantifying-cybersecurity/

Cyber-Risk Oversight 2020

Helps directors take a pragmatic approach to specific elements of cyber-risk such as insider threats, third-party exposure, M&A due diligence, and effective risk disclosure.
https://boardleadership.nacdonline.org/rs/815-YTL-682/images/2020_NACD_Cyber_Handbook.pdf?utm_medium=email&utm_source=noms&utm_campaign=Recruitment&mkt_tok=eyJpIjoiTURjeE4ySTJOekk1TnpVeSIsInQiOiJJbkpvQUt3QUdcLzRpQmVcL2FxZDdVaGI2QVZYZDZXZU5JUldWUGxRbVZLT1N4Vk9sdFFodjIyZVptNE4rOHRXUXRHMCtuM1BOTCtnYjZ1TWx4aklYOHlzT3N1am5XR2VuRGk4TXVYWDBRS29WcklpZVlJUDNialVuRjFnckk4UUM3In0%3D

Questions
Contact FIPCO’s Ken Shaurette at 800/722-3498 ext. 251 or email FIPCO IT Services for more information.

"Make Security Part of You and Your Institution's DNA!"

Threat Intelligence Newsletter: May 4, 2020

FIPCO®
IT Audit
Round Table
Discussions

If you would like to host an event, please contact: Becky Schowalter

Upcoming Threat Intelligence Peer Group Discussions
None available at the current time

****

Alerts & Warnings

New Android Malware Steals Banking Passwords, Private Data and Keystrokes
A new type of mobile banking malware has been discovered abusing Android's accessibility features to exfiltrate sensitive data from financial applications, read user SMS messages, and hijack SMS-based two-factor authentication codes. Called "EventBot" by Cybereason researchers, the malware is... https://thehackernews.com/2020/04/android-banking-keylogger.html?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+TheHackersNews+%28The+Hackers+News+-+Cyber+Security+Blog%29&_m=3n.009a.2217.aa0ao086k1.1e19

Asnarök" Trojan targets firewalls
Some Sophos firewall products were attacked with a new Trojan malware, dubbed Asnarök by researchers cyber-security firm Sophos, to steal usernames and hashed passwords starting with April 22 according to an official timeline. The malware exploits a zero-day SQL injection vulnerability that can lead to remote code execution on any unpatched physical and virtual firewalls it targets. https://malwaretips.com/threads/asnar%C3%B6k-malware-exploits-firewall-zero-day-to-steal-credentials.100401/

Single Malicious GIF Opened Microsoft Teams to Nasty Attack
Microsoft has disclosed that a since-patched flaw allowed an attacker to take over an organization's entire system of Microsoft Teams accounts. The subdomain takeover vulnerability in the company's collaboration platform, Microsoft Teams, potentially allowed an inside attacker to create a malicious GIF image that was then used to steal data... https://threatpost.com/single-malicious-gif-opened-microsoft-teams-to-nasty-attack/155155/

Fake Fedex and UPS delivery issues used in COVID-19 phishing
The online shopping and home delivery industries have experienced an influx over the past several weeks as people socially isolate and telecommute. Threat actors have been capitalizing on this recent adjustment, creating new scams luring victims through fake Coronavirus delivery issue emails. The emails contain malicious links or open malware. https://www.bleepingcomputer.com/news/security/fake-fedex-and-ups-delivery-issues-used-in-covid-19-phishing/

Attackers Gift Teddy Bears And Malware Using Best Buy Gift Cards
Hackers are sending cuddly stuffed teddy bears in the mail as a thank you. The hacking group FIN7 (aka Carbanak) is spearheading this gift exchange and including a nifty USB drive that will help you determine what purchases you can make with a gift card included with the bear. But beware! If you do insert the provided USB stick into your computer, you'll be gifted something that is definitely not cute and cuddly, and it could mean you lose control of your computers...
https://www.sosdailynews.com/news.jspx?&articleid=52722A2F70C95B6A2E7A246FBE3034A8&sx=79

Sophisticated Android Spyware Attack Spreads via Google Play
Cybersecurity company Kaspersky has disclosed a new campaign targeting specific victims primarily in Southeast Asia that it's dubbed the PhantomLance espionage campaign. Kaspersky believes that OceanLotus APT could be behind the attacks. The attacks are sophisticated and ongoing, targeting Andriod users in Asia. The campaign features complex spyware that is… https://threatpost.com/sophisticated-android-spyware-google-play/155202/

Microsoft warns of malware surprise pushed via pirated movies
Microsoft has issued a warning that pirate streaming devices and movie piracy sites are being targeted by threat actors, who are infecting victims with malware via fake movie torrents. The platforms have experienced a huge influx of traffic due to social isolating measures brought on by the COVID-19 pandemic, as… https://www.bleepingcomputer.com/news/security/microsoft-warns-of-malware-surprise-pushed-via-pirated-movies/

Personal Cloud Disk Drives Face Ransomware Risk + Latest Coronavirus Scams
Coronavirus Spotlight on Census and Costco Scams, The Coronavirus scammers are still at it! They've discovered more new ways of tricking people into either giving them money or letting them into their systems to wreak whatever havoc they care to. https://www.scambusters.org/personalcloud.html

Microsoft Office 365: US issues security alert over rushed remote deployments
CISA is concerned hasty deployments of Office 365 and Teams may lead to missed key security configurations. https://www.zdnet.com/article/microsoft-office-365-us-issues-security-alert-over-rushed-remote-deployments/?ftag=TRE-03-10aaa6b&bhid=78480402&mid=12813725&cid=717796056

****

Hints & Tips plus Security Awareness

Don't click links in unsolicited text messages
Common Sense; sometimes NOT. You might be seeing text messages promising money – maybe the economic impact payments, loans for small businesses, or an offer for money you can get. In fact, I recently saw a WhatsApp text message in Spanish that advertised money for people quarantined at home. If you've spotted messages like this, I hope you've also deleted them. These text messages going around

could lead you to a scam or a hacker, but not to anything helpful. https://www.consumer.ftc.gov/blog/2020/04/dont-click-links-unsolicited-text-messages?utm_source=govdelivery

The battle against ransomware: Lessons from the front lines
Ransomware is arguably the most significant cybercrime innovation in recent history. The ransomware business model is so effective that it is now the most common and devastating threat to organizations of all sizes. As a provider of cyber insurance, we have the misfortune of responding to ransomware attacks across tens of thousands of organizations, and the trends are worrying. https://www.helpnetsecurity.com/2020/04/28/ransomware-lessons/

Mozilla ranks video call apps by security and privacy features
2 of the 15 most popular video call apps meet Mozilla's Minimum Security Standards, according to a new report. https://www.techrepublic.com/article/mozilla-ranks-video-call-apps-by-security-and-privacy-features/?ftag=TREa988f1c&bhid=78480402&mid=12812446&cid=712423569

Best password managers for business in 2020: 1Password, Keeper, LastPass, and more
Everyone needs a password manager. It's the only way to maintain unique, hard-to-guess credentials for every secure site you and your team access daily. https://www.zdnet.com/article/best-password-managers/?ftag=TRE-03-10aaa6b&bhid=78480402&mid=12815612&cid=717796056

****

News & Views

Five best practices for achieving and maintaining SOC 2 compliance
A crucial framework for technology companies and cloud-based organizations, SOC 2 is both a technical audit and a requirement that comprehensive information security policies and procedures be written and followed. https://www.helpnetsecurity.com/2020/04/24/soc-2-compliance/

Financial sector is seeing more credential stuffing than DDoS attacks
The financial sector has seen more brute-force attacks and credential stuffing incidents than DDoS attacks in the past three years, F5's cyber-security unit said in a report published today. https://www.zdnet.com/article/financial-sector-has-been-seeing-more-credential-stuffing-than-ddos-attacks-in-recent-years/

CBD, COVID-19 and cancer: The unfounded facts
The COVID-19 pandemic creates the perfect storm of hopes and fears that dishonest business try to exploit with fake promises of protection and healing. But when these promises are not backed by science, the consequences can often cost you money and your good health… https://www.consumer.ftc.gov/blog/2020/04/cbd-covid-19-and-cancer-unfounded-facts?utm_source=govdelivery

Millions of Brute-Force Attacks Hit Remote Desktop Accounts
Experts have reported an increase in brute-force attacks targeting users of Microsoft's Remote Desktop Protocol (RDP). The number of brute force attacks aimed at taking over corporate desktops and infiltrating company networks has been in the millions per week. This is likely a result of threat actors taking advantage of… https://threatpost.com/millions-brute-force-attacks-rdp/155324/

Suspicious business emails increase, imposters pretend to be executives
U.S. small businesses report an increase in suspicious business emails over the past year, a cyber survey by HSB shows, and employees are taking the bait as they fall for phishing schemes and transfer tens of thousands of dollars in company funds into fraudulent accounts.
https://www.helpnetsecurity.com/2020/04/30/suspicious-business-emails/

****

"Ctrl -F" for The Board

CISOs: Quantifying cybersecurity for the board of directors
Only 9% of security teams feel as if they are highly effective in communicating security risks to the board and to other C-suite executives, according to a recent survey conducted by the Ponemon Institute.
https://www.helpnetsecurity.com/2020/04/21/quantifying-cybersecurity/

Questions
Contact FIPCO's Ken Shaurette at 800/722-3498 ext. 251 or email FIPCO IT Services for more information.

"Make Security Part of You and Your Institution's DNA!"

Threat Intelligence Newsletter: May 13, 2020

FIPCO®
IT Audit
Round Table
Discussions

If you would like to host an event, please contact: Becky Schowalter

Upcoming Threat Intelligence Peer Group Discussions
None available at the current time

****

Alerts & Warnings

Clipbanker – 13 Second Attack
In this article, the Cynet Research team reveals a highly complex attack that runs for only 13 seconds by using several malwares and different tactics. From our analysis, the threat that we discovered within our investigation is name the "ClipBanker" trojan. https://www.cynet.com/blog/threat-research-report-clipbanker-13-second-attack/?utm_source=hs_email&utm_medium=email&utm_content=87543959&_hsenc=p2ANqtz--6c3IhX69IWdui3x0nQHrK4PlyK13ofBDWSl2YGLTKegmRcHvhmcC7Z7RY8eREvosaqt7h5MRzKNYC3-CvJz-L7rR4tw&_hsmi=87543959

Microsoft Teams Impersonation Attacks Flood Inboxes
According to security researchers at Abnormal Security, Microsoft Teams has been hit by two separate attacks targeting as many as 50,000 users. The campaigns reportedly aim to phish Office 365 logins. The cyberattacks impersonate notifications from Microsoft Teams in order to prompt the victim to enter login credentials, which are... https://threatpost.com/microsoft-teams-impersonation-attacks/155404/

TrickBot Attack Exploits COVID-19 Fears with DocuSign-Themed Ploy
IBM X-Force recently disclosed that malicious actors are spreading the TrickBot trojan through fake messages that are COVID-19 themes. The new campaign capitalizes on public concern and interest in the Department of Labor's Family and Medical Leave Act (FMLA)… https://threatpost.com/trickbot-attack-covid-19docusign-themed-malw/155391/

****

Hints & Tips plus Security Awareness

Stop Suspicious AWS – Amazon Phishing
Report Suspicious emails from Amazon.
https://aws.amazon.com/security/report-suspicious-emails/

Did an ID thief steal your stimulus payment? Report it to FTC
Do you think your economic impact payment has landed in the hands of an identity thief? You can report it to the FTC and the IRS at the same time. Here's what to do.
https://www.consumer.ftc.gov/blog/2020/05/did-id-thief-steal-your-stimulus-payment-report-it-us?utm_source=govdelivery

CISA Releases Secure Video Conferencing Recommendations
CISA last week also released advisory guidance, "Cybersecurity Recommendations for Critical Infrastructure Using Video Conferencing." The guidance identifies the various threat vectors and includes recommendations for organizations to consider when adopting or expanding the use of video conferencing software and related collaboration tools. It also includes suggestions for the end-users who host and attend meetings.
https://www.cisa.gov/sites/default/files/publications/CISA_Cybersecurity_Recommendations_for_Critical_Infrastructure_Using_Video_Conferencing_S508C.pdf?utm_campaign=RiskCyber-20200504&utm_medium=email&utm_source=Eloqua

Coronavirus PPE Warning + Bar Code Swap, Lottery and Giveaway Scams
Coronavirus Supplies Scam Warning, Not all coronavirus scams arrive by email, text, or phone. There's also a chance they might turn up in your regular mailbox. Which is why the United States Postal Inspection Service (USPIS) has stepped into the battle against the crooks.
https://www.scambusters.org/codeswap.html

Cloud vs. On-Premises Two-Factor Authentication
Moving applications to the cloud can be a major game-changer when it comes to how and where users can access their work, not to mention decrease costs and increase productivity. However, moving to the cloud can also increase security risks if IT doesn't have a good idea of who is accessing which applications, from where, and what kind of devices are being used. https://go.duo.com/rs/074-UQX-410/images/Cloud%20vs%20On%20Premises%20Two-Factor.pdf?&utm_source=marketo&utm_medium=email&utm_campaign=nurtureconsideration&mkt_tok=eyJpIjoiTW1Jek16RXhabVkyWWpWbSIsInQiOiJyOXJiclVKTU9qeklnYmpSWU85Mko4UHQ2RStXTFNcL3FvbFNwTjZTc3drcmhNR1wvcTk0VDlNYW5MTmhLR3dvVnh0b1AxTnRRdUUxbTVseG9DUWh1WSt1WUdXM1lwakpaZFJxamhybFcyR3VFUVlNeUJVMmlhUHVXamlHZlVSY3p6In0%3D

Samsung patches 0-click vulnerability impacting all smartphones sold since 2014
South Korean smartphone vendor Samsung released this week a security update to fix a critical vulnerability impacting all smartphones sold since 2014. The security flaw resides in how the Android OS flavor running on Samsung devices handles the custom Qmage image format (.qmg), which Samsung smartphones started supporting on all devices released since late 2014.
https://www.zdnet.com/article/samsung-patches-0-click-vulnerability-impacting-all-smartphones-sold-since-2014/

****

News & Views

RATs in the Library
Remote Access Trojans Hide in Plain "Public" Site… https://blog.reversinglabs.com/blog/rats-in-the-library?utm_medium=email&_hsmi=87239592&_hsenc=p2ANqtz-9mihJkAnAE36puiR10XpxJ8_CX8OpEdzw3JxSoW9A5t9euC3JCYJbyA1ZcBjKv24gaPUWP&utm_content=87213578&utm_source=hs_email

Ransomware mentioned in 1,000+ SEC filings over the past year
According to the US Securities Exchange Commission, an increasing number of companies are identifying ransomware as a forward-looking risk factor in documents filed with the agency. The agency states that in the past year, more than 1,000 documents mentioning ransomware as a risk factor have been filed. Over 700 have... https://www.zdnet.com/article/ransomware-mentioned-in-1000-sec-filings-over-the-past-year/

Brute force attacks against remote desktop apps skyrocket during pandemic lockdown
A rise in remote workers has opened a window of opportunity for hackers, who are now trying to access enterprise networks by targeting Microsoft RDP accounts. https://www.techrepublic.com/article/brute-force-attacks-against-remote-desktop-apps-skyrocket-during-pandemic-lockdown/?ftag=TREa988f1c&bhid=78480402&mid=12819405&cid=712423569

How Cybercriminals are Weathering COVID-19
In many ways, the COVID-19 pandemic has been a boon to cybercriminals: With unprecedented numbers of people working from home and anxious for news about the virus outbreak, it's hard to imagine a more… https://krebsonsecurity.com/2020/04/how-cybercriminals-are-weathering-covid-19/

****

"Ctrl -F" for The Board

Fighting Coronavirus scams: taking stock
Since the beginning of the COVID-19 crisis, the FTC has released dozens of warning letters against people trying to make an illegal buck off the Coronavirus. More than a month in, it seems like a good time to look back at what's happened. If you follow this blog, you'll know these have been busy weeks – with advice about spotting the many scams we're all facing, news of the warning letters sent on a wide range of scams, and some enforcement actions filed. https://www.consumer.ftc.gov/blog/2020/05/fighting-coronavirus-scams-taking-stock?utm_source=govdelivery

Questions
Contact FIPCO's Ken Shaurette at 800/722-3498 ext. 251 or email FIPCO IT Services for more information.

"Make Security Part of You and Your Institution's DNA!"

Threat Intelligence Newsletter: May 18, 2020

FIPCO® IT Audit Round Table Discussions

If you would like to host an event, please contact: Becky Schowalter

Upcoming Threat Intelligence Peer Group Discussions
None available at the current time

****

Alerts & Warnings

Phantom in the Command Shell Campaigns Target Financial Industry
Researchers at Prevailion have reported a new operation called Phantom in the Command Shell. The operations have been targeting financial firms across the globe using the Evilnum malware, which is being distributed to victims using a Google Drive share link. https://www.herjavecgroup.com/phantom-command-shell-campaigns/?mkt_tok=eyJpIjoiTWpNeE16azNNRFZpWmpReSIsInQiOiJ1b2kzT00zTVl6TklTMUVkRUl5R3pEcnFuWlJTMFhWSTU0VndSd3hzRUljd3Rxb2Q0TzdmRnRHRkVNUUxyazlJYlI2RUw3MFVpYXdIcktGdytFd3dxZEhBaitEXC81SWpDV3FsNFJIZ015Q2JIS21vb2JER0VhM1o2dytqeUNTTjgifQ%3D%3D

Phishing emails caught exploiting DocuSign and COVID-19
A new attack aims to steal account credentials from people who use the online document signing platform. https://www.techrepublic.com/article/phishing-emails-caught-exploiting-docusign-and-covid-19/?ftag=TREa988f1c&bhid=78480402&mid=12829381&cid=712423569

Phishing campaign caught spoofing Zoom
The campaign impersonates Zoom emails, but steals the Microsoft account credentials of its victims… https://www.techrepublic.com/article/phishing-campaign-caught-spoofing-zoom/?ftag=TREa988f1c&bhid=78480402&mid=12829381&cid=712423569

YouTube Account Recovery Phishing
Phishing attacks against targeted channels have been successful in the past, as explained last year on ZDNet. Recently, our Remediation team found an interesting phishing page following a similar pattern that was targeting YouTube creators. https://blog.sucuri.net/2020/05/youtube-account-recovery-phishing.html?utm_campaign=Blog%20RSS&utm_source=hs_email&utm_medium=email&utm_content=87809021&_hsenc=p2ANqtz-_MQNPVwJXS9uYAYoTI0aUO0kjgNnD55lN8mHpbJBZ8RzXtUi5dZbX1CwZi-2lyfmMNbxgv59J-1eYVYwtKANPE88vK0w&_hsmi=87809021

“No risk” publications shouldn’t cost money
Some dishonest companies lie when they say that a product is “no risk.” That’s what the FTC says Progressive Business Publications, a business publication company, did. They had telemarketers call businesses, schools, nonprofits, and other organizations to offer samples of their newsletters and books at “no risk.” But they didn’t make clear that, by accepting the samples, your organization got enrolled in an expensive annual subscription. https://www.consumer.ftc.gov/blog/2020/05/no-risk-publications-shouldnt-cost-money?utm_source=govdelivery

Reverse RDP – The Path Not Taken
During 2019, we published our research on the Reverse RDP Attack: Part 1 and Part 2. In those blog posts, we described how we found numerous critical vulnerabilities in popular Remote Desktop Protocol (RDP) clients. In addition, we focused on a Path-Traversal vulnerability we found in Microsoft’s RDP client, a vulnerability that was also applicable as a guest-to-host VM escape in Hyper-V Manager.
https://www.sesin.at/2020/05/14/reverse-rdp-the-path-not-taken/?utm_source=hs_email&utm_medium=email&utm_content=87922087&_hsenc=p2ANqtz--ZwL3H2X_Zfa2CYGWy6xICqQfkgo4Y7eoE9wlbbcGVEvRO3dPCxKTtGIl1xVLsXmeSe11eDD14vxXqCH43YR8GtKwDTw&_hsmi=87922087

The Stalkerware Threat to Privacy
Cyberstalkers have a new weapon in their efforts to virtually follow their victims — stalkerware. Yes, that’s right — software whose sole purpose is to enable these crooks to spy on their victims…
https://scambusters.org/stalkerware.html

****

Hints & Tips plus Security Awareness

Password Blacklists: Do They Provide Enough Protection?
Password blacklists can lack some of the most common passwords. Here are some of the things you should consider when looking at password blacklists. https://www.enzoic.com/password-blacklists/?utm_medium=email&_hsmi=85738706&_hsenc=p2ANqtz-92DgjZoRxAqjAiWglP0rp2a5hzKzeA_R8QVDBZ6vYUUpBCO3qji_2m9gx8SKt2NsK7Jdv8&utm_content=85738706&utm_source=hs_automation

FFIEC Issues Statement on Risk Management for Cloud Computing Services
The Federal Financial Institutions Examination Council (FFIEC) on behalf of its members today issued a statement to address the use of cloud computing services and security risk management principles in the financial services sector. https://www.ffiec.gov/press/PDF/FFIEC_Cloud_Computing_Statement.pdf

VMware Publishes Workarounds for Vulnerabilities in vRealize Operations Manager
VMware has published workarounds to address unpatched vulnerabilities in vRealize Operations Manager (vROps). A remote attacker could exploit these vulnerabilities to take control of an affected system. https://www.vmware.com/security/advisories/VMSA-2020-0009.html

Most Businesses Vulnerable to Emerging Risks Not Covered by Their Cyber Insurance
According to a new study by the Hanover Insurance Group, Inc., most businesses are more vulnerable to emerging risks such as malware and ransomware attacks than traditional threats such as the breach of personally identifiable information. However, the report found most businesses were insured against traditional cyber threats instead of the emerging risks. The study, which was carried out in collaboration with Zogby Analytics, found that the cyber insurance coverage gap poses an existential threat to the majority of the businesses. https://www.cpomagazine.com/cyber-security/most-businesses-vulnerable-to-emerging-risks-not-covered-by-their-cyber-insurance/

Webinar On-Demand: What Cybercriminals See When They Infect a Host with Malware
Missed our webinar last month? Check it out when you have a free hour. Discover what an attacker managing a malware campaign sees as new systems become infected, how the stolen information included in malware log files gets monetized, and how to protect yourself.
https://spycloud.com/resource/webinar-keylogger-malware/?utm_campaign=Newsletter&utm_source=hs_email&utm_medium=email&utm_content=87753381&_hsenc=p2ANqtz--YEViFGCOD1I2-_8ATE9oC1360grPgcgn4njINWR7yMsul3ucTzTEkOKRuOOtd-6pcxeWyY7AL3k2P7XR2yNSM0YMrew&_hsmi=87808416

****

News & Views

99% of enterprise users reuse passwords across accounts
Very few users take appropriate action to significantly reduce the risk of password compromise, according to a Balbix report. https://www.helpnetsecurity.com/2020/05/08/reuse-passwords-enterprise/

FIRST releases updated coordination principles for Multi-Party Vulnerability Coordination and Disclosure
The Forum of Incident Response and Security Teams (FIRST) has released an updated set of coordination principles – Guidelines for Multi-Party Vulnerability Coordination and Disclosure version 1.1. https://www.helpnetsecurity.com/2020/05/11/first-coordination-principles/

Why a single online name and social cards will be the new norm
Each day, online users provide companies, organizations, and other individuals with vital personal information without much thought. As social networks and brands began to use this data to make money, people have lost their control over how their data is handled…
https://www.helpnetsecurity.com/2020/05/12/social-cards/

Fact vs. Hype: Zoom Credential “Leak” Analysis
Our team analyzed "leaked" Zoom customer credentials advertised on criminal forums to understand the origins of the stolen data. Spoiler: exposed logins from previous breaches enabled attackers to take over the stolen accounts. In fact, 100% of the credentials were in SpyCloud’s database already. In response... https://spycloud.com/zoom-credential-leak-analysis-fact-vs-hype/?utm_campaign=Newsletter&utm_source=hs_email&utm_medium=email&utm_content=87753381&_hsenc=p2ANqtz--YEViFGCOD1I2-_8ATE9oC1360grPgcgn4njINWR7yMsul3ucTzTEkOKRuOOtd-6pcxeWyY7AL3k2P7XR2yNSM0YMrew&_hsmi=87808416

****

"Ctrl -F" for The Board

Top 10 Routinely Exploited Vulnerabilities
The Cybersecurity and Infrastructure Security Agency (CISA), the Federal Bureau of Investigation (FBI), and the broader U.S. Government are providing this technical guidance to advise IT security professionals at public and private sector organizations to place an increased priority on patching the most commonly known vulnerabilities exploited by sophisticated foreign cyber actors. https://www.us-cert.gov/ncas/alerts/aa20-133a

SOC 2 and SOC 3: What’s the Difference?
Over the last decade, companies have increasingly looked to outsourcing as a way of reducing costs and improving inefficiencies. In addition to outsourcing in general, the increase in outsourcing of software as service and other cloud based technologies has skyrocketed over the last 10 years. Those increases in outsource… https://www.macpas.com/soc-2-and-soc-3-whats-the-difference/

Questions
Contact FIPCO’s Ken Shaurette at 800/722-3498 ext. 251 or email FIPCO IT Services for more information.

"Make Security Part of You and Your Institution's DNA!"

Threat Intelligence Newsletter: May 28, 2020

FIPCO®
IT Audit
Round Table
Discussions

If you would like to host an event, please contact: Becky Schowalter

Upcoming Threat Intelligence Peer Group Discussions
None available at the current time

****

Alerts & Warnings

U.S. Secret Service: "Massive Fraud" Against State Unemployment Insurance Programs
A well-organized Nigerian crime ring is exploiting the COVID-19 crisis by committing large-scale fraud against multiple state unemployment insurance programs, with potential losses in the hundreds of millions of dollars, according to a new alert issued by the U.S. Secret Service. https://securityboulevard.com/2020/05/u-s-secret-service-massive-fraud-against-state-unemployment-insurance-programs/

Cyber espionage tool looks to exfil from air-gapped networks
The cyber espionage framework looks to collect and exfiltrate information, even from air-gapped networks according to research by cybersecurity firm ESET. The framework, which has been in development since 2019, has been dubbed Ramsay and exploits several vulnerabilities and includes capabilities that appear to still be in development and could… https://www.securityweek.com/ramsay-espionage-framework-can-exfiltrate-data-air-gapped-networks

COVID-19 contact tracing text message scams
You've probably been hearing a lot about contact tracing. It's the process of identifying people who have come in contact with someone who has tested positive for COVID-19, instructing them to quarantine and monitoring their symptoms daily. There's no question, contact tracing plays a vital role in helping to stop the spread of COVID-19. But scammers, pretending to be contact tracers and taking advantage of how the process works, are also sending text messages. https://www.consumer.ftc.gov/blog/2020/05/covid-19-contact-tracing-text-message-scams?utm_source=govdelivery

Phishers are trying to bypass Office 365 MFA via rogue apps
Phishers are trying to bypass the multi-factor authentication (MFA) protection on users' Office 365 accounts by tricking them into granting permissions to a rogue application.
https://www.helpnetsecurity.com/2020/05/19/office-365-bypass-mfa/

WolfRAT Android Malware Targets WhatsApp, Facebook Messenger
A new Android malware family has been identified by security researchers after it was repeatedly spotted in campaigns against Thai targets. According to researchers, the malware family, dubbed WolfRAT, targets popular messaging apps to gather intelligence. WhatsApp and Facebook Messenger are among those utilized by the malware operators, who are… https://threatpost.com/wolfrat-android-malware-whatsapp-facebook-messenger/155809/

New DNS Vulnerability Lets Attackers Launch Large-Scale DDoS Attacks
Israeli cybersecurity researchers have disclosed details about a new flaw impacting DNS protocol that can be exploited to launch amplified, large-scale distributed denial-of-service (DDoS) attacks to takedown targeted websites. Called NXNSAttack, the flaw hinges on the DNS delegation mechanism to ...
https://thehackernews.com/2020/05/dns-server-ddos-attack.html?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+TheHackersNews+%28The+Hackers+News+-+Cyber+Security+Blog%29&_m=3n.009a.2231.aa0ao086k1.1edp

New phishing campaign impersonates LogMeIn to steal user credentials
LogMeIn is the parent company of LastPass, so attackers may also be attempting to access the password managers of compromised users, says Abnormal Security. https://www.techrepublic.com/article/new-phishing-campaign-impersonates-logmein-to-steal-user-credentials/?ftag=TREa988f1c&bhid=78480402&mid=12842966&cid=712423569

****

Hints & Tips plus Security Awareness

Reverse RDP attacks: How to protect your organization
A remote PC infected with certain malware could take over a client that tries to connect to it, says Check Point Research. Here's how to prevent… https://www.techrepublic.com/article/reverse-rdp-attacks-how-to-protect-your-organization/?ftag=TREa988f1c&bhid=78480402&mid=12839616&cid=712423569

3 Common Social Engineering Attacks That Have You Saying Goodbye To Your Data Without Even Realizing It
Social engineering isn't new by any stretch of the imagination. Con artists have been active since before the days of modern technology. Social engineering, however, has continued to evolve and take on new shapes. The challenge that many businesses and individuals face today is the realism behind social engineering attacks. They have become more sophisticated and can fool even the most tech-savvy executives. This… https://blog.nxtsoft.com/3-common-social-engineering-attacks-that-have-you-saying-goodbye-to-your-data-without-even-realizing-it?utm_campaign=Data%20Security%20Newsletter&utm_source=hs_email&utm_medium=email&utm_content=88166849&_hsenc=p2ANqtz--SLYlSdrE229bTkbTCR1bPDFsxLmj2iy_AVybsJFDbx04XhmYLvOPY4EsLixf7s3XX72Sw1uBPuwX8hToVaEoMcNgRlw&_hsmi=88166849

Credit reports have no charge, every week
If you're feeling anxious about your financial health during these uncertain times, you're not alone. That's why the three national credit reporting agencies are giving people weekly access to monitor their credit report... https://www.consumer.ftc.gov/blog/2020/05/credit-reports-are-now-free-every-week?utm_source=govdelivery

****

News & Views

Emotet Banking Malware Up 375% Now Targeting Weak Passwords
It looks like Emotet malware may be coming to a Wi-Fi network near you. Discovered in 2014 as a banking Trojan, Emotet's malware growth has been aggressive. In the "2020 State of Malware Report," Ma… https://www.sosdailynews.com/news.jspx?&articleid=C5D49F3FF26DD3429EF14756F6A75BD8&sx=79

Less than a quarter of Americans use a password manager
A large percentage of Americans currently do not take the necessary steps to protect their passwords and logins online, FICO reveals. https://www.helpnetsecurity.com/2020/05/18/use-password-manager/

Average US citizen had personal information stolen at least 4 times in 2019
A new study of publicly reported data shows the average person experienced a breach every three months last year… https://www.techrepublic.com/article/average-us-citizen-had-personal-information-stolen-at-least-4-times-in-2019/?ftag=TREa988f1c&bhid=78480402&mid=12839616&cid=712423569

BEC Attacks Skyrocket: Over $26 Billion In Damages And Growing
Since email phishing attacks were first discovered in 1995, using email as a weapon has been gaining steam over time. The ongoing commitment by cybercriminals to improve email phishing brings it to a new level of success. Business email compromise (BEC) attacks target a specific business and select employees. BEC is known for unleashing malware, including ransomware and financial attacks, and for tricking employees into handing over large sums of money. The FBI finds the cost of BEC to U.S. businesses topped $26 billion over the past three years.
https://www.sosdailynews.com/news.jspx?&articleid=7AC4622D3A1F3DCF50DC80669792FE88&sx=79

How secure are open source libraries?
Seven in 10 applications have a security flaw in an open source library, highlighting how use of open source can introduce flaws, increase risk, and add to security debt, a Veracode research reveals.
https://www.helpnetsecurity.com/2020/05/21/secure-open-source-libraries/

****

"Ctrl -F" for The Board

CISOs are critical to thriving companies: Here's how to support their efforts
Even before COVID-19 initiated an onslaught of additional cybersecurity risks, many chief information security officers (CISOs) were struggling. https://www.helpnetsecurity.com/2020/05/19/cisos-struggling/

Questions
Contact FIPCO's Ken Shaurette at 800/722-3498 ext. 251 or email FIPCO IT Services for more information.

"Make Security Part of You and Your Institution's DNA!"

Threat Intelligence Newsletter: June 8, 2020

If you would like to host an event, please contact: Becky Schowalter

Upcoming Threat Intelligence Peer Group Discussions
None available at the current time

****

Alerts & Warnings

New propagation module makes Trickbot more stealthy
Trickbot infections of Domain Controller (DC) servers has become more difficult to detect due to a new propagation module that makes the malware run from memory, Palo Alto Networks researchers have found. https://www.helpnetsecurity.com/2020/06/01/trickbot-propagation/

NSA Warns of Ongoing Russian Hacking Campaign Against U.S. Systems
On Thursday, the US National Security Agency (NSA) released a warning to government partners and private companies about an ongoing Russian hacking operation that targets operating systems behind computer infrastructure. This intrusion technique actively exploits a vulnerability that the NSA advised companies to take seriously. The notice is part of…
https://www.nytimes.com/reuters/2020/05/28/world/europe/28reuters-cyber-usa-russia.html

Remote workers being targeted with Google-branded cyberattacks
Remote workers have been targeted by up to 65,00 Google-branded impersonation attacks, according to a new study from cybersecurity specialist Barracuda Networks. This type of scam, called “spear phishing,” uses branded sites to trick victims into sharing their login credentials.
https://www.insurancebusinessmag.com/us/news/cyber/remote-workers-targeted-by-up-to-65000-googlebranded-cyberattacks-223688.aspx

The “return” of fraudulent wire transfers
Ransomware gangs targeting businesses are currently getting more public attention, but scammers trying to trick employees into performing fraudulent wire transfers are once again ramping up their efforts, US-headquartered law firm BakerHostetler has warned.
https://www.helpnetsecurity.com/2020/06/03/fraudulent-wire-transfers/

****

Hints & Tips plus Security Awareness

Solving the security challenges of remote working
Unprecedented times call for unprecedented actions and the ongoing COVID-19 pandemic has caused what is likely to be the biggest shift towards remote working that the world has ever seen. But, while the technology has been around for quite some time, recent events demonstrate just how few…
https://www.helpnetsecurity.com/2020/05/28/security-challenges-remote-working/

Zero trust security: A cheat sheet
Zero trust means rethinking the safety of every bit of tech on a network. Learn five steps to building a zero trust environment. https://www.techrepublic.com/article/zero-trust-security-a-cheat-sheet/?ftag=TREa988f1c&bhid=78480402&mid=12860433&cid=712423569

Lean into zero trust to ensure security in times of agility
Bad actors are rapidly mounting phishing campaigns, setting up malicious websites and sending malicious attachments to take full advantage of the pandemic and users’ need for information, their fears and other emotions. More often than not, the goal is the compromise of login credentials.
https://www.helpnetsecurity.com/2020/06/02/zero-trust-journey/

How to Pay a Ransom
Read Nicole Ferraro explain how you can negotiate with ransomware makers after your computer is infected with ransomware on Dark Reading : It’s Tuesday morning. You arrive at your desk […].
https://www.darkreading.com/theedge/how-to-pay-a-ransom/b/d-id/1337909

****

News & Views

Hackers Compromise Cisco Servers Via SaltStack Flaws
Cisco disclosed on Thursday that six of its VIRL-PE servers were compromised after threat actors used critical SaltStack vulnerabilities in a targeted attack. Cisco stated that the attackers used to known vulnerabilities that exist in the open-source Salt management framework and are used in Cisco products. Two Cisco products still... https://threatpost.com/hackers-compromise-cisco-servers-saltstack/156091/

Data Breach at Bank of America
Bank of America has disclosed that it suffered from a data breach affecting a small number of clients who had previously applied for their Paycheck Protection Program (PPP). Information involving Bank of America's clients was exposed in late April when the bank uploaded the applicants' details onto a the US…
https://www.infosecurity-magazine.com/news/data-breach-at-bank-of-america/

48% of employees are less likely to follow safe data practices when working from home
According to a Tessian survey, data protection concerns go out the window for remote employees.
https://www.techrepublic.com/article/48-of-employees-are-less-likely-to-follow-safe-data-practices-when-working-from-home/?ftag=TREa988f1c&bhid=78480402&mid=12860433&cid=712423569

Your Infant's Identity For Sale On The Dark Web
We never forget about our kids. Right? They are the apples of our eyes, hold the keys to our hearts, and the greatest things since sliced bread, and we always try our best to keep them safe. Don't we? While we are teaching them to safely cross the street, making sure they are fed, clothed, and have roofs over their heads, in this digital world we now live in, there is something else about which we also need to worry…their identities.
https://www.sosdailynews.com/news.jspx?&articleid=B8E9B6520331F4768FAEC704D4A59B77&sx=79

****

"Ctrl -F" for The Board

CISO Conversations: Mastercard, Ellie Mae Security Chiefs Discuss the People Problem
In this CISO Conversations feature, SecurityWeek talks to Mastercard CISO Ron Green, and Ellie Mae CISO Selim Aissi from the finance sector, concentrating on the people problem for CISOs.
https://www.securityweek.com/ciso-conversations-mastercard-ellie-mae-cisos-discuss-people-problem

Questions
Contact FIPCO's Ken Shaurette at 800/722-3498 ext. 251 or email FIPCO IT Services for more information.

"Make Security Part of You and Your Institution's DNA!"

Threat Intelligence Newsletter: June 12, 2020

FIPCO®
IT Audit
Round Table
Discussions

If you would like to host an event, please contact: Becky Schowalter

Upcoming Threat Intelligence Peer Group Discussions
None available at the current time

****

Alerts & Warnings

PoC RCE exploit for SMBGhost Windows flaw released
A security researcher has published a PoC RCE exploit for SMBGhost (CVE-2020-0796), a wormable flaw that affects SMBv3 on Windows 10 and some Windows Server versions.
https://www.helpnetsecurity.com/2020/06/08/smbghost-poc-rce-exploit/

Cybercriminals now spoofing job hunters to deploy password-stealing malware
Malicious files masquerading as curriculum vitae are being sent to businesses to install malware that can capture passwords and other sensitive information, says Check Point Research.
https://www.techrepublic.com/article/cybercriminals-now-spoofing-job-hunters-to-deploy-password-stealing-malware/?ftag=TREa988f1c&bhid=78480402&mid=12870439&cid=712423569

Exploits Target Patched Server Message Block
Publicly available and functional proof-of-concept (PoC) code that exploits a vulnerability in the Microsoft Server Message Block 3.1.1 (SMBv3) protocol CVE-2020-0796 in unpatched systems, according to a report with CISA. https://isssource.com/exploits-target-patched-server-message-block/?utm_medium=email&_hsmi=89196805&_hsenc=p2ANqtz-9NCmxfLPchoz3HcAzBXPz5I1OJrwbn3bVE-KyhPPqyfmInAbUiDsICd47VQ5LmqsG5ZNV4LZQdgEi7rhDar7lfGYtgHQ&utm_content=89196805&utm_source=hs_email

This new ransomware targets Windows and Linux in surprising ways
Aimed at SMBs, educational facilities, and software companies, the ransomware leverages Java to encrypt server-based files, according to BlackBerry and KPMG. https://www.techrepublic.com/article/new-java-based-ransomware-targets-windows-and-linux-servers/?ftag=TREa988f1c&bhid=78480402&mid=12870439&cid=712423569

PonyFinal Is Another New Ransomware To Watch Out For
Microsoft recently issued a security advisory about a new strain of ransomware that's been cropping up with increasing frequency in India, Iran and the US. https://www.neorhino.com/2020/06/08/ponyfinal-is-another-new-ransomware-to-watch-out-for/?utm_medium=email&_hsmi=89196805&_hsenc=p2ANqtz-99XLotsPh139FajjHed4KRhSerHtwH5lPQVwDrL4kNfuohEKS3JPI_3rUIHAo1mpsyXZyzyuw0fZiQaavuczrCdCG6lg&utm_content=89196805&utm_source=hs_email

Maze Ransomware adds Ragnar Locker to its extortion cartel
Another ransomware group has partnered with Maze Ransomware, Ragnar Locker, to utilize their data leak platform. Last week, it was discovered that LockBit ransomware had teamed up with the Maze operator. The massive data leak platform is used to extort victims whose files were stolen in a ransomware attack by… https://www.bleepingcomputer.com/news/security/maze-ransomware-adds-ragnar-locker-to-its-extortion-cartel/

UPnP vulnerability lets attackers steal data, scan internal networks
A vulnerability (CVE-2020-12695) in Universal Plug and Play (UPnP), which is implemented in billions of networked and IoT devices – personal computers, printers, mobile devices, routers, gaming consoles, Wi-Fi access points, and so on – may allow unauthenticated, remote attackers to…
https://www.helpnetsecurity.com/2020/06/09/cve-2020-12695/

****

Hints & Tips plus Security Awareness

The importance of effective vulnerability remediation prioritization
Too many organizations have yet to find a good formula for prioritizing which vulnerabilities should be remediated immediately and which can wait. https://www.helpnetsecurity.com/2020/06/09/importance-vulnerability-remediation-prioritization/

Dealing with a deceased relative’s debt
Especially during this time of crisis, dealing with the death of a loved one is hard. Dealing with a debt collector calling about their debts can make it even harder. If you’re in this situation and a debt collector calls, it’s important to know who is respo… https://www.consumer.ftc.gov/blog/2020/06/dealing-deceased-relatives-debt?utm_source=govdelivery

SIM Swap Scams: How to Protect Yourself
If your cell phone is your go-to device for checking your email, paying your bills, or posting to social media, you’re not alone. So imagine that your cell phone suddenly stops working:
https://www.consumer.ftc.gov/blog/2019/10/sim-swap-scams-how-protect-yourself

Businesses torn between paying and not paying ransoms
40% of consumers hold business leaders personally responsible for ransomware attacks businesses suffer, according to a research from Veritas Technologies.
https://www.helpnetsecurity.com/2020/06/10/businesses-torn-between-paying-and-not-paying-ransoms/

Venmo Mobile Cash Users Targeted by Scammers + Coronavirus Scams Update
How to beat the Venmo scammer, Sending and receiving money online from your mobile device is now easier than ever, thanks to apps like Venmo. https://scambusters.org/venmo.html

****

News & Views

Advanced Threat Protection Beyond AntiVirus
THE SECURITY GAPS NO ONE WILL TELL YOU ABOUT IN EPP\EDR AND NTA\NDR…
https://cdn2.hubspot.net/hubfs/3454686/Beyond%20The%20AV%20White%20Paper%20-%20Cynet.pdf?utm_medium=email&_hsmi=70660323&_hsenc=p2ANqtz--amzNX8PqYt7kdO_ottoOwPF0gkScf1js1unQ8zLcaFHoW_CGQzAF1J8Ct-54GsFynT33efjgrYdPzY9NFmISJq0sQIQ&utm_content=70660323&utm_source=hs_automation
New Partnership with FIPCO; https://www.fipco.com/solutions/it-audit-security/autonomous-endpoint-protection

NSA warns of new Sandworm attacks on email servers
NSA says Russia's military hackers have been attacking Exim email servers to plant backdoors since August 2019. https://www.zdnet.com/article/nsa-warns-of-new-sandworm-attacks-on-email-servers/

Why traditional network perimeter security no longer protects
Greek philosopher Heraclitus said that the only constant in life is change. This philosophy holds true for securing enterprise network resources. Network security has been and is constantly evolving, often spurred by watershed events such as the 2017 NotPetya ransom...
https://www.helpnetsecurity.com/2020/06/09/zta-perimeter-security/

3 common misconceptions about PCI compliance
Being the PCI guy at my company carries a certain amount of burden. Not only am I responsible for all of the ongoing compliance and yearly assessments, but I also have to interpret the PCI DSS scriptures on how PCI affects products, initiatives, and platform decisions.
https://www.helpnetsecurity.com/2020/06/10/pci-compliance-misconceptions/

****

"Ctrl -F" for The Board

Buyer Beware: How to Avoid Scams, Fraud, & Rumor During an Emergency
The amount of scams has risen since the start of the coronavirus disease 2019 (COVID-19) outbreak. Reports to the… https://www.consumer.ftc.gov/blog/2020/04/covid-19-scam-reports-numbers?utm_source=govdelivery&deliveryName=USCDC-481_DM30214

Questions
Contact FIPCO's Ken Shaurette at 800/722-3498 ext. 251 or email FIPCO IT Services for more information.

"Make Security Part of You and Your Institution's DNA!"

Threat Intelligence Newsletter: June 22, 2020

FIPCO®
IT Audit
Round Table
Discussions

If you would like to host an event, please contact: Becky Schowalter

Upcoming Threat Intelligence Peer Group Discussions
None available at the current time

****

Alerts & Warnings

This Scam Looks Like Credit Card Help
At first glance, this scam looks so helpful. It's a call or text message wanting to help you resolve an overpayment on your credit card. However, this sneaky con is actually a phishing scheme. And it's only likely to get more popular, as COVID causes many shoppers to buy online and businesses to only accept credit cards. https://www.bbb.org/article/scams/16909-bbb-tip-credit-card-scams

Getting stimulus checks from car dealerships? Nope.
During these difficult economic times, scammers will do almost anything to try to get your money. Including, it turns out, making bogus claims about economic stimulus checks to lure customers to auto sales events. https://www.consumer.ftc.gov/blog/2020/06/getting-stimulus-checks-car-dealerships-nope?utm_source=govdelivery

Criminals Using SIM Swapping Scam
The FBI San Francisco Division, in coordination with the Office of Private Sector (OPS), prepared this LIR to alert private sector partners about an ongoing Subscriber Identity Module (SIM) card swapping scheme to obtain financial and/or proprietary data. Commonly referred to as SIM swapping, SIM hacking, or similarly, phone-porting activity, criminals use both sophisticated and unsophisticated methods to conduct the scheme. https://www.youtube.com/watch?v=sFI3scZKpm0

****

Hints & Tips plus Security Awareness

How to hack-proof your network to repel crooks and scammers
Most of us have more devices connected to our home networks than we realize, and hackers know all the many different ways they can use them to invade our system. https://scambusters.org/hackproof.html

US bank customers targeted in ongoing Qbot campaign
F5 Labs has discovered ongoing attacks utilizing the Qbot malware payloads to steal banking credentials from customers of US financial institutions, including JP Morgan, Wells Fargo, Capital One, Bank of America, and Citibank. Qbot is a banking trojan with features that are used to steal financial data, such as logging… https://www.bleepingcomputer.com/news/security/us-bank-customers-targeted-in-ongoing-qbot-campaign/

Cynet Wants to Help Resource-Constrained Organizations with a Holistic SaaS Security Platform
Cybersecurity company Cynet recently announced the release of a SaaS version of its security platform, Cynet 360. Designed to help organizations with limited security resources, Cynet brings a unified defense across endpoints, network, files and users. The suite includes endpoint protection, EDR, vulnerability management, deception, threat intelligence and network and end-user analytics. https://securityboulevard.com/2018/11/cynet-wants-to-help-resource-constrained-organizations-with-a-holistic-saas-security-platform/ or contact FIPCO https://www.fipco.com/solutions/it-audit-security/autonomous-endpoint-protection

SANS Security Awareness Virtual Forum
Join us on Wednesday, August 5th, for the SANS Security Awareness Virtual Forum which is free to the community. This virtual event will be hosted from 9:30 am to 1:30 pm EST and includes multiple talks, an online scavenger hunt, video wars, and free resources. During the half-day forum, you'll gain insight on the latest proven advances and approaches in remotely communicating to, engaging and securing your workforce. You will hear from experienced security awareness professionals share their practical recommendations and lessons learned that you can apply right away within your own organization. https://www.sans.org/webcasts/security-awareness-virtual-forum-115605?utm_medium=Email&utm_source=Ouch&utm_content=672274&utm_campaign=STH+Ouch

****

News & Views

The FBI expects a surge of mobile banking threats
The increased use of mobile banking apps due to the COVID-19 pandemic is sure to be followed by an increased prevalence of mobile banking threats: fake banking apps and banking Trojans disguised as those apps, the FBI has warned. https://www.techrepublic.com/article/fbi-warns-about-cybercriminals-exploiting-mobile-banking-apps/?ftag=TREa988f1c&bhid=78480402&mid=12881198&cid=712423569

Dell report details rise in cyberattacks and disruptive events
A new report focuses on a surge in cyberattacks and other disruptions during the coronavirus pandemic and the costs of these events. https://www.techrepublic.com/article/dell-report-details-rise-in-cyberattacks-and-disruptive-events/?ftag=TREa988f1c&bhid=78480402&mid=12881198&cid=712423569

AWS said it mitigated a 2.3 Tbps DDoS attack, the largest ever
Amazon said its AWS Shield service mitigated the largest DDoS attack ever recorded, stopping a 2.3 Tbps attack in mid-February this year. https://www.zdnet.com/article/aws-said-it-mitigated-a-2-3-tbps-ddos-attack-the-largest-ever/

****

"Ctrl -F" for The Board

Endpoint security market to reach $18.6B by 2027
The endpoint security market is expected to grow at a CAGR of 5.9% from 2020 to reach $18.6 billion by 2027, according to Meticulous Research. https://www.helpnetsecurity.com/2020/06/16/endpoint-security-market/

Questions
Contact FIPCO's Ken Shaurette at 800/722-3498 ext. 251 or email FIPCO IT Services for more information.

"Make Security Part of You and Your Institution's DNA!"

Threat Intelligence Newsletter: June 29, 2020

FIPCO®
IT Audit
Round Table
Discussions

If you would like to host an event, please contact: Becky Schowalter

Upcoming Threat Intelligence Peer Group Discussions
None available at the current time

****

Alerts & Warnings

FTC, SBA warn companies about SBA loan promises
The latest recipients of government warning letters are six companies that said they could speed U.S. Small Business Administration (SBA) loans for businesses struggling to stay afloat during the COVID-19 pandemic. The letters – from the FTC and the SBA – direct the companies to remove all false claims from their websites immediately. https://www.consumer.ftc.gov/blog/2020/06/ftc-sba-warn-companies-about-sba-loan-promises?utm_source=govdelivery

BBB Scam Alert: Hiring freelance help? Watch out for imposters
Small businesses looking to hire a freelancer online, beware. Scammers are creating fake accounts on platforms like Upwork. They use photos and resumes of real professionals and entice businesses with low rates. https://www.bbb.org/article/news-releases/22645-bbb-scam-alert-hiring-freelance-help-watch-out-for-imposters

Phishing attacks impersonate QuickBooks invoices ahead of July 15 tax deadline
Targeting the CEO and others in an organization, the attacks spotted by cybersecurity firm Darktrace were detected due to artificial intelligence. https://www.techrepublic.com/article/phishing-attacks-impersonate-quickbooks-invoices-ahead-of-july-15-tax-deadline/?ftag=TREa988f1c&bhid=78480402&mid=12891818&cid=712423569

This Scam Looks Like Credit Card Help
At first glance, this scam looks so helpful. It's a call or text message wanting to help you resolve an overpayment on your credit card. https://www.bbb.org/article/scams/16909-bbb-tip-credit-card-scams

Hackers Using Google Analytics to Bypass Web Security and Steal Credit Cards
On Monday, researchers reported that hackers are exploiting Google's Analytics service to steal credit card information from compromised e-commerce sites. Kaspersky, Sansec, and PerimeterX all published reports claiming that attackers are injecting data-stealing code onto the infected sites along with a Google Analytics tracking code for their own account. https://thehackernews.com/2020/06/google-analytics-hacking.html

Self-Propagating Lucifer Malware Targets Windows Systems
Security experts have identified a new malware targeting Windows systems with crypto-jacking and DDoS attacks, named Lucifer for its devilish features. Lucifer is a self-propagating malware, and initially bombards PCs in hopes of taking advantage of vulnerabilities. The malware capitalizes on lists of unpatched vulnerabilities to obtain a foothold in… https://threatpost.com/self-propagating-lucifer-malware-targets-windows-systems/156883/

****

Hints & Tips plus Security Awareness

Google Yanks 106 'Malicious' Chrome Extensions
On Thursday, Google removed over 100 Chrome browser extensions that it found to be malicious, after reports that they were being used to siphon sensitive user data. Google also published the research behind the apps, in which Awake Security alleges millions of Chrome users have been targeted by threat actors… https://threatpost.com/google-yanks-106-malicious-chrome-extensions/156731/

VMware Patches Several Vulnerabilities Allowing Code Execution on Hypervisor
VMware addresses 10 vulnerabilities in ESXi, Workstation and Fusion products, including serious flaws that can be exploited for code execution on the hypervisor. Please see the advisory here: https://www.vmware.com/security/advisories/VMSA-2020-0015.html

The IRS won't call about your stimulus money
Most people have already gotten their economic stimulus payments, but the Internal Revenue Service is still sending them out. If you haven't gotten yours yet or have questions about it, the IRS has a number you can call to get answers to common questions. But the IRS won't be calling you. https://www.consumer.ftc.gov/blog/2020/06/irs-wont-call-about-your-stimulus-money-0?utm_source=govdelivery

Fixing all vulnerabilities is unrealistic, you need to zero in on what matters
As technology constantly advances, software development teams are bombarded with security alerts at an increasing rate. This has made it nearly impossible to remediate every vulnerability, rendering the ability to properly prioritize rem…. https://www.helpnetsecurity.com/2020/06/24/remediate-every-vulnerability-unrealistic/

New technique protects consumers from voice spoofing attacks
Fraudsters can record a person's voice for voice assistants like Amazon Alexa or Google Assistant and replay it to impersonate that individual. They can also stitch samples together to mimic a person's voice in order to spoof, or trick third parties. https://www.helpnetsecurity.com/2020/06/24/voice-spoofing-attacks/

****

News & Views

How much is your data worth on the dark web?
Credit card details, online banking logins, and social media credentials are available on the dark web at worryingly low prices, according to Privacy Affairs. https://www.helpnetsecurity.com/2020/06/19/dark-web-prices/

The State of Ransomware in 2020
Ransomware cyberattacks are a big business, so big in fact, that research anticipates a business is attacked by a cybercriminal every 11 seconds and damage costs from these attacks will hit around $20 billion by 2021. https://www.blackfog.com/the-state-of-ransomware-in-2020/

Questions
Contact FIPCO's Ken Shaurette at 800/722-3498 ext. 251 or email FIPCO IT Services for more information.

"Make Security Part of You and Your Institution's DNA!"

Threat Intelligence Newsletter: July 9, 2020

FIPCO®
IT Audit
Round Table
Discussions

If you would like to host an event, please contact: Becky Schowalter

Upcoming Threat Intelligence Peer Group Discussions
None available at the current time

****

Alerts & Warnings

Vulnerable drivers can enable crippling attacks against ATMs and POS systems
Newly discovered vulnerabilities could allow more persistent and destructive attacks on popular models of ATM and POS devices. https://www.csoonline.com/article/3564540/vulnerable-drivers-can-enable-crippling-attacks-against-atms-and-pos-systems.html

80,000 printers are exposing their IPP port online
For years, security researchers have warned that every device left exposed online without being protected by a firewall is an attack surface. Hackers can deploy exploits to forcibly take control over the device, or they can just connect to the exposed port if no authentication is required.
https://www.zdnet.com/article/80000-printers-are-exposing-their-ipp-port-online/

Fake "DNS Update" emails targeting site owners and admins
Attackers are trying to trick web administrators into sharing their admin account login credentials by urging them to activate DNSSEC for their domain. https://www.helpnetsecurity.com/2020/06/30/fake-dns-update/

FBI Issues Warning Of Uptick In Mobile Banking Malware During Pandemic
The FBI issued another warning recently about mobile banking applications. During the coronavirus pandemic, more people are downloading mobile banking apps so they can avoid the trip out to the financial institution and potentially expose themselves to the virus by making an in-person visit. Unfortunately, the hackers are also on top of this and are issuing their malware hoping it'll get downloaded so they can steal banking credentials.
https://www.sosdailynews.com/news.jspx?&articleid=31E7BCA19B9407A2FA77947FA488E06B&sx=79

Scams in online sales: when orders don't arrive
When local stores ran out of the supplies we needed to manage COVID-19, many of us turned to online sources. According to a new Data Spotlight, scammers ran online sites and took orders for scarce items, but didn't deliver. https://www.consumer.ftc.gov/blog/2020/07/scams-online-sales-when-orders-dont-arrive?utm_source=govdelivery

New Android Spyware Tools Emerge in Widespread Surveillance Campaign
Brand new Android spyware tools have been discovered being deployed in a widespread APT campaign designed to spy on the Uyghur ethnic minority group. Researchers discovered the surveillance campaign, which dates back to 2013 and includes three never-before-seen surveillance tools, through analyzing trojanized legitimate applications. The campaign's Android surveillance tools,… https://threatpost.com/four-android-spyware-tools-surveillance-campaign/157063/

Caller ID Spoofing Scams Prey on Trust to Steal Sensitive Information
Caller ID or phone spoofing is a scam whereby callers impersonate government officials, financial institutions, or legitimate company by using fraudulent displays of phone numbers (or "spoofs") — to gain the victim's trust and get them to disclose Personally Identifiable Information (PII) or sensitive financial information. https://www.fightingidentitycrimes.com/caller-id-spoofing-scams/

TrickBot malware now checks screen resolution to evade analysis
(an important reason traditional AV no longer works. Contact FIPCO for a demonstration of Cynet360)
The notorious TrickBot trojan has evolved again, this time acquiring the ability to check the screen resolutions of victims to detect whether the malware is running on a virtual machine or on the actual device. Researchers typically analyze malware while running a virtual machine that is outfitted with different analysis… https://www.bleepingcomputer.com/news/security/trickbot-malware-now-checks-screen-resolution-to-evade-analysis/

****

Hints & Tips plus Security Awareness

Emergency Windows 10 Update: Critical 'Large Image' Security Flaw Confirmed
Microsoft has issued an emergency patch for a serious vulnerability affecting the Windows 10. Microsoft chose not to wait for Patch Tuesday, as the vulnerability could lead to the compromise of Windows 10 devices or Windows Server System. Another vulnerability was also patched in the emergency out-of-band update, ranked as… https://www.forbes.com/sites/daveywinder/2020/07/01/one-large-image-could-compromise-windows-10-emergency-security-update-confirmed-crtitical-microsoft-vulnerability/#5c83e0783e3f

AA20-183A: Defending Against Malicious Cyber Activity Originating from Tor
This advisory—written by the Cybersecurity Security and Infrastructure Security Agency (CISA) with contributions from the Federal Bureau of Investigation (FBI)—highlights risks associated with Tor, along with technical details and recommendations for mitigation. Cyber threat actors can use Tor software and network infrastructure for anonymity and obfuscation purposes to clandestinely conduct malicious cyber operations… https://us-cert.cisa.gov/ncas/alerts/aa20-183a

Cyber Defense Magazine
3 Practices to Avoid Risk…
https://www.cyberdefensemagazine.com/newsletters/july-2020/mobile/index.html

5 Actions to Avoid SIM Swap Scam + Latest Covid Scams
Crooks still pulling off SIM swap trick despite security clampdown… https://scambusters.org/simswap.html

****

News & Views

How much is your data worth on the dark web?
Ransomware cyberattacks are a big business, so big in fact, that research anticipates a business is attacked by a cybercriminal every 11 seconds and damage costs from these attacks will hit around $20 billion by 2021. https://www.blackfog.com/the-state-of-ransomware-in-2020/

Major US Companies Targeted in New Ransomware Campaign
A security research group claims that Evil Corp targeted at least 31 victims in a hacking campaign that aimed to deploy the new WastedLocker malware. Many of the targeted organizations are Fortune 500 companies that are based in the US. If the attacks had succeeded, they could have had a… https://www.darkreading.com/attacks-breaches/major-us-companies-targeted-in-new-ransomware-campaign/d/d-id/1338189

****

"Ctrl -F" for The Board

Marred by garbage: Striking a balance for security data
Security applications are subject to the age-old computing axiom of "garbage in, garbage out." To work effectively, they need the right data. Too much irrelevant data may overwhelm the processing an… https://www.helpnetsecurity.com/2020/06/26/how-much-data/

200% increase in invoice and payment fraud BEC attacks
There has been a 200 percent increase in BEC attacks focused on invoice or payment fraud from April to May 2020, according to Abnormal Security. This sharp rise continues the trend. https://www.helpnetsecurity.com/2020/06/30/payment-fraud-bec-attacks/

Questions
Contact FIPCO's Ken Shaurette at 800/722-3498 ext. 251 or email FIPCO IT Services for more information.

"Make Security Part of You and Your Institution's DNA!"

Threat Intelligence Newsletter: July 13, 2020

FIPCO®
IT Audit
Round Table
Discussions

If you would like to host an event, please contact: Becky Schowalter

Upcoming Threat Intelligence Peer Group Discussions
None available at the current time

****

Alerts & Warnings

New Android Spyware Tools Emerge in Widespread Surveillance
Brand new Android spyware tools have been discovered being deployed in a widespread APT campaign designed to spy on the Uyghur ethnic minority group. Researchers discovered the surveillance campaign, which dates back to 2013 and includes three never-before-seen surveillance tools, through analyzing trojanized legitimate applications. The campaign's Android surveillance tools…
https://threatpost.com/four-android-spyware-tools-surveillance-campaign/157063/

Phishing attack spoofs Twitter to steal account credentials
A new phishing campaign spotted by Abnormal Security attempts to trick people with a phony Twitter security notification. https://www.techrepublic.com/article/phishing-attack-spoofs-twitter-to-steal-account-credentials/?ftag=TREa988f1c&bhid=78480402&mid=12914506&cid=712423569

****

Hints & Tips plus Security Awareness

Free Password Auditor
Scan Active Directory and find users with known compromised password in minutes…
https://www.enzoic.com/password-auditing-tool/?utm_medium=email&_hsmi=90271889&_hsenc=p2ANqtz--3rNmN4flmgz1VD_SxsDOXpf2C9rx84kun-Lx09SR_DOn7cCsrC7DAoHf9FeTgOaK68z61vpG65pYuE1VFARP4wXHOMg&utm_content=90271889&utm_source=hs_automation

5 NSA Approved Strategies for Improved VPN Security
The US National Security Agency has noticed a surge in cyberattacks targeting VPNs since the COVID-19 pandemic has forced more people to work from home. https://www.techrepublic.com/article/5-nsa-recommended-strategies-for-improving-your-vpn-security/?ftag=TREa988f1c&bhid=78480402&mid=12914506&cid=712423569

CCPA enforcement to put pressure on financial organizations' IT resources
Enforcement of the California Consumer Privacy Act (CCPA), which begins on July 1, 2020, is going to put additional pressure on already overstretched IT resources and budgets… https://www.helpnetsecurity.com/2020/07/03/ccpa-enforcement-pressure/

Managing Outsourced Risk
How to read a SOC1/SOC2… https://www.bluetoad.com/publication/?m=1336&i=666070&p=30

The Updated Do's and Don'ts of Password Security
Updated NIST guidelines revealed that some practices once considered foundational are rather outdated, so here are the new Do's and Don'ts for password policies. https://www.enzoic.com/password-security-dos-and-donts/?utm_medium=email&_hsmi=90271889&_hsenc=p2ANqtz-_kZdBoLH8VhefCId7sTFyNejYYAhKL32ENviTAzp0j0b_A924u4cRD9O_WGu9ZFowPQGQgdCqyGXAl2Gt0A7_Xw6h4NQ&utm_content=90271889&utm_source=hs_automation
Android Users Hit with 'Undeletable' Adware
According to researchers at Kaspersky, 14.8 percent of Android users who were targeted with mobile malware or adware last year were left with permanent and undeletable files. This is called a system partition infection, and the undeletable files can range from trojans that can install and run apps without the… https://threatpost.com/android-users-undeletable-adware/157189/

****

News & Views

451 Research: Love 'em or Hate 'em, Passwords Are Here to Stay
There has been renewed focus on compromised credentials, which have become the primary attack vector in the vast majority of data breaches. However, passwords remain a staple of many firms' security framework. https://www.enzoic.com/wp-content/uploads/451-Research_Advisory_BIB_Enzoic.pdf?utm_medium=email&_hsmi=90271889&_hsenc=p2ANqtz-_e69eAbaRoW6-Dr8pc4HEeRv561eGJeMMfB54E5GELXGVXfx3Cf0z_19oBfL68co5006LWVnakjMei-g44SccuJmCPNg&utm_content=90271889&utm_source=hs_automation

Questions
Contact FIPCO's Ken Shaurette at 800/722-3498 ext. 251 or email FIPCO IT Services for more information.

"Make Security Part of You and Your Institution's DNA!"

Threat Intelligence Newsletter: July 17, 2020

FIPCO®
IT Audit
Round Table
Discussions

If you would like to host an event, please contact: Becky Schowalter

Upcoming Threat Intelligence Peer Group Discussions
None available at the current time

****

Alerts & Warnings

Most Popular Home Routers Have 'Critical' Flaws
A recent security report from German think tank Fraunhofer Institute analyzed 127 popular home routers and concluded that most contained at least one critical security flaw. The devices, including popular ones from Netgear, Linksys, and D-Link, all contain serious vulnerabilities that are not patched in updates. The report explained that... https://threatpost.com/report-most-popular-home-routers-have-critical-flaws/157346/

Joker Malware Apps Once Again Bypass Google's Security to Spread via Play Store
Cybersecurity researchers took the wraps off yet another instance of Android malware hidden under the guise of legitimate applications to stealthily subscribe unsuspecting users for premium services without their knowledge. In a report published by Check Point research…
https://thehackernews.com/2020/07/joker-android-mobile-virus.html?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+TheHackersNews+%28The+Hackers+News+-+Cyber+Security+Blog%29&_m=3n.009a.2269.aa0ao086k1.1fbm

Scammers Move Credit Card Theft Online
For years, scammers have used a small device on ATMs, gas pumps, and other terminals, to harvest credit card information. But as technology improves, this "skimming" has become less effective. However, scammers aren't deterred! Now, they use a technique called "e-skimming" to steal credit card data from online shoppers instead. https://www.cnbc.com/2020/01/31/e-skimming-cyberattack-is-growing-along-with-online-shopping.html?utm_source=newsletter&utm_medium=email&utm_content=eskimming%20in%20this%20CNBC%20story&utm_campaign=scam-alert

Scammers impersonate the FTC, too

Scammers never seem to run out of new ways to try to take your money or steal your identity, especially in times of crisis like the one we're living through now. One of the latest schemes involves an email that claims—falsely—that it came from me. It might say you're entitled to some money from a phony "Global Empowerment Fund" and tell you to give your bank account number or credit card information. https://www.consumer.ftc.gov/blog/2020/07/scammers-impersonate-ftc-too?utm_source=govdelivery

Spawn Of TrickBot Trojan Bypasses 2FA

A recent IBM X-FORCE report finds victims of "TrickMo," a TrickBot variant, are being lulled into a false sense of security. This happens after Android users download a "security app," supposedly recommended by their bank. IBM… https://www.sosdailynews.com/news.jspx?&articleid=1B39180E75FC58FB214DB54A90B54926&sx=79

Utility company calling? Don't fall for it

Every day, millions of people who have lost their jobs are making difficult choices about how to pay their bills. As the Coronavirus continues to spread, scammers are taking advantage of people's heightened economic anxiety. Their latest ploy is posing as representatives from utility companies to dupe people out of their cash and personal information by convincing them their utilities will be shut off if they don't pay. https://www.consumer.ftc.gov/blog/2020/07/utility-company-calling-dont-fall-it?utm_source=govdelivery

****

Hints & Tips plus Security Awareness

The Incident Response Challenge 2020 — Results and Solutions Announced (if you'd like to know more about Cynet contact FIPCO)

In April 2020, Cynet launched the world's first Incident Response Challenge to test and reward the skills of Incident Response professionals. The Challenge consisted of 25 incidents, in increasing difficulty, all inspired by real-life scenarios that required participants to go beyond the textbook... https://thehackernews.com/2020/07/cynet-cybersecurity-challenge.html?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+TheHackersNews+%28The+Hackers+News+-+Cyber+Security+Blog%29&_m=3n.009a.2269.aa0ao086k1.1fbr

Mozilla turns off "Firefox Send" following malware abuse reports

Mozilla's Firefox Send service has been controversial as it allows threat actors to generate unique short-term links based on trusted URLs for sharing files. Although the feature is appreciated by many individuals, Mozilla has decided to suspend it due to its ability to be used for malicious purposes. Cybercriminals often… https://nakedsecurity.sophos.com/2020/07/08/mozilla-turns-off-firefox-send-following-malware-abuse-reports/

Joker billing fraud malware eluded Google Play security to infect Android devices

A new variant targeted Android users to subscribe them to premium services without their consent, according to Check Point Research… https://www.techrepublic.com/article/joker-billing-fraud-malware-eluded-google-play-security-to-infect-android-devices/?ftag=TREa988f1c&bhid=78480402&mid=12925417&cid=712423569

Protecting your small business, one video at a time
Small businesses like yours are important. They create jobs, support a competitive marketplace, and lift up local communities. As a small business owner, you've worked hard to start your business and make it into something you can be proud of. That's why it's important… https://www.consumer.ftc.gov/blog/2020/07/protecting-your-small-business-one-video-time?utm_source=govdelivery

Microsoft warns organizations of consent phishing attacks
In this type of phishing campaign, attackers trick people into giving a malicious app consent to access sensitive data, says Microsoft. https://www.techrepublic.com/article/microsoft-warns-organizations-of-consent-phishing-attacks/?ftag=TREa988f1c&bhid=78480402&mid=12925417&cid=712423569

Jury Duty Scam Detailed
Just a quick warning from Jim Stickley about a Jury Duty Scam where criminals try to get your social security number.
https://www.sosdailynews.com/news.jspx?&articleid=DAD2F958AAAF88E1977691B00882AA1E&sx=79

CVE-2020-1350 | WINDOWS DNS SERVER RCE VULNERABILITY
Microsoft recently published a new critical vulnerability in the Windows Domain Name Servers, dubbed 'SigRed', that could allow an unauthenticated, remote attacker to gain domain administrator privileges over targeted servers and seize complete control of an organization's IT infrastructure.
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1350

How secure is your web browser?
NSS Labs released the results of its web browser security test after testing Google Chrome, Microsoft Edge, Mozilla Firefox, and Opera, for phishing protection and malware protection.
https://www.helpnetsecurity.com/2020/07/16/how-secure-is-your-web-browser/

****

News & Views

USB storage devices: Convenient security nightmares
There's no denying the convenience of USB media. From hard drives and flash drives to a wide range of other devices, they offer a fast, simple way to transport, share and store data. However, from a business security perspective, their highly accessible and portable nature makes them a complete nightmare, with data leakage, theft, and loss all common occurrences. https://www.helpnetsecurity.com/2020/07/10/usb-storage-devices-convenient-security-nightmares/

Secret Service merging electronic and financial crime task forces to combat cybercrime
The Secret Service is combining its Electronic Crimes Task Forces (ECTFs) and Financial Crimes Task Forces (FCTFs) into one unified network, the agency announced Thursday. The new merged network of task forces, to be known as Cyber Fraud Task Forces (CFTFs), will detect, prevent and root out cyber-enabled financial crimes, such as business email compromise and ransomware scams, "with the ultimate goal of arresting and convicting the most harmful perpetrators", the Secret Service said in a press release.
https://www.cyberscoop.com/secret-service-reorganization-task-force-cybercrime-financial-crime/,
https://www.infosecurity-magazine.com/news/secret-service-launches-cyber/

How expired domain names can redirect you to malicious websites
Pages for inactive domain names can be exploited by cybercriminals to take you to malicious sites, says Kaspersky. https://www.techrepublic.com/article/how-expired-domain-names-can-redirect-you-to-malicious-websites/?ftag=TREa988f1c&bhid=78480402&mid=12925417&cid=712423569

Researchers extract personal data from video conference screenshots
According to researchers at Ben-Gurion University, video conference users should refrain from posting screenshotted images of Zoom, Microsoft Teams, and Google Meet conference sessions. The researchers easily identified users from public screenshots of video meetings on the platforms. With the pandemic and the shift to teleworking, video conferencing has increased…
https://www.helpnetsecurity.com/2020/07/14/researchers-extract-personal-data-from-video-conference-screenshots/

Promises for lower credit card interest rates weren't true
When you're having trouble paying your credit card bills, getting a lower interest rate to keep your balance in check could be a game changer. Unfortunately, companies that promise to get you those lower rates often end up leaving you deeper in debt. https://www.consumer.ftc.gov/blog/2020/07/promises-lower-credit-card-interest-rates-werent-true?utm_source=govdelivery

****

"Ctrl -F" for The Board

Ways Cybersecurity Can Help Your Staff Return to Work Safely
While the COVID-19 pandemic continues to impact organizations across the country, business leaders are steadily making decisions towards returning to offices and restoring a sense of normalcy…
https://blog.nxtsoft.com/ways-cybersecurity-can-help-your-staff-return-to-work-safely?utm_campaign=Data%20Security%20Newsletter&utm_medium=email&_hsmi=91350336&_hsenc=p2ANqtz--5eFzBPZYeuqmlaGMcfzW1I_Ra2q570yScL9Bdzzs9GHqgdAibdoHHKJMfAD5JWXzwAWVjJ-1eF2Ce8GlCcfqxgaRBAA&utm_content=91350336&utm_source=hs_email

****

Special Network Infrastructure Vunerability Alerts

Significant Vulnerabilities in Core Network Infrastructure Devices
Since the end of June, six providers of network infrastructure products have announced significant vulnerabilities in their software. At least two of the vulnerabilities below are being actively exploited by malicious actorsii,iii. WSIC encourages recipients of this Analytic Note to review the details provided and patch the vulnerabilities that could impact your network.

On 6/29/20, Palo Alto disclosed a vulnerability (tracked as CVE-2020-2021) in the Palo Alto Networks Operating System (PAN-OS), impacting multiple products. This vulnerability could allow an unauthenticated attacker to access protected resources. This vulnerability was scored as 10/10 (Critical) on the Common Vulnerability Scoring System (CVSS) Version 3. Please see this Palo Alto security advisory for additional information: https://security.paloaltonetworks.com/CVE-2020-2021

On 6/30/20, F5 disclosed a vulnerability (tracked as CVE-2020-5902) in BIG-IP, impacting multiple products. This vulnerability could allow unauthenticated attackers, or authenticated users, with network access to the Configuration utility, through the BIG-IP management port and/or self IPs, to execute arbitrary system commands, create or delete files, disable services, and/or execute arbitrary Java code. This vulnerability was scored as 10/10 (Critical) on the CVSS Version 3. Please see this F5 security advisory for additional information: https://support.f5.com/csp/article/K52145254

On 7/7/20, Citrix disclosed a total of eleven vulnerabilities in their Citrix Application Delivery Controller, Citrix Gateway, and Citrix SD-WAN WANOP products. The most significant vulnerability (tracked as CVE-2020-8197) could allow a low privileged user with management access to execute arbitrary commands. This vulnerability was scored as 8.8/10 (High) on the CVSS Version 3. Please see this Citrix security advisory for additional information on all of the vulnerabilities disclosed on 7/7/20: https://support.citrix.com/article/CTX276688

On 7/8/20, Juniper disclosed a vulnerability (tracked as CVE-2020-1654) in the Juno Operating System (Juno OS) SRX series. This vulnerability could allow attackers to cause an extended denial of service condition or execute code remotely. This vulnerability was scored as 9.8/10 (Critical) on the CVSS Version 3. Please see this Juno security advisory for additional information: https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11031&cat=SIRT_1&actp=LIST

On 7/8/20, Palo Alto disclosed a vulnerability (tracked as CVE-2020-2034) in PAN-OS, impacting multiple products. This vulnerability could allow unauthenticated network-based attacker to execute arbitrary OS commands with root privileges. An attacker would require some level of specific information about the configuration of an impacted firewall or perform brute-force attacks to exploit this issue. This vulnerability was scored as 8.1/10 (High) on the CVSS Version 3.1. Please see this Palo Alto security advisory for additional information: https://security.paloaltonetworks.com/CVE-2020-2034

On 7/13/20, SAP disclosed a vulnerability (tracked as CVE-2020-6287) in the NetWeaver Application Server (AS) Java component. This vulnerability could allow attackers to modify or extract highly sensitive information, as well as disrupt critical business processes. This vulnerability was scored as 10/10 (Critical) on the CVSS Version 3. Please see this SAP security advisory for additional information: https://launchpad.support.sap.com/#/notes/2934135

On 7/14/20, Microsoft disclosed a vulnerability (tracked as CVE-2020-1350) in Windows Domain Name System (DNS) servers, impacting multiple products. This vulnerability could allow attackers to run arbitrary code in the context of the Local System Account. Microsoft considers this vulnerability “wormable”, with the potential to spread via malware between vulnerable computers without user interaction. This vulnerability was scored as 10/10 (Critical) on the CVSS Version 3. Please see this Microsoft security advisory for additional information: https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1350

If you identify attacks exploiting any of these vulnerabilities on your network, or have related information, please email wsic@doj.state.wi.usto submit a cyber incident report.

Questions
Contact FIPCO’s Ken Shaurette at 800/722-3498 ext. 251 or email FIPCO IT Services for more information.

"Make Security Part of You and Your Institution's DNA!"

Threat Intelligence Newsletter: July 27, 2020

FIPCO®
IT Audit
Round Table
Discussions

If you would like to host an event, please contact: Becky Schowalter

Upcoming Threat Intelligence Peer Group Discussions
None available at the current time

****

Alerts & Warnings

Cybercriminals disguising as top streaming services to spread malware
Malicious actors are posing as Netflix, Hulu, and more, to launch phishing attacks, steal passwords, launch spam, and distribute viruses. Recent security report… https://www.techrepublic.com/article/cybercriminals-disguising-as-top-streaming-services-to-spread-malware/?ftag=TREa988f1c&bhid=78480402&mid=12937400&cid=712423569

Amazon-Themed Phishing Campaigns Swim Past Security Checks
Amazon has been used to perpetuate a pair of new phishing campaigns that aim to steal credentials and other personal information claiming to be Amazon package-delivery notices. Amazon has been in high demand lately due to the COVID-19 pandemic preventing many from leaving the house excessively. However, cybercriminals have capitalized... https://threatpost.com/amazon-phishing-campaigns-security-checks/157495/

Zoom Addresses Vanity URL Zero-Day
Check Point security and Zoom announced on Thursday that a new zero-day has been discovered within the "Vanity URL" feature on Zoom, which allows companies to create their own meeting domain. Through exploiting this zero-day, attackers could pose as a company employee, and then use socially engineered conversation to extract... https://threatpost.com/zoom-vanity-url-zero-day/157510/

NitroHack Modifies Discord, Steals Your Info, And Contacts Your Friends
Let's start with Discord. This is a communication tool that helps various communities connect, such as gamers, education providers, and businesses. It's freeware and to help improve how it can help its users, there are mechanisms that allow others, and even encourages them to code in new functionality. However, while this can be useful, it can also leave the product vulnerable to modification that puts users at risk for various attacks. And in this case, some researchers at MalwareHunterTeam have found this to be the case.
https://www.sosdailynews.com/news.jspx?&articleid=697609BDC2313973D23CE0BB4439DF36&sx=79

New 'Shadow Attack' can replace content in digitally signed PDF files
15 out of the 28 biggest desktop PDF viewers are vulnerable, German academics say.
https://www.zdnet.com/article/new-shadow-attack-can-replace-content-in-digitally-signed-pdf-files/?ftag=TRE-03-10aaa6b&bhid=78480402&mid=12942689&cid=717796056

****

Hints & Tips plus Security Awareness

How to protect your Twitter account from being hacked
Following the hacks of verified Twitter accounts for several high-profile people, including Bill Gates and Joe Biden, how can you prevent your own account from falling into the wrong hands?
https://www.techrepublic.com/article/how-to-protect-your-twitter-account-from-being-hacked/?ftag=TREa988f1c&bhid=78480402&mid=12937400&cid=712423569

Cracking Dictionaries: A Hacker's Guide For Password Thievery
any businesses struggle with password security, especially when employees don't take it as seriously as they should. Human nature being what it is, staff who don't use password-smarts at home are likely to bring that same behavior to work. The reality is that 60% of small-to-medium-sized businesses close within six months of a cyberattack and the average financial cost per businesses is…
https://www.sosdailynews.com/news.jspx?&articleid=BB4A12BCD12890FFF661D95D2181E95C&sx=79

Change Your Router Password to Secure Your Home Network
The pros keep telling us the days of passwords are almost done. They're often easy to guess or steal, and they're tough to remember. http://scambusters.org/hackproof.html

Hang up on business imposter scams
Scammers love to use the same old tricks in new ways. One of their favorites is to pose as a business or government official to pressure you into sending them money or personal information. Now, some scammers are pretending to be popular online shopping websites, phishing for your personal information.
https://www.consumer.ftc.gov/blog/2020/07/hang-business-imposter-scams?utm_source=govdelivery

SORTING FACT FROM FICTION ONLINE – Reserve your Spot
Do you believe everything you see online? In addition to a wealth of helpful information, there are plenty of sensationalized headlines, misleading stories and even complete falsehoods circulating on the internet, making it hard for even the most discerning reader to sort fact from fiction.
https://onlinexperiences.com/scripts/Server.nxp?LASCmd=AI:4;F:QS!10100&ShowUUID=B4A23980-0248-44C8-831C-BD40C9317650&AffiliateData=Email0720

****

News & Views

Infosec is a mindset as well as a job, but burnout can happen to anyone
Time and again (and again), survey results tell us that many cybersecurity professionals are close to burnout and are considering quitting their jobs or even leaving the cybersecurity industry entirely.
https://www.helpnetsecurity.com/2020/07/20/infosec-mindset/

Twitter Confirms 130 Accounts Hacked
A recent cyberattack that targeted verified users on Twitter is still being investigated by the platform. However, the social media giant has confirmed that a total of 130 accounts were compromised as part of a cryptocurrency campaign attempting to scam victims out of bitcoin. The major cybersecurity incident occurred two... https://www.infosecurity-magazine.com/news/twitter-confirms-130-accounts/

Dissecting Cybercrime – Journey of a Stolen Credit Card
We often don’t realize the full impact of cyber crime, which then relapses us into repeating the same mistakes. Even large companies do not completely understand how their data and services are being abused. I want to take you on a journey of observing credit card fraud and abuse from stealing a credit card to trafficking of stolen goods. Learning about these vectors of abuse will help you and your organization to mitigate a number of common attacks and abuses.
https://www.brighttalk.com/webcast/15025/423446?player-preauth=43jkQaIHYdokg1RLj8LqEvoQ%2B1oQnEs1XmsGC3J5EpQ%3D&utm_source=brighttalk-recommend&utm_campaign=network_weekly_email&utm_medium=email&utm_content=company&utm_term=292020

****

"Ctrl -F" for The Board

COVID-19 Recovery CISA Tabletop Exercise Package (CTEP)
CISA developed the COVID-19 Recovery CISA Tabletop Exercise Package (CTEP) to assist private sector stakeholders and critical infrastructure owners and operators in assessing short-term, intermediate, and long-term recovery and business continuity plans related to the COVID-19 pandemic. Approved by the White House Task Force, and with input from the Federal interagency, this CTEP also provides organizations the opportunity to discuss how ongoing recovery efforts would be impacted by concurrent response operations to a potential “second wave” of global pandemic infections. The COVID-19 pandemic continues to impact organizations across the country, business… https://www.cisa.gov/covid-19-recovery-ctep

Questions
Contact FIPCO’s Ken Shaurette at 800/722-3498 ext. 251 or email FIPCO IT Services for more information.

"Make Security Part of You and Your Institution's DNA!"

Threat Intelligence Newsletter: August 5, 2020

FIPCO®
IT Audit
Round Table
Discussions

If you would like to host an event, please contact: Becky Schowalter

Upcoming Threat Intelligence Peer Group Discussions
None available at the current time

****

Alerts & Warnings

A deceptive credit card interest rate reduction offer
Monthly credit card bills can be a drag, especially when you're feeling financially strapped. Finding ways to lower those bills — sometimes by simply calling your credit card company directly and asking for a lower rate — can save you lots of cash. So what about those companies that call with a "guaranteed" credit card interest rate reduction offer (for a small fee) and a promise to save you thousands of dollars? Most likely, it's a deal designed to dupe you out of money. https://www.consumer.ftc.gov/blog/2020/07/deceptive-credit-card-interest-rate-reduction-offer?utm_source=govdelivery

Attackers Exploiting High-Severity Network Security Flaw, Cisco Warns
According to Cisco, a high severity flaw in its network security software is being actively exploited by cybercriminals. Cisco's software is used by many Fortune 500 companies who are now at risk due to the vulnerability, which can lead to remote unauthenticated access to sensitive data. Patches for the flaw… https://threatpost.com/attackers-exploiting-high-severity-network-security-flaw-cisco-warns/157756/

Global Voicemail Scam Targets Enterprise Email; Mimics PBX System
A massive, global voicemail phishing scam was recently exposed and known to affect at least 100,000 email inboxes worldwide. IRONSCALES Security discovered this scam targets healthcare, real estate, IT, financial, and other enterprise with a spoofed (fake) voicemail to email translation. https://www.sosdailynews.com/news.jspx?&articleid=CCDADD660CFDDB28E01654C5EAE2EB1B&sx=79

You might live to regret opening that Microsoft Office document
Hackers seizing on trust placed in popular Microsoft Office software…
https://www.techradar.com/news/you-might-live-to-regret-opening-that-microsoft-office-document

FakeSpy Data-Stealing App Returns, Now Using U.S.P.S. As Cover
According to a report by Cybereason, postal services around the globe are now being targeted by an Android malware that's back with a vengeance. FakeSpy is believed to be...
https://www.sosdailynews.com/news.jspx?&articleid=87E2A8AADBAEDFF1007E8D50FBC8D3B6&sx=79

Researchers find critical RCE vulnerabilities in industrial VPN solutions
Critical vulnerabilities in several industrial VPN implementations for remotely accessing operational technology (OT) networks could allow attackers to overwrite data, execute malicious code or commands, cause a DoS condition, and more. https://www.helpnetsecurity.com/2020/07/28/vulnerabilities-industrial-vpn/

There's a Hole in the Boot
BootHole" vulnerability in the GRUB2 bootloader opens up Windows and Linux devices using Secure Boot to attack. All operating systems using GRUB2 with Secure Boot must release new installers and bootloaders. https://eclypsium.com/2020/07/29/theres-a-hole-in-the-boot/?utm_campaign=Threat%20Report&utm_medium=email&_hsmi=92259730&_hsenc=p2ANqtz-_ebcDdbOXi-uWlnXs-CmyGg3Avuddu8gmb_k2ComVGtiDeG7ZJlsaulvrrdeybbxiJGuvzBjELiQvACSoa03vCpgY3zw&utm_content=92259730&utm_source=hs_email

****

Hints & Tips plus Security Awareness

Bank Robbers Working Overtime: Financial Industry Most Hacked
It's easy to see why financial institutions are hacked more than any other business – it's where the money is. The "bank robbers" of the 21st century have been unusually busy since the ongoing coronavirus pandemic. The explosion of employees working remotely and the vulnerabilities they create become massive opportunities for cyber-crooks. Yes, hackers are usually the first to capitalize on epic events, whether good or bad. But at the moment, the months-long pandemic continues to provide targets ripe for hacking and none are more ready for picking than the financial industry.
https://www.sosdailynews.com/news.jspx?&articleid=E777C905537910705A74E35FC78C285F&sx=79

Steering Customers' Remote Work Strategy
CEO Chuck Robbins put it best "for 35 years and counting, Cisco has taken on complex challenges and used our technology to help others." As the leader for our Global Security Channel Sales organization in Europe, Middle East, Africa, Russia (EMEAR), I have seen first-hand how our partners have guided our customers in these most challenging times. https://blogs.cisco.com/partner/steering-customers-remote-work-strategy

The distinction between human and bot behavior is becoming increasingly blurred
There's no denying that the way people have been using the Internet and online stores has changed over the last couple of months. As consumers change their online habits, the distinction be…
https://www.helpnetsecurity.com/2020/07/28/distinction-between-human-and-bot-behavior/

Dangerous new Netflix phishing scam revealed - here's what you need to know
Spotting a Netflix phishing scam isn't always easy… https://www.techradar.com/news/dangerous-new-netflix-phishing-scam-hits-the-scene-heres-what-you-need-to-know

Impostor! Social Media Account Verification Fails Key Test
Can you trust social media account verification -- the process that tells a user that the person they're looking at online is who they say they are? Not always. http://scambusters.org/accountverification.html

****

News & Views

Cosmetics Giant Avon Leaks 19 Million Records
Researchers have uncovered a misconfigured cloud server operated by cosmetics brand Avon, allowing the public to access more than 19 million records. SafetyDetectives researchers found the Elasticsearch database on an Azure server that contained no password protection or encryption, meaning that anyone who has the server's IP address could access… https://www.infosecurity-magazine.com/news/cosmetics-giant-avon-leaks-19/

Cyberattacks and the long-term effects on organizations
As the coronavirus spreads, people and organizations turned to virtual tools and environments en mass. Businesses and their workers moved to remote operations. And, many cybercriminals recognize this has drastically changed the perimeter of organizations and created unprecedented opportunity for cyberattacks. How can organizations understand, respond to, and potentially limit the impact of cyberattacks? https://www2.deloitte.com/us/en/pages/advisory/articles/resilient-special-series-podcast-on-covid19.html?id=us:2em:3na:cyberrisk:awa:adv:072820:vpcov&ctr=cta2&sfid=0031400002HFVRwAAP

386 Million User Records from 18 Companies Leaked for Free
On July 21, 2020, multiple databases containing the stolen information of over 386 million consumers were posted online in a hacker forum — all for free. The exposed information was stolen from eighteen companies, including... Should I be Worried? The information stolen in data breaches is normally sold on the dark web for a profit and very rarely shared for free. The posting of these free databases was done for... https://www.fightingidentitycrimes.com/18-companies-368-million-records-data-breach/

Study Links Cybersecurity Directly to Employee Stress and Exhaustion
A new study looked at why people make cybersecurity mistakes that can easily lead to breaches and other major events. It turns out that it's not a question of "if" but of "when," as most people make mistakes during their tenure in any company. https://securityboulevard.com/2020/07/study-links-cybersecurity-directly-to-employee-stress-and-exhaustion/

****

"Ctrl -F" for The Board

Microsoft told employees to work from home. One consequence was brutal
Many people think they have a good idea of what working from home now means. At Microsoft, however, they've studied it. And it makes for sobering reading. https://www.zdnet.com/article/microsoft-told-employees-to-work-from-home-one-consequence-was-brutal/?ftag=TRE-03-10aaa6b&bhid=78480402&mid=12949976&cid=717796056

Significant Cyber Incidents
This timeline records significant cyber incidents since 2006. We focus on cyber attacks on government agencies, defense and high tech companies, or economic crimes with losses of more than a million dollars. https://www.csis.org/programs/technology-policy-program/significant-cyber-incidents

Questions
Contact FIPCO's Ken Shaurette at 800/722-3498 ext. 251 or email FIPCO IT Services for more information.

"Make Security Part of You and Your Institution's DNA!"

Threat Intelligence Newsletter: August 11, 2020

FIPCO® IT Audit Round Table Discussions

If you would like to host an event, please contact: Becky Schowalter

Upcoming Threat Intelligence Peer Group Discussions
None available at the current time

****

Alerts & Warnings

Small businesses targeted with unauthorized withdrawals
The last thing struggling small business owners need right now is to have money unlawfully taken from their pockets. According to a complaint filed today by the FTC, that's exactly what a company that offered financing to small business did to its customers. https://www.consumer.ftc.gov/blog/2020/08/small-businesses-targeted-unauthorized-withdrawals?utm_source=govdelivery

Rocketing Zoom Spoof Sites
At a time when the world is unsure about what tomorrow may bring, one community doing extremely well today are cybercriminals. Zoom video conferencing is a natural target for a hacker's cross hairs. With much of the…
https://www.sosdailynews.com/news.jspx?&articleid=832CE39282B55582595A0DB02D3C0BB8&sx=79

Stolen Email Threads Hide Valak Info-Stealing Malware
Anyone familiar with email threads, those linked chains of emails and responses, knows how cumbersome they can be. But now, there's another reason not to like email threads: they could be hiding malware called Valak. Discovered in 2019, Valak is now targeting organizations in healthcare, manufacturing, and financial services...
https://www.sosdailynews.com/news.jspx?&articleid=BD08D823425DEDA00B88935BCEBDCD14&sx=79

Newsletter WordPress Plugin Opens Door to Site Takeover
A WordPress plugin designed to create newsletters and email campaigns within the platform called Newsletter has been downloaded over 300,000 times. However, security researchers recently found that the plugin contains a pair of vulnerabilities that could potentially allow threat actors to achieve a site takeover. One vulnerability is an XSS… https://threatpost.com/newsletter-wordpress-plugin-site-takeover/158025/

Scammers and "customer service" — another imposter scam
If you want to contact a company's customer service department, you can do a quick search online and often find what looks like its phone number or email. But is the information at the top of your search results actually correct? https://www.consumer.ftc.gov/blog/2020/08/scammers-and-customer-service-another-imposter-scam?utm_source=govdelivery

****

Hints & Tips plus Security Awareness

Video shows how scammers tell you to pay
Scammers make up all kinds of stories to get your money, from telling you that you've won a prize, you owe a debt, or your family member is in an emergency. But some things stay the same: scammers want your money, they want it fast, and don't want you to be able to get it back. They'll ask you to pay in ways that make it hard to track them down — and once you know what these are, you'll have one more clue to tell if you're dealing with a scammer. https://www.consumer.ftc.gov/blog/2020/08/video-shows-how-scammers-tell-you-pay?utm_source=govdelivery

NIST Security Considerations for Exchanging Files Over the Internet
Every day, in order to perform their jobs, workers exchange files over the Internet through email attachments, file sharing services, and other means. To help organizations reduce potential exposure of sensitive information, NIST has released a new Information Technology Laboratory (ITL) Bulletin on secure file exchanges. The bulletin discusses several possible solutions for secure file exchanges, as well as numerous examples of methods for detecting file exchanges that aren't properly protected.
https://csrc.nist.gov/CSRC/media/Publications/Shared/documents/itl-bulletin/itlbul2020-08.pdf

What Is the Difference Between Credit Card Fraud and Identity Theft?
Credit Card Fraud vs. Identity Theft. Credit card fraud is a potential consequence of identity theft. Here, a thief steals your credit card information and then makes purchases in a store or online. Most credit card companies have a liability limit of $50. This means that even if a thief has charged thousands of dollars to your card, you'd likely only have to pay $50. More often than not, credit card companies simply wipe out any charges that are the result of fraud. In contrast, identity theft involves much more than a few fraudulent charges. Identity thieves can steal your personal information to open a new line of credit, open a new credit card, or obtain a false ID in your name. Unlike credit card fraud, there's no liability limit. That means you might end up paying for all the damage caused by an identity thief.
https://www.fightingidentitycrimes.com/difference-between-credit-card-fraud-and-identity-theft/

Cracking the Chinese Seeds Mystery
Those Chinese seeds. You'd have to have totally ignored the news in recent weeks if you haven't seen reports about unordered mystery packages of seeds, mailed from China, that have turned up in hundreds of mailboxes. https://scambusters.org/chineseseeds.html

****

News & Views

Digital Forensics Standards: Recent News And Research
Digital evidence is, of course, key in these types of crimes as well as others. Tasked in recent months with processing evidence from home, forensic examiners and their lab managers have juggled staying healthy with maintaining chain of custody and evidentiary integrity. Four new resources — two from the United States, and two from Europe — aim to address different aspects of these issues: https://www.forensicfocus.com/articles/digital-forensics-standards-recent-news-and-research/

Ransomware: Your biggest security headache refuses to go away
Ransomware attacks have been with us for decades: Here's why they will continue to create chaos for years to come. https://www.zdnet.com/article/ransomware-why-the-internets-biggest-headache-refuses-to-go-away/?ftag=TRE-03-10aaa6b&bhid=78480402&mid=12963539&cid=717796056

Social Engineering: Hacking Brains…It's Easier than Hacking Computers
The audience in the room is weirdly quiet. The contestant is in a small plexiglass booth with nothing but a phone, a laptop computer and some notes. On a set of speakers outside, the… https://www.tripwire.com/state-of-security/featured/social-engineering-hacking-brains/?utm_source=newsletter&utm_medium=email&utm_campaign=prospect

FBI issues warning over Windows 7 end-of-life
On Monday, the FBI sent a private industry notification to US private sector partners warning about Windows 7 computers reaching their end-of-life. According to the warning, the operating system fulfilled its shelf life earlier this year. The FBI stated that they had observed threat actors targeting computer network infrastructure after… https://www.zdnet.com/article/fbi-issues-warning-over-windows-7-end-of-life/

****

"Ctrl -F" for The Board

A Guide to Critical Infrastructure Security and Resilience
The U.S. Department of State and the U.S. Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency (CISA) developed "A Guide to Critical Infrastructure Security and Resilience" guide to serve as an overview of the U.S. all-hazards approach to critical infrastructure security and resilience. It is intended for both for domestic and international partners. https://www.cisa.gov/sites/default/files/publications/Guide-Critical-Infrastructure-Security-Resilience-110819-508v2.pdf

Social Engineering: Hacking Brains…It's Easier than Hacking Computers
The audience in the room is weirdly quiet. The contestant is in a small plexiglass booth with nothing but a phone, a laptop computer and some notes. On a set of speakers outside, the… https://www.tripwire.com/state-of-security/featured/social-engineering-hacking-brains/?utm_source=newsletter&utm_medium=email&utm_campaign=prospect

Questions
Contact FIPCO's Ken Shaurette at 800/722-3498 ext. 251 or email FIPCO IT Services for more information.

"Make Security Part of You and Your Institution's DNA!"

Threat Intelligence Newsletter: August 18, 2020

FIPCO®
IT Audit
Round Table
Discussions

If you would like to host an event, please contact: Becky Schowalter

Upcoming Threat Intelligence Peer Group Discussions
None available at the current time

****

Alerts & Warnings

Google Chrome Browser Bug Exposes Billions of Users to Data Theft
The vulnerability allows attackers to bypass Content Security Policy (CSP) protections and steal data from website visitors. A vulnerability in Google's Chromium-based browsers would allow attackers to bypass the Content Security Policy (CSP) on websites, in order to steal data and execute rogue code.
https://threatpost.com/google-chrome-bug-data-theft/158217/

Researchers flag two zero-days in Windows Print Spooler
In May 2020, Microsoft patched CVE-2020-1048, a privilege escalation vulnerability in the Windows Print Spooler service discovered by Peleg Hadar and Tomer Bar from SafeBreach Labs.
https://www.helpnetsecurity.com/2020/08/07/zero-days-windows-print-spooler/

New Malware Emerges From Under A Rock To Steal Your PII
Android users are being targeted yet again with a malware strain that emerged from the deep Black. From under a BlackRock to be precise. It targets 337 Android applications and has been on the move since at least May of this year. It's not completely new either. In fact, the researchers at ThreatFabric say it's based on leaked source code for another strain known as Xerxes, which was created from Parasite, which was code from MysteryBot, which used code previously from LokiBot. Why reinvent the wheel, right?
https://www.sosdailynews.com/news.jspx?&articleid=B0BFFA2C0DB702234F6B0D8115A96DFD&sx=79

Critical Adobe Acrobat and Reader Bugs Allow RCE
Adobe patched critical and important-severity flaws tied to 26 CVEs in Acrobat and Reader. Adobe has plugged 11 critical security holes in Acrobat and Reader, which if exploited could allow attackers to remotely execute code or sidestep security features in the app. https://threatpost.com/critical-adobe-acrobat-reader-bugs-rce/158261/

Android phones could spy on users
Vulnerabilities were found in a Qualcomm Snapdragon chip that could let attackers obtain photos, videos, call recordings, and other data on Android phones… https://www.techrepublic.com/article/android-phones-could-spy-on-users-via-flaws-in-qualcomm-chip/

ReVoLTE Attack Allows Hackers to Listen in on Mobile Calls
Rare attack on cellular protocol exploits an encryption-implementation flaw at base stations to record voice calls. https://threatpost.com/revolte-attack-hackers-listen-mobile-calls/158325/

****

Hints & Tips plus Security Awareness

1, 2, 3 videos to help you stop unwanted calls
It can be frustrating to deal with a bunch of unwanted calls. If you answer them, you might hear a recorded message of someone trying to sell you something. Or it could be a real person hoping to scare you into paying a debt you don't owe.These kinds of unwanted calls are often scams. Taking steps to stop them can help save you time and unnecessary stress — and maybe some money, too.
https://www.consumer.ftc.gov/blog/2020/08/1-2-3-videos-help-you-stop-unwanted-calls?utm_source=govdelivery

Control Baselines for Information Systems and Organizations
In addition to the control baselines, this publication provides tailoring guidance and a set of working assumptions to help guide and inform the control selection process for organizations. Finally, this publication provides guidance on the development of overlays to facilitate control baseline customization for specific communities of interest, technologies, and environments of operation. The control baselines were previously published in NIST SP 800-53, but moved so that SP 800-53 could serve as a consolidated catalog of security and privacy controls that can be used by different communities of interest.
https://csrc.nist.gov/publications/detail/sp/800-53b/draft

The State of Identity Fraud in 2020
August 27 at 11 pm CT. Identity fraud has continued to be an unwavering and pervasive threat throughout this year of uncertainty. In this session, you'll gain an understanding of the current and upcoming fraud trends and methodologies to help you better protect your customers.
https://gateway.on24.com/wcc/eh/2422888/lp/2450972/the-state-of-identity-fraud-in-2020/?partnerref=email6

Ransomware: These warning signs could mean you are already under attack
File-encrypting ransomware attacks can take months of planning by gangs. Here's what to look out for.
https://www.zdnet.com/article/ransomware-these-warning-signs-could-mean-you-are-already-under-attack/?ftag=TRE-03-10aaa6b&bhid=78480402&mid=12977879&cid=717796056

Fight Phishing Fraud With The Banks Never Ask That Campaign
Starting Sept. 1, banks are encouraged to register to participate in ABA's new #BanksNeverAskThat anti-phishing campaign—a fresh, bold plug-and-play campaign that ABA has created to fight phishing fraud by turning bank customers into expert scam spotters. Preview the campaign; https://www.aba.com/-/media/documents/extranet/banksneveraskthat/banksneveraskthat-brochure.pdf?utm_campaign=NEWSBYTES-20200812&utm_medium=email&utm_source=Eloqua,

Register:
https://onlinexperiences.com/scripts/Server.nxp?LASCmd=AI:4;F:QS!10100&ShowKey=105133&utm_campaign=NEWSBYTES-20200812&utm_medium=email&utm_source=Eloqua

AARP WI, Spot a Scam - Stop a Scam, WI 8-19-2020
Scammers are doing what they always do – using headlines as opportunities to steal money or sensitive personal information. The Coronavirus and the economic stimulus payments have created a perfect storm for scammers and they are coming out of the woodwork. AARP's Fraud Watch Network is dedicated to spreading t… https://aarp.cvent.com/events/aarp-wi-spot-a-scam-stop-a-scam-wi-8-19-2020/event-summary-0c6a1c52e11647bd8d8cf8ed3f29c8fe.aspx

****

News & Views

Digital Forensics Standards: Recent News And Research
Digital evidence is, of course, key in these types of crimes as well as others. Tasked in recent...
https://www.zdnet.com/article/fbi-issues-warning-over-windows-7-end-of-life/

Microsoft Office 365 is becoming the core of many businesses. And hackers have noticed.
As cloud-based services become the key to many business operations, hackers are refocusing their aim.
https://www.zdnet.com/article/microsoft-office-365-is-becoming-the-core-of-many-businesses-and-hackers-have-noticed/

Amazon Alexa 'One-Click' Attack Can Divulge Personal Data
Researchers disclosed flaws in Amazon Alexa that could allow attackers to access personal data and install skills on Echo devices. Vulnerabilities in Amazon's Alexa virtual assistant platform could allow attackers to access users' banking data history or home addresses – simply by persuading them to click on a malicious link. https://threatpost.com/amazon-alexa-one-click-attack-can-divulge-personal-data/158297/

The Secret SIMs Used By Criminals to Spoof Any Number
The unsolicited call came from France. Or at least that's what my phone said. When I picked up, a man asked if I worked with the National Crime Agency, the UK's version of the FBI. When I explained, no, as a journalist I don't give information to the police, he said why he had contacted me. "There are these special SIM cards out there," he said, referring to the small piece of hardware that slips inside a cell phone. "I'm actually ringing from one now," he added, before later explaining he runs an underground site that sells these cards. https://www.vice.com/en_us/article/n7w9pw/russian-sims-encrypted

****

"Ctrl -F" for The Board

CISA Warns of Phishing Attempts that Spoof SBA Loan Program
The US Cybersecurity and Infrastructure Security Agency (CISA) has issued an advisory warning of a phishing attack that sends users to a spoofed version of the Small Business Administration's (SBA's) COVID-19 loan relief webpage. https://www.fedscoop.com/cisa-spoofing-sba-loan-relief/

Questions
Contact FIPCO's Ken Shaurette at 800/722-3498 ext. 251 or email FIPCO IT Services for more information.

"Make Security Part of You and Your Institution's DNA!"

Threat Intelligence Newsletter: August 28, 2020

FIPCO®
IT Audit
Round Table
Discussions

If you would like to host an event, please contact: Becky Schowalter

Upcoming Threat Intelligence Peer Group Discussions
None available at the current time

****

Alerts & Warnings

Google Chrome Browser Bug Exposes Billions of Users to Data Theft
The targeted victim of a Utility Services Scam. She was lucky and hung up before they got her info but her story points out just how easy it is for criminals to call you pretending to be from your gas and electric company!
https://www.sosdailynews.com/news.jspx?&articleid=D527409DF64AB42FA8063A423038E2F7&sx=79

IcedID Trojan Rebooted with New Evasive Tactics
Security researchers have found that the IcedID Trojan has been redesigned to include new techniques in its attacks, including password-protected attachment, keyword obfuscation, and minimalist macro code. The updates were uncovered after a new phishing campaign launched recently that leveraged the malware. Paul Kimayong recently released a report on the… https://threatpost.com/icedid-trojan-rebooted-evasive-tactics/158425/

Researchers Sound Alarm Over Malicious AWS Community AMIs
Researchers have alerted the public to a growing threat posed by Amazon Web Services and its available pre-configured virtual servers, stating that threat actors can build Community Amazon Machine Images (AMI) infected with malware yet make them identical to legitimate ones. This poses a risk to AWS customers, as they... https://threatpost.com/malicious-aws-community-amis/158555/

Your email threads are now being hijacked by the QBot Trojan
Check Point researchers published a report detailing an ongoing campaign involving the QBot Trojan. Its operators have been targeting legitimate email threats to steal credentials and financial data through injecting the prolific malware by leveraging loopholes in the Microsoft Outlook software. Outlook is reportedly susceptible to a module that can... https://www.zdnet.com/article/your-email-threads-are-now-being-hijacked-by-qbot-trojan/

FBI/CISA Warn US Firms of State-Mandated Tax Malware
The FBI and Department of Homeland Security's Cybersecurity and Infrastructure Security Agency have released a joint warning pertaining to organizations doing business in China after news broke of an attempt to target US organizations with a dangerous malware hidden in government-mandated tax software. Trustwave researchers uncovered the campaign in June… https://www.infosecurity-magazine.com/news/fbicisa-warn-us-firms/

****

Hints & Tips plus Security Awareness

How do I select a risk assessment solution for my business?
One of the cornerstones of a security leader's job is to successfully evaluate risk. A risk assessment is a thorough look at everything that can impact the security of an organization.
https://www.helpnetsecurity.com/2020/08/18/select-risk-assessment-solution/

Google Fixes High-Severity Chrome Browser Code Execution Bug
Google Chrome users will receive a patch later this week that fixes a severe vulnerability that can be manipulated by attackers to execute arbitrary code. The flaw lied in the Chrome 85 stable channel, however, has since been fixed by the company. The flaw is a bug in the WebGL…
https://threatpost.com/google-fixes-high-severity-chrome-browser-code-execution-bug/158600/

Google fixes major Gmail bug seven hours after exploit details go public
Attackers could have sent spoofed emails mimicking any Gmail or G Suite customer.
https://www.zdnet.com/article/google-fixes-major-gmail-bug-seven-hours-after-exploit-details-go-public/?ftag=TRE-03-10aaa6b&bhid=78480402&mid=12995677&cid=717796056

Tips to help you avoid to post-disaster scams
Whether you're getting ready to deal with Laura or Marco, the storms about to hit the Gulf Coast, dealing with the ravages of wildfires out West, reeling from the derecho that struck the Midwest, or facing another natural disaster, handling the aftermath is never easy. But when scammers target people just trying to recover, it can be even worse. Here are some tips to help you avoid common post-disaster scams.
https://www.consumer.ftc.gov/blog/2020/08/tips-help-you-avoid-post-disaster-scams?utm_source=govdelivery

CIS Benchmarks
As one of a handful of CIS Certified Vendors, NNT has a broad range of CIS Benchmark reports which can be used to audit enterprise networks and then monitor continuously for any drift from your hardened build standard, to ensure systems stay within compliance 24/7. https://www.newnettechnologies.com/cis-benchmark.html#web-servers

The New Cracking Tools That Automate ATO & Credential Stuffing
Criminals are using new tools and old favorites for credential stuffing and account takeover. Here's what you need to know about popular cracking tools including Vertex, Sentry MBA, SNIPR, and OpenBullet, along with custom and target-specific account checkers—plus how you can protect your users and yourself from these attacks. https://spycloud.com/new-cracking-tools-automate-credential-stuffing-account-takeover-openbullet-sentry-mba/?utm_campaign=Newsletter&utm_medium=email&_hsmi=94021171&_hsenc=p2ANqtz-_jigtUtk8e-g7JQqLXok3HIs156l-_RMJOlCcjRrK532cWZc0WWEHu37yB72OeyxChtWVQ7_V2CF7cRDV3ArXjsvNb4g&utm_content=94021050&utm_source=hs_email

****

News & Views

Zero trust is critical, but very underused
Organizations must quickly adopt the zero trust mindset of "never trust, always verify" to mitigate the spread of breaches, limit access, and prevent lateral movement, according to an Illumio report.. https://www.techrepublic.com/article/zero-trust-is-critical-but-very-underused/?ftag=TREa988f1c&bhid=78480402&mid=12989596&cid=712423569

Driving for extra cash? Check your car insurance first
With more people seeking delivery services during the Coronavirus pandemic, many companies are looking for drivers to shuttle meals, medicine, groceries, and other items to people at home. Before you think about making some extra cash as a delivery driver using your own vehicle, you need to be aware of the insurance pitfalls. https://www.consumer.ftc.gov/blog/2020/08/driving-extra-cash-check-your-car-insurance-first?utm_source=govdelivery

Sophisticated Peer-to-Peer Botnet Discovered
A relatively recent peer-to-peer botnet has just been discovered by researchers. The botnet has been actively breaching Secure Shell servers since at least January and has been named FritzFrog. The botnet utilizes a worm malware that is multi-threaded, file-less, and leaves no signs of infection on the disks of targeted… https://www.infosecurity-magazine.com/news/sophisticated-peertopeer-botnet/

Three places for early warning of ransomware and breaches that aren't the dark web
For better or worse, a lot of cybercrime sleuthing and forecasting tends to focus on various underground sites and forums across the deep and dark web corners of the Internet. Whenever a report cites passwords, contraband or fraud kits trafficked in these underground dens, it makes elusive fraudsters and extortion players sound tangible. https://www.helpnetsecurity.com/2020/08/25/early-warning-of-ransomware-and-breaches/

Russian-backed organizations amplifying QAnon conspiracy theories, researchers say
According to researchers, Russian government-backed actors have played a role in amplifying conspiracy theories created and promoted by the prominent US-based group QAnon. This has raised significant concerns over foreign interference in the US elections, which will occur in November. Researchers state that Russia likely did not have involvement in… https://www.reuters.com/article/us-usa-election-qanon-russia-idUSKBN25K13T

Most organizations have no Active Directory cyber disaster recovery plan
Although 97% of organizations said that Active Directory (AD) is mission-critical, more than half never actually tested their AD cyber disaster recovery process or do not have a plan in place at all, a Semperis survey of over 350 identity-centric security leaders reveals…
https://www.helpnetsecurity.com/2020/08/26/active-directory-cyber-disaster-recovery-plan/

****

"Ctrl -F" for The Board

Pros and cons of password managers – Vault your Passwords
Tech consultants and journalists have their own conflicting opinions about the best way to manage access in a world full of security risks. https://www.techrepublic.com/article/extra-security-or-extra-risk-pros-and-cons-of-password-managers/?ftag=TREa988f1c&bhid=78480402&mid=13008079&cid=712423569

Questions
Contact FIPCO's Ken Shaurette at 800/722-3498 ext. 251 or email FIPCO IT Services for more information.

"Make Security Part of You and Your Institution's DNA!"

Threat Intelligence Newsletter: September 4, 2020

FIPCO®
IT Audit
Round Table
Discussions

If you would like to host an event, please contact: Becky Schowalter

Upcoming Threat Intelligence Peer Group Discussions
None available at the current time

****

Alerts & Warnings

Latest TrickBot Malware Has Even More Up Its Sleeve
No slouch when it comes to reinventing itself, TrickBot malware has evolved yet again. Considered the top threat to business on a global scale, TrickBot and its financial data-stealing abilities are prolific. In February of this year, TrickBot expanded its menu of mayhem, focusing on making it more difficult to detect and defend against. Now, just a few months later, TrickBot is at it again. Its latest added module, called Nworm, takes the ability to evade detection to a whole new level.
https://www.sosdailynews.com/news.jspx?&articleid=D4D1F43F6C3C6F85486516477C06741B&sx=79

New Threat Activity by Lazarus Group Spells Trouble For Orgs
North Korean hacking group known as Lazarus has allegedly launched several cyber campaigns that aim to raise finances for the country's missile program. Last week, the US government issued a warning about how the group was currently targeting banks in several different countries. Cybersecurity experts believe that these ventures bring… https://www.darkreading.com/threat-intelligence/new-threat-activity-by-lazarus-group-spells-trouble-for-orgs/d/d-id/1338812

A Critical Flaw Is Affecting Thousands of WordPress Sites
Hackers are currently actively exploiting a vulnerability in WordPress which the threat actors can manipulate to execute malicious commands and scripts on Websites running File Manager. File Manager is a WordPress plugin that has over 700,000 active installations, according to researchers. The security flaw has been patched, however, the first… https://www.wired.com/story/a-critical-flaw-is-affecting-thousands-of-wordpress-sites/

****

Hints & Tips plus Security Awareness

Beat the Predatory Lending Crooks
Are you "house rich but cash poor"? If so, you're a prime target for predatory lending scammers.
https://scambusters.org/predatorylending2.html

Extended Detection and Response (XDR)
A new product category that Gartner claimed as the top security and risk trend for 2020.
https://f.hubspotusercontent30.net/hubfs/3454686/XDR-ebook.pdf?utm_medium=email&_hsmi=93365437&_hsenc=p2ANqtz-9CXxqrXH8pPoildF-5N4Bz5lGMzJzR8jbvyjqYfTPXTZuXCVn18_0KGQxV6cWzczvgCj49kjaeSQzOZIzZPO9F84bNRA&utm_content=93365437&utm_source=hs_automation

CtrlAltBreach - Episode 3: RDP and RDG vulnerabilities
In this episode we are focusing on specific vulnerabilities that often open the door to ransomware. By exploiting these vulnerabilities attackers can gain access to your system and steal data or target backups and deploy ransomware. The discussion is lead by Alex Ricardo, manager for cyber business development. Our guest today is Josh Sudbury of Lodestone Security.
https://www.beazley.com/beazley_academy/ctrlaltbreach_rdp_rdg_vulnerabilities.html

Cisco Patches 'High-Severity' Bugs Impacting Switches, Fibre Storage
Cisco has recently patched nine bugs, eight of which are classified as high severity vulnerabilities that present an active threat to users. Cisco has disclosed all eight of the flaws that impact several different aspects of its networking gear, including switches and fiber storage functions. Six security alerts were issued… https://threatpost.com/cisco-high-severity-bugs-impact-switches-fibre-storage/158691/

Microsoft just made securing Windows 10 PCs a whole lot easier for IT admins
New security capabilities designed for SMEs allow IT admins to apply baseline security settings across an organization. https://www.techrepublic.com/article/microsoft-just-made-securing-windows-10-pcs-a-whole-lot-easier-for-it-admins/?ftag=TREa988f1c&bhid=78480402&mid=13018754&cid=712423569

A Layered Approach to Mitigating Brute Force and Automated Credential Stuffing Attacks
Read this case study example to learn exactly what US Signal implemented on a customer's website to mitigate 99% of malicious traffic including Account Take Over attacks.
https://ussignal.com/blog/mitigating-brute-force-automated-credential-stuffing-attacks?utm_medium=email&utm_campaign=August%202020%20Blogs&utm_content=August%202020%20Blogs+Preview+CID_a31bfbf2e9744d656094912f215ff1b3&utm_source=Email&utm_term=A%20Layered%20Approach%20to%20Mitigating%20Brute%20Force%20and%20Automated%20Credential%20Stuffing%20Attacks

The Rising Challenge of Account Takeover Fraud – What it is, How it Works, and How to Avoid it
Recent reports indicate that up to 15 billion consumer credentials are currently for sale on the dark web, with almost 25% of the leaked credentials including account information related to banking and other financial services. The availability of leaked or compromised data makes it extremely easy for hackers to conduct account takeover attacks on consumers' financial accounts.
https://www.arkoselabs.com/blog/account-takeover-fraud-ato-limits-of-legacy-solutions/

How can you spot a tech support scam
Are you getting pop-up warning messages on your computer screen? Or maybe a phone call that your computer has a virus? That may well be a tech support scam. But how do you know? And what do you do? https://www.consumer.ftc.gov/blog/2020/09/how-can-you-spot-tech-support-scam?utm_source=govdelivery

****

News & Views

BEC Wire Transfer Losses Soar 48% in Q2 2020
According to security vendor Agari, Business Email Compromise attacks that lead to wire transfer losses have increased dramatically from the previous quarter. BEC wire transfer losses soared by over 48% from Q1 2020, resulting in an average of more than $80,000. These conclusions were highlighted in the Anti-Phishing Working Group's… https://www.infosecurity-magazine.com/news/bec-wire-transfer-losses/

Qualifying A Digital Forensic Expert In Court (Voir Dire)
Most digital forensic practitioners possess an analytical mind. One of the reasons we become interested in the field is because we work to whittle down the digital elements of the case to try and present a clearer picture of the facts in the matter. Whether we are working in law enforcement attempting to implicate or exonerate a suspect, or at a corporate level trying to determine from where a threat actor may have originated, or in the private sector working litigation support in furtherance of a domestic or some other type of dispute, the ultimate goal behind the digital forensic processes and methodologies is to present these findings in a court of law. https://www.forensicfocus.com/legal/qualifying-a-digital-forensic-expert-in-court-voir-dire/

****

"Ctrl -F" for The Board

Phishing gangs mounting high-ticket BEC attacks, average loss now $80,000
Companies are losing money to criminals who are launching Business Email Compromise (BEC) attacks as a more remunerative line of business than retail-accounts phishing, APWG reveals.
https://www.helpnetsecurity.com/2020/09/01/high-ticket-bec-attacks/

Which cybersecurity failures cost companies the most and which defenses have the highest ROI?
Massachusetts Institute of Technology (MIT) scientists have created a cryptographic platform that allows companies to securely share data on cyber attacks they suffered and the monetary cost of their cybersecurity failures without worrying about revealing sensitive information to their competitors or damaging their own reputation. https://www.helpnetsecurity.com/2020/09/03/cost-cybersecurity-failures/

Questions
Contact FIPCO's Ken Shaurette at 800/722-3498 ext. 251 or email FIPCO IT Services for more information.

"Make Security Part of You and Your Institution's DNA!"

Threat Intelligence Newsletter: September 15, 2020

FIPCO®
IT Audit
Round Table
Discussions

If you would like to host an event, please contact: Becky Schowalter

Upcoming Threat Intelligence Peer Group Discussions
None available at the current time

Banks Never Ask That Campaign – Is your Bank Participating?
(MARKETING DEPARTMENTS BECOME AWARE)
October 1st the beginning of Cybersecurity Awareness month is the beginning of a new ABA supported launch for a campaign to complement customer awareness that address safeguarding customer information. You do need to be an ABA member, but registration is needed and began September 1. Registration provides access to several resources. https://www.aba.com/advocacy/community-programs/banksneveraskthat

****

Alerts & Warnings

The Phishing Scam is After Your Google Password
Don't let your curiosity get the better of you. A new scam appears to be an email from Google, informing you that someone has shared a photo album. But it's really a phishing scheme that's after your password… https://www.bbb.org/article/news-releases/23010-bbb-scam-alert-photo-sharing-message-is-phishing-for-your-google-password

Fake Browser Updates Source Of Ransomware And Banking Malware
An all-out alarm reported by Surcuri finds bogus alerts circulating about the need to download the latest browser update. Although it's always recommended to keep software up to date, this report finds hackers are exploiting that call to action in a big way. Using fake updates isn't exactly a new hacking exploit, but hackers are getting better at it over time and this latest attack is a solid example of that.
https://www.sosdailynews.com/news.jspx?&articleid=53145BB7E1358505ECA4883914955837&sx=79

Critical Adobe Flaws Allow Attackers to Run JavaScript in Browsers
As part of its regularly scheduled security updates, Adobe fixed five critical cross-site scriptings (XSS) flaws hidden in Adobe Experience Manager. The flaws could potentially allow threat actors to execute arbitrary JavaScript code in victims' browsers. Experience Manager is a popular platform used to manage content for building websites, applications, https://threatpost.com/critical-adobe-flaws-attackers-javascript-browsers/159026/

Bluetooth Bug Could Allow MITM Attacks
A new vulnerability within Bluetooth has been discovered by security researchers at the École Polytechnique Fédérale de Lausanne (EPFL) and Purdue University. The flaw could potentially allow attackers to perform malicious man in the middle attacks,… https://www.infosecurity-magazine.com/news/bluetooth-bug-could-allow-mitm/

Did someone tell you to pay with gift cards? It's a scam
Maybe someone said you've won the lottery, a prize or sweepstakes. Or they claim to be from the government and tell you there's a problem with your Social Security number. And, to collect your winnings or solve your problem, you have to pay with gift cards. But here's the thing: anyone who insists that you pay by gift card is always a scammer. https://www.consumer.ftc.gov/blog/2020/09/did-someone-tell-you-pay-gift-cards-its-scam?utm_source=govdelivery

****

Hints & Tips plus Security Awareness

Abusing Wi-Fi Beacons and Detecting & Preventing Attacks
Thursday, September 17, 2020, 11:00AM - 12:00PM PDT // 60 MINUTES, INCLUDING Q&A
All Wi-Fi networks periodically broadcast beacons to announce their presence. These beacons are not authenticated and can be spoofed by an adversary, but it's unclear what risks this poses in practice.
In this webcast, we discuss what kinds of attacks are possible by spoofing Wi-Fi beacons. For example, we show how an adversary can reduce the throughput of nearby devices, lower the transmission power of clients, and we show how spoofing beacons can facilitate advanced man-in-the-middle attacks. In the second part of the webcast, we describe a scheme to protect Wi-Fi beacons. This scheme has been standardized as part of the (draft) IEEE 802.11 standard. We give a high-level explanation of our scheme, and we give a demo of its implementation in Linux.
https://event.on24.com/eventRegistration/EventLobbyServlet?target=reg20.jsp&referrer=&eventid=2613764&sessionid=1&key=E7DA3246BF9AFCD8F3132B0FE3240921&regTag=&sourcepage=register&elq_mid=1736&elq_cid=78182

Windows 10 Activity Timeline: An Investigator's Gold Mine
Julie: Hi, everyone. Thanks for joining today's webinar: Windows 10 Activity Timeline: An Investigator's Gold Mine. My name is Julie O'Shea and I'm the manager of global marketing here at BlackBag. Before we start today, there are a few things… https://www.forensicfocus.com/webinars/windows-10-activity-timeline-an-investigators-gold-mine/

Prioritizing "critical" vulnerabilities: A threat intelligence perspective
Recently, there have been many vendor security advisories containing multiple critical vulnerabilities potentially impacting organizations that may be conflicted with patch prioritization when looking at the variables seen for… https://public.intel471.com/blog/prioritizing-critical-vulnerabilities/

Securing Active Directory accounts against password-based attacks
Traditional password-based security might be headed for extinction, but that moment is still far off. In the meantime, most of us need something to prevent our worst instincts… https://www.helpnetsecurity.com/2020/09/08/securing-active-directory-accounts-against-password-based-attacks/

****

News & Views

Credit Card Skimmer Hits Over 1500 Websites
Magecart-linked Inter skimmer hits over 1500 websites… https://www.infosecurity-magazine.com/news/credit-skimmer-1500

Cracking Dictionaries: A Hacker's Guide For Password Thievery
Many businesses struggle with password security, especially when employees don't take it as seriously as they should. Human nature being what it is, staff who don't use password-smarts at home are likely to bring that same behavior to work. The reality is that 60% of small-to-medium-sized businesses close within six months of a cyberattack and the average financial cost per businesses is $200,000. With statistics like these, one would think that fortified passwords should be mandatory and no… https://www.sosdailynews.com/news.jspx?&articleid=BB4A12BCD12890FFF661D95D2181E95C&sx=79

A FIPCO Partner Product showcase: Cynet 360, 2020 Fall Platform Update
We are in dire need of approaches that simplify and consolidate the cybersecurity toolset so that companies can afford the coverage required and to make effective breach protection accessible to those other than world-class experts. https://www.helpnetsecurity.com/2020/09/09/product-showcase-cynet-360-2020-fall-platform-update/

****

"Ctrl -F" for The Board

Timelines In Digital Forensic Investigation: From Investigation To Court
Timelines have become a mainstay of digital forensic analysis in both public and private sectors. They help to explain what was happening on a given device or set of devices during a cybersecurity incident, a crime, a collision, or other… https://www.forensicfocus.com/articles/timelines-in-digital-forensic-investigation-from-investigation-to-court/

A Little Humor: You should Probably Change Your Password
https://www.linkedin.com/posts/activity-6708491566295609344-XOid

Questions
Contact FIPCO's Ken Shaurette at 800/722-3498 ext. 251 or email FIPCO IT Services for more information.

"Make Security Part of You and Your Institution's DNA!"

Threat Intelligence Newsletter: September 23, 2020

FIPCO®
IT Audit
Round Table
Discussions

If you would like to host an event, please contact: Becky Schowalter

Upcoming Threat Intelligence Peer Group Discussions
None available at the current time

****

Alerts & Warnings

Malicious VPN Email And Pop-up Attacks
For many these days, working remotely is part of the new normal of this pandemic era. It's probably also be the first time that staffers are away from the watchful eyes of IT departments, and that's making it easier for hackers to do their jobs. Two years ago, the Census Bureau reported the average work commute added 200 hours a year to our jobs. It's easy to see why many staffers are content to swap their daily commutes for...
https://www.sosdailynews.com/news.jspx?&articleid=F19A1646D119E3BDFEF8C02A2DCB8B6F&sx=79

Scam Phone Calls: Hang Up, Look Up, and Call Back
Scam phone calls -- anyone who tells you they've never had one probably doesn't have a phone! The truth is that no one is safe. https://scambusters.org/scamphonecall.html

Windows Exploit Released For Microsoft 'Zerologon' Flaw
Security researchers and US government authorities have been alerting the public to a critical privilege escalation flaw in Microsoft services, urging admins to address the pressing security issue. A proof-of-concept exploit code has been recently released for a Windows flaw that could allow attackers to obtain administrative privileges within a... https://threatpost.com/windows-exploit-microsoft-zerologon-flaw/159254/

Fake check scams and your small business
If someone you don't know sends you a check and asks for money back, that's a scam. But what if you're a small business owner and someone "overpays" you and asks you to refund the balance? That's still a scam — a fake check scam, to be exact. https://www.consumer.ftc.gov/blog/2020/09/fake-check-scams-and-your-small-business?utm_source=govdelivery

****

Hints & Tips plus Security Awareness

How does XDR improve enterprise security in the face of evolving threats?
Cybercriminals will never run out of ways to breach the security protocols enterprises put in place. As security systems upgrade their defenses, attackers also level up their attacks. They develop stealthier ways to compromise networks to avoid detection and enhance the chances of penetration. https://www.helpnetsecurity.com/2020/09/11/how-does-xdr-improve-enterprise-security-in-the-face-of-evolving-threats/ (For more information or a demonstration contact FIPCO to see a full featured XDR product in action) https://www.fipco.com/solutions/it-audit-security/autonomous-endpoint-protection

Attacked by ransomware? Five steps to recovery
Ransomware has been noted by many as the most threatening cybersecurity risk for organizations, and it's easy to see why: in 2019, more than 50 percent of all businesses were hit by a ransomware attack… https://www.helpnetsecurity.com/2020/09/15/attacked-by-ransomware-five-steps-to-recovery/

Spot and stop dishonest charity fundraisers
What's worse than a bogus charity? A bogus charity with a dishonest fundraiser. That's what we saw today in a case announced today against Outreach Calling, Inc., its founder Mark Gelvan, and others.
The defendants in this FTC case are fundraisers that called millions of Americans on behalf of bogus charities. https://www.consumer.ftc.gov/blog/2020/09/spot-and-stop-dishonest-charity-fundraisers?utm_source=govdelivery

Lost or Stolen Social Security Card? What You Need to Know
Most of us use our Social Security number all of the time, whether it's at the doctor's office, at the bank, or applying for government benefits and filing taxes. You need a Social Security number to apply for jobs, to open a credit card account, and even to get married. Because we use this number so much, many of us have it memorized and very rarely have to pull out our Social Security cards – but what happens if your Social Security card is lost or stolen? https://www.fightingidentitycrimes.com/replacing-lost-stolen-security-card/

****

News & Views

Mitigating Credential Stuffing Attacks in the Financial Sector
(If You Think Multi-Factor Authentication Prevents Credential Stuffing, Think Again!), Financial services firms around the world are… https://securityboulevard.com/2020/06/mitigating-credential-stuffing-attacks-in-the-financial-sector/

Zoom Will Offer Two-Factor Authentication to All Users
Zoom has announced plans to roll out two-factor authentication (2FA) to all users. There will be several 2FA options for users to choose from: authentication apps like Google Authenticator, Microsoft Authenticator, and FreeOTP, or a code from Zoom sent via SMS or a phone call. https://www.darkreading.com/application-security/zoom-brings-two-factor-authentication-to-all-users/d/d-id/1338885

Magecart Attack Impacts More Than 10K Online Shoppers
One of the largest known Magecart campaigns in history occurred over the weekend, impacting nearly 2,000 e-commerce sites. The attacks may have been a result of Magecart operators leveraging a zero-day exploit, however, the exact technicalities of the attack remain unknown. The campaign has affected tens of thousands of customers... https://threatpost.com/magecart-campaign-10k-online-shoppers/159216/

Do Californians use CCPA to protect their privacy?
Californians regularly opt-out of companies selling their personal information, with "Do-not-sell" being the most common CCPA right exercised, happening nearly 50% of the time over access and deletion requests, DataGrail's Mid-Year CCPA Trends Report shows. https://www.helpnetsecurity.com/2020/09/16/ccpa-use/

My stolen credit card details were used 4,500 miles away
When cybersecurity reporter Danny Palmer found his card was apparently used on another continent, he set out to discover more. https://www.techrepublic.com/article/my-stolen-credit-card-details-were-used-4500-miles-away-i-tried-to-find-out-how-it-happened/?ftag=TREa988f1c&bhid=78480402&mid=13052288&cid=712423569

****

"Ctrl -F" for The Board

Finding security talent is a long-range proposition
Generating more talent in the cybersecurity field will depend on finding "ways to communicate knowledge so that it not only sticks, but also resonates and appeals to a new generation of learners who are hungry for purpose," writes Christos Makridis, a research professor at Arizona State University. Makridis points out that labor market analytics provider Emsi says the US has only half the cybersecurity talent it needs… https://www.forbes.com/sites/christosmakridis/2020/09/17/cybersecurity-talent-gaps-are-bigger-than-we-thought-and-heres-how-to-solve-them/#3b1f8f5f1c8a

Questions
Contact FIPCO's Ken Shaurette at 800/722-3498 ext. 251 or email FIPCO IT Services for more information.

"Make Security Part of You and Your Institution's DNA!"

Threat Intelligence Newsletter: September 30, 2020

FIPCO®
IT Audit
Round Table
Discussions

If you would like to host an event, please contact: Becky Schowalter

Upcoming Threat Intelligence Peer Group Discussions
None available at the current time

****

Alerts & Warnings

Malicious Code Resurgence across Wisconsin (WSIC Fusion Center)
Additional information about Emotet, including recommendations for network defenders, can be found on this CISA Alert page: https://us-cert.cisa.gov/ncas/alerts/TA18-201A Reporting Notice: To report a cybersecurity event to the WSIC, please visit https://wifusion.widoj.gov/ and click on the "Cyber Incident Reporting Form" button.

Blessing Loom Scam Could Land You in Jail
Hard financial times are luring more people than usual into pyramid schemes, notably, right now, a scam known as the "Blessing Loom" or "Gifting Circle." https://scambusters.org/blessingloom.html
Like all pyramid schemes, most recently one known as "Secret Sister," it works on the idea that the earlier participants make some or all of their money, while later ones lose out -- they pay their money but get nothing when the scheme collapses. https://www.consumer.ftc.gov/blog/2020/05/game-chain-letter-scam

Windows server flaw prompts emergency action
The US Cybersecurity and Infrastructure Security Agency has warned of a flaw in Microsoft Windows that could open government servers to hackers. The agency ordered government groups to immediately patch or unplug their servers, saying the flaw represented "an unacceptable risk to the federal civilian executive branch." https://fcw.com/articles/2020/09/21/cisa-windows-flaw-federal-networks.aspx

****

Hints & Tips plus Security Awareness

Ad threats: What are they and why do they matter?
Cybercriminals are constantly on the lookout for new opportunities to pounce. They sniff out weaknesses in the online ecosystem and attempt to strike whenever and wherever it is easiest to do so. This has given way to some entirely new methods of cyberattacks in recent years, including ad threats.
https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2020/ad-threats-what-are-they-and-why-do-they-matter

Tips to help you prepare for — and recover from — natural disasters
More than 85 large wildfires are ripping across the West Coast, from California to Oregon and Washington. In the Southeast, people are just beginning to recover from Hurricane Sally, while more storms are brewing in the Atlantic. And the Midwest continues to recover from the recent derecho…
https://www.consumer.ftc.gov/blog/2020/09/tips-help-you-prepare-and-recover-natural-disasters?utm_source=govdelivery

MOBILE BANKING (vendor whitepaper)
LEGAL FRAMEWORK, THREATS &FRAUD PREVENTION
https://www.pradeo.com/media/White_Paper_Mobile_Banking_Fraud_Prevention.pdf

Zerologon Vulnerability: Analysis and Detection Tools
What is Zerologon, In September 2020 Secura published an article disclosing a vulnerability in Windows Server (all known versions) Netlogon Remote Protocol. This vulnerability is known as CVE-2020-1472 or more commonly, Zerologon... https://www.cynet.com/zerologon/

Your best defense against ransomware: Find the early warning signs
As ransomware continues to prove how devastating it can be, one of the scariest things for security pros is how quickly it can paralyze an organization. Just look at Honda, which was forced to shut down all global operations in June, and Garmin, which had its services knocked offline for days in July. Consider what tools you may have in place to protect, traditional AV is not typically one of them!!
https://www.helpnetsecurity.com/2020/09/23/your-best-defense-against-ransomware-find-the-early-warning-signs/

This NIST Cybersecurity Practice Guide—Data Integrity: Recovering from Ransomware and Other Destructive Events
How can organizations develop and implement appropriate actions following a detected cybersecurity event. The solutions outlined in this guide encourage monitoring and detecting data corruption in commodity components as well as custom applications and data composed of open-source and commercially available components. https://csrc.nist.gov/publications/detail/sp/1800-11/final
https://www.helpnetsecurity.com/2020/09/24/nist-guide-recover-ransomware/

****

News & Views

Report documents more sophisticated ransomware scams
Ransomware operators are teaming up for elaborate operations resembling organized cybercrime, reports Positive Technologies, a provider of enterprise security. Also, cybercrooks are increasingly threatening to publish data online if a ransom is not paid. https://www.techrepublic.com/article/how-ransomware-operators-are-joining-forces-to-carry-out-attacks/

CYBER SECURITY STANDARDS AND FRAMEWORKS
Assessment and Effective Communication of Risk, vendor white paper… https://www.enzoic.com/wp-content/uploads/cs-hub-report.pdf

A look at the top threats inside malicious emails
Web-phishing targeting various online services almost doubled during the COVID-19 pandemic: it accounted for 46 percent of the total number of fake web pages, Group-IB reveals.
https://www.helpnetsecurity.com/2020/09/21/top-threats-inside-malicious-emails/

Why it's probably time to change your passwords – a fun look at WHY?
Lax password security has created a thriving underground market for cybercriminals, sometimes with email addresses and usernames thrown in. The technique of generating random passwords is also used for brute-force attacks, with one experiment producing 100 billion guesses per second.
https://www.youtube.com/watch?v=aHaBH4LqGsI

****

"Ctrl -F" for The Board

Justifying your 2021 cybersecurity budget
Sitting in the midst of an unstable economy, a continued public health emergency, and facing an uptick in successful cyber attacks, CISOs find themselves needing to enhance their cybersecurity posture while remaining within increasingly scrutinized budgets.
https://www.helpnetsecurity.com/2020/09/18/justifying-your-2021-cybersecurity-budget/

Protecting Organizations From Today's Top Cyber Threats
Cyber threats are constantly evolving. As recently as 2016, Trojan malware accounted for nearly 50% of all breaches. Today, they are responsible for less than seven percent. That's not to say that Trojans are any less harmful. According to the 2020 Verizon Data Breach Investigations Report (DBIR), their backdoor and remote-control capabilities are still used by advanced threat actors to conduct sophisticated attacks. Staying ahead of evolving threats is a challenge that keeps many IT professionals awake at night. Understanding today's most important cyber threats is the first step toward protecting any organization from attack. https://www.cisecurity.org/blog/protecting-organizations-from-todays-top-cyber-threats/

Questions
Contact FIPCO's Ken Shaurette at 800/722-3498 ext. 251 or email FIPCO IT Services for more information.

"Make Security Part of You and Your Institution's DNA!"

Threat Intelligence Newsletter: October 5, 2020

FIPCO®
IT Audit
Round Table
Discussions

If you would like to host an event, please contact: Becky Schowalter

Upcoming Threat Intelligence Peer Group Discussions
None available at the current time

****

Alerts & Warnings

Alien Android Banking Trojan Sidesteps 2FA
A new variant of the infamous Cerberus banking Trojan named Alien has been ruthlessly targeting victims' credentials for over 200 popular mobile apps, including Microsoft Outlook and Bank of America. The banking trojan is gaining access to Android devices worldwide through utilizing an advanced authentication bypass tool that allows it… https://threatpost.com/alien-android-2fa/159517/

Google removes 17 Android apps designed to deploy Joker malware
Google has been combatting malicious apps landing in its Play Store for years, trying to figure out loopholes in its systems that allow for these apps to evade detection. Recently, the pervasive malware Joker has found its way into the app buying platform, infecting 17 applications. Google has since removed… https://www.techrepublic.com/article/google-removes-17-android-apps-designed-to-deploy-joker-malware/

Home Working Network Attacks Lead 2020 Scam Surge
The past few months of this crazy year have seen a huge scam surge and changing the most common types of con tricks. https://scambusters.org/scamsurge.html

Heard about the "waiting package" phishing scam?
Phishing scams can be hard to spot. For example, we've been hearing about one where people get a text message saying that there's a package waiting for them, and asking them to click a link to learn more. Sounds innocent enough, right? Unfortunately not.
https://www.consumer.ftc.gov/blog/2020/09/heard-about-waiting-package-phishing-scam?utm_source=govdelivery

Banks vulnerable to credential stuffing, US FBI warns
The US FBI has issued a Private Industry Notification to the financial sector about credential stuffing attacks fed by billions of stolen credentials available on the darknet. One problem is that many bank customers are reluctant to use multifactor authentication, says Chris Pierson, CEO of security company BlackCloak. https://www.bankinfosecurity.com/fbi-warns-credential-stuffing-attacks-on-rise-a-15075

This worm phishing campaign is a game-changer in password theft, account takeovers
A new worm phishing campaign discovered by cybersecurity architect and bug bounty hunter Craig Hays has gained widespread attention as a new method of password theft. Hays outlined the phishing attempt in a recent report, stating that it went beyond usual tactics and basic attempts to compromise a network, claiming… https://www.zdnet.com/article/this-worm-phishing-campaign-is-a-game-changer-in-password-theft-account-takeovers/

New Vulnerabilities Bypass Multi-Factor Authentication for Microsoft 365
Proofpoint researchers recently discovered critical vulnerabilities in multi-factor authentication (MFA) implementation in cloud environments where WS-Trust is enabled. These vulnerabilities could allow at… https://www.proofpoint.com/us/blog/cloud-security/new-vulnerabilities-bypass-multi-factor-authentication-microsoft-365

****

Hints & Tips plus Security Awareness

So Many Logs, So Little Time: Efficient Windows Event Log Analysis
Windows Event Logs record evidence of many significant types of activity, including when a machine was booted or shut down, when users logged in and out and from where, device insertions, network connections and so much more. But knowing how… https://www.forensicfocus.com/news/on-demand-webinar-so-many-logs-so-little-time-efficient-windows-event-log-analysis/

Compromised Personal Network Indicators and Mitigations
This document provides guidance for government teleworkers with authorization to connect government-issued equipment to personal networks. It describes potential indicators of compromise and mitigation practices that can be used to minimize damage if the network is believed to be compromised… https://media.defense.gov/2020/Sep/17/2002499615/-1/-1/0/%0ACOMPROMISED_PERSONAL_NETWORK_INDICATORS_AND_MITIGATIONS_20200914_FINAL.PDF/COMPROMISED_PERSONAL_NETWORK_INDICATORS_AND_MITIGATIONS_20200914_FINAL.PDF?utm_campaign=RiskCyber-20200929&utm_medium=email&utm_source=Eloqua

Have you gotten a collection call about a debt you don’t recognize?
Nobody likes getting debt collection calls. But have you ever gotten one for a debt you already paid — or you know isn’t yours? Or have you been threatened and harassed by a debt collector until you paid up? If so, we want you to know how to protect yourself. https://www.consumer.ftc.gov/blog/2020/09/have-you-gotten-collection-call-about-debt-you-dont-recognize?utm_source=govdelivery

****

News & Views

Malware attacks becoming more sophisticated
Malware attacks declined by 8% last quarter, finds an analysis compiled by WatchGuard from nearly 42,000 of its appliances installed worldwide. WatchGuard Chief Technology Officer Corey Nachreiner notes the sophistication increased, with more "crypters" or "packers" used to evade detection.
https://www.darkreading.com/endpoint/malware-attacks-declined-but-became-more-evasive-in-q2/d/d-id/1339010

Microsoft releases Digital Defense Report detailing increasingly advanced cyberattacks
There's been a surge in cybersecurity activity as companies continue to operate remotely and cybercriminals look to exploit the ongoing coronavirus pandemic.
https://www.techrepublic.com/article/microsoft-releases-digital-defense-report-detailing-increasingly-advanced-cyberattacks/?ftag=TREa988f1c&bhid=78480402&mid=13082254&cid=712423569

MITRE Shield shows why deception is security's next big thing
Seasoned cybersecurity pros will be familiar with MITRE. Known for its MITRE ATT&CK framework, MITRE helps develop threat models and defensive methodologies for both the private and public sector cybersecurity communities. https://www.helpnetsecurity.com/2020/09/30/mitre-shield-deception/

****

"Ctrl -F" for The Board

GRC teams have a number of challenges meeting regulatory demands
Senior risk and compliance professionals within financial services company's lack confidence in the security data they are providing to regulators, according to Panaseer.
https://www.helpnetsecurity.com/2020/09/28/grc-teams-challenges-meeting-regulatory-demands/

Questions
Contact FIPCO's Ken Shaurette at 800/722-3498 ext. 251 or email FIPCO IT Services for more information.

"Make Security Part of You and Your Institution's DNA!"

Threat Intelligence Newsletter: October 15, 2020

FIPCO®
IT Audit
Round Table
Discussions

If you would like to host an event, please contact: Becky Schowalter

Upcoming Threat Intelligence Peer Group Discussions
None available at the current time

****

Alerts & Warnings

FBI warns of risks of using wireless hotel networks
The FBI has issued a new warning against the use of hotel Wi-Fi connections, due to public offerings may contain vulnerabilities as a result of poor security measures. The FBI states that this is true for libraries, coffee shops, and other locations with free public Wi-Fi. In the advisory, the...
https://www.ic3.gov/media/2020/201006.aspx

Comcast TV Remote Hack Opens Homes to Snooping
Researchers disclosed the 'WarezTheRemote' attack, affecting Comcast's XR11 voice remote control.
https://threatpost.com/comcast-tv-remote-homes-snooping/159899/

PoetRAT malware evolves to be slimmer, faster and harder to detect
Description: Cisco Talos is tracking the behavior of the attackers behind the PoetRAT threat, who continue to target public and private entities in Azerbaijan. They observed multiple new campaigns indicating a change in the actor's capabilities and showing their maturity toward better operational security. This actor continues to use spear-phishing attacks to lure a user to download a malicious document from temporary hosting providers. The malware comes from malicious URLs included in the email, resulting in the user clicking and downloading a malicious document. Previous versions of PoetRAT deployed a Python interpreter to execute the included source code which resulted in a much larger file size compared to the latest version's switch to Lua script.
References: https://blog.talosintelligence.com/2020/10/poetrat-update.html

BBB Scam Alert: Phony Amazon callers use BBB phone number
How the Scam Works: You answer the phone, and it is a recorded message claiming to be from Amazon stating there is a problem with your Amazon account. The message ranges from...
https://www.bbb.org/article/news-releases/23214-bbb-scam-alert-phony-amazon-callers-use-bbb-phone-number

****

Hints & Tips plus Security Awareness

Why CIOs need to focus on password exposure, not expiration
Both NIST and Microsoft have recently come out against forced periodic password resets for a variety of reasons, including... https://www.helpnetsecurity.com/2020/10/05/focus-on-password-exposure-not-expiration/

Ransomware Prevention and Response for CISOs
Document provides an aggregate of already existing federal government and private industry best practices and mitigation strategies focused on the prevention and response to ransomware incidents.
https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view

Why developing cybersecurity education is key for a more secure future
Cybersecurity threats are growing every day, be they are aimed at consumers, businesses or governments. The pandemic has shown us just how critical cybersecurity is to the successful operation of our respective economies and our individual lifestyles. https://www.helpnetsecurity.com/2020/10/05/why-developing-cybersecurity-education-is-key-for-a-more-secure-future/

Do your part for CyberSecurity Awareness Month
October is Cybersecurity Awareness Month (CSAM) - a time to implement stronger security practices and prioritize educating and training employees in your organization. Own your role in protecting your organization and "Do Your Part. #BeCyberSmart." To kick off this month, LogMeIn has created some new cybersecurity resources for you. https://explore.logmein.com/lastpass-october-newsletter-pros/from-passwords-to-passwordless-ebook?cid=LP_NA_ADH_Newsletter_Expired-Prospects-and-Trialers-Passwordless&utm_medium=email&utm_source=newsletter&utm_campaign=lp-na-en-adh-lead-2020-10-06-newsletter-expired-prospects-and-trialers-passwordless&utm_content=expired-prospects-and-trialers-passwordless-group6-button&mkt_tok=eyJpIjoiWVdFME9EQmhPVGxoT0RRMCIsInQiOiJyQWdYRm5RbEE3Sm41anQ5aXIxWHIxeWZvSUJvOU4rNDdLeVUzMm9wTHhDWUxtS0thYll6M21OMiswdVdiVEJBTHcrdXhhXC9zbTdoV1p4WE9yRmNIWXZKbFFuV2hhZWluT1haYlFidzh3YzZlVHpHRlBzVWhBenY0N1I0Y2pmelMifQ%3D%3D

Call Spoofing: It's Down to You to Spot and Stop
Caller ID has been around for about 30 years but, sadly, call spoofing -- creating and using fake numbers -- has been with us for almost as long. It has led hundreds of thousands, if not millions, of people to fall into the clutches of scammers. https://scambusters.org/callspoofing2.html or learn more at
https://www.fcc.gov/consumers/guides/spoofing-and-caller-id

Three common mistakes in ransomware security planning
As the frequency and intensity of ransomware attacks increase, one thing is becoming abundantly clear: organizations can do more to protect themselves. Unfortunately, most organizations are dropping the ball. Most victims receive adequate warning of potential vulnerabilities yet are woefully unprepared to recover when they are hit. Here are just a few recent examples of both prevention and incident response failures: https://www.helpnetsecurity.com/2020/10/07/mistakes-ransomware-security-planning/

****

News & Views

Is passwordless authentication actually the future?
While passwords may not be going away completely, 92 percent of respondents believe passwordless authentication is the future of their organization, according to a LastPass survey.
https://www.helpnetsecurity.com/2020/10/02/is-passwordless-authentication-actually-the-future/

Ransomware Vaccine Intercepts Requests to Erase Shadow Copies
A new ransomware “vaccine” could transform the way organizations treat cyberattacks, preventing certain ransomware families from erasing shadow copies and promoting data recovery. The technology, which has been named “Raccine,” targets ransomware families that leverage the command vssadmin.exe to delete shadow copies on the targeted machine. The preventative software was released…
https://www.securityweek.com/ransomware-vaccine-intercepts-requests-erase-shadow-copies

Credential Stuffing: the Culprit of Recent Attacks
With only a few months left in 2020, let’s reflect on the major data breaches that have occurred so far and brace ourselves for what is to come: https://www.infosecurity-magazine.com/blogs/credential-stuffing-recent-attacks

Using a WordPress flaw to leverage Zerologon and attack companies’ Domain Controllers
Recently, a critical vulnerability called Zerologon – CVE-2020-1472 – has become a trending subject around the globe. https://securityaffairs.co/wordpress/109175/hacking/zerologon-dc-hack.html

****

"Ctrl -F" for The Board

Business E-mail Compromise: The 3.1 Billion Dollar Scam
This Public Service Announcement (PSA) is an update to the Business E-mail Compromise (BEC) information provided in Public Service Announcements… While the article may be dated, the Scam still occurs regularly today. https://www.ic3.gov/media/2016/160614.aspx

Questions
Contact FIPCO’s Ken Shaurette at 800/722-3498 ext. 251 or email FIPCO IT Services for more information.

"Make Security Part of You and Your Institution's DNA!"

Threat Intelligence Newsletter: October 21, 2020

FIPCO®
IT Audit
Round Table
Discussions

If you would like to host an event, please contact: Becky Schowalter

Upcoming Threat Intelligence Peer Group Discussions
None available at the current time

The #BanksNeverAskThat anti-phishing campaign has been a huge success since its launch on Oct. 1. Thousands of banks of all sizes, from across the country, have been doing their part to educate their customers about phishing scams and how to spot them. Register now, there is still time to leverage the resources, just because October awareness month ends, awareness does not: https://www.aba.com/advocacy/community-programs/banksneveraskthat?utm_campaign=Phishing-Campaign_Banker-Reg_E3_20200917.html&utm_medium=email&utm_source=Eloqua

****

Alerts & Warnings

ATM cash-out: A rising threat requiring urgent attention
The PCI Security Standards Council (PCI SSC) and the ATM Industry Association (ATMIA) issued a joint bulletin to highlight an increasing threat that requires urgent awareness and attention. https://www.helpnetsecurity.com/2020/10/09/atm-cash-out-threat/

Critical Zerologon Flaw Exploited in TA505 Attacks
Microsoft has reported a new campaign utilizing the critical Zerologon vulnerability previously disclosed to the public. Just days after witnessing the nation-state hacking group Mercury was observed leveraging the flaw, the TA505 Russian speaking threat group known for the Dridex banking Trojan and Locky Ransomware has been using the same… https://www.darkreading.com/threat-intelligence/critical-zerologon-flaw-exploited-in-ta505-attacks/d/d-id/1339141

Amazon Prime Day Spurs Spike in Phishing, Fraud Attacks
Security researchers have observed a recent spike in phishing attempts and malicious website creation that aims to defraud Amazon customers. Amazon Prime Day will occur over two days this year, the 13 and 14 of October, however, the recently increased threat to Amazon customers may turn the event into a… https://threatpost.com/amazon-prime-day-spurs-spike-in-phishing-fraud-attacks/159960/

BleedingTooth Vulnerabilities Allow Zero-Click Attacks
Bluetooth vulnerabilities could be exploited to run arbitrary code or access sensitive information. https://www.securityweek.com/bleedingtooth-vulnerabilities-linux-bluetooth-allow-zero-click-attacks

Google warns of severe 'BleedingTooth' Bluetooth flaw in Linux kernel
A new vulnerability has been disclosed by Google, a high-severity flaw that affects Linux devices. The bug reportedly lies in the Bluetooth stack within Linux kernel versions 5.9 and below that support BlueZ. Cybersecurity firms are urging users to update the Linux kernel to version 5.9, which was released just… https://www.zdnet.com/article/google-warns-of-severe-bleedingtooth-bluetooth-flaw-in-linux-kernel/

****

Hints & Tips plus Security Awareness

PSA: Business E-Mail Compromise Scam
Public service announcement warning of the dangers of business e-mail compromise scams (BECs) https://www.fbi.gov/video-repository/psa-business-e-mail-compromise-scam.mp4/view

7 Top Anti-Scam Tips for Cyber Security Month
"Do your part. #BeCyberSmart." That's the theme of this year's National Cyber Security Awareness Month (NCSAM), which runs throughout October, with a host of ideas and tips to help users avoid Internet scams and other malware. https://www.scambusters.org/cybersecurity2.html

Integrating Cybersecurity and Enterprise Risk Management (ERM): NISTIR 8286
The increasing frequency, creativity, and variety of cybersecurity attacks means that all enterprises should ensure cybersecurity risk receives the appropriate attention along with other risk disciplines–legal, financial, etc.–within their enterprise risk management (ERM) programs. This document is intended to help cybersecurity risk management practitioners at all levels of the enterprise, in private and public sectors, to better understand and practice cybersecurity risk management within the context of ERM. https://csrc.nist.gov/publications/detail/nistir/8286/final

The anatomy of an endpoint attack
Cyberattacks are becoming increasingly sophisticated as tools and services on the dark web – and even the surface web – enable low-skill threat actors to create highly evasive threats. https://www.helpnetsecurity.com/2020/10/12/anatomy-of-an-endpoint-attack/

Wormable Apple iCloud Bug Allows Automatic Photo Theft
Ethical hackers have reportedly been earning large payouts from Apple's bug bounty program for their involvement in discovering 55 bugs during a three-month hack that exposed a wormable Apple iCloud vulnerability that could be exploited for photo theft. The ethical hackers searched through Apple's infrastructure and systems, discovering a total... https://threatpost.com/3-month-apple-hack-vulnerabilities-critical/159988/

****

News & Views

Top 10 Security Projects for 2020-2021
Security and risk management leaders should focus on these 10 security projects to drive business-value and reduce risk for the business. https://www.gartner.com/smarterwithgartner/gartner-top-security-projects-for-2020-2021/

Marketing Firm Spills Nearly Three Million Records
Friendemic, a digital marketing provider that offers services to US car dealerships, has exposed almost three million records consisting of personally-identifiable information (PII) following a misconfiguration in the cloud settings. The privacy breach was discovered by Aaron Phillips at Comparitech, who was conducting routine internet crawls to check for issues… https://www.infosecurity-magazine.com/news/marketing-firm-spills-nearly-three/

Can Hackers Take A Bite Out Of Your Mobile Pay Solution?
With the many digital payment options available today, finding the most secure providers can be a challenge. The popularity of digital wallets has grown over time and writing checks and even using plastic cards for payments are quickly becoming the dinosaurs of our non-digital past. Many users now own mobile wallets and pay for goods and services. And using Apple Pay, Google Pay or another service for those transactions may offer peace of mind knowing your payment data is safe and out of the reach of hackers.
https://www.sosdailynews.com/news.jspx?&articleid=98AFD2BFEC907438BCDB397136B75172&sx=79

All Zoom users get end-to-end encryption (E2EE) option next week
Starting next week, Zoom users – both those who are on one of the paid plans and those who use it for free – will be able to try out the solution's new end-to-end encryption (E2EE) option.
https://www.helpnetsecurity.com/2020/10/15/zoom-e2ee-end-to-end-encryption/

****

"Ctrl -F" for The Board

Why are certain employees more likely to comply with information security policies than others?
Information security policies (ISP) that are not grounded in the realities of an employee's work responsibilities and priorities expose organizations to higher risk for data breaches, according to a research from Binghamton University, State University of New York.
https://www.helpnetsecurity.com/2020/10/09/comply-with-information-security-policies/

Questions
Contact FIPCO's Ken Shaurette at 800/722-3498 ext. 251 or email FIPCO IT Services for more information.

"Make Security Part of You and Your Institution's DNA!"

Threat Intelligence Newsletter: October 27, 2020

If you would like to host an event, please contact: Becky Schowalter

Upcoming Threat Intelligence Peer Group Discussions
None available at the current time

****

Alerts & Warnings

Massive New Phishing Campaigns Target Microsoft, Google Cloud Users
A series of phishing campaigns are allegedly targeting public cloud users, according to researchers from cybersecurity firm Greathorn. The campaigns aim to compromise Microsoft Office 365 and Gmail accounts by leveraging intriguing headlines pertaining to current events. The phishing emails contain malicious links that, when opened, lead victims to… https://www.darkreading.com/attacks-breaches/massive-new-phishing-campaigns-target-microsoft-google-cloud-users/d/d-id/1339204

Threatening phone scams are targeting parents and immigrants
Two disturbing phone scams have popped up on the FTC's radar. Both scams have one thing in common: they want to trick (and scare) you out of money. If you live on Staten Island, pay close attention, since these two scams seem to be targeting people in your area. But we know that scammers don't often stick with one area, so they could expand their target area any time now.
https://www.consumer.ftc.gov/blog/2020/10/threatening-phone-scams-are-targeting-parents-and-immigrants?utm_source=govdelivery

Impacted Products: VMware ESXi VMSA-2020-0023
Please see the advisory here: https://www.vmware.com/security/advisories/VMSA-2020-0023.html

Google's Waze Can Allow Hackers to Identify and Track Users
Google's Waze app contains a serious security vulnerability that allows hackers to identify users and track their locations. The flaw has since been patched and was an API flaw that allowed security researcher Peter Gasper to use the app to uncover the true identity of drivers using it. Gasper is… https://threatpost.com/googles-waze-track-users/160332/

Scams that start on social media

Scammers are hiding out on social media, using ads and offers to market their scams, according to people's reports to the FTC and a new Data Spotlight. In the first six months of 2020, people reported losing a record high of almost $117 million to scams that started on social media. https://www.consumer.ftc.gov/blog/2020/10/scams-start-social-media?utm_source=govdelivery

Windows GravityRAT Malware Now Also Targets macOS and Android Devices

A Windows-based remote access Trojan believed to be designed by Pakistani hacker groups to infiltrate computers and steal users' data has resurfaced after a two-year span with retooled capabilities to target Android and macOS devices… https://thehackernews.com/2020/10/windows-gravityrat-malware-now-also.html?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+TheHackersNews+%28The+Hackers+News+-+Cyber+Security+Blog%29&_m=3n.009a.2337.aa0ao086k1.1gz2

Overpaid your utility bill? That's probably a scam

You get a robocall saying you paid too much on a utility bill. To make up for this mistake, they say, you'll get a cash refund and a discount on your future bills. All you have to do is press a number to get your money and discount. You say to yourself: "What luck!" You might think this strange surprise will help you save some much-needed money. https://www.consumer.ftc.gov/blog/2020/10/overpaid-your-utility-bill-thats-probably-scam?utm_source=govdelivery

****

Hints & Tips plus Security Awareness

Android Smartphone Malware: How To Tell If Yours Has It And How To Avoid It

Those ugly little viruses that love to live in Android devices are a problem and many users may suspect they have malware, but aren't aware of how to tell or what to do about it. Different malware types bring their own symptoms, making it difficult to figure out what type the malware is, much less… https://www.sosdailynews.com/news.jspx?&articleid=FE9B1E7B49BC21C32C7F3866EBD1B09A&sx=79

IRS Annual Dirty Dozen Top Tax Scams For 2020

The IRS posted its annual list of the top tax scams for 2020, called the "Dirty Dozen." Every year, the IRS takes a look at the most prevalent tax scams affecting U.S. taxpayers. In its continued effort to keep us safe from tax fraudsters, the IRS tells us what these scams can look like so we can avoid becoming a victim. They also remind us that although scams increase during tax time and crisis events, they continue to happen year-round. https://www.sosdailynews.com/news.jspx?&articleid=A3E4DE989F0C2454DF16D7FFF37DD365&sx=79

Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments

The U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) is issuing this advisory to highlight the sanctions risks associated with ransomware payments related to malicious cyber-enabled activities. Demand for ransomware payments has increased du… https://home.treasury.gov/system/files/126/ofac_ransomware_advisory_10012020_1.pdf

Cyber monitoring: CSIAC Webinar 11/17

You cannot monitor what you cannot measure. In the world of computer communications, monitoring takes on two distinct forms: performance measuring and monitoring physical parameters, and security monitoring of network traffic and computer processes. Only one of these monitoring approaches work. We examine the failure of security monitoring in terms of scope and effectiveness, and discuss the risk that monitoring introduces to a mission. Presenter: Dr. Kamal T. Jabbour, a member of the scientific and technical cadre of senior executives, is Senior Scientist for Information Assurance, Information Directorate, Please register in advance for the webinar at: https://www.anymeeting.com/PIID=EF56DB8688493E

Alternative Live Streams:

- Facebook: https://r.csiac.org/facebook
- YouTube: https://r.csiac.org/youtube

How a Great Deal Lures You Into a Survey Scam
Since many of us are spending more time at home these days, you might be tempted to take a more favorable view of one of those survey or feedback requests that either arrive randomly in your online mailbox or appear in an online ad. https://www.scambusters.org/survey2.html

CISA offers the following resources to share in your communities and with your stakeholders for National Cybersecurity Awareness Month (NCSAM) and beyond:

- Telework Guidance and Best Practices: https://www.cisa.gov/telework
- Assessments, Prevention, and Response Resources: https://www.cisa.gov/cyber-resource-hub
- Cybersecurity Awareness and Best Practices Resources: https://www.cisa.gov/publication/cisa-cyber-essentials
- Election Security and Disinformation Resources: https://www.cisa.gov/protect2020
- Mitigating Cyber Risks To The Nation's Critical Infrastructure: https://www.cisa.gov/national-risk-management

Reporting fraud helps everyone – and now it's easier to do
You can help the FTC and its partners fight fraud in your community — and you don't even need to wear a superhero cape (unless you want to). Your story is your superpower. When you tell the FTC about frauds, scams, and other kinds of bad business practices, you're helping the FTC and our law enforcement partners spot and stop scams. To make it easier, the FTC just launched ReportFraud.ftc.gov.
https://www.consumer.ftc.gov/blog/2020/10/reporting-fraud-helps-everyone-and-now-its-easier-do?utm_source=govdelivery

****

News & Views

Why ransomware has become such a huge problem for businesses
Ransomware has evolved into a significant threat for all types of organizations. How and why is it such a pervasive issue, and how can organizations better defend themselves against it?
https://www.techrepublic.com/article/why-ransomware-has-become-such-a-huge-problem-for-businesses/?ftag=TREa988f1c&bhid=78480402&mid=13121701&cid=712423569

BEC Attacks: Nigeria No Longer the Epicenter as Losses Top $26B
BEC fraudsters now have bases of operation across at least 39 counties and are responsible for $26 billion in losses annually — and growing. A study of more than 9,000 instances of business email compromise (BEC) attacks all over the world shows that the number has skyrocketed over the past year, and that the social-engineering scam has expanded well beyond its historic roots in Nigeria.
https://threatpost.com/bec-attacks-nigeria-losses-snowball/160118/

25 Days, 25 Questions: Professional Digital Forensics Qualifications In Court
Every day a question was posed to the enthusiastic digital forensic community and the next day I posted my comments/views on the same. The idea of 25 days 25 questions initiative was to achieve three major purposes:
Part 1: https://www.forensicfocus.com/articles/25-days-25-questions-part-1-process-and-practice/
Part 2: https://www.forensicfocus.com/articles/25-days-25-questions-part-2-professional-digital-forensics-qualifications/
Part 3: https://www.forensicfocus.com/legal/25-days-25-questions-part-3-professional-digital-forensics-qualifications-in-court/
Part 4: Coming Soon but not yet available: https://www.forensicfocus.com/articles/25-days-25-questions-part-4-professional-digital-forensics-qualifications/

Can we trust passwordless authentication?
We are beginning to shift away from what has long been our first and last line of defense: the password. It's an exciting time. Since the beginning, passwords have aggravated people. Meanwhile, passwords have become the de facto first step in most attacks. Yet I can't help but think, what will the consequences of our actions be? https://www.helpnetsecurity.com/2020/10/20/can-we-trust-passwordless-authentication/

****

"Ctrl -F" for The Board

Banks risk losing customers with anti-fraud practices
Many banks across the U.S. and Canada are failing to meet their customers' online identity fraud and digital banking needs, according to a survey from FICO.
https://www.helpnetsecurity.com/2020/10/16/banks-risk-losing-customers-with-anti-fraud-practices/

Do Your Part. #BeCyberSmart.
Cybersecurity starts with YOU and is everyone's responsibility. There are currently an estimated 4.8 billion Internet users—over 62% of the world's population! This number will only grow, making the need to "Protect It" more important than ever. https://www.cisa.gov/national-cyber-security-awareness-month?ACSTrackingID=USCDC_481-DM40789&ACSTrackingLabel=%23BeCyberSmart%3A%205%20Ways%20to%20Protect%20Your%20Health%20Tech&deliveryName=USCDC_481-DM40789

Avoiding the snags and snares in data breach reporting: What CISOs need to know
US laws and guidance governing data breaches and how they must be reported have created problems for chief information security officers, including criminal charges.
https://www.csoonline.com/article/3584783/avoiding-the-snags-and-snares-in-data-breach-reporting-what-cisos-need-to-know.html

Questions
Contact FIPCO's Ken Shaurette at 800/722-3498 ext. 251 or email FIPCO IT Services for more information.

"Make Security Part of You and Your Institution's DNA!"

Threat Intelligence Newsletter: November 10, 2020

FIPCO®
IT Audit
Round Table
Discussions

If you would like to host an event, please contact: Becky Schowalter

Upcoming Threat Intelligence Peer Group Discussions
None available at the current time

****

Alerts & Warnings

Non-filers: Expect a letter about your stimulus check
The IRS announced "National EIP Registration Day," taking place November 10. That's when the IRS and partners will do a final push to reach out to people who don't normally file taxes. They want to be sure they know that they may qualify for a payment and should register at IRS.gov to request their EIP. https://www.consumer.ftc.gov/blog/2020/11/non-filers-expect-letter-about-your-stimulus-check?utm_source=govdelivery

Google discloses actively exploited Windows zero-day (CVE-2020-17087)
Google researchers have made public a Windows kernel zero day vulnerability (CVE-2020-17087) that is being exploited in the wild in tandem with a Google Chrome flaw (CVE-2020-15999) that has been patched on October 20. https://www.helpnetsecurity.com/2020/11/02/cve-2020-17087/

Scammers Abuse Google Drive to Send Malicious Links
Cybercriminals have launched a new campaign leveraging legitimate Google Drive features to trick unsuspecting users into opening malicious links. The feature allows the attackers to create push notifications or emails that ask the recipient to share a Google Doc. This then lets the cybercriminals to distribute malicious links via a… https://threatpost.com/scammers-google-drive-malicious-links/160832/

Shop 'Til You Drop? FBI Warns Of Escalation In Online Shopping Scams
At a time when the coronavirus pandemic makes online shopping more vital than ever, dissatisfied consumers have been ringing the scam alarm loudly and more often than ever before. Some consumers report receiving products they didn't order and were not what they purchased. The FBI recently released an alert about online shopping and the increasing number of scams surrounding purchases and promises made but never kept.
https://www.sosdailynews.com/?articleid=%201358034C6AFF03874F7FD1DDDA202583

VMWare ESXi patches
VMSA-2020-0023.1 - VMware ESXi, Workstation, Fusion and NSX-T updates address multiple security vulnerabilities (CVE-2020-3981, CVE-2020-3982, CVE-2020-3992, CVE-2020-3993, CVE-2020-3994, CVE-2020-3995) Please see the updated advisory here: https://www.vmware.com/security/advisories/VMSA-2020-0023.html

Games in Microsoft Store Can Be Abused for Privilege Escalation on Windows
A new flaw in Windows can allow malicious actors to exploit the vulnerability to escalate privileges to SYSTEM on Windows 10 through utilizing access through the Microsoft Store. Researchers at IOActive uncovered the threat, which was patched in October as part of Microsoft's monthly Patch Tuesday. The flaw is known… https://www.securityweek.com/games-microsoft-store-can-be-abused-privilege-escalation-windows

****

Hints & Tips plus Security Awareness

How to fix the security holes in Microsoft Teams
It's time to address security challenges related to the hasty embrace of Microsoft Teams, writes Frank Trovato of Info-Tech Research Group. Trovato examines "the data security chaos inherent in most MS Teams implementations" and explains how to patch the biggest security holes.
https://securityboulevard.com/2020/10/ms-teams-the-gateway-drug-to-security-chaos/

Identity Fraud Gets A Makeover: Mitigating The Challenge Of Change
As the appearance and methodology of identity fraud continues to evolve, those at Javelin Strategy & Research have been studying the changes since 2003. Their "2019 Identity Fraud Study" is a window into identity fraud trends and how they morph and improve over time. With the continuing advent of new technologies, our response to these changes must include…
https://www.sosdailynews.com/news.jspx?&articleid=A829B8A135344E1A4EAD5FF849E60EBF&sx=79

How to Spot and Stop Phone Tracking Apps
How much do you trust your cell phone? Is it respecting your privacy or running a phone tracking app that lets others know where you are and what you're doing? And your phone knows an awful lot about you.
https://www.scambusters.org/phonetracking.html

Developing a Threat Hunting & Research Team Maturity Model - Why a maturity model?
As I looked into how to approach this question I came across the idea of using a maturity model. According to the Institute of Internal Auditors (IIA), a maturity model describes process components that are believed to lead to better outputs and better outcomes. Maturity models are…
https://www.happythreathunting.com/single-post/2017/10/29/Threat-Hunting-Team-Maturity-Model

The ThreatHunting Project
Hunting for adversaries in your IT environment https://www.threathunting.net/

****

News & Views

The 10 vulnerabilities most commonly discovered by bug bounty hunters in 2020
HackerOne's list was topped by cross-site scripting, and found improper access control and SSRF vulnerabilities to be climbing in number and risk potential. https://www.techrepublic.com/article/the-10-vulnerabilities-most-commonly-discovered-by-bug-bounty-hunters-in-2020/?ftag=TREa988f1c&bhid=78480402&mid=13150964&cid=712423569

Report: 36B records have been exposed in 2020
An additional 8.3 billion records were exposed in the third quarter, bringing the annual total to 36 billion, the highest ever recorded, finds Risk Based Security. The figures include stolen data as well as cloud misconfigurations that theoretically exposed data. https://www.infosecurity-magazine.com/news/number-of-breached-records-hits-36/

Hackers have only just wet their whistle. Expect more ransomware and data breaches in 2021
The COVID-19 pandemic provided a huge opening for bad actors this year, thanks to remote work. Security experts expect more advanced cybersecurity threats in the coming year.
https://www.techrepublic.com/article/hackers-have-only-just-wet-their-whistle-expect-more-ransomware-and-data-breaches-in-2021/?ftag=TREa988f1c&bhid=78480402&mid=13150964&cid=712423569

BEC attacks increase in most industries, invoice and payment fraud rise by 155%
BEC attacks increased 15% quarter-over-quarter, driven by an explosion in invoice and payment fraud, Abnormal Security research reveals. https://www.helpnetsecurity.com/2020/11/03/bec-attacks-increase-quarter-over-quarter/

****

"Ctrl -F" for The Board

Cybersecurity Trends That Will Dominate the Market in 2020-21
The single biggest trend that is likely to see traction, also partly due to COVID-19, is an accelerated shift to cloud technologies and the associated security systems and services…
https://www.entrepreneur.com/article/358776

Questions
Contact FIPCO’s Ken Shaurette at 800/722-3498 ext. 251 or email FIPCO IT Services for more information.

"Make Security Part of You and Your Institution's DNA!"

Threat Intelligence Newsletter: November 19, 2020

FIPCO® IT Audit Round Table Discussions

If you would like to host an event, please contact: Becky Schowalter

Upcoming Threat Intelligence Peer Group Discussions
None available at the current time

****

Alerts & Warnings

Ragnar Locker Ransomware Gang Takes Out Facebook Ads in Key New Tactic
Ragnar Locker group has taken out public Facebook ads, threatening to release stolen data obtained from a ransomware attack against Italian liquor seller Campari. The attack occurred on November 3 and resulted in the theft of 2TB of sensitive data. Ragnar operators are demanding a $15 million ransom be paid… https://threatpost.com/ragnar-locker-ransomware-facebook-ads/161133/

Watch Out for This New Holiday Shopping Scam
The holiday shopping season is upon us. With the pandemic, many local in-person events, such as popup holiday markets or craft fairs, have moved online. Scammers are creating phony copycat events that charge for admission and steal your credit card information. https://www.bbb.org/article/news-releases/23394-bbb-scam-alert-beware-of-virtual-holiday-market-scams

Hot Topic: Ransomware on the Radar
Both the State banking regulators and the Treasury Department have issued recent advisories to financial institutions regarding the ransomware threat. Ransomware is defined as a form of malicious software ("malware") designed to block access to a computer system or data, often by encrypting data or programs, in order to extort ransom payments from victims in… https://complianceguru.com/2020/11/hot-topic-ransomware-on-the-radar/?utm_medium=email&utm_content=99804577&utm_source=hs_email Fillable PDF of the R-SAT: https://www.csbs.org/sites/default/files/2020-10/R-SAT_0.pdf

****

Hints & Tips plus Security Awareness

What You Need to Know About Ransomware
Ransomware is a type of malicious software, or malware, that blocks access to a system, device, or file until a ransom is paid. It is an illegal, moneymaking scheme that can be installed through deceptive links in an email message, instant message, or website. https://www.cisecurity.org/newsletter/what-you-need-to-know-about-ransomware/

Help veterans avoid scams
On Veterans Day, we celebrate our veterans — more than 18 million strong. We thank you for your service and sacrifice. It's also a good time to arm yourself with some tips to avoid fraud. We know that scammers follow the headlines, and their schemes evolve to take advantage of the things catching our attention now. Knowing what to look for helps all of us steer clear of a con artist.
https://www.consumer.ftc.gov/blog/2020/11/help-veterans-avoid-scams?utm_source=govdelivery

How to manage personal information for your Google account
In the name of security, make sure the information displayed on your Google account is limited. Jack Wallen shows you how. https://www.techrepublic.com/article/how-to-manage-your-personal-information-for-your-google-account/?ftag=TREa988f1c&bhid=78480402&mid=13159641&cid=712423569

Google patches two more Chrome zero-days
In its latest set of updates, Google released two patches for Chrome zero-day vulnerabilities being exploited in the wild. Over the past three weeks, Google has patched a total of five zero-day flaws in Chrome. The bugs affect Chrome version 86.0.4240.198, and it is recommended that the updates be implemented… https://www.zdnet.com/article/google-patches-two-more-chrome-zero-days/

Ransomware Self-Assessment Tool (R-SAT): What Banks and Credit Unions Need to Know
(warning – vendor presentation) Date: Tuesday, November 17th, 2020 Time: 2:00PM - 3:00PM CST
Over the past few years, ransomware attacks have hit numerous companies, including several community banks. These attacks result in costs as low as thousands of dollars and as expensive as sudden bank or credit union failure. https://go.tandem.app/2020-ransomware-guidance.html

****

News & Views

Why report fraud?
Scams come in many forms: texts, emails, letters, and lots of calls. Scammers plot schemes from tech support scams to fake check scams to try to knock us off balance just long enough to take advantage. They want to get our money and personal information, like account numbers and our Social Security number. How can we fight back? By sharing your story and reporting what happened to the FTC…
https://www.consumer.ftc.gov/blog/2020/11/why-report-fraud?utm_source=govdelivery

Settlement requires Zoom to better secure your personal information
Daily life has changed a lot since the pandemic started. Because face-to-face interactions aren't possible for so many of us, we've turned to videoconferencing for work meetings, school, catching up with our friends, even seeing the doctor. When we rely on technology in these new ways, we share a lot of sensitive personal information. We may not think about it, but companies know they have an obligation to protect that information. The FTC just announced a case against videoconferencing service Zoom about the security of consumers' information and videoconferences, also known as "Meetings."
https://www.consumer.ftc.gov/blog/2020/11/settlement-requires-zoom-better-secure-your-personal-information

Identity Fraud Gets A Makeover: Mitigating The Challenge Of Change
With the continuing advent of new technologies, our response to these changes must include hindering identity fraud now and in the future. Javelin, like other cybersecurity enterprises, believes the better consumers understand identity fraud, the more equipped they are to protect themselves.
https://www.sosdailynews.com/news.jspx?&articleid=A829B8A135344E1A4EAD5FF849E60EBF&sx=79

Build Your 2021 Cybersecurity Plan With This Free PPT Template
The end of the year is coming, and it's time for security decision-makers to make plans for 2021 and get management approval. Typically, this entails making a solid case regarding why current resources, while yielding significant value, need to be reallocated and enhanced. The Definitive 2021...
https://thehackernews.com/2019/11/cybersecurity-plan-template.html?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+TheHackersNews+%28The+Hackers+News+-+Cyber+Security+Blog%29&_m=3n.009a.2352.aa0ao086k1.1hce

Auto-Schedule USER Access Reviews - The Whys and Hows (warning vendor webinar)
Access Reviews are a key component of a secure enterprise. They are part of the NIST Cybersecurity Framework (PR.AC.4) and mandated by regulations like SOX, PCI-DSS, HITRUST and ISO 27001.
https://us02web.zoom.us/webinar/register/2616043350751/WN_6Q1tjnrATJi6GKaF0b4arw

****

"Ctrl -F" for The Board

Cybersecurity Trends That Will Dominate the Market in 2020-21
The single biggest trend that is likely to see traction, also partly due to COVID-19, is an accelerated shift to cloud technologies and the associated security systems and services…
https://www.entrepreneur.com/article/358776

Questions
Contact FIPCO's Ken Shaurette at 800/722-3498 ext. 251 or email FIPCO IT Services for more information.

"Make Security Part of You and Your Institution's DNA!"

Threat Intelligence Newsletter: November 24, 2020

FIPCO®
IT Audit
Round Table
Discussions

If you would like to host an event, please contact: Becky Schowalter

Upcoming Threat Intelligence Peer Group Discussions
None available at the current time

****

Alerts & Warnings

Microsoft Office targeted as malware activity soars
Malware activity jumped 128% in the third quarter of the year compared with the previous quarter, finds the latest "Threat Landscape Report" from Nuspire. Microsoft Office suite programs were the top targets of malware, which includes "phony legal documents and invoices containing macros that launch when the document is opened." https://www.techrepublic.com/article/how-to-combat-the-latest-and-most-aggressive-botnets-and-malware/

Scams Ramp Up Ahead of Black Friday Cybercriminal Craze
Cybercriminals are preparing for one of the largest hacking days in the US, Black Friday, and Cyber Monday. The shopping holidays attract scammers and hackers due to their nature in pushing a high volume of traffic through eCommerce sites in preparation for the holiday season. Due to the pandemic, shoppers… https://threatpost.com/scams-black-friday-cybercriminal-craze/161239/

Deep Fake Video & Ransomware Blackmail Threat
Crooks may soon be combining a pair of already wicked scams -- deep fake videos and ransomware -- into a single threat that will strike fear into the hearts and minds of victims. Deep fake videos are fabricated with software that makes an individual seem to be saying and doing things they've never done in reality. We've seen a lot of them in the recent election campaign. https://scambusters.org/deepfake2.html

Has your password been Compromised?
The HIBP list was updated 11/18, and now contains approximately 613 million password hashes. You can download the updated list from https://haveibeenpwned.com/Passwords

Inside the Cit0Day Breach Collection
If you've done that already and then find yourself in the Cit0day data then it's a non-event for two reasons: Being in one of the 23k breaches isolates your risk to that breach alone; because you've not reused the password anywhere else, exposure in that one place doesn't put you at risk anywhere else.
https://www.troyhunt.com/inside-the-cit0day-breach-collection/

****

Hints & Tips plus Security Awareness

How disinformation can become a cybersecurity problem
The term "disinformation" is often thrown around in politics, but it also affects businesses, writes Rodney Joffe of Neustar. Security teams help use "information security frameworks to give organizations methods to identify and counter disinformation-based attacks," Joffe notes.
https://www.securityinfowatch.com/security-executives/article/21162305/how-security-teams-can-combat-disinformation-attacks

eBook Security Orchestration for Dummies (SOAR) vendor sponsored
What is SOAR? https://app.hushly.com/runtime/content/nal2GrSBFtzPcYph

Customers wondering: high-interest banking app or highway robbery?
“It’s been almost a month and we still don’t have our money. We’re broke and putting groceries on credit cards...” That’s just one of many customer reviews posted about the mobile banking app offered by Beam Financial Inc. and founder Yinan Du – the defendants in a lawsuit filed today by the Federal Trade Commission. https://www.consumer.ftc.gov/blog/2020/11/customers-wondering-high-interest-banking-app-or-highway-robbery?utm_source=govdelivery

VMWare Vulnerability Updates
Updates address multiple security vulnerabilities…
https://www.vmware.com/security/advisories/VMSA-2020-0020.html
https://www.vmware.com/security/advisories/VMSA-2020-0023.html
https://www.vmware.com/security/advisories/VMSA-2020-0026.html

****

News & Views

Ransomware Self-Assessment Tool (R-SAT): What Banks and Credit Unions Need to Know
Vendor Webinar Recording: https://go.tandem.app/2020-rsat-webinar-on-demand-lp.html
Download the slide deck from the presentation: https://go.tandem.app/rs/246-QXH-030/images/TAN 20201117-RSAT Webinar RH.pdf

Microsoft gives Linux a security boost with these new attack detection tools
Microsoft has added new endpoint detection and response capabilities to Linux machines. The new features were made public through a preview feature. This will allow for Linux users to be better protected against threats and have the ability to take action quickly when one arises. Linux EDR will also help… https://www.techrepublic.com/article/microsoft-gives-linux-a-security-boost-with-these-new-attack-detection-tools/

Consumers wary of data breaches during holidays
Data breaches are a top concern for consumers, especially amid the increase in online shopping due to the coronavirus pandemic. A recent survey by Generali Global Assistance found that many consumers want retailers to offer identity protection services. https://www.retaildive.com/news/study-two-thirds-of-shoppers-concerned-about-holiday-data-breaches/589283/

****

"Ctrl -F" for The Board

Cybersecurity investments won't wane soon
Demand for cybersecurity providers shows no sign of slowing down in the current environment, writes financial industry executive Rahul Bhushan. Bhushan chronicles the many ways cybercriminals strike and points out that one report pegs the effect on the world economy at US$6 trillion by next year. https://www.investmentweek.co.uk/opinion/4023256/growth-cybersecurity-accelerated-covid-19-last

Ideas for closing the skills gap in cybersecurity
Creating a consistent career path for cybersecurity professionals and training those with educational backgrounds outside of technical fields are two ways that the industry can close the skills gap. "We have made this industry very complex because we haven't banded together — in public sector, private sector, academics — to come up with a cohesive picture of what is cybersecurity," says (ISC)2 Chief Operating Officer Wesley Simpson. https://securityboulevard.com/2019/11/reasons-behind-the-cybersecurity-skills-gap/

Questions
Contact FIPCO's Ken Shaurette at 800/722-3498 ext. 251 or email FIPCO IT Services for more information.

"Make Security Part of You and Your Institution's DNA!"

Threat Intelligence Newsletter: December 3, 2020

FIPCO®
IT Audit
Round Table
Discussions

If you would like to host an event, please contact: Becky Schowalter

Upcoming Threat Intelligence Peer Group Discussions
None available at the current time

****

Alerts & Warnings

VMware patches serious vulnerabilities in ESXi hypervisor, SD-WAN Orchestrator
VMware has patched critical vulnerabilities affecting its ESXi enterprise-class hypervisor and has released a security update for its SD-WAN Orchestrator, plugging a handful of serious security holes.
https://www.helpnetsecurity.com/2020/11/20/vulnerabilities-esxi-hypervisor/

Google Services Weaponized to Bypass Security in Phishing, BEC Campaigns
Cybercriminals are increasingly exploiting Google Services to conduct phishing and business email compromise (BEC) attacks, according to research firm Armorblox. Attackers are leveraging services provided by Google, such as Forms, Firebase, Docs, and more. A report from Armorblox shows how Google Forms and Docs are being used by malicious actors https://threatpost.com/google-services-weaponized-to-bypass-security-in-phishing-bec-campaigns/161467/

A Facebook Messenger Flaw Could Have Let Hackers Listen In
Facebook has been hosting a bug bounty program for roughly 10 years, which has provided the company with hundreds of bug reports before Facebook employees noticed any vulnerabilities. Recently, Facebook paid out $60,000 to an ethical hacker for reported a bug in Facebook Messenger that could have allowed an attacker… https://www.wired.com/story/facebook-messenger-bug-bounty/

Veterans and imposter scams
During the past four years, the FTC logged more than 378,000 reports from veterans — and nearly 161,000 were fraud-related. More than 24,000 of those reported a loss (with total losses of $205 million). Veterans had a median loss of $755, compared to active duty servicemembers who reported a median loss of $500 over the same period. https://www.consumer.ftc.gov/blog/2020/11/veterans-and-imposter-scams-0?utm_source=govdelivery

The New Normal? Stealing Your Identity One Piece At A Time
Little by little, cybercriminals are stealing our identities. Although identity theft is nothing new, a change in the way cybercriminals are improving identity fraud is. Compiling files on consumers is now trending with hackers as more pieces of our identities become available. The coronavirus pandemic is providing an avalanche of PII (personally identifiable information) and increased opportunities for identity theft. Hackers love taking advantage of a crisis situation and the pandemic translates to larger and more devastating opportunities for identity abuse.
https://www.sosdailynews.com/news.jspx?&articleid=A0464D2211F65FE8391D0BDE42478720&sx=79

5G Phone Confusion Opens Scam Floodgates
Wherever there's confusion, misunderstanding, conspiracy theories and fake news, there's bound to be a scam. So it is with the latest debate about the safety of 5G, the new cellular phone technology that's current being rolled out across the US. https://scambusters.org/5g.html

****

Hints & Tips plus Security Awareness

5 key areas to cover in a cyberattack response plan
Because cyberattacks often occur at off-hours, enterprises should determine how "key business leaders, stakeholders and individuals with required skills will be contacted outside of their normal working hours," writes John Pironti, president of IP Architects. Pironti lays out that and four other key areas a response plan should cover. https://www.isaca.org/resources/news-and-trends/newsletters/atisaca/2020/volume-24/five-key-considerations-for-developing-a-cybersecurity-emergency-action-plan

This holiday season, help friends and family avoid a scam
When you talk with friends and family over the holidays, you may hear about new puppies, old sports rivalries, and dreams of the next vacation. As you join the conversation, why not share some ideas from the FTC's Pass it On campaign to protect the people you care about from scams?
https://www.consumer.ftc.gov/blog/2020/11/holiday-season-help-friends-and-family-avoid-scam?utm_source=govdelivery

VMSA-2020-0026.1 - VMSA-2020-0023.3 VMware ESXi multiple security vulnerabilities
Updated security advisory to add VMware Cloud Foundation 3.x and 4.x versions in the response matrix of sections 3(a) and 3(b).
Please see the updated advisory here:
https://www.vmware.com/security/advisories/VMSA-2020-0026.html
Please see the updated advisory here:
https://www.vmware.com/security/advisories/VMSA-2020-0023.html

****

News & Views

American Bank Systems hit by ransomware attack, full 53 GB data dump leaked
American Bank Systems (ABS), a service provider to US banks and financial institutions has suffered a ransomware attack with some of its clients' data leaked. https://securityreport.com/american-bank-systems-hit-by-ransomware-attack-full-53-gb-data-dump-leaked/

Holiday shopping season 2020
The holiday season is upon us and retailers are already preparing for what they hope will be a successful shopping season. Because of COVID-19, it's likely that we'll be going online to look for those perfect gifts. With so many deals around and what seem like eternal "Black Friday" sales, it's important to keep some online shopping tips in mind. https://www.consumer.ftc.gov/blog/2020/11/holiday-shopping-season-2020?utm_source=govdelivery

XDR: Unifying incident detection, response and remediation
According to IBM's Cost of a Data Breach Report 2020, the average time it took a company in 2019 to identify and contain a breach was 279 days. It was 266 days in 2018… It's clear that time is not on CISOs' side and they need to act fast. FIPCO has partnered with one of the best solutions available, contact us to learn more and get a demonstration, it's the coming way to mature your information/cyber security program. https://www.helpnetsecurity.com/2020/11/24/xdr-extended-detection-and-response/

****

"Ctrl -F" for The Board

The 8 most common cybersecurity weaknesses to watch for in small businesses
A single weakness or vulnerability can compromise the integrity of an entire enterprise, yet many executives are profoundly unaware of the security shortcomings that exist within their organization. Fortunately, with a proactive approach, most exploitable openings can be closed.
https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2020/the-8-most-common-cybersecurity-weaknesses-to-watch-for-in-small-businesses

Questions
Contact FIPCO's Ken Shaurette at 800/722-3498 ext. 251 or email FIPCO IT Services for more information.

"Make Security Part of You and Your Institution's DNA!"

Threat Intelligence Newsletter: December 8, 2020

FIPCO®
IT Audit
Round Table
Discussions

If you would like to host an event, please contact: Becky Schowalter

Upcoming Threat Intelligence Peer Group Discussions
None available at the current time

****

Alerts & Warnings

Attacks are rising in all vectors and types
DDoS, web application, bot, and other attacks have surged exponentially compared to the first half of 2019, according to CDNetworks. https://www.helpnetsecurity.com/2020/11/27/attacks-are-rising-in-all-vectors-and-types/

Don't Click on Suspicious Zoom Meeting Invites
Thanks to the global pandemic keeping people at home, the popular video conferencing platform Zoom has seen usage grow exponentially in 2020. Naturally, this has attracted the attention of hackers and scammers. With a huge user base to target, con artists are using old tricks in new scams to try to steal your information. How the Scam Works: Out of the blue, you receive an email, text, or social media message that includes Zoom's logo and a message saying something like, "Your Zoom account has been suspended. Click here to reactivate." or "You missed a meeting, click here to see the details and reschedule." You might even receive a message welcoming you to the platform and requesting you click on a link to activate your account. Scammers registered more than 2,449 Zoom-related domains from late April to early May this year alone. Con artists use these domain names, which include the word "Zoom," to send you an email that looks like it's coming from the official video conferencing service.
More information: https://dzone.com/articles/be-aware-of-zoom-phishing-scams?utm_source=newsletter&utm_medium=email&utm_content=egistered%20more%20than%202%2C449%20Zoom-related%20domains&utm_campaign=scam-alert

Magecart Attack Convincingly Hijacks PayPal Transactions at Checkout
A new credit card skimmer is utilizing postMessage to create convincing PayPal transactions that are illegitimate and steal payment data. The new credit card skimming campaign comes during the holiday season when more customers are using e-commerce sites and shopping online. The malicious process hijacks PayPal transactions during checkout, causing… https://threatpost.com/magecart-hijacks-paypal-transactions/161697/

FBI Issues Tips to Avoid Common Scams
The FBI last week warned consumers of common online and social media shopping scams used by criminals during the holiday season. These scams include too-good-to-be-true deals via phishing e-mails, advertisements or posts that appear to offer vouchers or gift cards but are designed to steal personal and/or credit card information. Other frauds outlined by the FBI include reshipping scams, gift card scams and more. The press release, describes tips to avoid being victimized by these fraud and how to report them. https://www.fbi.gov/contact-us/field-offices/washingtondc/news/press-releases/ho-ho-ho-holiday-scams?utm_campaign=RiskCyber-20201201&utm_medium=email&utm_source=Eloqua&utm_content=%5B989163%5D-%2Fcontact-us%2Ffield-offices%2Fwashingtondc%2Fnews%2Fpress-releases%2Fho-ho-ho-holiday-scams

Service email accounts can be an overlooked risk
With credential-stuffing attacks on the rise, service email accounts — those that aren't handled by humans — shouldn't be overlooked, writes Kevin Sheu of cloud security provider Bitglass. Trying to prevent "every instance of credential abuse is foundationally difficult" because "the attacker needs to be right only once," Sheu notes. https://securitybrief.eu/story/how-a-vantage-point-sees-threats-before-they-impact

The Internet's Most Notorious Botnet Has an Alarming New Trick
Over the past few months, the cybersecurity industry's most notorious tool, TrickBot, has also become its most potent enemy. Despite takedown attempts by Microsoft and the US Cyber Command, the tool has been developed even further, with its operators implementing a new technique that infects machines beyond operating systems and… https://www.wired.com/story/trickbot-botnet-uefi-firmware/

Fake calls from Apple and Amazon support: What you need to know
I've personally had the Apple calls, over 15 one Sunday about every 5 minutes from a different number. Scammers are calling people and using the names of two companies everyone knows, Apple and Amazon, to rip people off. Here's what you need to know about these calls.
https://www.consumer.ftc.gov/blog/2020/12/fake-calls-apple-and-amazon-support-what-you-need-know?utm_source=govdelivery

****

Hints & Tips plus Security Awareness

On the first day of consumer protection…
Welcome to the FTC's 12 Days of Consumer Protection, a holiday series to help you save money and avoid scams. Each day, we'll cover a new topic — from shopping online and bogus shipping notifications to temporary job scams and fake charities. We'll give you practical information you can use every day and share with your family, friends, and community so they can be safe too.
https://www.consumer.ftc.gov/blog/2020/12/first-day-consumer-protection?utm_source=govdelivery

Debt collectors: Mind the "No Parking" signs on credit reports
There's a virtual "NO PARKING" sign planted smack in the middle of your credit report. It means that debt collectors can't report your debt — or your supposed debt — to credit reporting agencies without first trying to check with you. https://www.consumer.ftc.gov/blog/2020/11/debt-collectors-mind-no-parking-signs-credit-reports?utm_source=govdelivery

3 steps to embracing the NIST privacy framework
Enterprises addressing data privacy should build on the National Institute of Standards and Technology framework, writes Zachary Curley of AT&T Cyber Security Solutions. Curley outlines the NIST framework, as well as ready-set-go steps for implementation. https://www.nextgov.com/ideas/2020/11/data-privacy-and-data-governance-will-be-top-business-priorities-2021/170245/

How to handle the proliferation of privileged access
Restricting privileged access can be a problem even under the best circumstances, so monitoring for suspicious activity is a must, writes Michael Crouse of Forcepoint. "By gathering a baseline of users' normal activity, agencies can monitor behavior in real-time — tracking everything from keystrokes to psychological factors," Crouse points out. https://gcn.com/articles/2020/11/23/privileged-user-access.aspx

5 ways to make sure printers aren't a security risk
The advanced characteristics of this generation's printers create potential access points for hackers, says Shivaun Albright, HP's chief technologist for printing security. Albright lays out five ways enterprises can make their printers more secure, including installing the latest firmware upgrades.
https://www.darkreading.com/endpoint/printers-cybersecurity-threats-too-often-ignored/a/d-id/1339362

Consumers vastly misjudge the vulnerability of their home networks
Internet users in the United States vastly underestimate how often their home networks are targeted by cyber threats. That's one of the key findings of a new Comcast report.
https://www.helpnetsecurity.com/2020/12/02/consumers-misjudge-vulnerability-home-networks/

How Attackers Use BloodHound To Get Active Directory Domain Admin Access
Hackers can use tools like BloodHound to visualize the shortest path to owning your domain. But that doesn't mean you can't use it to find and protect your organization's weak spots. Here's how.
https://mcpmag.com/articles/2019/11/13/bloodhound-active-directory-domain-admin.aspx

****

News & Views

FBI warns of email forwarding rules being abused in recent hacks
The US FBI released a Private Industry Notification (PIN) last week claiming that cybercriminals are exploiting email forwarding rules to maintain anonymity and hide their presence on hacked email accounts. The PIN was made public yesterday and contains valuable information about how the technique is being actively used in recent… https://www.zdnet.com/article/fbi-warns-of-email-forwarding-rules-being-abused-in-recent-hacks/

IBM Uncovers Global Phishing Campaign Targeting the COVID-19 Vaccine Cold Chain
At the onset of the COVID-19 pandemic, IBM Security X-Force created a threat intelligence task force dedicated to tracking down COVID-19 cyber threats against organizations that…
https://securityintelligence.com/posts/ibm-uncovers-global-phishing-covid-19-vaccine-cold-chain/

Hackers Evade MFA, Increase Business Email Compromise Attacks
The ability to verify if the person logging-into a data system is whom they claim to be has been a challenge for enterprise. Hackers who use password spraying and other tricks are able to gain access to email and other accounts, and that's a big problem for enterprise security. The FBI reports an estimated $1.77 billion in losses last year due to business email compromise (BEC). That's almost half the entire amount of financial losses due to all cybercrime in the U.S.
https://www.sosdailynews.com/news.jspx?&articleid=2E34E30C983DEE1CBDDC9409F0DF8125&sx=79

****

"Ctrl -F" for The Board

How a deepfake video could cause corporate chaos
Randori, a cybersecurity company, has released its list of top threats for the new year, with a surprising pick at the top: deepfake videos. "Imagine an attacker on a video system, silently recording a board meeting, then manipulating that private information to contain false and damning information that if leaked, would create business chaos," says Chief Technical Officer David Wolpoff.
https://www.eweek.com/security/why-data-security-will-face-even-harsher-hackers-in-2021

Questions
Contact FIPCO's Ken Shaurette at 800/722-3498 ext. 251 or email FIPCO IT Services for more information.

"Make Security Part of You and Your Institution's DNA!"

Threat Intelligence Newsletter: December 15, 2020

FIPCO®
IT Audit
Round Table
Discussions

If you would like to host an event, please contact: Becky Schowalter

Upcoming Threat Intelligence Peer Group Discussions
None available at the current time

NIST Identifying and Protecting Assets Against Ransomware - Other Destructive Events
Download the Final Practice Guide, The NCCoE has released the final NIST Cybersecurity Practice Guide SP 1800-25, Identifying and Protecting Assets Against Ransomware and Other Destructive Events.
https://www.nccoe.nist.gov/projects/building-blocks/data-integrity/identify-protect

****

Alerts & Warnings

Slow Browser? It May Have Been Hijacked By Malware
Before calling your internet provider to complain about a slow browser think about this: It's no secret malware loves to hide in all kinds of things like adware, spyware, scareware, and fake browser updates. Finding your browser is not only slow, but also acting strangely is a sign something isn't quite right. If after going through the internet provider's standard toolbox for troubleshooting doesn't help, it's time to think about malware…
https://www.sosdailynews.com/news.jspx?&articleid=0077236D4FEF9D451A78E05A13E58B15&sx=79

Ransomware groups outsource to call centers
Ransomware groups appear to be using an outsourced call center to contact victims suspected of restoring data from backup servers to avoid paying ransom, says Coveware CEO Bill Siegel. The calls, from people speaking heavily accented English, follow a script or template and say that antivirus software and third-party IT specialists will not prevent attacks. https://www.zdnet.com/article/ransomware-gangs-are-now-cold-calling-victims-if-they-restore-from-backups-without-paying/

Fraudulent charge? Might be the set up for a scam

Want some advice about scams? Stay calm. Con artists use that feeling of alarm to trick victims to acting before they can think. BBB Scam Tracker is seeing reports of a con that claims that your Amazon, PayPal, or other account has been compromised. Scammers hope you'll panic and fall for their scheme.
https://www.bbb.org/article/scams/23214-bbb-scam-alert-phony-amazon-callers-phishing

'Fingerprint-Jacking' Attack Technique Manipulates Android UI

Researchers have been conducting studies into the technique of fingerprint-jacking, in which threat actors overcome fingerprint scanning technologies for malicious intent. fingerprint-jacking is a user-interface based attack that steals users' biometric data when stored in Android apps. Many different smartphone models consist of fingerprint scanners that authorize access to enable…
https://www.darkreading.com/threat-intelligence/fingerprint-jacking-attack-technique-manipulates-android-ui-/d/d-id/1339684

****

Hints & Tips plus Security Awareness

How to avoid holiday identity theft

If you're holiday shopping from home this year, you're not alone. That's why it's smart to be extra mindful of online scammers and hackers. From keeping your information private to using credit card security features, here are our top tips for protecting your identity this holiday season and beyond. https://www.experian.com/blogs/ask-experian/how-to-protect-your-identity-during-the-holiday-season/?pc=crm_exp_0&cc=emm_a_m_act_8990120201206_FTT_20201206_x_102

Holiday Scams – Inside the FBI Podcast

Shop Safely and Smartly Online… https://www.fbi.gov/news/podcasts/inside-the-fbi-holiday-scams-120120. Check out other podcasts from the FBI at: https://www.fbi.gov/news/podcasts

Do Yourself a Favor: Be Crime Smart.

Getting educated and taking a few basic steps may well keep you from becoming a victim of crime and fraud—and save you a great deal of time and trouble. You can also help us protect your families and communities by reporting suspicious activities and helping find wanted fugitives and missing kids.
https://www.fbi.gov/scams-and-safety

****

News & Views

Hackers hide web skimmer inside a website's CSS files

Cybercrime groups have been experimenting with hiding web skimmers inside various locations of an online store, and have recently been implanting the malicious code inside the CSS files of target sites. The web skimmers are also known… https://www.zdnet.com/article/hackers-hide-web-skimmer-inside-a-websites-css-files/

National Cyber Security Centre Cyber Awareness Campaign
The United Kingdom (UK) National Cyber Security Centre (NCSC) has launched a new cyber security campaign encouraging the public to adopt six behaviors to stay safe online.
The six Cyber Aware behaviors recommended by the NSCS are:
https://www.ncsc.gov.uk/cyberaware/home

New ACSC Cybersecurity Campaign Begins by Focusing on Ransomware Threats
The Australian Cyber Security Centre (ACSC) has launched a new cyber security campaign encouraging all Australians to protect themselves against online threats. The initial focus of the campaign is ransomware threats, and the ACSC provides easy-to-follow security advice at cyber.gov.au to help Australians act now and stay secure. https://us-cert.cisa.gov/ncas/current-activity/2020/12/09/new-acsc-cybersecurity-campaign-begins-focusing-ransomware-threats

The 3 underlying technologies of zero trust
The best way to start implementing zero trust security is "to assess where risk is the highest…
https://www.isaca.org/resources/news-and-trends/industry-news/2020/harnessing-zero-trust-security

****

"Ctrl -F" for The Board

Consider the timing of cybersecurity training
Cybersecurity training should be offered "at an employee's exact moment of need: when they display behavior that puts the company in jeopardy and don't even realize it," writes CEO Stephen Burke of Cyber Risk Aware. Burke outlines eight training and education principles to change the culture…
https://www.scmagazine.com/perspectives/eight-ways-to-instill-a-cybersecurity-awareness-culture/

Questions
Contact FIPCO's Ken Shaurette at 800/722-3498 ext. 251 or email FIPCO IT Services for more information.

"Make Security Part of You and Your Institution's DNA!"

Threat Intelligence Newsletter: December 22, 2020

FIPCO®
IT Audit
Round Table
Discussions

If you would like to host an event, please contact: Becky Schowalter

Upcoming Threat Intelligence Peer Group Discussions
None currently available

FREE Live Active Shooter Preparedness Webinar hosted by CISA on January 7th, 2021 at 9am CST
Wisconsin Public and Private Sector Partners, I am pleased to announce that CISA will be hosting a 2 hour Active Shooter Preparedness Webinar specifically for our Wisconsin-based partners. This is an event that we typically host in-person, but due to the continued concerns related to COVID-19, we have opted to provide you this valuable training opportunity and associated resources via a live webinar which will be conducted on January, 7th at 9am (CST). Details related to the Active Shooter Preparedness Webinar and how to register are included in the attached flyer. Should you have any questions please feel free to reach out to myself and Mitch Paine, our Region V Training and Exercise Coordinator, at james.paine@hq.dhs.gov. Please feel free to share this information within your respective organizations and membership groups. Thanks and have a happy and safe holidays! The link to register for the event is: https://www.govevents.com/details/43216/cisa-active-shooter-preparedness-webinar--cisa-region-v-wi/

InfraGard/FBI Quarterly Threat Briefing
Cyber Threats to Third Party Service Providers, Its Evolution and What We Can Do About It, Wednesday, 13 January 2021, 9:00am – 11:30am PST
Registration Link: https://attendee.gotowebinar.com/register/3079662112210610700

SolarWinds and FireEye breaches: A guide for the Perplexed
Cynet Senior Analysts wrote an insightful report: Solarigate – The guide for the Perplexed, to help you better understand how this attack unfolded and where it stands today, including:

- How the attack unfolded and was ultimately discovered
- What is the impact of this attack
- What can you do to protect endpoints from this threat

Download the report here: https://go.cynet.com/hubfs/Cynet-report-SolariGate-Guide-for-the-Perplexed.pdf?utm_medium=email&_hsmi=103394529&_hsenc=p2ANqtz-8D2gkLSu3wpAGlqN6WI4P2V83dwM66Z3GiWapQVFaZ9D_bzcKHOtT6_wBziQFFTDxGBAZEB-qXCyBa3rdQMbgooJEIAw&utm_content=103394529&utm_source=hs_email

****

Alerts & Warnings

Grandma got a scam call from a reindeer
When it comes to unwanted calls, there are a few universal truths. First, you can't trust caller ID. Second, nobody likes a robocall. And third, it's all about call blocking. If you watch The Mandalorian, here's where you say, "This is the Way." (If you don't watch it, this just means: call blocking…it's good.)
https://www.consumer.ftc.gov/blog/2020/12/grandma-got-scam-call-reindeer?utm_source=govdelivery

Ad-injecting malware hijacks Chrome, Edge, Firefox
When searching for things online, has a greater number of ads than usual been popping up at the top of your search results? If it has, and you're using Microsoft Edge, Google Chrome, Yandex Browser, or Mozilla Firefox, you might have fallen prey to the ad-injecting Adrozek malware.
https://www.helpnetsecurity.com/2020/12/11/ad-injecting-malware/

Vendors Respond to Method for Disabling Their Antivirus Products via Safe Mode:
Microsoft AV, Bitdefender, Kaspersky, and several vendors have issued a response after a researcher showed that their antivirus products can be disabled remotely using a method that involves the Windows Safe Mode. https://www.securityweek.com/vendors-respond-method-disabling-their-antivirus-products-safe-mode

Santa doesn't need your Social Security number
This year, during the pandemic, your holidays might be moving a bit online. On the 10th day of Consumer Protection, maybe you're planning to send e-cards to family and friends.
https://www.consumer.ftc.gov/blog/2020/12/santa-doesnt-need-your-social-security-number?utm_source=govdelivery

Extraordinary Vulnerabilities Discovered in TCL Android TVs, Now World's 3rd Largest TV Manufacturer.
The following piece is the culmination of a three-month long investigation into Smart TVs running Android. Having lived through this research experience, I can wholeheartedly say that there were multiple moments that I, and another security researcher that I met along the way, couldn't believe what was happening. On multiple occasions I found myself feeling as though, "you couldn't even make this up…"
https://sick.codes/extraordinary-vulnerabilities-discovered-in-tcl-android-tvs-now-worlds-3rd-largest-tv-manufacturer/

SolarWinds Sunburst Backdoor, Part II: DGA & The List of Victims
As described in the first part of our analysis, the DGA (Domain Generation Algorithm) of the Sunburst backdoor produces a domain name that may look like: https://blog.prevasio.com/2020/12/sunburst-backdoor-part-ii-dga-list-of.html

****

Hints & Tips plus Security Awareness

Joining forces to stop income scams
Today, the FTC joined forces with numerous federal, state, and local government partners in Operation Income Illusion, an effort to fight income scams and help people recognize and avoid them.
https://www.consumer.ftc.gov/blog/2020/12/joining-forces-stop-income-scams?utm_source=govdelivery

Ransomware Fundamentals
Ransomware has claimed many major organizations throughout the 21st century. Many large enterprises underestimate hackers, believing that an IT team can defend against any form of cyber attack. However, ransomware attacks often target nontechnical employees, implementing strategic attacks that…
https://blog.nxtsoft.com/ransomwarefundamentals?utm_campaign=Data%20Security%20Newsletter&utm_medium=email&_hsmi=102981541&_hsenc=p2ANqtz8z0t1AlEmu6E8VCiA9xz209NZWyyibURWSqigYlP_85jFmqYYLBXc_q6zFm8N_Ct5O5TnxJ6k0ElspHWooSXT5lJ5HxA&utm_content=102981541&utm_source=hs_email

How to Protect Your Kids Online with Parental Controls
Are you wondering about -- or maybe even desperate -- to restrict your children's online and viewing activities through parental controls? https://www.scambusters.org/parentalcontrol.html

****

News & Views

Three signs your SOC is ready for XDR
Over the past year, there's been a movement growing in the industry towards Extended Detection and Response, or XDR, https://www.fipco.com/solutions/it-audit-security/autonomous-endpoint-protection. While a few offerings represent broad portfolio consolidation and convergence towards packaging multiple solutions into one, there's an undeniable demand for a more outcome-oriented approach to threat detection and response. Check out Cynet360
https://www.helpnetsecurity.com/2020/12/14/soc-xdr-ready/

Employee monitoring should be a collaborative process
Software to monitor work-at-home employees should be automated "to be extremely dynamic without requiring personnel to comb through employee data," writes Isaac Kohen, vice president of research and development at Teramind. Kohen suggests making the monitoring process collaborative because when explained, "employees are surprisingly open to monitoring protocols."
https://www.isaca.org/resources/news-and-trends/industry-news/2020/why-employee-privacy-matters-more-than-ever

Who's affected by income scams?
The FTC and its law enforcement partners announced actions against several income scams that conned people out of hundreds of millions of dollars by falsely telling them…
https://www.consumer.ftc.gov/blog/2020/12/whos-affected-income-scams?utm_source=govdelivery

'MountLocker' Ransomware Adds to Affiliate Extortion Racket
BlackBerry researchers are tracking a relatively new ransomware variant called MountLocker and the operators behind it, who are using affiliate cybercriminal gangs to help spread the malware, exfiltrate data and extort victims, sometimes for millions of dollars.
https://www.bankinfosecurity.com/mountlocker-ransomware-adds-to-affiliate-extortion-racket-a-15583

SolarWinds Incident Response: 4 Essential Security Alerts
Numerous security alerts have been issued regarding the supply chain attack targeting software vendor SolarWinds and, by extension, its customers.
https://www.theguardian.com/world/2020/dec/14/solarwinds-breach-orion-hacked-cyber-espionage

Ransomware becoming more about theft than about freezing data
Cybercriminals have adjusted their approach to ransomware by exfiltrating confidential data and threatening to release it to the public, Acronis reports. The security company's report finds that "more than 1,000 companies globally had their data leaked ... in 2020, a trend that is expected to accelerate in the coming year, overtaking encryption as the criminals' primary tactic."
https://www.itwire.com/security/acronis-predicts-2021-will-be-the-%E2%80%98year-of-extortion%E2%80%99.html

Exploring the Push for Zero Trust
Increasing pressure on many organizations to meet compliance requirements has resulted in a push to adopt a zero trust approach. But for implementation to be successful, enterprises must obtain a thorough understanding of the nuances of the framework.
https://www.isaca.org/resources/news-and-trends/isaca-podcast-library/exploring-the-push-for-zero-trust

Microsoft says it found malicious software in its systems
Yesterday, Microsoft announced that it had also been targeted by the SolarWinds espionage campaign after uncovering malware within its systems. The tech giant uses the networking management software Orion found to be the source of the attack impacting a half dozen federal agencies so far. Microsoft's own products may have…https://www.channelnewsasia.com/news/business/microsoft-says-it-found-malicious-software-in-its-systems-13797692

****

"Ctrl -F" for The Board

4 ways CISOs can win the "arms race" against attackers
With cyberattackers using tools driven by artificial intelligence, "using AI to defend against these attacks is no longer optional," writes Ilan Rubin. Rubin outlines four ways chief information security officers can win the "arms race," including by choosing solutions that are user-friendly. https://securitybrief.eu/story/how-cisos-can-come-out-on-top-of-the-cyber-arms-race

Fraud & identity intelligence: How to reduce fraud with a comprehensive view of identity
Identity fraud continues to be a significant challenge for today's financial services and lending firms and fraud attempts are spiking every year. Our recent 2020 True Cost of Fraud™ Study found that financial services firms saw a 42% increase in successful monthly fraud attempts while lending firms saw an increase of 38%. What's become painfully clear is that…http://pages.marketing.americanbanker.com/how-to-reduce-fraud-with-a-comprehensive-view-of-identity.html?source=LexisNexis

Questions
Contact FIPCO's Ken Shaurette at 800/722-3498 ext. 251 or email FIPCO IT Services for more information.

"Make Security Part of You and Your Institution's DNA!"

Threat Intelligence Newsletter: January 12, 2021

FIPCO®
IT Audit
Round Table
Discussions

If you would like to host an event, please contact: Becky Schowalter

Upcoming Threat Intelligence Peer Group Discussions
None available at the current time

****

Alerts & Warnings

Email Scammers Get Clever With Outlook Phishing Trick
Email scams are a dime a dozen. Ever since we started using digital messaging, scammers have been on our tails, using email to try to steal information and trick us into sending money, or even into spreading fake news. https://www.scambusters.org/emailscam.html

Beware: PayPal phishing texts state your account is 'limited'
A PayPal text message phishing campaign is underway that attempts to steal your account credentials and other sensiti...https://www.bleepingcomputer.com/news/security/beware-paypal-phishing-texts-state-your-account-is-limited/

New alleged MuddyWater attack downloads a PowerShell script from GitHub
Security expert spotted a new piece of malware that leverages weaponized Word documents to download a PowerShell scri...https://securityaffairs.co/wordpress/112972/hacking/muddywater-attack-github-imgur.html

Malware: How it Sneaks In and What it Does to Your PC or Mobile
Malware. The word strikes fear into the hearts of computer and mobile users these days. And with good reason. https://scambusters.org/malware1.html

Google discloses Windows zero-day exploited in the wild
Windows zero-day (not yet patched) is used as part of an exploit chain that also includes a Chrome zero-day (already patched). https://www.zdnet.com/article/google-discloses-windows-zero-day-exploited-in-the-wild/

****

Hints & Tips plus Security Awareness

A closer look at fileless malware, beyond the network
Cybersecurity is an arms race, with defensive tools and training pushing threat actors to adopt even more sophisticated and evasive intrusion techniques as they attempt to gain a foothold in victim networks. Most new modern endpoint protection (EPP) services are…
https://www.helpnetsecurity.com/2021/01/04/fileless-malware/

The Cost of Breach
Taking place January 13 at 1:00 p.m. ET, this webinar will look at the complexity of analyzing the cost of a cybersecurity breach. https://go.dowjones.com/cyber-webinar-12?utm_campaign=Approved_PROMO_20201222_WSJ%20Industry%20Events_Cyber_0113%20webinar_Speaker%20Announcement_HTML_Email&utm_medium=email&utm_source=Eloqua

Three Rules for Dodging Fake Storage Cards and Memory Sticks
The cost of computer and mobile storage devices is falling rapidly -- but not so fast that you can pick up a really big one for a really low price. That part of the market is the domain of scammers.
https://scambusters.org/storage.html

Not All WiFi Is Good WiFi
WiFi has become a part of pretty much any device that has network access. From mobile phones and tablets to desktop computers and laptops. The time to plug in an Ethernet cable has long since passed. And while just a few years ago it was considered high risk to allow WiFi access in corporate offices, now it is just a standard part of doing business. Unfortunately, when….
https://www.sosdailynews.com/news.jspx?&articleid=8EFD67A6C24B7B92BE059D1738149976&sx=79

How to make sure printer security isn't a weak link
Properly administered access controls can keep printers from becoming security liabilities, writes Brien Posey of Relevant Technologies. Posey also suggests putting printers on isolated network segments because that "makes it a lot tougher for a hacker to steal data en route to the printer."
https://www.itprotoday.com/data-security-and-encryption/why-it-may-be-time-revisit-security-printers

Exploring the Push for Zero Trust – ISACA Podcast
Increasing pressure on many organizations to meet compliance requirements has resulted in a push to adopt a zero trust approach. But for implementation to be successful,…
https://www.isaca.org/resources/news-and-trends/isaca-podcast-library/exploring-the-push-for-zero-trust

****

News & Views

Here We Go Again – A New Emotet Wave
Over the last couple of days, Cynet CyOps and Research teams have been engaged in another wave of the infamous Emotet trojan. This time, with some tweaks and changes under its belt, Emotet keeps reminding us that it is here to stay. https://www.cynet.com/attack-techniques-hands-on/here-we-go-again-a-new-emotet-wave-observed-by-cynet/

When a Sunburst Turns Supernova – A Recent Solarigate Development
In addition to the recent discoveries following the SolarWinds supply chain attack and the newly discovered SUNBURST backdoor, the investigation of the attack has led to the discovery of an additional malware that also uses the SolarWinds Orion product as its delivery method but is unlikely to be related to the preceding unfolding event and used by a different threat actor. https://www.cynet.com/attack-techniques-hands-on/when-a-sunburst-turns-supernova-a-recent-solarigate-development/

Three million users installed 28 malicious Chrome or Edge extensions
Extensions could redirect users to ads, phishing sites, collect user data, or download malware on infected systems. https://www.zdnet.com/article/three-million-users-installed-28-malicious-chrome-or-edge-extensions/

One Million Compromised Accounts Found at Top Gaming Firms
Security researchers have discovered roughly 500,000 breached employee credentials related to popular video game companies. Researchers also uncovered a million compromised internal accounts for sale on the dark web. Threat intelligence firm Kela moved to investigate the top 25 publicly listed companies in the sector, soon finding a thriving market… https://www.infosecurity-magazine.com/news/one-million-compromised-accounts/

Time to invest in privileged access management tools?
As remote work continues into the new year, more enterprises will need privileged access management tools "to protect key application and server stacks from abuse, misconfiguration, change management violations and threat actors," writes Simon Persin of Turnkey Consulting. Persin notes that "IT security will play an increasingly visible role in business development in the next 12 months and beyond."
https://www.computerweekly.com/opinion/Security-Think-Tank-Cyber-effectiveness-efficiency-key-in-2021

An argument for outsourcing security functions
Spending on managed security service providers is expected to surpass $46 billion by 2025, writes Mary Pratt. Pratt outlines the pros and cons, noting that "each organization must reach its own conclusions about what it should outsource and keep in-house." https://searchsecurity.techtarget.com/tip/15-benefits-of-outsourcing-your-cybersecurity-operations

****

"Ctrl -F" for The Board

A hacker's predictions on enterprise malware risk
2020 has ended with a stunning display of nation-state cyber capabilities. The Kremlin's SVR shocked the cybersecurity industry and U.S. government with its intrusions into FireEye and the U.S. Office of the Treasury by way of SolarWinds, revealing only traces of its long-term, sophisticated campaigns. Has your endpoint security been improved beyond traditional AV and signatures?
https://www.helpnetsecurity.com/2021/01/07/hackers-predictions-enterprise-malware-risk/

Questions
Contact FIPCO's Ken Shaurette at 800/722-3498 ext. 251 or email FIPCO IT Services for more information.

"Make Security Part of You and Your Institution's DNA!"

Threat Intelligence Newsletter: January 18, 2021

FIPCO®
IT Audit
Round Table
Discussions

If you would like to host an event, please contact: Amy Petersen

Upcoming Threat Intelligence Peer Group Discussions
None available at the current time

****

Alerts & Warnings

Experts Sound Alarm On New Android Malware Sold On Hacking Forums
Cybersecurity researchers have exposed the operations of an Android malware vendor who teamed up with a second threat actor to market and sell a remote access Trojan (RAT) capable of device takeover and exfiltration of photos, locations, contacts, and messages from popular apps such as Facebook...
https://thehackernews.com/2021/01/experts-sound-alarm-on-new-android.html?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+TheHackersNews+%28The+Hackers+News+-+Cyber+Security+Blog%29&_m=3n.009a.2396.aa0ao086k1.1ifj

FBI Issues Egregor Ransomware Advisory
The FBI has released a Private Industry Notification (TLP: white) warning of an increased threat to businesses from the Egregor ransomware operators. The notification describes Egregor's ransomware-as-a-service operation model and suggests mitigations organizations can apply…
https://www.govinfosecurity.com/fbi-issues-alert-on-growing-egregor-ransomware-threat-a-15733

Trump Sex Scandal Video Is a RAT
Cyber-attackers are disguising malware as a video file depicting a fake sex scandal involving United States President Donald Trump. https://www.infosecurity-magazine.com/news/trump-sex-scandal-video-is-a-rat

Target for new COVID scam: Small business owners
There's a new coronavirus-related scam making the rounds, but this time the crooks are targeting small businesses. It starts with an email that claims to come from the "Small Business Administration Office of Disaster Assistance." It says you're eligible for a loan of up to $250,000 and asks for personal information like birth date and Social Security number. Let's do a CSI-style investigation to spot clues that the email is a fake…https://www.consumer.ftc.gov/blog/2021/01/target-new-covid-scam-small-business-owners?utm_source=govdelivery

Improved Qbot Banking Trojan Continues As A Force To Be Reckoned With
Since cybersecurity experts first discovered Qbot banking trojan in 2008, the malware continues to improve and expand its devastating bag of tricks, making it more persistent and effective than ever before. It has consistently morphed over time, with each new version bringing more harmful financial attacks. Security pros have watched…
https://www.sosdailynews.com/news.jspx?&articleid=E5F5FDC2B99BDA5988D59BA6E7D12AD7&sx=79

Google exposes malicious exploits targeting Windows and Android users
Due to Google's Project Zero, zero-day vulnerabilities and bugs that could infect systems with malware can be uncovered. The project has unveiled a group of vulnerabilities that could have affected a large amount of customers had they not been discovered and patched. Two malicious servers were discovered hoping to pursue… https://www.techrepublic.com/article/google-exposes-malicious-exploits-targeting-windows-and-android-users/

****

Hints & Tips plus Security Awareness

Got Malware? Here's How To Check and What To Do
Every week, an estimated 2,500 websites become newly compromised either with malware or links that lead to them. Every week. That means 130,000 new threats in a year. Every year…
https://www.scambusters.org/malware2.html

What Makes APT threats
Advanced persistent threats (APTs) are typically driven by experienced cyberactors, significant funding and a target that possesses extremely sensitive data. The depth of these threats means that virtually no enterprise is immune, even those which have implemented highly sophisticated cybersecurity measures…
https://www.isaca.org/resources/news-and-trends/isaca-podcast-library/what-makes-a-threat-an-apt

When Talk Isn't Cheap: Audio Deepfakes Targeting Enterprises On The Rise
Call it what you will…creepy, bizarre, disturbing…but audio deepfake "cloning" scams are hitting new highs in the business sector. Improvements in the technology allow audio deepfakes to show up everywhere from business to social media. Being aware of the growing threat is an important first step, but knowing that voicemails from co-workers, upper-management, vendors, and others can be faked presents…
https://www.sosdailynews.com/news.jspx?&articleid=53F193BE25F0FBCF414067DA70503A2F&sx=79

****

News & Views

Can SolarWinds survive?
For breached companies it's a long, painful road to restoring trust…
https://www.scmagazine.com/home/solarwinds-hack/can-solarwinds-survive-for-breached-companies-its-a-long-painful-road-to-restoring-trust/?utm_source=reach&utm_medium=email&utm_campaign=events_01_04

SolarWinds CEO Shares New Information About the Attack
In a blog post, SolarWinds CEO Sudhakar Ramakrishna writes, "We believe we have found a highly sophisticated and novel malicious code injection source the perpetrators used to insert the SUNBURST malicious code into builds of our Orion Platform software." Ramakrishna adds that they are sharing the information because "we believe that sharing this information openly will help the industry guard against similar attacks in the future and create safer environments for customers…"
https://orangematter.solarwinds.com/2021/01/11/new-findings-from-our-investigation-of-sunburst/

Does your health app protect your sensitive info?
New health apps are popping up every day, promising to help you track your health conditions, count your calories, manage your medications, or predict your ovulation. These apps often ask for some of your most sensitive personal information, like your health history, medication list, or whether you have ever suffered a miscarriage… https://www.consumer.ftc.gov/blog/2021/01/does-your-health-app-protect-your-sensitive-info?utm_source=govdelivery

New Zealand Central Bank Hit by Cyber Attack
On Sunday, New Zealand's central bank was responding to a breach of one of its data systems. The third-party file accessed stored "sensitive information". The Governor of the Reserve Bank of New Zealand, Adrian Orr, stated the breach was contained and the extent of the information accessed would take time…
https://www.securityweek.com/new-zealand-central-bank-hit-cyber-attack

****

"Ctrl -F" for The Board

A roll call of 2020 data breaches
The editorial team at GearBrain has chronicled a list of data breaches from 2020, including the hack of restaurant parent company Landry's, announced last January. The website estimates that more than 125 enterprises were victimized during the year, with most losing customers' data…
https://www.gearbrain.com/data-breach-cybersecurity-tracker-2020-2649780775.html

It's time for a national privacy law in the US
Consumer data privacy is no longer a necessary evil but a competitive differentiator for any company participating in the global economy. The EU's GDPR represents the world's most comprehensive regulation for privacy best practices, holding companies to stringent standards for data collection, storage and use…
https://www.helpnetsecurity.com/2021/01/12/us-national-privacy-law/

Questions
Contact FIPCO's Ken Shaurette at 800/722-3498 ext. 251 or email FIPCO IT Services for more information.

"Make Security Part of You and Your Institution's DNA!"

Threat Intelligence Newsletter: January 27, 2021

FIPCO®
IT Audit
Round Table
Discussions

If you would like to host an event, please contact: Amy Petersen

Upcoming Threat Intelligence Peer Group Discussions
None available at the current time

NIST Cyber Security Framework Training CISO Series
A series of educational videos and interviews with CISOs about the challenges and solutions they face and how to overcome them… https://www.cynet.com/ciso-life?submissionGuid=bda62884-81b1-4b03-af0b-595013523a80

Get Ready for National Consumer Protection Week (NCPW)
March is right around the corner, and you know what that means…it's almost time for National Consumer Protection Week (NCPW)! This year, NCPW is February 28 – March 6, 2021. So now's the time to jump into planning… https://www.consumer.ftc.gov/blog/2021/01/get-ready-ncpw-2021?utm_source=govdelivery

****

Alerts & Warnings

NSA Warns Enterprises Not to Use Third-Party DNS Resolvers
The US National Security Agency (NSA) has released recommendations for enterprises to securely adopt encrypted DNS. The document "explain[s] the benefits and risks of adopting the encrypted domain name system (DNS) protocol, DNS over HTTPs (DoH), in enterprise environments." The NSA recommends against using third-party DNS resolvers to "ensure proper use of essential enterprise security controls, facilitate access to local network resources, and protect internal network information…"
https://www.nsa.gov/News-Features/Feature-Stories/Article-View/Article/2471956/nsa-recommends-how-enterprises-can-securely-adopt-encrypted-dns/

Ignoring Your Credit Report Can Be Very Costly Indeed
As you're reading this, a cyberthief could be buying a new car with your credit. It could be the beginning of a massive spending spree on your dime, and in the end, there may be very little left of your funds and your credit. Hacker's with access to…
https://www.sosdailynews.com/news.jspx?&articleid=38B51807FBD3C6C516C0464A5B9B7F22&sx=79

FBI Warns About Vishing – Voice Phishing Attacks
The FBI has issued a TLP:WHITE Private Industry Notification (PIN) warning that cyber threat actors are using Voice over Internet Protocol (VoIP) platforms to contact employees at companies around the world and try to trick them into visiting a webpage that harvests their personal data. The threat actors have used the account credentials they collect to access companies' networks. https://www.securityweek.com/fbi-warns-employee-credential-phishing-phone-chat...https://www.techrepublic.com/article/fbi-warns-of-voice-phishing-attacks-targeting-employees-at-large-companies/?ftag=TREa988f1c&bhid=78480402&mid=13241219&cid=712423569

Threat Actors Abusing Browser Extensions
Previously Netskope Threat Labs published a blog post about a Lnkr ad injector campaign launched using Google Chrome extensions. As Figure 1 illustrates, the number of Lnkr infections spiked dramatically in November 2019 and again in the spring of 2020, when Brian Krebs uncovered information about the source of the infected Chrome extensions. Today, we're revisiting the Lnkr adware because… https://cyware.com/news/eliciting-current-activities-of-malicious-browser-extensions-24ff8a7a

Fourth malware strain Found – SolarWinds Breach
Used in the broad SolarWinds breach a 4th strain of malware has been identified, though it was only deployed on a few targets' networks… https://www.zdnet.com/article/fourth-malware-strain-discovered-in-solarwinds-incident/

Cisco warns on critical security vulnerabilities in SD-WAN software, so update now
Cisco has warned its users to update networking software immediately due to four severe flaws affecting the Smart Software Manager Satellite, and SD-WAN DNA. SD-WAN has three critical command injection vulnerabilities with a collective score of 9.9 out of 10. Vulnerabilities of this nature require immediate action. According to Cisco,…https://www.zdnet.com/article/cisco-warns-on-critical-security-vulnerabilities-in-sd-wan-software-so-update-now/

'LuckyBoy' Malvertising Campaign Hits iOS, Android, XBox Users
A new campaign is targeting mobile and other connected device users through utilizing cloaking and obfuscation techniques to evade detection. The malvertising campaign has been named LuckyBoy and consists of a multi-stage, tag-based approach and attack method. Andriod, Xbox, and iOS users are being targeted in the attacks. According to… https://www.securityweek.com/luckyboy-malvertising-campaign-hits-ios-android-xbox-users

****

Hints & Tips plus Security Awareness

Attackers Exploit Poor Cyber Hygiene to Compromise Cloud Security Environments
The US Cybersecurity and Infrastructure Security Agency (CISA) has released Analysis Report AR21-013A: Strengthening Security Configurations to Defend Against Attackers Targeting Cloud Services, after becoming aware of cyber-attacks leveraging weaknesses in cloud security services. Threat actors are leveraging phishing and other techniques to exploit poor cyber hygiene practices and misconfigurations in cloud services. CISA has listed steps organizations can take to improve their cloud security posture… https://www.bleepingcomputer.com/news/security/cisa-hackers-bypassed-mfa-to-access-cloud-service-accounts/

17 types of Trojans and how to defend against them
Trojan malware comes in many different types, but all require a user action to initiate…https://www.csoonline.com/article/3602790/17-types-of-trojans-and-how-to-defend-against-them.html

Why "limited trust" is a realistic target
Professionals guarding companies' information security can't go back to being "the department of 'no,' " advises Jack Freund, head of cyberrisk methodology at VisibleRisk. Freund writes that "zero trust should not equal zero business" and that a realistic target should be "limited trust, so as to securely enable the organization's strategic objectives…"https://www.isaca.org/resources/news-and-trends/newsletters/atisaca/2021/volume-2/zero-trust-should-not-equal-zero-business

Microsoft Implements Windows Zerologon Flaw 'Enforcement Mode'
Microsoft is allegedly pushing a domain controller "enforcement mode" by default to help mitigate the threat posed by the critical Zerologon flaw. Microsoft is aiming to force all companies to update their systems and address the flaw, as it represents a severe security risk to businesses, agencies, and organizations. Microsoft… https://threatpost.com/microsoft-implements-windows-zerologon-flaw-enforcement-mode/163104/

How To Timeline Login Information From Windows Event Logs
Justin: Alright. So, hello. And this is a recorded video, so just kind of, welcome, whenever you're watching this. I'm Justin Tolman, I am the Director of Training for AccessData, and today, for the next little bit, we'll be talking… https://www.forensicfocus.com/articles/how-to-timeline-login-information-from-windows-event-logs/

2 companies offer online training courses
Cybersecurity companies Fortinet and Cybrary are offering free training courses online, trying to help an industry coping with a growing skills gap. "Making content free to allow people to acquire skills, explore cybersecurity as a potential career, or to skill up to enhance their capabilities for potential employers is critical in these times," says Cybrary CEO Ryan Corey… https://www.scmagazine.com/home/security-news/network-security/free-cyber-career-training-coursework-emerges-as-a-perk-in-tough-times/

Cisco urges users to update to new routers after vulnerabilities disclosed
Description: Cisco disclosed 74 vulnerabilities in some of its RV series of wireless routers last week, urging users to purchase new hardware rather than patching them. The vulnerabilities all exist in products that have already reached their end-of-life. The affected devices include the Cisco Small Business RV110W, RV130, RV130W and RV215W systems, which could all be use as firewalls, VPNs or standard routers. All of the vulnerabilities require that an attacker has login credentials for the targeted device, and therefore are not easily exploitable. This should give users a small runway to upgrade to new gear...
https://www.zdnet.com/article/cisco-says-it-wont-patch-74-security-bugs-in-older-rv-routers-that-reached-eol/

****

News & Views

Ransomware Attacks And Amounts Up; Cyber Insurance Claims Skyrocket
A report published by Coalition, a U.S. cyber insurance provider, found that in the first half of 2020, ransomware attacks against enterprise were up 260% and ransom demands were 47% more costly than ever before…
https://www.sosdailynews.com/news.jspx?&articleid=E99A3BD8303F512A0FA97E7B236A4CA3&sx=79

Numbers show EU is serious about data breaches
Italy, Germany and France are the three European countries most likely to level fines for violating the General Data Protection Regulation, states a study by law firm DLA Piper. Other findings: Overall financial penalties have increased significantly, as have notifications of data breaches…
https://finance.yahoo.com/news/gdpr-fines-dla-piper-report-144510440.html?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cyLnNtYXJ0YnJpZWYuY29tL3JlZGlyZWN0LmFjdGlvbj9saW5rPWh0dHBzJTNBJTJGJTJGZmluYW5jZS55YWhvby5jb20lMkZuZXdzJTJGZ2Rwci1maW5lcy1kbGEtcGlwZXItcmVwb3J0LTE0NDUxMDQ0MC5odG1sJmVuY29kZWQ9bmR4RENIekxBR0RtcVdCZ0NpZkN6bUJXY05QU1JQ&guce_referrer_sig=AQAAAIOhdpmgyrEewi3kTvmWVhtJnGDa9hXKcSK8xVqVxccWN6VfcPu3k4XL-VfVBchTIc1L_kHmEb50x06BajWP75LyECuvFsROVnLkkyN1kipjgpC11qCrYR5eAFT1mBHjXVi-u-YwXttWp_67jS7qU61_3K-zjE6VEec8Ttlsua0_

Malwarebytes Targeted by SolarWinds Hackers
On Tuesday, Cybersecurity firm Malwarebytes conceded that it was targeted by the same hackers responsible for the SolarWinds attack, in which suspected Russian nation-state hackers compromised the systems of the IT management company in a sophisticated supply chain attack. Although Malwarebytes has not used any SolarWinds products, an internal investigation…. How Many others have there been in your supply chain that just don't know yet?... https://www.securityweek.com/malwarebytes-targeted-solarwinds-hackers

Top 50 Security Threats of Today
Data Security IsEssential to Our FutureIn the most obvious sense, effective data security assures the safety of our financial assets, protects individual privacy, and guards the integrityof our systems and infrastructure — from democratic elections to basic municipal functionality. In a broader and less direct sense, though,security is the essential first ingredient to… https://www.splunk.com/pdfs/ebooks/top-50-security-threats.pdf

CISA discovers token abuse around SolarWinds hack, calls for full rebuild of affected networks
An alert from the Cybersecurity and Infrastructure Security Agency at the Department of Homeland Security pointed to evidence of initial access vectors beyond SolarWinds' Orion platform, and abuse of SAML authentication tokens that mirror behaviors of the actor behind the compromise. An attacker gaining access to these tokens could be catastrophic for identity validation and likely requires a full rebuild of the network. The agency referenced guidance from Microsoft for further instructions…
https://www.scmagazine.com/home/security-news/updated-cisa-directive-discovers-saml-token-abuse-around-solarwinds-hack-calls-for-full-rebuild-of-affected-networks/?utm_source=reach&utm_medium=email&utm_campaign=events_1_18

Cracking down on ticket bots that leave you out in the cold
For most of us, it's been a long time since we've been able to attend a live event. Think back, if you can, to the last time you tried to buy tickets online to go to a concert, a game, or a play. Were you shut out because tickets sold out before you got yours? You're not alone. So what happened?... https://www.consumer.ftc.gov/blog/2021/01/cracking-down-ticket-bots-leave-you-out-cold?utm_source=govdelivery

****

"Ctrl -F" for The Board

The aftermath of the SolarWinds breach: Organizations need to be more vigilant
In the wake of the SolarWinds breach in which several key US agencies were hacked in an espionage campaign likely perpetrated by Russian actors, security experts are voicing concerns regarding how organizations manage and implement cybersecurity best practices. It may be necessary for entities to change how they vet vendors…https://www.techrepublic.com/article/the-aftermath-of-the-solarwinds-breach-organizations-need-to-be-more-vigilant/

Questions
Contact FIPCO's Ken Shaurette at 800/722-3498 ext. 251 or email FIPCO IT Services for more information.

"Make Security Part of You and Your Institution's DNA!"

Threat Intelligence Newsletter: February 3, 2021

FIPCO®
IT Audit
Round Table
Discussions

If you would like to host an event, please contact: Amy Petersen

Upcoming Threat Intelligence Peer Group Discussions
None available at the current time

****

Alerts & Warnings

Scam "US Trading Commission" website is not the FTC
It's often said that imitation is the sincerest form of flattery, but we are not flattered at all by a scam website designed to look like a Federal Trade Commission site and steal your money. https://www.consumer.ftc.gov/blog/2021/01/scam-us-trading-commission-website-not-ftc?utm_source=govdelivery

SonicWall hit by attackers leveraging zero-day vulnerabilities in its own products?
On Friday evening, SonicWall announced that it "identified a coordinated attack on its internal systems by highly sophisticated threat actors exploiting probable zero-day vulnerabilities on certain SonicWall secure remote access products." https://www.helpnetsecurity.com/2021/01/25/sonicwall-zero-day-vulnerabilities/

Why you should be wary about clicking on unsubscribe links in email messages
Managing email can be a big challenge, so it's tempting to click that "unsubscribe" link when you receive unwanted email. https://scambusters.org/unsubscribe.html

****

Hints & Tips plus Security Awareness

What Makes the Perfect Scam?
Find out how scams and scammers are evolving and how you can stay safe.
https://www.aarp.org/podcasts/take-on-today/info-2021/new-episodes-perfect-scam.html

Tips to Avoid Social Media Cybercrime
We love social media these days. Facebook, Snapchat, Twitter, LinkedIn, and many others can lead to lots of sharing and fun, but also carry significant risks. This is particularly true now that cybercriminals are collating data and using it against us for targeting phishing attacks. Online social networks may seem all in fun and harmless, but they are anything but that. Anyone participating in a social network online assumes some risk of becoming a victim of a con artist or other criminal. But this does not mean you should opt out of getting involved.
https://www.sosdailynews.com/news.jspx?&articleid=26B1E34A7BC4C9B1D084570A5C15777B&sx=79

****

News & Views

Know which threat actors you're fighting to control
With cybercrime "on a seemingly unstoppable rise," it pays to know which types of criminals might strike your business, writes Bernard Brode of Microscopic Machines. Brode catalogs threats from organized international gangs all the way down to human error, because "mistakes—even seemingly benign ones—have the potential to cause massive damage to business networks."
https://www.securityinfowatch.com/cybersecurity/article/21207268/7-cyber-threat-actors-to-watch-for-in-2021

****

"Ctrl -F" for The Board

Communicating cyberrisk
While cybersecurity professionals often bring a technical background — and mindset — to their roles, boards of directors take a more strategic view when it comes to cybersecurity. By highlighting cyberrisk as a strategic enterprise risk and drilling down on topics such as related legal and regulatory concerns, security professionals can effectively raise important considerations to the board.
https://www.isaca.org/resources/news-and-trends/newsletters/atisaca/2021/volume-2/communicating-cyberrisk-to-organizational-leadership

Questions
Contact FIPCO's Ken Shaurette at 800/722-3498 ext. 251 or email FIPCO IT Services for more information.

"Make Security Part of You and Your Institution's DNA!"

Threat Intelligence Newsletter: February 10, 2021

FIPCO®
IT Audit
Round Table
Discussions

If you would like to host an event, please contact: Amy Petersen

Upcoming Threat Intelligence Peer Group Discussions
None available at the current time

****

Alerts & Warnings

Phishing scam targets only highest-ranking execs
A phishing scheme targeting only CEOs and other high-ranking executives of companies illustrates why top management "must lead from the front and act as a personal example to make sure everyone sees security as a top priority," says Ironscales CEO Eyal Benishti. The scam involves fake password alerts for the widely used Microsoft Office 365 software suite… https://www.scmagazine.com/home/security-news/phishing/phishing-scheme-shows-ceos-may-be-most-valuable-asset-and-greatest-vulnerability/

Agent Tesla Upgrades with New Delivery & Evasion Tactics
Agent Tesla, a remote access Trojan, has been upgraded to include new evasion tactics as well as the ability to target more applications for credential theft, updated communication tactics, and new techniques for surpassing endpoint defense. The new version targets Microsoft Anti-Malware Software Interface as a means to bypass endpoint… https://www.darkreading.com/perimeter/agent-tesla-upgrades-with-new-delivery-and-evasion-tactics/d/d-id/1340041

Cryptojacking malware targeting cloud apps gets new upgrades, worming capability
A piece of cryptojacking malware with a penchant for targeting the cloud has gotten some updates that makes it easier to spread and harder for organizations to detect when their cloud applications have been commandeered… https://www.scmagazine.com/home/security-news/malware/cryptojacking-malware-targeting-cloud-apps-gets-new-upgrades-worming-capability/?utm_source=newsletter&utm_medium=email&utm_campaign=SCUS_Newswire_{{%27now%27|date:%27%Y%m%d%27}}&hmSubId={{contact.cms_id_encrypted}}&email_hash={{contact.email|md5}}&oly_enc_id=0795J7353967J0E

Trickbot malware now maps victims' networks using Masscan

The Trickbot malware has been upgraded with a network reconnaissance module designed to survey local networks after infecting a victim's computer. This new module, dubbed masrv, uses the…..Do you have an endpoint solution that would detect his anomalous activity?... https://www.bleepingcomputer.com/news/security/trickbot-malware-now-maps-victims-networks-using-masscan/

****

Hints & Tips plus Security Awareness

How to Hack a Human; Social Media, Social Engineering, and Business Email Compromise

Over the last decade, phishing - a type of social engineering attack - has transformed from something more like spam to the threat most likely to cause a breach. During that same period, the number of adults on social media platforms like Facebook increased by almost, 300%... https://www.tessian.com/research/how-to-hack-a-human/?utm_campaign=jannewsletter&utm_medium=email&_hsmi=108835018&_hsenc=p2ANqtz-_mkRo3BMyaV4ZzpJTCedJvGvmlpr_XnGxnV6EL0CXWHACQdcOZTE18SeBR4hYk7mmPsuDrCgspERfIESfyVUfre_AWoA&utm_source=marketing

What is credential stuffing?

Credential stuffing is a type of cyberattack where cybercriminals take large databases of usernames and passwords, often stolen through recent data breaches, and attempt to "stuff" the account logins into other web applications using an automated process. In a credential stuffing attack, the fraudster uses access to consumer accounts to make fraudulent purchases, conduct phishing attacks, and steal information, money, or both. Credential stuffing is especially dangerous for consumers who use the same username and password combinations for more than one account, giving a cyber thief access to all of those accounts at one swipe…Continue reading "What is Credential Stuffing? What You Need to Know to Stay Safe from Account Hacking"
https://www.fightingidentitycrimes.com/credential-stuffing/

Why Browser Incognito Mode Doesn't Protect Privacy

Have you ever clicked on the "in private," "incognito" or similar private mode option in your browser and thought you couldn't be tracked? Forget it. With a couple of minor exceptions, you really haven't done anything to protect your privacy. Most people realize by now that it's next to impossible to surf the Internet securely using a conventional browser. Sites you visit can place cookies (small pieces of code) on your device, unless you severely restrict them…https://www.scambusters.org/incognito.html

Large US Banks Pilot new Data Sharing Risk Assessment Service

The Clearing House, JPMorgan Chase, PNC Bank, TD Bank, Truist, US Bank, Wells Fargo, along with data aggregators Finicity and Plaid, piloted the new *Streamlined Data Sharing Risk Assessment* that enables financial apps and data aggregators to provide assessment information more efficiently to financial institutions (FIs) with standardized risk assessments. The goals are to both save time in the risk assessment process and to better protect consumer data. The risk assessment is provided by third-party risk assessment firms TruSight and KY3P by IHS Markit and uses work by the Clearing House's Connected Banking initiative that determined what information apps and aggregators need to satisfy due diligence requirements…https://www.theclearinghouse.org/connected-banking

A Practical Guide to Cybersecurity with a Password Manager
Do you think that people are your weakest security link? Think again. It's your passwords. After all, the world's most-hacked password is 123456. Employees want to simplify their digital lives—not to create and memorize long, difficult passwords. Make it easy for them…https://go.dashlane.com/rs/403-EXY-689/images/2021_01_Guide_to_Cybersecurity_for_IT_Admins_ebook_Final.pdf

New Research: How to Hack a Human
Want to get inside the mind of a hacker? We interviewed 10 of them to learn how bad actors leverage social media and OOO messages to craft targeted - and believable - social engineering attacks. Bonus guide for employee education included…
https://f.hubspotusercontent20.net/hubfs/1670277/%5BCollateral%5D%20Tessian%20Research/%5BTessian%20Research%5D%20How%20to%20Hack%20a%20Human/%5BTessian%20Research%5D%20How%20to%20Hack%20a%20Human.pdf?__hstc=&__hssc=&hsCtaTracking=cc714894-d846-443e-b53a-9cc9a60b628d%7C7d381ce4-d28e-47cb-98de-ce7dd2283fd5

Optimizing frameworks
Leveraging frameworks can play an important role in organizations having the right security policies and procedures in place. Governance frameworks such as COBIT can be customized according to the specific mitigation techniques and risk appetite of an organization for efficient implementation…
https://www.isaca.org/resources/news-and-trends/isaca-podcast-library/framework-overload

****

News & Views

US plan would give banks 36 hours to report incidents
The Office of the Comptroller of the Currency, the Federal Deposit Insurance Corporation and the Federal Reserve System's board of governors have proposed a rule that would require banks to report cybersecurity events within 36 hours. A public comment period will last until April 12, 2021…
https://www.jdsupra.com/legalnews/financial-agencies-contemplate-36-hour-6483925/

A different tack on security: Indicators of behavior
Nicolas Fischbach and Alan Ross argue that using indicators of compromise to chase cyberattacks is an outdated strategy. Instead, they recommend using indicators of behavior, examining every time a "document is created, saved, changed, mailed, shared, uploaded, downloaded or deleted" so that "those actions are analyzed as a series to determine context and intent…"
https://www.techrepublic.com/article/cybersecurity-pros-should-switch-from-indicators-of-compromise-to-indicators-of-behavior/

How zero-trust principles go beyond the cloud
Adopting a zero-trust approach to cybersecurity "doesn't mean a wholesale rip-and-replace effort is needed on the technology side," says Andrew Rafla of accounting/consulting firm Deloitte. Rafla points out that zero trust "is not dependent upon or solely focused on cloud environments—the concept can be applied to on-premise environments as well…" https://thebossmagazine.com/zero-trust-cybersecurity/

The top frauds of 2020 per the Federal Trade Commission
2020 was a tough year. Between the pandemic and the economic crisis, we all had our hands full. And scammers didn't take any time off either — 2020 was a busy year for fraud. In 2020, the FTC got more than 2.2 million reports about fraud, with people telling us they lost nearly $3.3 billion.
https://www.consumer.ftc.gov/blog/2021/02/top-frauds-2020?utm_source=govdelivery

Emotet Malware Disrupted
The FBI worked alongside foreign law enforcement and private sector partners in an innovative, coordinated effort to take down a destructive malware known as Emotet. https://www.fbi.gov/news/stories/emotet-malware-disrupted-020121?utm_campaign=email-Daily&utm_medium=email&utm_source=stories&utm_content=%5B1078872%5D-%2Fnews%2Fstories%2Femotet-malware-disrupted-020121

****

"Ctrl -F" for The Board

Effective data governance means striking a balance
Striking the proper balance with data governance—that is, making it "simultaneously restrictive and enabling"—is key to running a successful enterprise, Eric Avidon writes. Donald Farmer of TreeHive Strategy notes that "[w]hen a system is well-governed, it actually becomes a capability." https://searchbusinessanalytics.techtarget.com/feature/Data-governance-framework-key-to-analytics-success

6 ways enterprises can mitigate cyberrisks
Because "[a] determined, well-resourced adversary can penetrate any network," enterprises should focus on containing risk and preparing for recovery, writes Scott Algeier, executive director of the Information Technology—Information Sharing and Analysis Center. Algeier covers six calls to action to make sure security awareness flows through the whole organization. https://www.isaca.org/resources/news-and-trends/industry-news/2021/cost-effective-steps-to-managing-cyberrisk

Questions
Contact FIPCO's Ken Shaurette at 800/722-3498 ext. 251 or email FIPCO IT Services for more information.

"Make Security Part of You and Your Institution's DNA!"

Threat Intelligence Newsletter: February 15, 2021

FIPCO®
IT Audit
Round Table
Discussions

If you would like to host an event, please contact: Amy Petersen

Upcoming Threat Intelligence Peer Group Discussions
None available at the current time

****

Alerts & Warnings

Credit card skimmer piggybacks on Magento 1 hacking spree
Back in the fall of 2020 threat actors started to massively exploit a vulnerability in the no-longer maintained Magento 1 software branch. As a result, thousands of e-commerce shops were compromised and many of them injected with credit card skimming code…https://malwaredevil.com/2021/02/02/credit-card-skimmer-piggybacks-on-magento-1-hacking-spree/

Google Chrome Zero-Day Afflicts Windows, Mac Users
Google has released a warning to its customers stating that a zero-day vulnerability is being actively exploited by attackers and encouraging Google Chrome browser users to maintain aware of the issue and implement a patch as soon as it is available. The flaw lies in the V8 open-source web engine…
https://threatpost.com/google-chrome-zero-day-windows-mac/163688/

Microsoft Warns of Under-Attack Windows Kernel Flaw
Microsoft's scheduled monthly batch of security patches landed with a loud thud Tuesday with fixes for at least 56 security vulnerabilities in a range of operating system and software products…
https://www.securityweek.com/patch-tuesday-microsoft-warns-under-attack-windows-kernel-flaw

How Scalping Bots Rip Off Would-be Buyers
Technology has delivered a new enemy at our doorsteps when we try to buy things that are likely to be in heavy demand -- scalping bots…https://scambusters.org/scalpingbots.html

Vulnerabilities in widely used TCP/IP stacks open IoT, OT devices to attack
Forescout researchers have discovered nine vulnerabilities affecting nine different TCP/IP stacks widely used in IoT and OT devices…https://www.helpnetsecurity.com/2021/02/11/vulnerabilities-tcp-ip-iot/

****

Hints & Tips plus Security Awareness

Protecting Your Identity Online
Chances are, you handle a lot of the business of real life in the digital world. In a single day, you might connect with friends and coworkers, order groceries to your doorstep, pay bills, file health insurance claims, and view the funds in your retirement account all on the internet. While handl… https://www.trueidentity.com/identity-theft-resource/protecting-your-identity-online?channel=paid&cid=eml:retentid:tidp:995EduFeb02082021tidmfr&utm_source=retentid&utm_medium=email&utm_campaign=995EduFeb02082021tidmfr

VMWare ESXI Vulnerability Updates
VMSA-2020-0029.1 - VMware ESXi, Workstation, Fusion and Cloud Foundation updates address a denial of service vulnerability (CVE-2020-3999)Please see the updated advisory here… https://www.vmware.com/security/advisories/VMSA-2020-0029.html

VMWare VSphere Replication Vulnerability Fix
A command injection vulnerability in vSphere Replication was privately reported to VMware . Updates are available to address this vulnerability in the affected product… https://www.vmware.com/security/advisories/VMSA-2021-0001.html

Adobe Patches Reader Vulnerability Exploited in the Wild
Adobe has released patches for 50 vulnerabilities, including a Reader zero-day vulnerability that has been exploited in the wild…https://www.securityweek.com/adobe-patches-reader-vulnerability-exploited-wild

****

News & Views

NIST Offers Tools to Help Defend Against State-Sponsored Hackers
Nations around the world are adding cyberwarfare to their arsenal, employing highly skilled teams to launch attacks against other countries. These adversaries are also called the “advanced persistent threat,” or APT, because they possess the tools and resources to pursue their objectives repeatedly over an extended period, adapting to defenders’ efforts to resist them…https://www.nist.gov/news-events/news/2021/02/nist-offers-tools-help-defend-against-state-sponsored-hackers

Financial Regulator Hit by 240,000 Malicious Emails in Q4 2020
The UK’s financial regulator, the Financial Conduct Authority (FCA), was hit by nearly 240,000 malicious emails in the first quarter of 2020 alone, the FOI found. This highlights the pressure weighing on high profile organizations to protect their assets and maintain high levels of cybersecurity and awareness. A litigation firm… https://www.infosecurity-magazine.com/news/fca-240000-malicious-emails-q4-2020/

Most zoombombing incidents are inside jobs
Most zoombombing incidents are “inside jobs” according to a study featuring researchers at Binghamton University, State University of New York… https://www.helpnetsecurity.com/2021/02/09/most-zoombombing-incidents-are-inside-jobs/

Punk Kitty Ransom - Analysing HelloKitty Ransomware Attacks
February 9, the company behind the gaming blockbuster Cyberpunk 2077 announced that it had been hit by a ransomware attack and the hackers claimed to have stolen source code for upcoming games. The most likely culprit at this time of the known ransomware groups is a group known as HelloKitty…
https://www.cadosecurity.com/post/punk-kitty-ransom-analysing-hellokitty-ransomware-attacks

How data breaches filter down and affect customers
The effects of data breach ripple down to consumers, finds a survey of 4,800 people from 12 major countries by F-Secure. About 20% admitted to using an online service that had experienced a breach, and of those respondents, 3 in 5 reported being the target of cybercriminals…
https://www.siliconrepublic.com/enterprise/data-breaches-cybercrime-security

Double Trouble: The Dangers of Ransomware 2.0 : InfoSecurity Magazine Online
Welcome to the latest issue of Infosecurity Magazine, FireEye Breach: A Tipping Point in Nation State Attacks, Securing Cloud Environments in Modern Organizations, Double Trouble: The Dangers of Ransomware 2.0…https://edition.pagesuite-professional.co.uk/html5/reader/production/default.aspx?pubname=&edid=f73de865-57f0-49d7-9a61-318ea24773c7

Researchers identify 223 vulnerabilities used in recent ransomware attacks
Ransomware groups – and APTs – are leveraging an expanding list of vulnerabilities, misconfigurations and technologies to overwhelm IT security teams… https://www.scmagazine.com/home/security-news/ransomware/researchers-identify-223-vulnerabilities-used-in-recent-ransomware-attacks/?utm_source=newsletter&utm_medium=email&utm_campaign=SCUS_Newswire_{{%27now%27|date:%27%Y%m%d%27}}&hmSubId={{contact.cms_id_encrypted}}&email_hash={{contact.email|md5}}&oly_enc_id=0795J7353967J0E

****

"Ctrl -F" for The Board

The case for a risk committee as part of governance
Boards should appoint a separate risk committee to "eventually align with, and support, the board's overall governance of risks," M. Muneer and Ralph Ward write. They add that audit committee members might not have the background needed, noting the "forensic, numbers-driven structure of audit lacks the more dynamic, hypothetical approach needed to avoid dangers…"
https://www.forbesindia.com/blog/enterprise/why-companies-need-risk-management-committees/

Questions
Contact FIPCO’s Ken Shaurette at 800/722-3498 ext. 251 or email FIPCO IT Services for more information.

"Make Security Part of You and Your Institution's DNA!"

Threat Intelligence Newsletter: February 25, 2021

FIPCO®
IT Audit
Round Table
Discussions

If you would like to host an event, please contact: Amy Petersen

Upcoming Threat Intelligence Peer Group Discussions
None available at the current time

****

Alerts & Warnings

Imposter Scams Lead Way to Victims' $3.2 Billion Losses
Crooks are raking in more than $3 billion a year in the US because of a massive increase in the number of imposter scams in the past year… https://scambusters.org/imposter3.html

Masslogger Swipes Microsoft Outlook, Google Chrome Credentials
According to researchers, Cybercriminals are targeting Windows users with a new and improved variant of the Masslogger Trojan. The malicious software is spyware that is designed to steal credentials from popular applications such as Microsoft Outlook, Google Chrome, and other messenger accounts. Researchers allegedly uncovered the campaign in mid-January, finding…
https://threatpost.com/masslogger-microsoft-outlook-google-chrome/164011/

****

Hints & Tips plus Security Awareness

Using Strategic Choices to Ensure Continuous and Effective Cybersecurity
The cybersecurity marketplace can be a little overwhelming, so organizations must take a thoughtful approach when sourcing cybersecurity tools. Yong Hong Ow and Baksheesh Singh Ghuman explain the use of strategic choices when making your selection… https://www.tripwire.com/state-of-security/security-data-protection/strategic-choices-continuous-effective-cyber-security/?utm_source=The%20State%20of%20Security%20Newsletter&utm_medium=email&utm_campaign=FO-02-15-2021&utm_content=httpswwwtripwirecomstateofsecuritysecuritydataprotectionstrategicchoicescontinuouseffectivecybersecurity&mkt_tok=MzE0LUlBSC03ODUAAAF7SsMyKaeTaS9nHyzFsBScQP5tKwvFpn517WMd5sPSeyNiO0lfTdGwfP1031xyw26r1H1r8wWXClcmRTnAkd_F0tY6yquSCwEoZ0y9xPBh2ilvcw

****

News & Views

The Perils of Overlooking Physical Security
With today's advanced cloud capabilities, cybersecurity is an obvious priority at many organizations. But that can leave physical security diminished or outright neglected. In this episode of the podcast, security experts Dustin Brewer and Frank Downs discuss what makes it so important to secure physical assets and how enterprises can do so effectively… https://www.isaca.org/resources/news-and-trends/isaca-podcast-library/the-perils-of-overlooking-physical-security

State of malware
Spyware activity spiked in 2020, and the malware-as-a-service business model got more sophisticated… https://www.techrepublic.com/article/state-of-malware-3-key-findings-in-the-latest-malwarebytes-report/?ftag=TREa988f1c&bhid=78480402&mid=13269630&cid=712423569

Cybersecurity 2021: Tabletop exercises should top the 2021 security agenda
Privacy considerations that moved to the forefront last year will intensify in 2021, writes lawyer Andrew Droke of Baker Donelson. Droke outlines key considerations and suggests immediate actions, such as customized tabletop exercises to "help refine your incident response plan…"
https://www.cpomagazine.com/data-privacy/data-privacy-top-considerations-for-2021/

NIST hints at upgrades to its system for scoring a phish's deceptiveness
Future plans for the methodology include the incorporation of operational data gathered from multiple organizations… https://www.scmagazine.com/home/security-news/phishing/nist-hints-at-upgrades-to-its-system-for-scoring-a-phishs-deceptiveness/?utm_source=newsletter&utm_medium=email&utm_campaign=SCUS_Newswire_{{%27now%27|date:%27%Y%m%d%27}}&hmSubId={{contact.cms_id_encrypted}}&email_hash={{contact.email|md5}}&oly_enc_id=0795J7353967J0E

****

"Ctrl -F" for The Board

Top 100 Cybersecurity News Sites
With millions of websites and downloadable files available on the internet, potential risks of security breach are high, especially with the fast development in technology. In this article, we will list top 100 cybersecurity news sites so you can stay updated and on the lookout…
https://www.cyberdefensemagazine.com/top-100-cybersecurity-news-sites/

Questions
Contact FIPCO’s Ken Shaurette at 800/722-3498 ext. 251 or email FIPCO IT Services for more information.

"Make Security Part of You and Your Institution's DNA!"

Threat Intelligence Newsletter: March 5, 2021

FIPCO®
IT Audit
Round Table
Discussions

If you would like to host an event, please contact: Amy Petersen

Upcoming Threat Intelligence Peer Group Discussions
None available at the current time

****

Alerts & Warnings

NYS DFS Cyber Alert: Instant Quote Site Targeted for NPI
The New York State Department of Financial Services last week released a cyber alert warning regulated entities of an aggressive campaign targeting public-facing instant quote websites to steal nonpublic information for use in unemployment benefit frauds. DFS urges all regulated entities with instant quote websites - and similar public-facing websites that display or transmit both redacted and unredacted NPI - to immediately review those websites for evidence of hacking. See the alert for more information, including an overview of the campaign and recommendations to mitigate the threat…
https://www.dfs.ny.gov/industry_guidance/industry_letters/il20210216_cyber_fraud_alert?utm_campaign=RiskCyber-20210222&utm_medium=email&utm_source=Eloqua

Imposter Scams Lead Way to Victims' $3.2 Billion Losses
Crooks are raking in more than $3 billion a year allegedly uncovered the campaign in mid-January, finding…
https://threatpost.com/masslogger-microsoft-outlook-google-chrome/164011/

Sneaky New e-Payment Skimmer Avoids Security Detection
Just recently, Visa's Payment Fraud Disruption team posted a Security Alert on its website about its latest discovery. The company's eCommerce Threat Disruption (eTD) tool found a new JavaScript skimmer technology that's targeting merchant websites across the globe. Visa's eTD tool was created to identify any compromise in e-commerce transactions on a merchant website. Visa's eTD tool worked as designed until the beginning of this year when they found a new payment-skimming malware they call "Baka..."
https://www.sosdailynews.com/news.jspx?&articleid=8BE90FC57DFAB59C85372C56E8DDBC57&sx=79

IRS Annual Dirty Dozen Top Tax Scams For 2021
The IRS posted its annual list of the top tax scams for 2021, called the "Dirty Dozen." Every year, the IRS takes a look at the most prevalent tax scams affecting U.S. taxpayers. In its continued effort to keep us safe from tax fraudsters, the IRS tells us what these scams can look like so we can avoid becoming a victim. They also remind us that although scams increase during tax time and crisis events, they continue to happen year-round…
https://www.sosdailynews.com/news.jspx?&articleid=A3E4DE989F0C2454DF16D7FFF37DD365&sx=79

Real ID Card Deadline Sparks Scam Surge
The launch of a new personal identification system in the United States, popularly known as Real ID, is being targeted by scammers to steal from victims… https://scambusters.org/realid.html

Phishing campaign alters prefix in hyperlinks to bypass email defenses
Better integration between email and web security systems could serve as a defense…
https://www.scmagazine.com/home/security-news/phishing/phishing-campaign-alters-prefix-in-hyperlinks-to-bypass-email-defenses/?utm_source=newsletter&utm_medium=email&utm_campaign=SCUS_Newswire_{{%27now%27|date:%27%Y%m%d%27}}&hmSubId={{contact.cms_id_encrypted}}&email_hash={{contact.email|md5}}&oly_enc_id=0795J7353967J0E

****

Hints & Tips plus Security Awareness

Not All WiFi Is Good WiFi
WiFi has become a part of pretty much any device that has network access. From mobile phones and tablets to desktop computers and laptops. The time to plug in an Ethernet cable has long since passed. And while just a few years ago it was considered high risk to allow WiFi access in corporate offices, now it is just a standard part of doing business. Unfortunately, when dealing with technology that everyone is using, cybercriminals are generally also going to get involved. And when it comes to WiFi, there are plenty of opportunities for cybercriminals to attack. Fortunately, most of this risk can be easily eliminated through awareness and proper security controls…
https://www.sosdailynews.com/news.jspx?&articleid=8EFD67A6C24B7B92BE059D1738149976&sx=79

What Changes Do We Need To See In eDiscovery? Part VII
Forensic Focus talks about how to deal with structured data in ediscovery cases.
I'm baaaaa–ack! And you thought I was done with my earlier six-part series, but I have a new topic to add to my rants and raves… https://www.forensicfocus.com/articles/what-changes-do-we-need-to-see-in-ediscovery-part-vii/

How do I select a network monitoring solution for my business?
A recent report predicts that home networks, remote working software and cloud systems will be at the center of a new wave of attacks in 2021… https://www.helpnetsecurity.com/2021/02/22/select-network-monitoring-solution/

VMware Releases Multiple Security Updates
VMware has released security updates to address multiple vulnerabilities--CVE-2021-21972, CVE-2021-21973, CVE-2021-21974—ESXi, vCenter Server, and Cloud Foundation. A remote attacker could exploit some of these vulnerabilities to take control of an affected system… https://us-cert.cisa.gov/ncas/current-activity/2021/02/24/vmware-releases-multiple-security-updates

VMware patches bug that put many large networks at risk
VMware has patched a critical vulnerability that was found in its vCenter Server VMware utility that could have allowed for remote code execution on a vulnerable server. Positive Technologies discovered the flaw and reported VMware to the bug. In a press release published on Wednesday, the security company explained how… https://www.techrepublic.com/article/vmware-patches-bug-that-put-many-large-networks-at-risk/

****

News & Views

Digital forensics can help prevent the next attack
Although digital forensics is generally thought of as cleaning up after a cyberattack, the "lessons learned from this process can be used to both support your security's offense as well as its defense," writes Anas Chbib of AGT-Advanced Germany Technology. "What is the point of committing mistakes if you don't learn from them?"   You too can receive this with the FIPCO Cynet XDR solution, ask to see more…
https://betanews.com/2021/02/19/digital-forensics-best-offense/

The Pandemic and Internal Fraud
As the Pandemic increases so does the rise in the potential for Internal aud...https://blog.nxtsoft.com/the-pandemic-and-internal-fraud?utm_campaign=ThreatAdvice%20Partners&utm_medium=email&_hsmi=112457645&_hsenc=p2ANqtz-8UdreQrnC-19eXem1vPfJmloCf-IgyhXPzsJDp0HeLJodt6wVfuSw6x5UpkIITlXADAed6nm4-riKrmtopuyegd-aL8g&utm_content=110644295&utm_source=hs_email

Microsoft Flaw Fixed in February Had Been Exploited Since Summer 2020
One of the vulnerabilities that Microsoft fixed in its February 2021 Patch Tuesday release has been exploited in the wild since the summer of 2020. The high-severity privilege elevation issue can be exploited "by triggering a use-after-free condition in the win32k.sys core kernel component."
https://www.bleepingcomputer.com/news/security/recently-fixed-windows-zero-day-actively-exploited-since-mid-2020/

Small firm shares details of "terrifying" cyberattack
Nate Tabak shares the play-by-play of how a small trucking and logistics company handled a ransomware attack, likely the result of a phishing email. "To see someone in the inside of your system, it's very terrifying," says the manager of the company, identified only as George.
https://www.freightwaves.com/news/inside-a-ransomware-attack-on-a-small-trucking-company

****

"Ctrl -F" for The Board

This cybersecurity threat costs business millions. And it's the one they often forget about
Phishing emails that dupe users into sending cyber criminals wire transfers is by far the most lucrative form of cybercrime - here's what you need to know…https://www.zdnet.com/article/this-cybersecurity-threat-costs-business-millions-and-its-the-one-they-often-forget-about/?utm_medium=email&_hsmi=112318587&_hsenc=p2ANqtz--QdLuOHzdcLEwz72A5T5zIO_bwvTX5phkku3-O1oRRvMtwn0p92WTCU3RUdEVkYa19Va1bkZZf_pvXnmJvwUGcuG_WDA&utm_content=112318587&utm_source=hs_email

Opinion: Don't confuse data security with data privacy
Data security and data privacy are two different topics and must be treated as such, writes Pankaj Srivastava, CEO and founder of Practicalspeak. Srivastava offers four tips about privacy; among them are that companies should "boldly display and tell your customers what data you want to collect, how you will use it and how it will benefit them…"
https://www.forbes.com/sites/forbesbusinesscouncil/2021/02/19/four-ways-to-improve-your-companys-privacy-practices/?sh=24f29448568f

Questions
Contact FIPCO's Ken Shaurette at 800/722-3498 ext. 251 or email FIPCO IT Services for more information.

"Make Security Part of You and Your Institution's DNA!"

Threat Intelligence Newsletter: March 9, 2021

FIPCO®
IT Audit
Round Table
Discussions

If you would like to host an event, please contact: Amy Petersen

Upcoming Threat Intelligence Peer Group Discussions
None available at the current time

CISA Issues Emergency Directive and Alert on Microsoft Exchange Vulnerabilities
The Cybersecurity and Infrastructure Security Agency last week issued Emergency Directive 21-02 and Alert AA21-062A addressing critical vulnerabilities in Microsoft Exchange products. CISA is aware of widespread domestic and international exploitation of these vulnerabilities that can allow an attacker to access on-premises Exchange servers and gain persistent system access and control of an enterprise network. https://cyber.dhs.gov/ed/21-02/?utm_campaign=RiskCyber-20210308&utm_medium=email&utm_source=Eloqua

****

Alerts & Warnings

Cisco Warns of Critical Auth-Bypass Security Flaw
Cisco has allegedly fixed a critical security flaw affecting its Nexus 3000 Series Switches and Cisco Nexus 9000 Series Switches. The vulnerability could allow for a remote attacker to bypass authentication, according to the company. The bug is one of three critical flaws patched by Cisco this past week. https://threatpost.com/cisco-critical-security-flaw/164255/

When it comes to scams, let's look out for one another
This pandemic has brought lots of side effects. Lost jobs, lost income, and lost homes are themes we see around the country — and scammers know just how to take advantage of these worries. Another side effect of the pandemic is isolation, which scammers also like to use to their advantage. During National Consumer Protection Week, which starts today, I'm asking you to join me in fighting isolation to fight scams. https://www.consumer.ftc.gov/blog/2021/03/when-it-comes-scams-lets-look-out-one-another?utm_source=govdelivery

WordPress Sites Have Plugin Flaw Making Them Vulnerable To Cyberattacks
WordPress website builder has become the most widely used content management system in the world. With 455 million active sites, it's big news when WordPress finds a plugin is flawed. It has discovered that the bug allows account takeovers and other attacks by cybercriminals. The good news is that WordPress has a patch available that resolves the issue and they urge their users to apply the update immediately. In the meantime, those who haven't applied the patch should be aware of the risks if they wait to do so.
https://www.sosdailynews.com/news.jspx?&articleid=36990859508B5051BAF569BA2FA1F5A2&sx=79

Latest TrickBot Malware Has Even More Up Its Sleeve (sure glad we implemented an advance XDR solution at the WBA)
No slouch when it comes to reinventing itself, TrickBot malware has evolved yet again. Considered the top threat to business on a global scale, TrickBot and its financial data-stealing abilities are prolific. Earlier this year, TrickBot expanded its menu of mayhem, focusing on making it more difficult to detect and defend against. Now, TrickBot is at it again. Its latest added module takes the ability to evade detection to a whole new level.
https://www.sosdailynews.com/news.jspx?&articleid=D4D1F43F6C3C6F85486516477C06741B&sx=79

Multi-payload platform stealthily delivers malware and ransomware
The delivery method for the six-year-old Gootkit financial malware has been developed into a complex and stealthy delivery system for a wide range of malware, including ransomware.
https://www.helpnetsecurity.com/2021/03/02/gootloader-malware-ransomware/

Microsoft Warns that 4 Exchange Server Zero-Days Are Under Attack by Chinese Hacking Group
Microsoft late Tuesday raised the alarm after discovering Chinese cyber-espionage operators chaining multiple zero-day exploits to siphon e-mail data from corporate Microsoft Exchange servers.
https://www.securityweek.com/microsoft-4-exchange-server-zero-days-under-attack-chinese-apt-group
https://us-cert.cisa.gov/ncas/current-activity/2021/03/02/microsoft-releases-out-band-security-updates-exchange-server

No, the government won't call/text/email you for money
Lots of people are having trouble sleeping, thanks to the pandemic and all the parts of our lives it's affecting. And it doesn't help when you get a call saying you owe the government money. Oh, and, they add, you'll go to jail if you don't pay up immediately. That's a scam, a.
https://www.consumer.ftc.gov/blog/2021/03/no-government-wont-calltextemail-you-money?utm_source=govdelivery

Fraudulent fundraiser uses illegal robocalls to harass consumers
In 2015, the FTC and state partners sued and shut down four sham charities that harassed millions of people with more than 1.3 billion illegal robocalls about donating to charity. The FTC and 46 charity state regulators from 38 states and the District of Columbia are holding the fundraisers that made those illegal calls accountable in a lawsuit announced today. https://www.consumer.ftc.gov/blog/2021/03/fraudulent-fundraiser-uses-illegal-robocalls-harass-consumers?utm_source=govdelivery

****

Hints & Tips plus Security Awareness

Lessons Learned from the SolarWinds SUNBURST Attack
Webinar Overview – week of March 15.
While much has been analyzed in regards to the SolarWinds SUNBURST attack, only a few have taken a step back as the tide receded to see the full picture from start to finish. But security professionals need this hindsight view to understand the attack development, surface important attack tactics, technologies and process insights, and apply the right strategic defense measures to prevent being a victim of su.
https://cynet.easywebinar.live/lessons-learned-from-the-solarwinds-sunburst-attack-registration?utm_content=156827232&utm_medium=social&utm_source=linkedin&hss_channel=lis-Y-mziLszYY

Since breaches are inevitable, know the law beforehand
Because privacy violations "have proven to be inevitable," it's necessary to understand the plethora of local, state, national and international laws governing notifications, writes attorney Salar Atrizadeh. In this tutorial, Atrizadeh identifies the laws IT experts in the US should become aware of.
https://www.isaca.org/resources/news-and-trends/industry-news/2021/understanding-the-importance-of-us-privacy-and-identity-theft-laws

Prepare early for next Calif. rules, attorneys advise
Even though the California Privacy Rights Act doesn't take effect until Jan. 1, 2023, attorneys are advising clients to prepare well in advance. Companies that don't have a handle on their data maps should move now, because "you're going to need that information come 2023," says Ashley Shively of law firm Holland & Knight. https://news.bloomberglaw.com/tech-and-telecom-law/fresh-wave-of-california-privacy-rules-means-business-prep-now

Which scams are having the most devastating impact on consumers?
Online Scams Rise During COVID-19 Pandemic: 2020 BBB Scam Tracker Risk Report (https://www.bbb.org/globalassets/local-bbbs/council-113/media/bbb-institute/riskreport2020/2020-BBBscamtracker-riskreport.pdf) uses data submitted by consumers to BBB Scam Tracker (https://www.bbb.org/scamtracker/us) to shed light on how scams are being perpetrated, who is being targeted, which scams have the greatest impact, and much more.
https://bbb.org/bbbscamtrackerriskreport/

Strong governance necessary to comply with GDPR
Transparency and strong data governance are necessary to avoid running afoul of the EU General Data Protection Regulation, says attorney Carolyn Bigg of DLA Piper. Even companies transferring data internally can be affected, Bigg says, a change from several years ago.
https://www.cdotrends.com/story/15401/gdpr-can-make-data-sharing-ai-minefield

****

News & Views

Money Mule Scams Are More Common Than You Would Expect
A money mule scam is when someone sends money to you and asks you to send a portion of it to someone else. They often ask you to use gift cards or wire transfers. The money they are providing you is likely stolen. Drug trafficking and human tracking are also common sources of the money, and they're lying about the reason they need you to send it. The relationship, job, prize or other reason they use is not real and they are only using you to launder money.
https://www.sosdailynews.com/news.jspx?&articleid=32AD05A975572FDAEA29E1D7F49AB150&sx=79

Vaccine spearphishing attacks increase
Spearphishing campaigns tied to COVID-19 rose sharply from last October through the end of January, Barracuda Networks reports. Fleming Shi, Barracuda's chief technology officer, says the campaigns are particularly dangerous because people are "racing for the openings" to be vaccinated.
https://www.cyberscoop.com/covid-vaccine-scam-phishing-barracuda-check-point/

****

"Ctrl -F" for The Board

Navigating the US Federal Government Agency ATO Process for IT Security Professionals
T security professionals such as risk managers and information security managers maintain a US federal government agency's information system using the Federal Information Security Management Act (FISMA) in a manner that is unique to the US federal government. To do so, they encounter the Authority to Operate (ATO) security authorization process, which is in place for the security of the agency's information systems. https://www.isaca.org/resources/isaca-journal/issues/2017/volume-2/navigating-the-us-federal-government-agency-ato-process-for-it-security-professionals

Questions
Contact FIPCO's Ken Shaurette at 800/722-3498 ext. 251 or email FIPCO IT Services for more information.

"Make Security Part of You and Your Institution's DNA!"

Threat Intelligence Newsletter: March 12, 2021

FIPCO®
IT Audit
Round Table
Discussions

If you would like to host an event, please contact: Amy Petersen

Upcoming Threat Intelligence Peer Group Discussions
None available at the current time

****

Alerts & Warnings

US Warns of Fake Unemployment Benefit Websites
On March 5, the US Justice Department issued a warning informing the public that cyber-criminals have launched a campaign impersonating state workforce agencies in an attempt to lure in unemployed Americans and steal personal data. The Justice Department published the advisory after several reports that threat actors had been creating… https://www.infosecurity-magazine.com/news/us-warns-of-fake-unemployment/

Android users hit by banking trojan in 10 Play Store apps
Another day, another Android banking trojan caught targeting unsuspecting users but this time it does it from Play Store without any prevention… https://www.hackread.com/android-users-banking-trojan-10-play-store-apps/

This malware disables Google's only security mechanism against malware-infected apps on the Play Store. While the Android and iOS fanbase can be found constantly at war over the advantages one offers as compared to the other, there is one place where iOS wins by miles. We are talking about security with the latest malware discovered by Kaspersky Lab among an app on the Play Store…
https://www.hackread.com/play-store-android-malware-disables-play-protect-evade-detection/

Fake Google reCAPTCHA Phishing Attack Swipes Office 365 Passwords
A new phishing attack targeted Microsoft users has emerged, according to researchers. The phishing campaign seeks to steal Office 365 credentials via leveraging a fraudulent Google reCAPTCHA system. The operation appears to be sophisticated due to the reCAPTCHA ploy and top-level domain landing pages featuring logos of the victim's companies… https://threatpost.com/google-recaptcha-phishing-office-365/164566/

A New Sophisticated ZLoader Invoice Scam Arises
Forcepoint reports on a new ZLoader invoicing scheme that uses new techniques in order to infiltrate victim machines. The new techniques show adeptness on the part of the code writers in the form of Microsoft product knowledge…
https://exchange.xforce.ibmcloud.com/collection/465cbffc4d394850dd28e201156b2f6e

Malicious VPN Email And Pop-up Attacks
For many these days, working remotely is part of the new normal of this pandemic era. It's probably also be the first time that staffers are away from the watchful eyes of IT departments, and that's making it easier for hackers to do their jobs. The Census Bureau has reported the average work commute added 200 hours a year to our jobs, making it easy to see why many staffers are content to swap out their daily commutes. But beware! Researchers have discovered a fake VPN scam that specifically targets remote employees…
https://www.sosdailynews.com/news.jspx?&articleid=F19A1646D119E3BDFEF8C02A2DCB8B6F&sx=79

Recent Zoom-Themed Phish
Cofense reports on yet another Zoom-themed phishing campaign using the video conferencing software as a ruse to steal Microsoft credentials…
https://exchange.xforce.ibmcloud.com/collection/eeab6293e2692456c066edfa46d16896

****

Hints & Tips plus Security Awareness

Why IRS Texts and Emails Signal a Tax Scam
Fraudsters launch new tax scams and revive old ones, Crooks are using three new tax scams to defraud victims and steal their identity information, while continuing to rely on dozens more well-tested tricks…
https://scambusters.org/taxscam2021.html

Be Sure you have an Endpoint Security Vendor and Solution with the Right Answers
On Monday, March 2, 2021, Microsoft publicly announced that the HAFNIUM APT group (a state-sponsored attack group operating out of China) is actively exploiting on-premises versions of Microsoft Exchange Server in limited and targeted attacks by utilizing 0-day vulnerabilities that expose Microsoft's customers to remote code execution attacks, without requiring authentication…
https://www.cynet.com/blog/china-chopper-observed-in-recent-ms-exchange-server-attacks/?utm_content=156492093&utm_medium=social&utm_source=linkedin&hss_channel=lis-Y-mziLszYY

Credential exposure trends: You need a better password
SpyCloud researchers recovered more than 4.6 billion pieces of personally identifiable information and nearly 1.5 billion stolen account credentials from 854 breach sources in 2020, the company announced in its 2021 Credential Exposure Report… https://www.helpnetsecurity.com/2021/03/05/credential-exposure-trends-2020/

NIST Cybersecurity Framework: A cheat sheet for professionals
The US National Institute of Standards and Technology's framework defines federal policy, but it can be used by private enterprises, too. Here's what you need to know…
https://www.techrepublic.com/article/nist-cybersecurity-framework-the-smart-persons-guide/?ftag=TREa988f1c&bhid=78480402&mid=13292271&cid=712423569

Microsoft's MSERT Tool Can Now Detect Exchange Server Indicators of Compromise
Microsoft has updated its MSERT security scanning tool that enables it to detect web shell scripts used in the recent Exchange Server attacks…
https://www.bleepingcomputer.com/news/security/microsofts-msert-tool-now-finds-web-shells-from-exchange-server-attacks/

****

News & Views

Aon: Cyber insurance prices may rise as much as 50%
The pricing of cyber insurance policies could jump between 20% to 50% this year, as ransomware events lead to heightened claim severity and frequency, according to an Aon report. Key areas of concern include cyberextortion, vendor risks, and errors-and-omissions exposures arising from digital transformation efforts, the report says…
https://www.businessinsurance.com/article/20210304/NEWS06/912340248/Cyber-insurance-rates-to-increase-20-50-this-year-Aon

What Virginia's Consumer Data Protection Act means for your privacy program
And maybe your information security program. The new law will take effect Jan. 1, 2023, the same day as the California Privacy Rights Act proposition that amends the California Consumer Privacy Act…
https://iapp.org/news/a/what-the-virginia-consumer-data-protection-act-means-for-your-privacy-program/

Password Spraying: How Common Passwords Threaten Your Organization
When hackers target your organization with a password spraying attack, hackers are betting that one (or more) of your employees is logging in with a commonly used password. Luckily, there are a few simple, proactive steps you can take to mitigate password spray attacks and other credential-based attacks to protect your client and employee accounts… https://www.enzoic.com/password-spraying/?utm_medium=email&_hsmi=114800630&_hsenc=p2ANqtz-82nlnXLoDJx4U-H15rekmauLQiQB0YLKRi4LXcD9x7vzoiZ5TNPx5G8KIG49IsrRHC5ohC6frvg-DQymxMp6yj7tE6lg&utm_content=114799135&utm_source=hs_email

RoboKill the robocall?
The search for the Death Star that will destroy illegal robocalls once and for all is still underway, but the solution is one step closer. The FTC just announced that judges have selected winners in Robocalls: Humanity Strikes Back, a contest to come up with tech tools to further the fight against annoying pre-recorded calls. The winner: a mobile app that blocks and forwards robocalls to a crowd-sourced honeypot. But the contest has broader implications for business…
https://www.ftc.gov/news-events/blogs/business-blog/2015/08/robokill-robocall

****

"Ctrl -F" for The Board

Guidance on Remediating Networks Affected by the SolarWinds and Active Directory/M365 Compromise Since December 2020, CISA has been responding to a significant cybersecurity incident involving an advanced persistent threat (APT) actor targeting networks of multiple U.S. government agencies, critical infrastructure entities, and private sector organizations. The APT actor added malici…
https://us-cert.cisa.gov/ncas/current-activity/2021/03/09/guidance-remediating-networks-affected-solarwinds-and-active

How Va.'s privacy law stacks up with Calif.'s
Six attorneys from Crowell & Moring dissect the second major privacy law at the US state level, Virginia's Consumer Data Protection Act. This article tackles the differences and similarities between the new Virginia law and its predecessor in California…
https://www.retailconsumerproductslaw.com/2021/03/virginia-consumer-data-protection-act-s-b-1392/

Report: Boards poorly informed about cybersecurity
Publicly traded companies may be putting themselves at risk by under-reporting "actionable" cybersecurity conditions to regulators and shareholders, states a report from SecurityScorecard and other groups. "Board members find these reports off-putting—poorly written and overloaded with acronyms and technical shorthand," the report found, resulting in a "struggle to get a sense of the overall risk status of the organization..." https://www.scmagazine.com/home/security-news/data-breach/public-companies-may-not-grasp-responsibility-to-investors-in-sharing-info-on-cyber-risk/

Questions
Contact FIPCO's Ken Shaurette at 800/722-3498 ext. 251 or email FIPCO IT Services for more information.

"Make Security Part of You and Your Institution's DNA!"

Threat Intelligence Newsletter: March 22, 2021

FIPCO®
IT Audit
Round Table
Discussions

If you would like to host an event, please contact: Amy Petersen

Upcoming Threat Intelligence Peer Group Discussions
None available at the current time

****

Alerts & Warnings

DoS attacks surge as cybercriminals take advantage of the pandemic
DDoS attacks reached a record high during the pandemic as cybercriminals launched new and increasingly complex attacks, a Link11 report reveals. https://www.helpnetsecurity.com/2021/03/18/ddos-attacks-pandemic/

Mimecast Says SolarWinds Hackers Stole Source Code:
Email security company Mimecast says the SolarWinds hackers have stolen some of its source code, but it does not believe its products have been impacted. https://www.securityweek.com/mimecast-says-solarwinds-hackers-stole-source-code

$4,000 COVID-19 'Relief Checks' Cloak Dridex Malware
Cybercriminals have been taking advantage of the American Rescue Plan, the recently signed Covid-19 relief legislation. Researchers at Cofense found that threat actors are impersonating the IRS to distribute emails donning the agency's official logo originating from a spoofed domain. The emails ask users to click on a malicious link. https://threatpost.com/covid-19-relief-checks-dridex-malware/164853/

Exchange Cyberattacks Escalate as Microsoft Rolls One-Click Fix
According to researchers, a slew of dangerous attacks against Microsoft Exchange Serves are accelerating following the public disclosure of the ProxyLogon security bugs group. The incident may also be motivated by public proof of concepts that have emerged, giving attackers a step-by-step guide to exploiting the ProxyLogon flaw. The entire. https://threatpost.com/microsoft-exchange-cyberattacks-one-click-fix/164817/

****

Hints & Tips plus Security Awareness

Your Choices When a Free Password Manager Starts Charging
A big shakeup in the world of password managers is about to take place. One of the most popular of them all, which used to be free, has started charging users. And, like most security software these days, it's a recurring charge, which potentially means you'll be paying for the rest of your computing life. SCAMBUSTERS. https://scambusters.org/passwordmanager.html

Spotting scammy emails
Let’s say you get an email about a charge to your credit card for something you aren’t expecting or don’t want. Your first instinct may be to immediately call the company or respond to the email and to stop the payment. Scammers know that, and are taking advantage of it in a new phishing scheme.
https://www.consumer.ftc.gov/blog/2021/03/spotting-scammy-emails?utm_source=govdelivery

****

News & Views

Expert predicts delayed effects from a difficult 2020
The ransomware attacks of 2021 "will have a much more visible impact on the physical world," predicts Ilia Sotnikov, an executive at Netwrix. Among Sotnikov's other key trends to watch: Delayed effects from the sudden and wrenching digital transformations of last year, when "[o]rganizations had to prioritize service availability over security." https://informationsecuritybuzz.com/articles/top-seven-cybersecurity-ripple-effects-from-2020/

Why protecting a business includes the supply chain
The Industry 4.0 era has brought about unprecedented arrays of cyberattacks, meaning every company should have stated policies, particularly involving vendors, writes Joseph Chukwube, founder of a digital marketing agency. Such measures might "require redesigns of the core process architecture," Chukwube adds. https://www.business2community.com/cybersecurity/best-practices-for-supply-chain-cybersecurity-in-2021-02391360

Consumers aware of security concerns, but not doing much to change password habits
The recent remote work trend caused by the pandemic has increased password security risks of both companies and individuals. Despite this fact, Americans continue to put personal life and businesses at risk by using the same passwords for both home and work.
https://www.helpnetsecurity.com/2021/03/18/change-password-habits/

****

"Ctrl -F" for The Board

How the CISO can garner support from senior management
Chief information security officers need the support of executive leadership for their security teams to thrive. Building that support requires establishing trust in security as a business enabler, a process that requires patience and discipline. https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2021/how-the-ciso-can-build-support-from-senior-management

8 areas of expertise every board should have
Corporate governance at the board level now requires expertise on risk management and technology, write Glenn Davis and Ivan Garces of accounting and consulting firm Kaufman Rossin. Davis and Garces outline eight specific areas of expertise boards should have, starting with expertise in government partnerships and procurement regulations. https://www.directorsandboards.com/news/what-will-post-pandemic-board-directors-look

Questions
Contact FIPCO's Ken Shaurette at 800/722-3498 ext. 251 or email FIPCO IT Services for more information.

"Make Security Part of You and Your Institution's DNA!"

Threat Intelligence Newsletter: March 26, 2021

FIPCO®
IT Audit
Round Table
Discussions

If you would like to host an event, please contact: Amy Petersen

Upcoming Threat Intelligence Peer Group Discussions
None available at the current time

****

Alerts & Warnings

Fintech Giant Fiserv Used Unclaimed Domain
If you sell Web-based software for a living and ship code that references an unregistered domain name, you are asking for trouble. But when the same mistake is made by a Fortune 500 company, the results can range from costly to disastrous. Here's the story of one such goof committed by Fiserv a $15 billion firm that provides online banking software and other technology solutions to thousands of financial institutions… https://krebsonsecurity.com/2021/03/fintech-giant-fiserv-used-unclaimed-domain/

Slow Browser? It May Have Been Hijacked By Malware
Before calling your internet provider to complain about a slow browser think about this: It's no secret malware loves to hide in all kinds of things like adware, spyware, scareware, and fake browser updates. Finding your browser is not only slow, but also acting strangely is a sign something isn't quite right. If after going through the internet provider's standard toolbox for troubleshooting doesn't help, it's time to think about malware…
https://www.sosdailynews.com/news.jspx?&articleid=0077236D4FEF9D451A78E05A13E58B15&sx=79

CopperStealer Malware Targets Facebook and Instagram Business Accounts
A new password and cookie stealer malware called CopperStealer has emerged, targeting accounts of tech giants such as Apple, Google, Amazon, and Facebook. According to researchers, the malware operators have hijacked the online accounts existing within these entities since 2019, later using them for criminal activities. The operation has gone… https://threatpost.com/copperstealer-hijacks-accounts/164919/

Five Months After Takedown Attempt, CISA and FBI Warn of Ongoing TrickBot Attacks
The Cybersecurity and Infrastructure Security Agency (CISA) and FBI have warned of an uptick in attacks deploying the TrickBot malware, largely utilizing phishing campaigns as the initial infection vector. The two entities released a joint advisory to the public on Wednesday, alerting individuals of the sophisticated attacks. According to the… https://www.securityweek.com/five-months-after-takedown-attempt-cisa-and-fbi-warn-ongoing-trickbot-attacks

Fraudsters jump on Clubhouse hype to push malicious Android app
Popular new app Clubhouse is being impersonated in a campaign pushing a fraudulent and malicious copycat to Andriod users. There is currently no Andriod version of the app, allowing scammers to falsely advertise the fake copy as the new Android version. The app recently gained popularity after Elon Musk tweeted… https://www.zdnet.com/article/fraudsters-jump-on-clubhouse-hype-to-push-malicious-android-app/

Latest Mirai Variant Targets SonicWall, D-Link and IoT Devices
A new Mirai variant is targeting known flaws in D-Link, Netgear and SonicWall devices, as well as newly-discovered flaws in unknown IoT devices… https://threatpost.com/mirai-variant-sonicwall-d-link-iot/164811/

Ignore bogus COVID vaccine survey
Scammers are using a new trick to steal your money and personal information: a bogus COVID vaccine survey… https://www.consumer.ftc.gov/blog/2021/03/ignore-bogus-covid-vaccine-survey?utm_source=govdelivery

Purple Fox malware evolves to propagate across Windows machines
An upgraded version of the Purple Fox malware, which has been around since 2018, has been observed in a new aggressive and expanding campaign. The malware historically relied on exploit kits and phishing emails to spread until recently when researchers found a weeks-long campaign that utilized the malware variant. The… https://www.zdnet.com/article/purple-fox-malware-evolves-to-propagate-across-windows-machines/

Active Exploits Hit WordPress Sites Vulnerable to Thrive Themes Flaws
Attackers are currently targeting WordPress users who have not implemented patches to their plugins. Thrive Themes, a company that offers various products connected to WordPress, recently released patches for vulnerabilities within its services. However, researchers found that users who have failed to implement the fixes are being actively targeted by… https://threatpost.com/active-exploits-wordpress-sites-thrive-themes/165013/

****

Hints & Tips plus Security Awareness

Serious Google Chrome Zero-Day Exploits Fixed; Update Your Browser Now
Google is in the news today and within a month of the last time regarding a more and more familiar topic. That is another zero-day flaw in its Chrome browser. This one is also being actively exploited by attackers. And as is usual protocol with Google, very little information is being provided at the moment. The company is waiting until the majority of users get their browsers updated before providing too many juicy details to would-be attackers…
https://www.sosdailynews.com/news.jspx?&articleid=31EA09E2EB632D5E1FD9D28E014B33DC&sx=79

What Is A VPN And Do I Need One At Home
VPNs have been discussed before, but sometimes it’s good to refresh your memory about technology. There’s been a lot of talk about these mysterious VPNs-Virtual Private Networks-lately, especially with the increase in working from home. It’s become a rather common thing. Facebook announced that…
https://www.sosdailynews.com/news.jspx?&articleid=DE7C8BAE9749DBD80595477E3D4B60BB&sx=79

How to stay ahead of the rise of synthetic fraud
While banks have been successful in reducing card fraud in recent years, a new and rising threat has emerged: synthetic identity fraud. By combining real and falsified information on digital platforms, financial criminals have been able to commit this type of fraud with impunity…
https://www.helpnetsecurity.com/2021/03/22/synthetic-fraud/

Review the SolarWinds attack on a timeline – On Demand Webinar
From attack penetration and manipulation of the company’s development build process, followed by the injection of the malware, to the mass infection of companies globally; Investigate the SolarWinds aftermath - including follow-up vulnerabilities that were exposed in SolarWinds’ software and their ramifications; Predict the evolvement of supply chain attacks – are nation states already today pinpointing key suppliers and working to gain a foothold for the future D-day?; Defense measures to be applied - ensure you’re not a victim of a supply chain attack even though you have no visibility or control over your supplier’s security… https://go.cynet.com/hubfs/Sunburst-Webinar.mp4?utm_medium=email&_hsmi=2&_hsenc=p2ANqtz-_Yu54In4Dl--VTKXHtfzqdAa7vE4I9GkU9OafZfl_Q3NZGRlMGTsqVxpQa42fDht9S2G8zWYGc2f3hyh-jK8xgwXbWqA&utm_content=2&utm_source=hs
email for answers to questions or options to expand your endpoint protection email itservices@fipco.com

No Spying! Why You Need An Authenticator Phone App
Think you're safe using a security check like two-step verification when you sign on to an app or website? You may not be, according to a tech expert at Microsoft. But you can increase your security by choosing the right verification method.
Two-step verification is a process in which you're asked to key in some extra information in addition to your password. Sometimes, it's referred to as multi-factor authentication (MFA).
We explained how it works in an earlier issue: https://scambusters.org/passwordsecurity2.html. But, in simple terms, it blocks crooks' attempts to sign on to accounts using stolen usernames and passwords...
https://scambusters.org/authenticator.html

Cybersecurity for the Small Business Owner
The internet is a digital highway that facilitates nearly all aspects of modern life. Just as ancient traders had to deal with bandits, every small business with an online presence is vulnerable. Cybersecurity challenges range from minor nuisances to large scale crippling attacks by bad actors…
https://blog.nxtsoft.com/cybersecurity-for-the-small-business-owner?utm_campaign=ThreatAdvice%20Partners&utm_medium=email&_hsmi=117538560&_hsenc=p2ANqtz82rXzYu1eTQjZLoV1OAE4KK2P5XTaDZ1x9cuMVb0YRhGC3cFc4ydPEHWLdSwtlIvOPVeQyvLhqLqDzTpcGj0d22pnklA&utm_content=117473520&utm_source=hs_email

****

News & Views

Time for financial companies to rise to the occasion

Financial service organizations should see emerging opportunities along with emerging threats from cybercriminals, argues Jodi Chavez of Tatum, a talent and consulting firm. "Those that are able to demonstrate advanced technical capabilities as part of their core accounting function should stand to gain a distinct competitive advantage," Chavez writes… https://www.cpapracticeadvisor.com/firm-management/article/21212424/get-off-the-hackers-hit-list-evolving-competencies-for-finance-firms-today

2020 to 2022 Emerging Technology Roadmap

Midsize EnterprisesIT professionals from 218 midsize enterprises (MSEs) collaborated to map the adoption of 112 emerging technologies by deployment stage, deployment risk and enterprise value… https://www.ebulletinsresources.com/hubfs/D1/Gartner/emerging-tech-roadmap-mse-2020-2022.pdf?hsCtaTracking=bfc50a2f-57bd-46d2-8cff-19458c18afb5%7C9b1dda28-4722-424f-a0ad-f93bf670330b

NIST Releases Practice Guide for BYOD Security

The National Institute of Standards and Technology’s National Cybersecurity Center of Excellence released the NIST Cybersecurity Practice Guide Special Publication 1800-22 Mobile Device Security: Bring Your Own Device…
https://www.nccoe.nist.gov/projects/building-blocks/mobile-device-security/bring-your-own-device?utm_campaign=RiskCyber-20210323&utm_medium=email&utm_source=Eloqua

****

"Ctrl -F" for The Board

5 ways the pandemic changed security at the edge

Pandemic-related events of the past year have set the table for permanent changes in computing at the edge, writes Bruce Kornfeld of StorMagic. Kornfeld highlights five trends, including "secure by default" practices for a remote workforce that uses virtual networks and multifactor authentication…
https://www.eweek.com/security/how-2020-forever-changed-security-at-the-edge/

Questions
Contact FIPCO’s Ken Shaurette at 800/722-3498 ext. 251 or email FIPCO IT Services for more information.

"Make Security Part of You and Your Institution's DNA!"

Threat Intelligence Newsletter: April 9, 2021

FIPCO® IT Audit Round Table Discussions

If you would like to host an event, please contact: Amy Petersen

Upcoming Threat Intelligence Peer Group Discussions
None available at the current time

NCCoE Learning Series Webinar: What's Ahead from NIST in Cybersecurity and Privacy?
What do government agencies, private-sector organizations, and others need to know about the National Institute of Standards and Technology's (NIST's) approach to cybersecurity and privacy-related matters in 2021 and beyond?... https://event.on24.com/eventRegistration/console/EventConsoleApollo.jsp?&eventid=2958993&sessionid=1&username=&partnerref=&format=fhvideo1&mobile=false&flashsupportedmobiledevice=false&helpcenter=false&key=27829987C1F14CCA9838624EEAF5D530&text_language_id=en&playerwidth=1000&playerheight=1000&overwritelobby=y&newConsole=true&nxChe=true&newTabCon=true&eventuserid=426581375&contenttype=A&mediametricsessionid=367898184&mediametricid=4138554&usercd=426581375&mode=launch

Give yourself some credit (reports)
One important back-to-basics step you can take this Financial Literacy Month (or anytime) is checking your credit report... https://www.consumer.ftc.gov/blog/2021/04/give-yourself-some-credit-reports?utm_source=govdelivery

****

Alerts & Warnings

DDoS attacks in 2021: What to expect?
We're only three months into 2021, and Akamai has mitigated 3 out of the 6 largest DDoS attacks they have ever witnessed. Two of these hit the same company on the same day, and the attackers' goal was extort money from the target… https://www.helpnetsecurity.com/2021/03/30/2021-ddos/

College Students Targeted in Newest IRS Scam
The Internal Revenue Service (IRS) has warned of a scam targeting college students. The scam is a phishing attempt in which the perpetrators are posing as the IRS with subject lines such as “Tax Refund Payment,” according to a warning released by the agency. The IRS sought to alert educators… https://www.darkreading.com/vulnerabilities---threats/college-students-targeted-in-newest-irs-scam/d/d-id/1340558

Why passwords are to blame for loss of revenue, identity attrition and poor customer experiences
Transmit Security has released a state of customer authentication report that includes customer experience insights based on its survey of 600 U.S. consumers. According to the report findings, organizations are losing potential customers and a substantial amount of revenue due to their dependency on traditional password systems and outdated customer authentication models… https://www.helpnetsecurity.com/2021/04/01/dependency-on-traditional-password-systems/

FBI & CISA Warn of Active Attacks on FortiOS Vulnerabilities
The FBI and the Department of Homeland Security’s Cybersecurity and Infrastructure Security Agency have issued a joint advisory warning administrators that APT groups are currently exploiting three different vulnerabilities that existing the Fortinet FortiOS. News of the active exploits was allegedly broken to the public… https://www.darkreading.com/risk/fbi-and-cisa-warn-of-active-attacks-on-fortios-vulnerabilities/d/d-id/1340579

New IRS imposter scam targets college students and staff
If you’re a college student, faculty, or staff member, you’re going to want to pay attention to this one. IRS imposters are sending phishing emails to people with “.edu” email addresses, saying they have information about your “tax refund payment.” What do they really want? Your personal information… https://www.consumer.ftc.gov/blog/2021/04/new-irs-imposter-scam-targets-college-students-and-staff?utm_source=govdelivery

Fake LinkedIn job offers scam spreading More_eggs backdoor
According to researchers, threat actors are using zip files to trick LinkedIn users into executing the More_eggs backdoor… https://www.hackread.com/fake-linkedin-job-offers-scam-more-eggs-backdoor/

Don’t Click That Link: SMS Scams
In October 2020, the Satori team received several text messages (all to the same phone number) claiming that the recipient had won a MacBook Pro. The messages were all from different numbers with links that had different .info domains and were recently registered, according to Domain Registration records… https://www.humansecurity.com/blog/dont-click-that-link-sms-scams?utm_medium=email&_hsmi=119935181&_hsenc=p2ANqtz--XaiHEydJk8YMJyIsHot8j_w4AEkTo2M-iK3YE5Xc_XSM9ChPJsRaV4SzH6t6pBcMeq1RXIAhx_OlZXDKxF3d-cS0xEw&utm_content=119935181&utm_source=hs_email

Is It Genuine? Check That Photo with Reverse Image Search
Are you looking online a new home, a pet, or maybe a collectible item? Or perhaps you're seeking any one of hundreds of other items that call for a photo to convince you to commit.
But chances are you've already heard about how fake photos are being used by scammers to trick victims into parting with their money. It's not as tough as it sounds because you can do it on Google and one or two other sites with just a couple of clicks. You upload the photo at Google Images (https://images.google.com) and the web giant will look virtually everywhere to see if it can find a match. reverse image searching is not guaranteed to identify fake photo scams. But it's an important weapon in the never-ending fight against these fraudsters… https://scambusters.org/reverseimage.html

Reverse Image search for your phone… https://www.cnet.com/how-to/google-reverse-image-search-for-your-phone-or-browser-how-to-do-it-and-why/

Cybersquatting: Attackers Mimicking Domains of Major Brands Including Facebook, Apple, Amazon and Netflix to Scam Consumers
Users on the internet rely on domain names to find brands, services, professionals and personal websites. Cybercriminals take advantage of the essential role that domain names play on the internet by registering names that appear related to existing domains or brands, with the intent of profit…
https://unit42.paloaltonetworks.com/cybersquatting/

****

Hints & Tips plus Security Awareness

Password Auditing - Need Help Auditing for Compromised Passwords?
A Quick & no cost Password Auditing Tool Password audits have become more difficult as new data breaches expose credentials every day. These passwords are quickly fed into hackers' cracking dictionaries, changing which passwords you need to keep out of your organization. Based on our audit of over 1,000 corporate domains and over 1.5 million user accounts, nearly 20% of real-world corporate user accounts were highly vulnerable to password attacks due to weak or compromised passwords…
https://www.enzoic.com/password-auditing-tool/?utm_campaign=SWaudit&utm_source=hs_email&utm_medium=email&_hsenc=p2ANqtz-962Xq74QvNn8JssxJ_SZX3GTraG0QOBEdqR4bmT7P-tZI3FS8-GpXFM4Zj9A3cIAk76oH-

CISA Adds Two Web Shells to Exchange Server Guidance
The Department of Homeland Security's Cybersecurity and Infrastructure security agency (CISA) updated its' guidance for ongoing Microsoft Exchange Server security issues. The guidance includes two new Malware Analysis Reports. Both reports are included in the "Mitigate Microsoft Exchange Server Vulnerabilities" and identifies a Web shell in compromised exchange servers. CISA…
https://www.darkreading.com/risk/cisa-adds-two-web-shells-to-exchange-server-guidance/d/d-id/1340525

Should I, Could I Freeze My Credit Report?
Having your private information or identity stolen is no picnic. It takes quite a long time to make it right, so one of the best ways to help ensure that neither happens in the first place is to protect it as much as you can. In light of the recent Capital One data breach, many may be considering putting a freeze on their credit reports and that is a great idea. But, be sure to know what that means before taking that action…
https://www.sosdailynews.com/news.jspx?articleid=%20105F18D0F86495FB473FE2FD7116A273

Does your smartphone have a spyware?
To run its services, a mobile application requires to access some information on the device hosting it, including some about its user. While most apps could properly work by only accessing and using these data locally, 65% of them are actually programmed to send the collected information out of the devices…
https://www.pradeo.com/media/infographic-spyware-en.pdf

ISCMA: NIST An Information Security Continuous Monitoring Program Assessment
The ISCMAx tool available under Supplemental Material is a macro-enabled Microsoft Excel application that runs on Windows-based systems only. ISCMAx is not intended to be a production-level product… https://csrc.nist.gov/publications/detail/nistir/8212/final

“MITRE Madness”: A Guide to Weathering the Upcoming Vendor Positioning Storm
The few weeks of early April and the days after April 20th have become “MITRE Madness” for the cybersecurity industry. After the MITRE ATT&CK evaluation results are published, a gaggle of vendors rush to spin their results in blogs, whitepapers, webinars, articles and more trying to position themselves as the best…
https://info.cynet.com/preparing-for-mitre-madness-webinar/?utm_content=160959317&utm_medium=social&utm_source=linkedin&hss_channel=lis-Y-mziLszYY

A Quick & Free Password Auditing Tool
Password audits have become more difficult as new data breaches expose credentials every day. These passwords are quickly fed into hackers’ cracking dictionaries, changing which passwords you need to keep out of your organization… https://www.enzoic.com/password-auditing-tool/?utm_medium=email&_hsmi=120103429&_hsenc=p2ANqtz-8uXafNyUJkyGH-F13JvLjpK6I3bkwmlSPTjVFRjqIcfsuz-78x8jISP9hZOAMD-jLDPiHAG9Y5cJ-gpoDL8OBrfo5CQQ&utm_content=120085715&utm_source=hs_email

5 key cybersecurity risks in 2021, and how to address them now
With an unexpected year of massive change behind us, many organizations have now an extensive remote workforce, new technologies in use, and digital transformation under way across the board. While this has introduced many opportunities for SMBs, it has also come with a host of cybersecurity challenges…
https://www.helpnetsecurity.com/2021/04/02/key-cybersecurity-risks-2021/

Want to get around a CAPTCHA? That’ll be 0.00094c, please
Shopping or booking an appointment online can seem increasingly like busywork. Please prove that you’re not a bot: select all the photos that show traffic lights. Do some light arithmetic. Squint and retype these increasingly indecipherable letters (“Is that a lowercase H or a lowercase B?”)
https://www.helpnetsecurity.com/2021/04/01/get-around-captcha/

How to use the new HTTPS-Only mode in Firefox
Firefox's new feature automatically redirects from HTTP to HTTPS and should be considered a must-use for the security-minded. Jack Wallen explains, and shows you how to enable it…
https://www.techrepublic.com/article/how-to-use-the-new-https-only-mode-in-firefox/?ftag=TREa988f1c&bhid=78480402&mid=13324369&cid=712423569

Top 10 Brands Spoofed In Phishing Attacks
The numbers don’t lie, but cybercriminals sure do. A recent report by Vade Secure shows a dramatic uptick in spoof email phishing. Amazon alone is up over 400% in one year, taking the number eight spot in most-targeted brand spoofs. Phishing emails are at the heart of spoofing, and the URL website links in the emails lead to fake websites that look like the real deal. Some of our country’s biggest and best-known companies are being used as spoof bait…
https://www.sosdailynews.com/news.jspx?&articleid=52FE7D76C2C33CE89DC73D57EDC9C827&sx=79

****

News & Views

What Changes Do We Need To See In eDiscovery?
Three parts with the third being "How to deal with Structured Data". In case you missed it, all three parts are listed below for reference:
#1 - https://www.forensicfocus.com/articles/what-changes-do-we-need-to-see-in-ediscovery-part-vii/
#2 - https://www.forensicfocus.com/articles/what-changes-do-we-need-to-see-in-ediscovery-part-viii/
#3 - https://www.forensicfocus.com/articles/what-changes-do-we-need-to-see-in-ediscovery-part-ix/

Free Email Service Can Be Very Costly
Those pesky scam emails directed at you, whether for your personal or business account, are being aided by unlikely sources. So far this year, Gmail, AOL, and Yahoo email services, among others, inadvertently helped hackers scam almost 6,600 enterprise organizations, according to a study by Barracuda Networks. The rate in which they facilitate business email compromise (BEC) attacks is alarming. Since April of this year over a four-month period, malicious email accounts using these providers accounted for 45% of all BEC attacks…
https://www.sosdailynews.com/news.jspx?&articleid=98F6E1FC24D3BC1AAE563AED91A27136&sx=79

Online Retail Biggest Hacking Target: 154% Increase And Growing
Adapting to the everyday limitations during coronavirus has opened a Pandora's Box for cybercriminals. Navigating life online has arguably made some thi…
https://www.sosdailynews.com/news.jspx?articleid=%20A9BC8D121362D501AEB7C6DADA91077C

93% of consumers concerned about data security when filling out online forms
Source Defense provides in-depth analysis of the client-side threat landscape and specific attacks like formjacking, Magecart and web browser threats… https://www.helpnetsecurity.com/2021/03/30/data-security-online-forms/

Facebook data of 500M+ users from 106 countries leaked online
The data was leaked earlier today (03 Apr 2021) on an infamous hacker forum without users' Facebook accounts passwords. What does this mean to your institution. Greater chance that customers will be defrauded as hackers bypass validation questions used in online registration…
https://www.hackread.com/facebook-data-users-106-countries-leaked-online/

The impact of the CCPA on companies' privacy practices
A new DataGrail report examined how millions of California consumers are exercising their privacy rights – to access their data, delete their data, and stop the sale of their data to a third-party – according to the CCPA, which went into effect on January 1, 2020…
https://www.helpnetsecurity.com/2021/04/05/consumers-ccpa-privacy-practices/

Ignoring Your Credit Report Can Be Very Costly Indeed
As you're reading this, a cyberthief could be buying a new car with your credit. It could be the beginning of a massive spending spree on your dime, and in the end, there may be very little left of your funds and your credit. Hacker's with access to financial accounts can do significant damage to your credit, quickly and with anonymity. In this unprecedented time of coronavirus and a historic level of hacking, there's never been a more crucial time to pay attention to your credit report…
https://www.sosdailynews.com/news.jspx?&articleid=38B51807FBD3C6C516C0464A5B9B7F22&sx=79

Zero Trust creator talks about implementation, misconceptions, strategy
A little over a decade ago, John Kindervag outlined the Zero Trust security model. As a VP and Principal Analyst on the Security and Risk Team at Forrester Research, he spent years doing primary research and the result was a new model of trust, a new approach to cybersecurity, and a security strategy designed to stop the mounting data breaches… https://www.helpnetsecurity.com/2021/04/06/john-kindervag-zero-trust/

Office Depot Configuration Error Exposes One Million Records
Researchers have found a misconfigured Easticsearch server belonging to Office Depot, a popular office supplies store chain. One million customers' personal information was exposed on the misconfigured server, according to researchers. The database was not protected by a password and was initially found by a Website Planet team on March… https://www.infosecurity-magazine.com/news/office-depot-configuration-error/

Facebook tackles deepfake spread and troll farms in latest moderation push
Earlier this week, Facebook published its latest Coordinated Inauthentic Behavior report, in which it listed its most recent efforts to curb coordinated illegitimate behavior across the social media platform. According to the report, Facebook investigated and wiped out a long-running troll farm located in Albania with a widespread impact. The… https://www.zdnet.com/article/facebook-tackles-deepfake-spread-and-troll-farms-in-latest-moderator-report/

4 Biggest Challenges to Third-Party Risk
Join CyberGRX and Compliance Week as we break down the SolarWinds Cyber Attack, and discuss preventative measures to ensure your ecosystem is secure…
https://info.cybergrx.com/thank-you-solar-winds-webinar?submissionGuid=f37e0863-3089-460b-9b2b-31596dcef1b7&__hstc=&__hssc=&hsCtaTracking=4a44d73a-76c1-4076-b122-

****

"Ctrl -F" for The Board

Corporate doxing is on the rise: Here's how hackers are doing it and how to stop them
Doxing is the act of harvesting confidential information about someone in order to inflict harm or gain some benefit using that info. Traditionally thought to be a risk for individuals, Kaspersky reports that it's increasingly being used to target corporate employees: 1,646 unique instances of one particular type of attack were detected by Kaspersky in February 2021, alone...
https://www.techrepublic.com/article/corporate-doxing-is-on-the-rise-heres-how-hackers-are-doing-it-and-how-to-stop-them/?ftag=TREa988f1c&bhid=78480402&mid=13316581&cid=712423569

Board directors need to play an active role in protecting their org from cyber risks
Cybersecurity failure is a "clear and present danger" and critical global threat, yet responses from board directors have been fragmented, risks not fully understood, and collaboration between industries limited, according to a WEF report… https://www.helpnetsecurity.com/2021/03/31/board-directors-cybersecurity-role/

Alarming number of consumers impacted by identity theft, application fraud and account takeover

A new report, developed by Aite Group, and underwritten by GIACT, uncovers the striking pervasiveness of identity theft perpetrated against U.S. consumers and tracks shifts in banking behaviors adopted as a result of the pandemic… https://www.helpnetsecurity.com/2021/03/15/consumers-impacted-by-identity-theft/

Fed issues ‘synthetic identity fraud’ definition

Synthetic identity fraud is reported to be the fastest-growing type of financial crime (Off-site) in the United States, accounting for billions in losses annually. Moreover, the use of multiple definitions for synthetic identity fraud throughout the industry poses a fundamental problem – inconsistent categorization and reporting, making it difficult to identify and mitigate this type of fraud. The Federal Reserve issued a recommended definition of “synthetic identity fraud” after convening an industry group… https://fedpaymentsimprovement.org/news/blog/synthetic-identity-fraud-defining-it-to-fight-it/?utm_campaign=NewsWatch%20Today&utm_medium=email&_hsmi=120404554&_hsenc=p2ANqtz-_104TTJN4LSFASeuzgXjAqRnzPQdJMOsrrxyGQmKB6XvQMv9tHq4K6Ek8mJo_JPWg1x1xIQRUKyX5QMjfCAJbIxbrbxw&utm_content=120403074&utm_source=hs_email

Questions

Contact FIPCO’s Ken Shaurette at 800/722-3498 ext. 251 or email FIPCO IT Services for more information.

"Make Security Part of You and Your Institution's DNA!"

Threat Intelligence Newsletter: April 19, 2021

FIPCO®
IT Audit
Round Table
Discussions

If you would like to host an event, please contact: Amy Petersen

Upcoming Threat Intelligence Peer Group Discussions
None available at the current time

****

Alerts & Warnings

2 scraped LinkedIn databases with 500m and 827m records sold online
Although, none of the databases contain LinkedIn users' passwords; the data in the records is enough for cybercriminals to carry out a number of attacks including SIM Swapping, identity scams, phishing, and SMSishing, etc… https://www.hackread.com/linkedin-scraped-databases-sold-online/

If you haven't patched this old VPN vulnerability, assume your network is compromised
The National Cyber Security Center (NCSC) has released a critical security alert detailing how cybercriminals are actively exploiting a Fortinet VPN vulnerability to distribute ransomware. Kaspersky reported on the flaw earlier this month, stating that criminals are seeking out unpatched systems and are able to exploit the flaw to remotely… https://www.zdnet.com/article/critical-security-alert-if-you-havent-patched-this-two-year-old-vpn-vulnerability-assume-your-network-is-compromised/

Credential Swiping Attacks Target 45% Of Office 365 Users
As corporate hacks become daily events, most users don't realize that as a result, bits and pieces of their identities are available on the dark web. Their PII is listed for sale or for free to hackers, and they're the only ones who know what they'll do with that information. A study by Cofense found 45% of credential swiping targets use Outlook, Teams, and Office 365 as email phishing lures. With approximately 115 million Microsoft Teams users, cybercriminals know Office 365 is a very ripe target… https://www.sosdailynews.com/news.jspx?&articleid=BF57AFCAE2C7A5ACCB5EE215A1AB980A&sx=79

Attackers are using SEO tactics to lure victims onto malicious sites
100,000 malicious Google sites that seem legitimate are being used by attackers to install a remote access trojan and later infect the victim's systems with ransomware, credential-stealers, banking trojans and other malware. The malicious sites contain popular business keywords, including business-form related convincing Google's web crawler that the intended content meets conditions for a high page-rank score, which increases the likelihood that victims will visit the webpage… https://threatpost.com/google-sites-solarmarket-rat/165396/

Copy and Paste Plea Exposes Your Identity
Why you should be wary of Facebook copy and paste requests…
https://scambusters.org/copyandpaste.html

****

Hints & Tips plus Security Awareness

Simplify, Then Add Lightness – Why We Need Simplicity to Better Defend Ourselves
Webinar Overview, the founder of Lotus, claimed he preferred cars that were lighter and easier to drive than horsepower-heavy machines that could barely turn. That simple choice led to accolades across the world and better cars. Today's cybersecurity market faces a similar dilemma – do we continue to build heavily layered security systems with numerous tools that are hyper-specific, if "best-in-class", or is it time to start removing bloated stacks in favor of agility?...https://cynet.easywebinar.live/registration-simplify-then-add-lightness-why-we-need-simplicity-to-better-defend-ourselves?utm_content=162140185&utm_medium=social&utm_source=linkedin&hss_channel=lis-tcrKPWp0hz

Sandboxie Plus
Sandboxie is a sandbox-based isolation software for 32- and 64-bit Windows NT-based operating systems. It is being developed by David Xanatos since it became open source, before that it was developed by Sophos (which acquired it from Invincea, which acquired it earlier from the original author Ronen Tzur). It creates a sandbox-like isolated operating environment in which applications can be run or installed without permanently modifying the local or mapped drive. An isolated virtual environment allows controlled testing of untrusted programs and web surfing… https://sandboxie-plus.com/

****

News & Views

Emotet Trojan Takes Top Spot On Most Wanted Malware Threat List
According to Check Point's Global Threat Index, Emotet trojan is the most widely used and most costly malware in cybercrime today. Since 2014, Emotet has been continually improved and updated over time. According to the Department of Homeland Security, Emotet's dedicated developers have now brought the cost of each security incident close to $1 million to repair. Just that alone makes it easy to see why Emotet is cause for great concern within the cybersecurity and business communities alike…
https://www.sosdailynews.com/news.jspx?&articleid=88C39148626E854714A6A29E5080789A&sx=79

****

"Ctrl -F" for The Board

CISO Guidance ebook Excerpts
Several chapters relating to the rules of Information Security…
https://www.routledge.com/rsc/downloads/CISO_Freebook_Final.pdf

Questions
Contact FIPCO's Ken Shaurette at 800/722-3498 ext. 251 or email FIPCO IT Services for more information.

"Make Security Part of You and Your Institution's DNA!"

Threat Intelligence Newsletter: April 27, 2021

FIPCO®
IT Audit
Round Table
Discussions

If you would like to host an event, please contact: Amy Petersen

Upcoming Threat Intelligence Peer Group Discussions
None available at the current time

****

Alerts & Warnings

CISA: Patch New Exchange Server Vulnerabilities Now (reinforcing the importance) Otherwise be sure you have a more robust endpoint detection and response solution in place.
Included in Microsoft's Patch Tuesday this month are fixes for four additional vulnerabilities in on-premise Exchange Servers. These new flaws were detected by the National Security Agency. The Cybersecurity and Infrastructure Security Agency (CISA) has given US federal agencies until12:01am EDT on Friday, April 16 to deploy the Microsoft updates. Agencies are also required to apply/maintain controls, report completion by noon EDT on April 16, and to immediately report related cyber incidents and indicators of compromise… https://www.bleepingcomputer.com/news/security/nsa-discovers-critical-exchange-server-vulnerabilities-patch-now/

NSA: 5 Security Bugs Under Active Nation-State Cyberattack
The National Security Agency (NSA) has released an alert warning that five vulnerabilities are being actively targeted by nation-state actors. The bugs affect VPN solutions, collaboration-suite software, and virtualization technologies in widely deployed platforms from Citrix, Fortinet, Pulse Secure, Synacor, and VMware. According to the NSA, the goal of the… https://threatpost.com/nsa-security-bugs-active-nation-state-cyberattack/165446/

Credential Swiping Attacks Target 45% Of Office 365 Users
As corporate hacks become daily events, most users don't realize that as a result, bits and pieces of their identities are available on the dark web. Their PII is listed for sale or for free to hackers, and they're the only ones who know what they'll do with that information. A study by Cofense found 45% of credential swiping targets use Outlook, Teams, and Office 365 as email phishing lures. With approximately 115 million Microsoft Teams users, cybercriminals know Office 365 is a very ripe target…
https://www.sosdailynews.com/news.jspx?&articleid=BF57AFCAE2C7A5ACCB5EE215A1AB980A&sx=79

Zero-day vulnerabilities in SonicWall email security are being actively exploited
SonicWall released a security alert on Tuesday stating that they had published fixes to address three critical issues being actively exploited in the wild. The company urged its customers to apply the patches as soon as possible. The vulnerabilities lie in its email security solution, impacting hosted and on-premises email… https://www.zdnet.com/article/zero-day-vulnerabilities-in-sonicwall-email-security-are-being-exploited-in-the-wild/

Alarm Sounds On Danger of QR Codes
Remember when, a few years ago, we reported: "QR code scams are in their early days, but as more and more organizations see the benefit of using these codes, expect the crooks to exploit the same opportunity too." (See https://scambusters.org/qrcode.html) Maybe you don't recall our warning. But that's exactly what's happened, with new alerts about how these scannable "Quick Response" black-and-white boxes of dots and squares are now being used to trick more victims than ever into giving away confidential information or downloading malware… https://scambusters.org/qrcode2.html

****

Hints & Tips plus Security Awareness

Protecting the human attack surface from the next ransomware attack
As we head into 2021, ransomware is making another resurgence, particularly in targeted attacks from highly organized hacker groups. In fact, cybercrime is surging since the start of the pandemic…
https://www.helpnetsecurity.com/2021/04/16/human-attack-surface/

VMWare Privilege escalation vulnerability (CVE-2021-21981)
VMware NSX-T contains a privilege escalation vulnerability due to an issue with RBAC (Role based access control) role assignment. Successful exploitation of this issue may allow attackers with local guest user account to assign privileges higher than their own permission level…
https://www.vmware.com/security/advisories/VMSA-2021-0006.html

Why Autonomous XDR Is Going to Replace NGAV/EDR
Insurance carriers are beginning to include the question on their lists when engaging with prospective insured whether they have replaced their NGAV, why go half way. Lean XDR a step beyond just EDR…
https://www.fipco.com/solutions/it-audit-security/xdr

2020 MITRE’s ATT&CK Results - How do you make heads and tails of them?
MITRE’s ATT&CK results are released! The question is, how do you make heads and tails of them? Thursday 4/29 11 am…
https://cynet.easywebinar.live/mitre-results-apr-thank-you?key=5405b19e3d621e2c16b9788211229b67

What Are “Dark Patterns”?
Harry Brignull coined the term “dark pattern” in 2010, defining it as “a user interface that has been carefully crafted to trick users into doing things, such as buying insurance with their purchase or signing up for recurring bills…” https://teachprivacy.com/dark-patterns-reading-list-and-resources/?utm_source=Opt-in+Newsletter&utm_campaign=441abc8d98-08.25.20_COPY_01&utm_medium=email&utm_term=0_b681bb8bd9-441abc8d98-161074597

Cybersecurity only the tip of the iceberg for third-party risk management
Most companies are missing key risks at more than one stage of the vendor risk lifecycle, yet few are expanding their TPRM programs to address these risks, according to Prevalent.
https://www.helpnetsecurity.com/2021/04/21/tprm-programs/

Free and Low Cost Online Cybersecurity Learning Content
During this unusual time in our lives, many of us find we want to improve our knowledge, skills or even prepare for new career opportunities. If you are interested in cybersecurity careers, there are numerous online education providers to choose from. Many online courses are available from your local community college, four-year universities, even the prestigious Centers of Academic Excellence programs – please review all options… https://www.nist.gov/itl/applied-cybersecurity/nice/resources/online-learning-content

****

News & Views

Today's Forecast--Cloud Jacking With Threat Of Third-Party Access
Cloud security has become a growing concern now that more organizations depend on the cloud for data storage; much of it since the surge in remote work. What should be a safe outlet for storing data has become a growing security threat for companies that assume all is well in the cloud. Cloud jacking, when an organization's cloud account is stolen or overtaken by an attacker, is on the rise. The biggest reasons for these attacks are often unchecked third-party access to the cloud and misconfigured default settings…
https://www.sosdailynews.com/news.jspx?&articleid=EC16DEEA4B7C82F2291B86F3D37B9E40&sx=79

SontiQ Scam News Summary
Review 2021 and other popular scams from the past few years… https://www.sontiq.com/scam-news-summary/

****

"Ctrl -F" for The Board

CISO Guidance ebook Excerpts
Several chapters relating to the rules

Questions
Contact FIPCO's Ken Shaurette at 800/722-3498 ext. 251 or email FIPCO IT Services for more information.

"Make Security Part of You and Your Institution's DNA!"

Threat Intelligence Newsletter: May 12, 2021

FIPCO®
IT Audit
Round Table
Discussions

If you would like to host an event, please contact: Amy Petersen

Upcoming Threat Intelligence Peer Group Discussions
None available at the current time

New Infosec Leader Community
The Slack Channel for security executives outside of the Fortune 2000 to build their network, ask questions, share insights, get guidance and more. Expands knowledge and sharing for you outside the financial services community across the world.
This can be a great opportunity for you to have a platform to build a network with colleagues ask questions, consult, and share insights with likeminded peers. Information security professional are indicating they found this community extremely valuable, educational, and interactive.

This can be a great opportunity for you to “deeper the relationship and learn more” by networking with other information security professionals.

For more details and to consider a recommendation to join the community email us at itservices@fipco.com

****

Alerts & Warnings

Costco Issues Scam Warning
Costco Wholesale Corporation has released a scam warning, advising its customers to be wary of more than a dozen digital scams currently targeting its customer base. Costco posted screenshots of 14 fraudulent emails, texts, and posts, in which cybercriminals are impersonating Costco to scam its customers. It seems as though… https://www.infosecurity-magazine.com/news/costco-issues-scam-warning/

Passwordstate password manager hacked in supply chain attack
Click Studios, the company behind the Passwordstate enterprise password manager, notified customers that attackers compromised the app's update mechanism to deliver malware in a supply-chain attack after breaching its networks… https://www.bleepingcomputer.com/news/security/passwordstate-password-manager-hacked-in-supply-chain-attack/

Financial sector saw a 125% increase in mobile phishing attacks during 2020
Average quarterly exposure to phishing attacks on mobile devices in the financial sector rose by 125% – and malware and app risk exposure increased by more than five times…
https://www.scmagazine.com/home/security-news/mobile-security/financial-sector-saw-a-125-increase-in-mobile-phishing-attacks-during-2020/?utm_source=newsletter&utm_medium=email&utm_campaign=SCUS_Newswire_{{%27now%27|date:%27%Y%m%d%27}}&hmSubId={{contact.cms_id_encrypted}}&email_hash={{contact.email|md5}}&oly_enc_id=0795J7353967J0E

Critical Cisco SD-WAN, HyperFlex Bugs Threaten Corporate Networks
Cisco has rolled out patches addressing severe vulnerabilities that could be exploited to perform remote code execution and privilege escalation. The flaws lie in the SD-WAN vManage Software. The bugs could allow an unauthenticated attacker to steal information from vulnerable networks. Cisco also disclosed a denial-of-service issue in the same… https://threatpost.com/critical-cisco-sd-wan-hyperflex-bugs/165923/

Panda Stealer Targets Crypto Wallets
A new information stealer referred too as Panda is targeting cryptocurrency wallets and credentials for applications such as Telegram, NordVPN, Discord, and Steam. The Panda stealer uses spam emails to trick victims and a difficult-to-detect fileless distribution method deployed by Phobos ransomware. The attacks are primarily targeting users in US… https://www.infosecurity-magazine.com/news/panda-stealer-targets-crypto/

Malicious Office 365 Apps Are the Ultimate Insiders
Phishers targeting Microsoft Office 365 users increasingly are turning to specialized links that take users to their organization's own email login page. After a user logs in, the link prompts them to install a malicious but innocuously-named app that gives the attacker persistent, password-free access to any of the user's emails and files, both of which are then plundered to launch malware and phishing scams against others…
https://krebsonsecurity.com/2021/05/malicious-office-365-apps-are-the-ultimate-insiders/

Joint NCSC-CISA-FBI-NSA Cybersecurity Advisory on Russian SVR Activity
CISA has joined with the United Kingdom's National Cyber Security Centre (NCSC), the Federal Bureau of Investigation (FBI), and the National Security Agency (NSA), in releasing a Joint Cybersecurity Advisory on Russian Foreign Intelligence Service (SVR) tactics, techniques, and procedures. Further TTPs associated with SVR cyber actors provides additional details on SVR activity including exploitation activity following their initial compromise of SolarWinds Orion software supply chain…
https://us-cert.cisa.gov/ncas/current-activity/2021/05/07/joint-ncsc-cisa-fbi-nsa-cybersecurity-advisory-russian-svr

****

Hints & Tips plus Security Awareness

THE PRACTICAL GUIDE TO THE MITRE ATT&CK EVALUATION
With hundreds of cybersecurity products to choose from, the task of evaluating competing solutions is extremely time consuming and overly daunting. While virtually every buyer should ultimately speak to several vendor reference clients and run a proof of Value (POV) evaluation - a live trial - in their environment, deciding which products to put in the evaluation mix is in itself difficult. The product selection exercise is only exacerbated with the tremendous reach of digital media, where we are overrun with incessant, and sometimes confusing, vendor messaging and…
https://go.cynet.com/hubfs/2020_MITRE_ATTACK_GUIDE.pdf?utm_medium=email&_hsmi=125143473&_hsenc=p2ANqtz-9JfzTJE-nJr726tOksr8tfKENf4lFWJhHyemw5I4-mjlMgCDeF1LP5QvA56QZXu5Mx_qCN9VeFjn33Apg7YxVhm9zeKQ&utm_content=125143473&utm_source=hs_automation

Google Plans to Automatically Enable Two-Factor Authentication
Google is planning to eventually automatically enable two-factor authentication on users' accounts to better secure them and prevent hacking. Google made the announcement on World Password Day, stating that it will ask people who have already enrolled themselves in the two-step verification feature to confirm their participation. Those who have…
https://www.darkreading.com/endpoint/google-plans-to-automatically-enable-two-factor-authentication/d/d-id/1340949

Complimentary Master Class to learn the infrastructure, security strategies, and tactics you need to rapidly adapt and thrive in a hybrid work environment.
In five short, easy to digest modules, you will learn:

- How to transform your application experience through visibility and analytics
- How to support the new hybrid work environment
- How to secure your workforce, workplace, and workloads
- Collaboration best practices for the trusted workplace
- The leadership and management tactics for this next normal

https://masterclass.govtech.com/How-to-Securely-Collaborate-in-the-New-Normal-137386.html?appCore=https://cms.erepublic.com/common/forms/ajax_form/137386

EDR, XDR And MDR: Understanding The Differences Behind The Acronyms
Navigating the vendor landscape is a challenge for many IT departments, particularly when looking at detection and response solutions, and especially since the cybersecurity industry is overly reliant on acronyms. EDR, MDR and XDR are three emerging endpoint security technologies built to…
https://www.forbes.com/sites/forbestechcouncil/2021/04/15/edr-xdr-and-mdr-understanding-the-differences-behind-the-acronyms/?sh=54e636ad49e2

Defending Against Software Standards and Technology (NIST), provides an overview of software supply chain risks and recommendations on how software customers and vendors can use the NIST Cyber Supply Chain Risk Management (C-SCRM) Framework and the Secure Software Development Framework (SSDF) to identify, assess, and mitigate software supply chain risks… https://www.cisa.gov/publication/software-supply-chain-attacks

Oversharing On Social Media: If Opportunity Knocks, Know When Not To Answer
Sharing online can be irresistible, especially when quizzes, surveys and other fun opportunities allow your voice to be heard. It's important to note that bad actors are…
https://www.sosdailynews.com/news.jspx?&articleid=C89525B3FD3FE318B7543541104C350B&sx=79

Data Exposure Report 2021
Code42, in partnership with Ponemon Institute, surveyed U.S. business decision makers and IT security leaders. The report uncovered the factors that are leading to the growing problem of Insider Risk including analysis of data loss after COVID-19, the challenges of building a program to address these risks, and why operating in maintenance mode with outdated tools may be a sunk cost to leave in 2020...
https://3qmwh315nk51z8bsi30vjk11-wpengine.netdna-ssl.com/wp-content/uploads/2020/12/DER_Fall2020_Final.pdf

NIST Releases Draft Cyber Supply Chain Risk Management Practices
The National Institute for Standards and Technology last week released its revised draft of its Cyber Supply Chain Risk Management Practices for Systems and Organizations (SP 800-161) for public review. The updates included in the latest revision are designed to help organizations identify, assess, and respond to cyber supply chain risks while still aligning with other fundamental NIST cybersecurity risk management guidance. Comments are due by June 14. NIST anticipates releasing a second draft in September 2021 and a final version by April 2022... https://csrc.nist.gov/publications/detail/sp/800-161/rev-1/draft?utm_campaign=RiskCyber-20210503&utm_medium=email&utm_source=Eloqua

My Identity Has Been Stolen: Now What?
Wednesday, May 19th at 1 PM; Virtual offices, online shopping, COVID-19 vaccination cards and surveys, credit card fraud, unemployment and tax fraud, data breaches and data leaks – the list goes on…and on. We're all vulnerable – but what do you do when you realize your personal information has been compromised? Who should you go to first? Whether it's you, a family member, colleague, employee, client – a stolen identity means hours upon hours of work, hassle, and stress…
https://www.sontiq.com/webinar-stolen-identity-now-what/?utm_source=Marketo&utm_medium=Email&utm_campaign=Stolen-Identity-Webinar-EM1&mkt_tok=Njc5LVNBSS01NjMAAAF81hbKLYBZof7zX3T1FX2xTcXBaBCDDKwGlKpYujE5SRslAMklO2XAy5fyce2ohVSIle_OfJBcHcwslhH94jd8oESOwWppUVUdBquhBbhG7Q

****

News & Views

How security pros, the insurance industry, and regulators can combat ransomware
AIG is one of the top cyber insurance companies in the U.S. Today's columnist, Erin Kennealy of Guidewire Software, offers ways for security pros, the insurance industry and government regulators to come together so insurance companies can continue to offer insurance for ransomware.
https://www.scmagazine.com/perspectives/how-security-pros-the-insurance-industry-and-regulators-can-combat-ransomware/?utm_source=newsletter&utm_medium=email&utm_campaign=SCUS_Newswire_{{%27now%27|date:%27%Y%m%d%27}}&hmSubId={{contact.cms_id_encrypted}}&email_hash={{contact.email|md5}}&oly_enc_id=0795J7353967J0E

The State of Cybersecurity with Steve Hines | NXT Up! Episode 12
Cyber attacks. Cyber crime. Cyber war. Where are we now in the cyber landscape, and how did we get here? Steve Hines, Co-Founder of ThreatAdvice by NXTsoft, unpacks the state of cybersecurity in 2021… https://blog.nxtsoft.com/the-state-of-cybersecurity-with-steve-hines-nxt-up-episode-12?utm_campaign=ThreatAdvice%20Partners&utm_medium=email&_hsmi=123671885&_hsenc=p2ANqtz-9Gfs600jVsL1GrPe-dfKyjVihq_WadwjrBFEa6AI6lIUiHMD8V-jTxQt0aRP-X_VwPDzKqlylvduse53hrWtHowYt2Dg&utm_content=123050712&utm_source=hs_email

Multi-Gov Task Force Plans to Take Down the Ransomware Economy
60 global entities have proposed a plan to hunt down and stop ransomware gangs by attacking their financial operations. The Institute for Security and Technology created the coalition with more than 60 members from software companies, government agencies, nonprofits, academic institutions and cyber security vendors. Microsoft and Amazon are among… https://threatpost.com/gov-task-force-ransomware-economy/165715/

Ransomware Task Force Releases Report
The Institute for Security and Technology's Ransomware Task Force last week released the report, "Combatting Ransomware: A Comprehensive Framework for Action: Key Recommendations from the Ransomware Task Force."
https://securityandtechnology.org/wp-content/uploads/2021/04/IST-Ransomware-Task-Force_Final_Report.pdf?utm_campaign=RiskCyber-20210503&utm_medium=email&utm_source=Eloqua

Robbing Banks The 21st Century Way With ATM Heists
Old school bank robberies, where the bad guys slip the teller a note, show a gun and run out with a bag full of money are, for the most part, history. Stealing cash money from ATM machines isn't exactly news, but continuing improvements to how it's being done is newsworthy. Not only is cash being stolen from ATMs, but credit and debit card data is being heisted too. Like most cybercrime, hackers improve their methods over time. Now, ATM hacks are becoming commonplace…
https://www.sosdailynews.com/news.jspx?&articleid=F26CDD63661475BF2D46ED518E7882FF&sx=79

Experts Share Thoughts for World Password Day:
Cybersecurity experts from several companies have shared thoughts for World Password Day. Will passwords soon die?... https://www.securityweek.com/cybersecurity-experts-share-thoughts-world-password-day

Misconfigured Database Exposes 200K Fake Amazon Reviewers
A misconfigured database has allegedly exposed a coordinated scheme by Amazon vendors to boost product ratings through utilizing fake accounts and reviews. Security researchers at SafetyDetectives located a China-based Elasticsearch server that was exposed to the public online, lacking any password protection or encryption. After looking further into the exposed… https://www.infosecurity-magazine.com/news/database-exposes-200k-fake-amazon/

****

"Ctrl -F" for The Board

What in the World Is a CISO?
Whilst employment has taken a downward curve over the last year or so, there are a variety of approaches I use when applying for a role to help my CV stand out. One key point is knowing what the job entails before submitting my cover letter and CV… https://www.tripwire.com/state-of-security/featured/what-in-the-world-is-a-ciso/?utm_source=The%20State%20of%20Security%20Newsletter&utm_medium=email&utm_campaign=FO-04-26-2021&utm_content=httpswwwtripwirecomstateofsecurityfeaturedwhatintheworldisaciso&mkt_tok=MzE0LUlBSC03ODUAAAF8swiZeBVOrFQY-Q4Y6q2A4aJKHgErVurkJVS7Q6-7dKCJAJdFvhAIcS1L6XWA4pBPSf8wlvqUDEhj0MnMQ-oY9DGoxLo4bIIrjXHyuWkpV_H3yQ

Questions
Contact FIPCO's Ken Shaurette at 800/722-3498 ext. 251 or email FIPCO IT Services for more information.

"Make Security Part of You and Your Institution's DNA!"

Threat Intelligence Newsletter: May 19, 2021

If you would like to host an event, please contact: Amy Petersen

Upcoming Threat Intelligence Peer Group Discussions
None available at the current time

NIST Releases Tips and Tactics for Dealing With Ransomware
Used in cyberattacks that can paralyze organizations, ransomware is malicious software that encrypts a computer system's data and demands payment to restore access. To help organizations protect against ransomware attacks and recover from them if they happen, the National Institute of Standards and Technology (NIST) has published an infographic offering a series of simple tips and tactics… https://www.nist.gov/news-events/news/2021/05/nist-releases-tips-and-tactics-dealing-ransomware

****

Alerts & Warnings

Cybersecurity warning: Russian hackers are targeting these vulnerabilities, so patch now
Attackers working on behalf of Russian Intelligence have updated their attack techniques, warns a joint alert from the US and UK... https://www.zdnet.com/article/cybersecurity-warning-russian-hackers-are-targeting-these-vulnerabilities-so-patch-now/?utm_medium=email&_hsmi=126241591&_hsenc=p2ANqtz-_e5tdJlPRuIqNnWh05FG1L21wqLvkRTCa5osRlmqqFJ8WxurvNtkQ279ei1grRVmQqUlBGW8Kf8ZdE_3i1NZQZNbOcHJTnxUzPfjFJmj3Rq4PGao0&utm_content=126241591&utm_source=hs_email

NCSC, CISA, FBI and NSA: Russian Threat Actors' TTPs
The UK's National Cyber Security Centre (NCSCX), the US Cybersecurity and Infrastructure Security Agency (CISA), the FBI, and the NSA have issued a joint alert listing the tactics, techniques, and procedures (TTPs) that Russian cyber threat actors are using. The report details 12 critical vulnerabilities that the threat actor group is currently exploiting… https://thehackernews.com/2021/05/top-11-security-flaws-russian-spy.html

Fake Chrome App Anchors Rapidly Worming 'Smish' Cyberattack
A new malware on Android impersonating the Google Chrome App has spread to hundreds of thousands of people. The app is a part of a hybrid cyberattack that also uses mobile phishing to steal credentials. Targets first receive an SMS text asking for custom fees to be paid to release…
https://threatpost.com/fake-chrome-app-worming-smish-cyberattack/166038/

Adobe Issues Patch for Acrobat Zero-Day
Adobe released several patches, including one for Acrobat. The vulnerability with Acrobat is being exploited in limited attacks on Adobe Readers users with Windows. The CVE-2021-28550 zero-day vulnerability affects Windows and macOS systems. The exploitation of the flaw could allow arbitrary code execution. 43 patches for 12 of its products were… https://www.darkreading.com/vulnerabilities---threats/adobe-issues-patch-for-acrobat-zero-day/d/d-id/1340983

Zix tricks: Phishing campaign creates false illusion that emails are safe
The malicious scheme hides behind multiple layers of redirect links in order to confuse security systems…
https://www.scmagazine.com/home/email-security/zix-tricks-phishing-campaign-creates-false-illusion-that-emails-are-safe/

****

Hints & Tips plus Security Awareness

THE PRACTICAL GUIDE TO THE MITRE ATT&CK EVALUATION
With hundreds of cybersecurity products to choose from, the task of evaluating competing solutions is extremely time consuming and overly daunting. While virtually every buyer should ultimately speak to several vendor reference clients and run a proof of Value (POV) evaluation - a live trial - in their environment, deciding which products to put in the evaluation mix is in itself difficult. The product selection exercise is only exacerbated with the tremendous reach of digital media, where we are overrun with incessant, and sometimes confusing, vendor messaging and…
https://go.cynet.com/hubfs/2020_MITRE_ATTACK_GUIDE.pdf?utm_medium=email&_hsmi=125143473&_hsenc=p2ANqtz-9JfzTJE-nJr726tOksr8tfKENf4lFWJhHyemw5I4-mjlMgCDeF1LP5QvA56QZXu5Mx_qCN9VeFjn33Apg7YxVhm9zeKQ&utm_content=125143473&utm_source=hs_automation

Contact FIPCO for more information and a POV of the Cynet solution at itservices@fipco.com.

Worst passwords of the decade: A historical analysis
Cybersecurity breaches are on the rise, so it's perplexing that so many people continue to use the same basic passwords. Perhaps it's the exhaustion of having to remember dozens of unique passwords? Whatever the reason, using a "bad" password won't keep the bad guys out…
https://resources.infosecinstitute.com/topic/worst-passwords-of-the-decade-a-historical-analysis/?utm_source=marketing%20cloud&utm_medium=email%20batch&utm_campaign=infosec%2aware&utm_content=2021-05-12&crmid=00Q0y00001m3DRwEAM

****

News & Views

Here’s the breakdown of cybersecurity stats only law firms usually see
BakerHostetler, a law firm with a massive data and privacy presence, compiles data from their client’s experiences to offer a rare lawyer’s perspective on cyber statistics. SC spoke to Craig Hoffman, partner at BakerHostetler and the main editor of the report, about the real outcomes from breaches… https://www.scmagazine.com/home/security-news/legal-security-news/heres-the-breakdown-of-cybersecurity-stats-only-law-firms-usually-see/?utm_source=newsletter&utm_medium=email&utm_campaign=SCUS_Newswire_{{%27now%27|date:%27%Y%m%d%27}}&hmSubId={{contact.cms_id_encrypted}}&email_hash={{contact.email|md5}}&oly_enc_id=0795J7353967J0E

Ransomware "Threatens Safety and Health of Americans"
The growth of ransomware has reached crisis proportions to the point where it "jeopardizes the safety and health of Americans." SCAMBUSTERS… https://scambusters.org/ransomware5.html

Security awareness training doesn’t solve human risk
Traditional employee risk mitigation efforts such as security awareness training and phishing simulations have a limited impact on improving employees’ real-world cybersecurity practices, according to Elevate Security and Cyentia Institute… https://www.helpnetsecurity.com/2021/05/12/solve-human-risk/

****

"Ctrl -F" for The Board

With All This Talk About the CCPA Litigation Risk, how Many CCPA Class Actions Actually Got Filed in 2020?
The California Consumer Privacy Act provided plaintiffs with a private right of action to pursue statutory damages following data security breaches that impact certain sensitive categories of personal information and are caused by a business’s failure to institute reasonable and appropriate security. Although the CCPA does not permit private suits with respect to alleged violations of the CCPA’s privacy (as opposed to security) provisions, the lack of a specified private right of action has not deterred some plaintiffs from filing suit. More on CCPA Litigation and Class Actions… https://www.natlawreview.com/practice-groups/Media-Privacy-Internet-FCC?utm_content=c584e3a2a324553da6f0db5639ed53da&utm_campaign=2021-05-11Cybersecurity%20Legal%20News&utm_source=Robly.com&utm_medium=email

Questions
Contact FIPCO’s Ken Shaurette at 800/722-3498 ext. 251 or email FIPCO IT Services for more information.

"Make Security Part of You and Your Institution's DNA!"

Threat Intelligence Newsletter: May 21, 2021

FIPCO®
IT Audit
Round Table
Discussions

If you would like to host an event, please contact: Amy Petersen

Upcoming Threat Intelligence Peer Group Discussions
None available at the current time

Darkside Ransomware
It's important to note that Darkside, like other ransomware as a service ("RAAS") groups rely on multiple independent "entrepreneurs" to compromise your network and deploy the ransomware. That means there's no one "signature" for these actors. They use what works for them and the tooling they have available. While Darkside is a Russian-language speaking group, there's indication that they're state-encouraged, it's more likely they're in the "state-ignored" space (Healey's "The Spectrum of State Responsibility" is a useful tool for these nuances: (Page2 Thanks to WICTRA Mike Heimberger)
https:///public/2012/mar/National_Responsibility_for_CyberAttacks,_2012.pdf

****

Alerts & Warnings

Cross-browser tracking vulnerability compromises user anonymity
The vulnerability affects top browsers including Chrome, Firefox, Safari, and even Tor browser.
https://www.hackread.com/cross-browser-tracking-compromises-user-anonymity/

Spotting cryptocurrency investment scams
Cryptocurrency has gotten lots of attention as a new way to invest. But here's the thing: scammers are taking advantage of people's understanding (or not) of cryptocurrency investments, and how they work. And younger people are losing big. https://www.consumer.ftc.gov/blog/2021/05/spotting-cryptocurrency-investment-scams?utm_source=govdelivery

Bizarro Banking Trojan Sports Sophisticated Backdoor
Bizarro, a new Brazilian banking trojan, has launched a campaign targeting customers of roughly 70 known banks located throughout Europe and South America, according to researchers. The advanced malware has taken its operation global, seeking to harvest targets' bank logins. Kaspersky released an analysis on Bizarro earlier this week, stating. https://threatpost.com/bizarro-banking-trojan-backdoor/166211/

Consumers Warned About Surge in Meal Kit Delivery Scams
Cybersecurity firm Tessain has warned consumers to be vigilant about a surge in meal kit delivery scams after uncovering SMS scams impersonating popular companies such as Gousto and HelloFresh. The uptick in meal kit delivery scams is likely a result of their increase in popularity during the Covid-19 lockdown. The…https://www.infosecurity-magazine.com/news/consumers-warned-surge-meal-kit/

All Wi-Fi devices impacted by new FragAttacks vulnerabilities
Newly discovered Wi-Fi security vulnerabilities collectively known as FragAttacks (fragmentation and aggregation attacks) are impacting all Wi-Fi devices (including computers, smartphones, and smart devices) going back as far as 1997. https://www.bleepingcomputer.com/news/security/all-wi-fi-devices-impacted-by-new-fragattacks-vulnerabilities/

Vishing attacks spoof Amazon to try to steal your credit card information
The attacks used fake order receipts and phone numbers in an attempt to steal credit card details from unsuspecting victims, says Armorblox. https://www.techrepublic.com/article/vishing-attacks-spoof-amazon-to-try-to-steal-your-credit-card-information/?utm_medium=email&_hsmi=128626919&_hsenc=p2ANqtz--nSTyrtusZhLPZWqgIQUQqzT6IEyGVgMWGGLxI97m8F8C4jM6RkL7bN2nDsr3SzJNRTMqxjJFMUgDTiD_cziX2OpXsYqGkj93imuDuaP5KLg6Gb6E&utm_content=128626919&utm_source=hs_email

****

Hints & Tips plus Security Awareness

Compromised Email Account? Here's What To Do
An email account can be compromised in a number of different ways. In some cases, your password may be weak and easily guessed or obtained through a public breach. In other cases, you may have clicked on a malicious link in an email, social networking site, or webpage. Or, you may have downloaded an app or file that contained malicious scripts. https://www.cisecurity.org/newsletter/compromised-email-account-heres-what-to-do/

How to Beat Browser Modifier Scams
How's your browser? Is it misbehaving, showing unexpected ads? Turning up weird results when you do a search? If so, you could be a victim of a browser modifier or hijacker. You'll find lots more information on individual browser modifiers and uninstallation here: https://www.2-spyware.com/remove-browsermodifier.html Read the article about these Scams at the following link: https://scambusters.org/browsermodifier.html

How penetration testing can promote a false sense of security
Penetration testing in and of itself is a good way to test cybersecurity, but only if every nook and cranny of the digital environment is tested; if not, there is no need to test.
https://www.techrepublic.com/article/how-penetration-testing-can-promote-a-false-sense-of-security/

Hang up on auto warranty robocalls
Have you gotten a recorded phone message from "Susie" with the "Vehicle Service Department" calling about your vehicle warranty? That's, like, so retro. But fanny packs, scrunchies, and tie dye are back — and so are vehicle warranty robocalls. https://www.consumer.ftc.gov/blog/2021/05/hang-auto-warranty-robocalls

Why You Must Archive All of Your Business Records
Organizations generate large volumes of electronic data, most of it unstructured. Content-generating sources include email, text messaging, telephony, collaboration systems like Microsoft Teams and Zoom, desktop productivity applications, CRM systems, social media and a wide range of other tools and capabilities.
Retaining records can be accomplished with simple backup, but this is an inefficient method of records retention that is fraught with problems: it normally retains an incomplete set of business records, data can easily be deleted or modified, and searching for and producing data is difficult, time-consuming and risky. As a result, organizations should implement archiving capabilities that will enable them to retain, find and produce all their business records. Warning Registration required for whitepaper….
https://ostermanresearch.com/2021/05/17/orwp_0339/

****

News & Views

Ransomware attackers are now using triple extortion tactics
Attackers are not only demanding ransom from organizations, but also threatening their customers, users and other third parties… https://www.techrepublic.com/article/ransomware-attackers-are-now-using-triple-extortion-tactics/#ftag=RSS56d97e7

Why Web Application Security Is Important
Internet security is complex but its importance is undeniable, especially when ransomware, DDoS attacks, and online identity theft are common. https://www.hackread.com/why-web-application-security-is-important/

Chrome now automatically fixes breached passwords on Android
Google is rolling out a new Chrome on Android feature to help users change passwords leaked online following data breaches with a single tap. [...]
https://www.bleepingcomputer.com/news/security/chrome-now-automatically-fixes-breached-passwords-on-android/?_hsmi=78978938&_hsenc=p2ANqtz-9G4EAk7f8Mhrru7Z5fJbD0EVjHAGvsnCWqgGGaBJt3VwB2hR-dhSqVWvyOs85QcmEc2lBxxQiWl-BE4MLwVfvjUdxvjQ

DHS announces program to mitigate vulnerabilities below the operating system
A notable rise in firmware vulnerabilities comes at a time when more run-of-the-mill criminals have access. CISA proposed a multi-step approach to tackle the growing threat.
https://www.scmagazine.com/home/security-news/vulnerabilities/dhs-announces-program-to-mitigate-vulnerabilities-below-the-operating-system/?utm_source=newsletter&utm_medium=email&utm_campaign=SCUS_Newswire_{{%27now%27|date:%27%Y%m%d%27}}&hmSubId={{contact.cms_id_encrypted}}&email_hash={{contact.email|md5}}&oly_enc_id=0795J7353967J0E

3.4 billion credential stuffing attacks hit financial services organizations
Akamai published a report that provides an analysis of both global and financial services-specific web application and credential stuffing attack traffic, revealing significant increases across the attack surfaces year over year from 2019 to 2020. https://www.helpnetsecurity.com/2021/05/20/financial-services-credential-stuffing/

****

"Ctrl -F" for The Board

Improving the Nation's Cybersecurity
On May 12, 2021, President Biden issued Executive Order (EO) 14028. The EO was published into the Federal Register on May 17, 2021…. https://securitystudio.com/improving-the-nations-cybersecurity/

Questions
Contact FIPCO's Ken Shaurette at 800/722-3498 ext. 251 or email FIPCO IT Services for more information.

"Make Security Part of You and Your Institution's DNA!"

Threat Intelligence Newsletter: June 1, 2021

FIPCO®
IT Audit
Round Table
Discussions

If you would like to host an event, please contact: Amy Petersen

Upcoming Threat Intelligence Peer Group Discussions
None available at the current time

CISA Releases Best Practices for Preventing Business Disruption from Ransomware Attacks
In light of the recent ransomware attack on the Colonial Pipeline, the Cybersecurity and Infrastructure Security Agency (CISA) and the Federal Bureau of Investigation (FBI) urge critical infrastructure (CI) asset owners and operators to adopt a heightened state of awareness, as well as implement the recommendations listed in the Mitigations section of this Joint Cybersecurity Advisory… https://us-cert.cisa.gov/ncas/alerts/aa21-131a

****

Alerts & Warnings

Look Out for this New Package Delivery Scam
In a new spin on the package delivery scheme, scammers are no longer posing as mail carriers. Instead, they're impersonating US Customs and Border Protection, claiming to have intercepted a package addressed to the victim…https://www.cbp.gov/newsroom/national-media-release/cbp-warns-telephone-scam?utm_source=newsletter&utm_medium=email&utm_content=issued%20a%20public%20warning&utm_campaign=scam-alert#:~:text=Callers%20impersonate%20CBP%20personnel&text=The%20resident's%20banking%20information%20is,solicit%20money%20over%20the%20telephone

Data of 100M Android users exposed from exposed cloud storage syncing
The data of more than 100 million Android app users has been found exposed because of misconfigurations relating to third-party services. Detailed May 20 by researchers at Check Point Software Technologies Ltd., the exposure relates to 23 popular apps...https://siliconangle.com/2021/05/23/data-100m-android-users-exposed-faulty-cloud-storage-syncing/

Watch out as fake ransomware attack infects PCs with StrRAT
StrRAT malware steals credentials and changes file name extension to .crimson but it does not encrypt any data like in a ransomware attack…https://www.hackread.com/fake-ransomware-attack-strrat-infects-pcs/
https://www.zdnet.com/article/this-massive-phishing-campaign-delivers-password-stealing-malware-disguised-as-ransomware/

Know The Signs: A Ransomware Attack Is Closer Than You Think
Ransomware attacks have crippled countless organizations in many sectors including commercial, finances, healthcare, government services, and education. They've proven devastating and expensive to fix, with some organizations never recovering and having to permanently close their doors. According to a Coveware report, the average ransom payment at the end of 2019 was $84,116, over twice the ransom amount of attacks earlier that same year…
https://www.sosdailynews.com/news.jspx?&articleid=80847174CF103BE9C88D8002868F6DE2&sx=79

BREACH vulnerability – Its Very Common in an Internal Scan
When you run a penetration test on your web application, the report may point out BREACH as a high-risk vulnerability. BREACH attack works by trying to guess the secret keys in a compressed and encrypted response. Attacker makes many requests and...https://techcommunity.microsoft.com/t5/iis-support-blog/breach-vulnerability/ba-p/2385272?_hsmi=78978938&_hsenc=p2ANqtz-9L8ZHonFI2mben8VrvZwUyWCeVzJAjColE9PvIFRywNjGxqaZ1JLjA-YG_63vxqUlFveQhOozZigQKk7LP0F03mpljnA

Multiple Vulnerabilities in VMware vCenter Server Could Allow for Remote Code Execution
Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than those who operate with administrative user rights. A pre-requisite of exploiting these vulnerabilities is that the malicious actor must have network access over port 443 to exploit these vulnerabilities. Successful exploitation of these vulnerabilities could allow an attacker to execute arbitrary code in context of the user running the application…https://www.vmware.com/security/advisories/VMSA-2021-0010.html

This phishing attack is using a call centre to trick people into installing malware on their Windows PC
A new and prolific phishing campaign is aiming to lure victims into believing that they have opened a subscription with a movie-streaming service, tricking them into calling a phone number to cancel the subscription. However, after contacting the call center, someone guides them through a procedure that eventually infects the… https://www.zdnet.com/article/this-phishing-attack-is-using-a-call-centre-to-trick-people-into-installing-malware-on-their-windows-pc/
https://therecord.media/malware-uses-underground-call-centers-to-trick-users-into-infecting-themselves/

Fake Copyright Infringement Warnings Used to Spread Ransomware
https://www.techlicious.com/blog/fake-copyright-infringement-warnings-used-to-spread-ransomware/

****

Hints & Tips plus Security Awareness

How Security Teams and Counsel Can Successfully Navigate the Complex Challenges of Trust, Security, and Safety

June 10, 2021 ~ 1:00pm CDT, In the latest episode of Nisos' ongoing panel series on critical issues at the nexus of law and cybersecurity, our panel of experts will discuss how security teams and legal counsel can successfully navigate the complex challenges of trust and safety. Trust, Security, and Safety teams have changed in the last ten years. As the technology industry has boomed with new and varied digital platforms and marketplaces, threats have escalated…
https://team-nisos.zoom.us/webinar/register/6716201403897/WN_Tn5dwlYvQB6N0ybmIrF3yw

The 20 Critical Security Controls: From Framework to Operational to Implementation

The 20 CSC provide an excellent bridge between the high level security framework requirements and the operational commands needed to implement them. Implementation is a 3-7 year process depending on a wide variety of factors and constraints. This talk discusses our…
https://www.youtube.com/watch?v=2N5SNKloEv0

Welcome to CIS Controls v8 – Webinar from CIS

Based on feedback from users around the world and working in a breadth of industries, we enhanced CIS Controls Version 8 to keep up with modern systems and software. Learn about the newly released CIS Controls v8 including its creation, changes from v7, new updates for resources and tools, and more. https://cisecurity.wistia.com/medias/t796o3og6m?utm_source=Pardot&utm_medium=Email&utm_campaign=v8_release Download CIS Controls v 8 Here...
https://learn.cisecurity.org/cis-controls-download?utm_source=wistia&utm_medium=partner

Cyberrisk Quantification Purity Tests

Measurement can be a tricky thing. Many practitioners want more ways to measure the effectiveness of cybersecurity programs to determine whether they are doing the right things to protect their organizations. Executives want…https://www.isaca.org/resources/news-andtrends/newsletters/atisaca/2021/volume-14/cyberrisk-quantification-purity-tests?utm_source=isaca&utm_medium=emailinternal&utm_campaign=newatisaca&utm_content=edmi_newatisaca_20210526&utm_term=tips-trade-jack-freund&cid=edmi_2007137&Appeal=EDMi&sp_rid=MTE4MTI5NDgxNzQwS0&sp_mid=33377258&spMailingID=33377258&spUserID=MTE4MTI5NDgxNzQwS0&spJobID=1944166079&spReportId=MTk0NDE2NjA3OQS2

CSIAC Podcast - Hypertext Markup Language (HTML) Smuggling

HTML smuggling was previously used with Dropbox for file sharing. Dropbox is no longer a preferred file sharing application. HTML smuggling is making its appearance on phishing emails as a means to increase their success rate. Attackers are constantly changing their strategy in order to make it more difficult to detect and evade security measures…https://www.csiac.org/podcast/html-smuggling/

****

News & Views

Global Credential Stuffing Attempts Hit 193 Billion in 2020
According to security vendor Akamai, there was roughly 193 billion credential stuffing attempts during 2020 due to surging numbers of online users. Akamai detailed its findings in its latest report, the 2021 State of the Internet / Security publication, looking to reveal the scale of attempts to hack users'accounts… https://www.infosecurity-magazine.com/news/global-credential-stuffing-193/

Skip the myths—make a cybersecurity response plan
Companies, regardless of size, often don't plan incident responses thoroughly enough because they buy into common myths, says Gabriel Whalen, who manages CDW's information security solutions practice. Speaking at RSA Conference 2021, Whalen ticked off four myths: Cyberinsurance will take care of everything; small businesses don't get attacked; a stout perimeter defense is all you need; and developing a plan is too expensive…https://biztechmagazine.com/article/2021/05/rsa-2021-4-common-myths-cybersecurity-incident-response-planning

How a Texas school outsmarted a ransomware attack
When Athens Independent School District in Texas got hit with ransomware, it was staring at a $50,000 problem. Learn how they solved the problem and recovered their encrypted data without paying a dime… https://resources.infosecinstitute.com/topic/back-up-your-backups-how-this-school-outsmarted-a-ransomwareattack/?utm_source=marketing%20cloud&utm_medium=email%20blast&utm_campaign=infosec%20aware&utm_content=2021-05-26&crmid=0030y00002DsSD0AAN

****

"Ctrl -F" for The Board

'Privateer' Threat Actors Emerge from Cybercrime Swamp
A new type of cybercriminal is emerging in a cyber-threat landscape that's historically been dominated by either state-sponsored threat actors or financially-motivated criminals that are hunted and prosecuted by law enforcement… https://threatpost.com/privateer-threat-actors-emerge/166483/?utm_medium=email&_hsmi=129879233&_hsenc=p2ANqtz--f2LnTND7OAg_c8Mcw2a9BRDR4SW7rGSWHMVm8jR2C9S18z7VCUJy99NUL-BDMCXLpqJ3eJBkUA5R7g-Y4wmliehFfUZKPm8Ik44H4cP9NYNyiinc&utm_content=129879233&utm_source=hs_email

Questions
Contact FIPCO's Ken Shaurette at 800/722-3498 ext. 251 or email FIPCO IT Services for more information.

"Make Security Part of You and Your Institution's DNA!"

Threat Intelligence Newsletter: June 7, 2021

FIPCO®
IT Audit
Round Table
Discussions

If you would like to host an event, please contact: Amy Petersen

Upcoming Threat Intelligence Peer Group Discussions
None available at the current time

****

Alerts & Warnings

Suspected APT29 Operation Launches Election Fraud Themed Phishing Campaigns
The campaign's phishing e-mails purported to originate from the USAID government agency and contained a malicious link that resulted in an ISO file being delivered.
https://www.volexity.com/blog/2021/05/27/suspected-apt29-operation-launches-election-fraud-themed-phishing-campaigns/
or
https://www.nytimes.com/2021/05/28/us/politics/russia-hack-usaid.html?referringSource=articleShare
or
https://www.microsoft.com/security/blog/2021/05/27/new-sophisticated-email-based-attack-from-nobelium/

- **Cryptocurrency Crooks Use Covid Pandemic to Hide Scams**
- **Cryptocurrency Users and Investors Face New Wave of Scams**
- **Cryptocurrency Scammers Trade on Investor Ignorance**
- **Ransomware 'Threatens Safety and Health of Americans**

https://scambusters.org/?s=cryptocurrency

https://help.coinbase.com/en/coinbase/privacy-and-security/avoiding-phishing-and-scams/avoiding-cryptocurrency-scams

More money is coming to families…and scammers are ready
As part of the American Rescue Plan Act, eligible families will get monthly payments from the government from July 15 through December 2021. The Internal Revenue Service (IRS) will send these monthly payments directly to people through direct deposit, paper checks, or debit cards. Unlike economic impact payments, these payments are an advance on families' child tax credit. People who are eligible will get up to half of their child tax credit in these monthly payments and the other half when they file their 2021 taxes. https://www.consumer.ftc.gov/blog/2021/06/more-money-coming-familiesand-scammers-are-ready?utm_source=govdelivery

****

Hints & Tips plus Security Awareness

Need an Incident Response Plan Template
Check out the link at the bottom of our Cynet resources webpage for a customizable template to build your response plan. https://www.fipco.com/solutions/it-audit-security/autonomous-endpoint-protection

Help Stop Fake News Superspreaders
It sounds like a contradiction but it's true: Fake news has become a fact... of life. And, despite all the warnings and counterattacks, it's getting worse. People, either thoughtlessly or maliciously, are passing on bogus news and doctored photos at a record rate. Technical experts are trying to create artificial intelligence (AI) formulas to detect and remove it. Meanwhile, organizations from political groups to academics are getting seriously worried. https://scambusters.org/fakenews5.html

Your guide to protecting your privacy online
The things we do throughout the course of our day give businesses access to information about our habits, tastes, and activities. Some might use it to deliver targeted ads to you, or to give you content based on your location, like stores nearby or the weather forecast. Others might sell or share that information. Whether you use a computer, tablet, or mobile phone to go online, there are things you can do to protect your privacy. https://www.consumer.ftc.gov/blog/2021/06/your-guide-protecting-your-privacy-online?utm_source=govdelivery

Unlocking the Mystery of VPN's: Why You Need One
You may have heard about VPN's (Virtual Private Network) more often lately, even popping up in TV ads for VPN service providers. What's behind the sudden surge of VPN's and why would you want or need one? For those who use WiFi internet connections at home or work, for shopping, banking, or just plain fun, VPN's provide a layer of security that WiFi cannot. Although free public WiFi is found most everywhere, it's long been a favorite for hackers because there is virtually no online security offered when using it.
https://www.sosdailynews.com/news.jspx?&articleid=14C2195807D26E1B4F834A3AC5193FC7&sx=79

Behavior indicators can point to breaches earlier
Indicators of compromise are necessary in data protection but "often come into play only when an attack is taking place or has already occurred," writes Michael Crouse of Forcepoint. Crouse advocates for a new set of data—indicators of behavior—that can smoke out breaches before they take place.
https://www.hstoday.us/subject-matter-areas/cybersecurity/shutting-down-cyber-attacks-before-they-begin-by-monitoring-user-behavior/

An Approach to Decluttering Your Security Stack – Roundtable Discussion
If you took a look at your security stack, what are the chances you could find some room to clear? This is the problem of our current market. As threats expand and evolve, new tools and platforms pop up to defend against them. To stay protected – in theory – you'd need to have as many of these tools as possible. But what then? You might be left with a tangle of systems that don’t communicate and actually make your security less effective. https://info.cynet.com/roundtable-june11/

****

News & Views

Re-Checking Your Pulse: Updates on Chinese APT Actors Compromising Pulse Secure VPN Devices
On April 20, 2021, Mandiant published detailed results of our investigations into compromised Pulse Secure devices by suspected Chinese espionage operators. This blog post is intended to provide an update on our findings, give additional recommendations to network defenders, and discuss potential implications for U.S.-China strategic relations. https://www.fireeye.com/blog/threat-research/2021/05/updates-on-chinese-apt-compromising-pulse-secure-vpn-devices.html

Why a risk-based approach to cybersecurity makes sense
Too many companies look at incidents such as the one involving Colonial Pipeline and take a "sky-is-falling" approach, says Danielle Parks, who analyzes return on security investment at Nucleus Research. Parks lays out the questions enterprises should ask to assess their risks and how to proceed accordingly.
https://mytechdecisions.com/it-infrastructure/why-you-should-take-a-risk-based-approach-to-cybersecurity/

White House warns companies to step up cybersecurity
The White House warned corporate executives and business leaders on Thursday to step up security measures to protect against ransomware attacks after intrusions disrupted operations at a meatpacking company and a southeastern oil pipeline.
https://www.businessinsurance.com/article/20210603/NEWS06/912342279/US-warns-companies-on-cybersecurity?utm_campaign=BI20210603BreakingNewsAlert&utm_medium=email&utm_source=ActiveCampaign&vgo_ee=lUA%2FUooU5KKf49IM7qf%2FDXwFoqDlMHNmyq65fGLdufk%3D&utm_campaign=BI20210603BreakingNewsAlert&utm_medium=email&utm_source=ActiveCampaign&vgo_ee=lUA%2FUooU5KKf49IM7qf%2FDXwFoqDlMHNmyq65fGLdufk%3D

****

"Ctrl -F" for The Board

How blockchain could break down governance silos
Blockchain technology could improve government operations because most departments work in silos and a lack of connection "foments a larger concern about data integrity and consistency," writes Shraddha Goled. Goled outlines the advantages of blockchain and provides examples of its use around the world, including in Singapore's banking system. https://analyticsindiamag.com/blockchain-technology-for-better-governance/

Questions
Contact FIPCO's Ken Shaurette at 800/722-3498 ext. 251 or email FIPCO IT Services for more information.

"Make Security Part of You and Your Institution's DNA!"

Threat Intelligence Newsletter: June 11, 2021

FIPCO®
IT Audit
Round Table
Discussions

If you would like to host an event, please contact: Amy Petersen

Upcoming Threat Intelligence Peer Group Discussions
None available at the current time

Ransomware Risk Management: Preliminary Draft NISTIR 8374 Available for Comment
NIST's National Cybersecurity Center of Excellence (NCCoE) has released a new Preliminary Draft report, NIST Interagency or Internal Report (NISTIR) 8374, Cybersecurity Framework Profile for Ransomware Risk Management.
Ransomware is a type of malicious attack where attackers encrypt an organization’s data and demand payment to restore access. In some instances, attackers may also steal an organization’s information and demand additional payment in return for not disclosing the information to authorities, competitors, or the public. Ransomware can disrupt or halt organizations’ operations. This report defines a Ransomware Profile, which identifies security objectives from the NIST Cybersecurity Framework that support preventing, responding to, and recovering from ransomware events. The profile can be used as a guide to managing the risk of ransomware events. That includes helping to gauge an organization's level of readiness to mitigate ransomware threats and to react to the potential impact of events.
https://csrc.nist.gov/publications/detail/nistir/8374/draft

****

Alerts & Warnings

Cyber attacks more sophisticated, data exfiltration ‘not going away’: risk expert
Ransomware attacks are "size- and industry-agnostic," and many organizations don't have a plan if one occurs, says Jaycee Roth of the Toronto office of Kroll, formerly known as Duff & Phelps. Roth adds that attackers "are getting a lot smarter about exactly what type of information they're taking out of the door with them: usually sensitive in nature, or financial data that helps strengthen their side of the negotiation."
https://www.canadianlawyermag.com/practice-areas/privacy-and-data/cyber-attacks-more-sophisticated-data-exfiltration-not-going-away-risk-expert/356810

Beware of “Ransomware system update” emails!
Emails referencing the Colonial Pipeline ransomware attack and looking like they’ve been sent from the corporate IT help desk have been hitting employees’ inboxes and asking them to download and run a “ransomware system update.” https://www.helpnetsecurity.com/2021/06/07/ransomware-system-update-emails/

How a malicious bot tries to evade detection by morphing
Targeting Windows and Linux systems, the Necro Python bot changes its code to evade traditional security detection, says Cisco Talos. https://www.techrepublic.com/article/how-a-malicious-bot-tries-to-evade-detection-by-morphing/?ftag=TREa988f1c&bhid=78480402&mid=13393914&cid=712423569

Looking for work? Avoid job scams
If you’re looking for a job, there are lots of things to think about, from wages and commute time to benefits and employee resources. And, if you identify as LGBTQ+, you might also look for whether a workplace is LGBTQ+ friendly. To make your job search safe and successful, learn how to spot and avoid job scams. https://www.consumer.ftc.gov/blog/2021/06/looking-work-avoid-job-scams?utm_source=govdelivery

****

Hints & Tips plus Security Awareness

CISA Resources to Reduce Ransomware Risk
June 24 at 11:00 a.m. Central, the total number of ransomware attacks quintupled globally over the last two years and are expected to rise 20 to 40 percent this year.
https://www.infosecinstitute.com/webinar/cisa-helps-you-fight-ransomware/?utm_source=marketing%20cloud&utm_medium=email%20blast&utm_campaign=infosec%20insights&utm_content=2021-06-04&crmid=0030y00002DsSD0AAN

Microsoft Patch Tuesday Fixes 6 In-The-Wild Exploits, 50 Flaws
In this month’s Patch Tuesday update, Microsoft issued fixes for 5 critical exploits and 45 vulnerabilities rated important in severity in Microsoft Windows, .NET Core, and Visual Studio, Microsoft Office, Microsoft Edge, SharePoint Server, Hyper-V, Visual Studio Code, and more. Microsoft researchers discovered a highly targeted malware campaign that has. https://threatpost.com/microsoft-patch-tuesday-in-the-wild-exploits/166724/

Scam Shields Up for Amazon Prime Day!
Amazon Prime Day -- days (plural), actually -- happens later this month and scammers have lined up a host of hacks, con tricks, and frauds to catch out unwary shoppers. SCAMBUSTERS

How to spot a government impersonator scam
Scammers often disguise themselves as people working for the government and might pretend to offer help. But, really, they’re after your money or personal information. For Pride Month, the FTC wants the LGBTQ+ community to know about government imposter scams and how to avoid them.
https://www.consumer.ftc.gov/blog/2021/06/how-spot-government-impersonator-scam?utm_source=govdelivery

How to create a good and strong password
Want to keep your online accounts safe and secure?
https://cybernews.com/best-password-managers/how-to-create-a-strong-password/?utm_source=newsletter&utm_medium=email&utm_campaign=CyberNewsLetter_Welcome

****

News & Views

Is cyber insurance leading to an increase in ransom payments?
According to new research, ransomware victims are more likely to pay ransom demands by relying on their cyber insurance. According to a new report, in the first half of 2020, ransomware payments accounted for 41% of the total filed cyber-insurance claims. For example, in the recent Colonial Pipeline attack, the energy firm paid a $4.4 million ransom. It has since been revealed that Colonial Pipeline had a cyber-insurance protection policy covering them for at least £15 million, although it is unclear whether the firm utilized the policy. With more companies falling victim to ransomware attacks, does cyber-insurance policies mean that ransomware gangs are more likely to be paid off? https://threatpost.com/cyber-insurance-ransomware-payments/166580/

Stand up to cyberbullying
Pride Month is about connecting with and showing support for people in the LGTBQ+ community. It's also about standing up and protecting those we care for, so today we're talking about cyberbullying.
https://www.consumer.ftc.gov/blog/2021/06/stand-cyberbullying?utm_source=govdelivery

8.4B passwords posted online
A major leak of 8.4 billion passwords was posted on a forum popular with hackers, apparently compiled from previous breaches. The forum user who uploaded the text files is calling them "RockYou2021," after a 2009 data breach that involved more than 32 million passwords.
https://cybernews.com/security/rockyou2021-alltime-largest-password-compilation-leaked/

Can your MFA implementations stymie MFA bypass attacks?
Shay Nahari, Head of Red-Team services at CyberArk, says that they've been increasingly asked by customers to probe their multi-factor authentication (MFA) defenses, which lead them to pinpoint four main attack vectors used by threat actors to circumvent MFA controls, by exploiting: architectural and design flaws, insecure channels, side channel attacks and insufficient attack surface coverage.
https://www.helpnetsecurity.com/2021/06/09/mfa-bypass-attacks/

Lawyers doubling as PR reps can be a mistake, pro says
Handing off a cybersecurity incident response to lawyers often doesn't go well because "lawyers are not necessarily great communicators," says Jonathan Englert, founder of Australia-based PR company AndironGroup. The problem, Englert says, could be a narrative that is inaccurate or damages the company's reputation. https://ia.acs.org.au/article/2021/cyber-attack--who-ya-gonna-call-.html

****

"Ctrl -F" for The Board

2021 Cyberthreat Defense Report
https://www.isc2.org/-/media/ISC2/Research/Cyberthreat-Defense-Report/2021/CyberEdge-2021-CDR-Report-v10--ISC2-Edition.ashx?la=en&hash=60BC7C7969857E2FF07B714896F079EF5C9C1C39

Questions
Contact FIPCO's Ken Shaurette at 800/722-3498 ext. 251 or email FIPCO IT Services for more information.

"Make Security Part of You and Your Institution's DNA!"

Threat Intelligence Newsletter: June 18, 2021

FIPCO®
IT Audit
Round Table
Discussions

If you would like to host an event, please contact: Amy Petersen

Upcoming Threat Intelligence Peer Group Discussions
None available at the current time

Ransomware Risk Management: Preliminary Draft NISTIR 8374 Available for Comment
NIST's National Cybersecurity Center of Excellence (NCCoE) has released a new Preliminary Draft report, NIST Interagency or Internal Report (NISTIR) 8374, Cybersecurity Framework Profile for Ransomware Risk Management.
Ransomware is a type of malicious attack where attackers encrypt an organization's data and demand payment to restore access. In some instances, attackers may also steal an organization's information and demand additional payment in return for not disclosing the information to authorities, competitors, or the public. Ransomware can disrupt or halt organizations' operations. This report defines a Ransomware Profile, which identifies security objectives from the NIST Cybersecurity Framework that support preventing, responding to, and recovering from ransomware events. The profile can be used as a guide to managing the risk of ransomware events. That includes helping to gauge an organization's level of readiness to mitigate ransomware threats and to react to the potential impact of events.
https://csrc.nist.gov/publications/detail/nistir/8374/draft

****

Alerts & Warnings

Cyber attacks more sophisticated, data exfiltration 'not going away': risk expert
Ransomware attacks are "size- and industry-agnostic," and many organizations don't have a plan if one occurs, says Jaycee Roth of the Toronto office of Kroll, formerly known as Duff & Phelps. Roth adds that attackers "are getting a lot smarter about exactly what type of information they're taking out of the door with them: usually sensitive in nature, or financial data that helps strengthen their side of the negotiation."
https://www.canadianlawyermag.com/practice-areas/privacy-and-data/cyber-attacks-more-sophisticated-data-exfiltration-not-going-away-risk-expert/356810

Beware of “Ransomware system update” emails!
Emails referencing the Colonial Pipeline ransomware attack and looking like they’ve been sent from the corporate IT help desk have been hitting employees’ inboxes and asking them to download and run a “ransomware system update.” https://www.helpnetsecurity.com/2021/06/07/ransomware-system-update-emails/

How a malicious bot tries to evade detection by morphing
Targeting Windows and Linux systems, the Necro Python bot changes its code to evade traditional security detection, says Cisco Talos. https://www.techrepublic.com/article/how-a-malicious-bot-tries-to-evade-detection-by-morphing/?ftag=TREa988f1c&bhid=78480402&mid=13393914&cid=712423569

Looking for work? Avoid job scams
If you’re looking for a job, there are lots of things to think about, from wages and commute time to benefits and employee resources. And, if you identify as LGBTQ+, you might also look for whether a workplace is LGBTQ+ friendly. To make your job search safe and successful, learn how to spot and avoid job scams. https://www.consumer.ftc.gov/blog/2021/06/looking-work-avoid-job-scams?utm_source=govdelivery

Attackers need only one opening—here are 3 to avoid
The most common mistake in cybersecurity "involves thinking that your employees know cybersecurity best practices offhand," Ben Canner writes. Canner mentions two other major mistakes to avoid: Not monitoring critical databases and applications, and letting IT teams burn out for want of automated solutions. https://solutionsreview.com/security-information-event-management/it-only-takes-one-cybersecurity-mistake-to-let-hackers-in/

Vulnerability allows cross-browser tracking in Chrome, Firefox, Safari, and Tor
Protecting user privacy is a foundational capability of the web browser, and scheme flooding violates that capability. https://fingerprintjs.com/blog/external-protocol-flooding/

Millions of Connected Cameras Open to Eavesdropping
According to a warning released by the Cybersecurity and Infrastructure Security Agency, millions of connected security and home cameras contain a critical software vulnerability that could allow for remote attackers to view video feeds. The bug has been designated as a 9.1 CVSS score, meaning that it is of high. https://threatpost.com/millions-connected-cameras-eavesdropping/166950/

Victims Lose Thousands In Training Scams – Scam Job Offers
Since more of us have been confined to our homes than is usual, it's no surprise there's been a surge in online training. It many cases, it's because we want to use the extra time on our hands to extend our knowledge and skills -- and maybe make a little money. https://www.bbb.org/new-york-city/scam-job-offers/

These Are Some of The Newest Scams Out There
WHAT'S NEW IN old SCAMS? https://scambusters.org/scamlines.html
2020 Top 10 Fraud Scams: https://fraud.org/top-ten-scams-20/

Cisco Security

- Cisco Jabber Desktop and Mobile Client Software Vulnerabilities
- Cisco Email Security Appliance and Cisco Web Security Appliance Certificate Validation

Vulnerability

- Vulnerabilities Allow Hackers to Disrupt, Hijack Schneider PowerLogic Devices
- Cisco DNA Center Certificate Validation Vulnerability
- Cisco AnyConnect Secure Mobility Client for Windows Denial of Service Vulnerability
- More. https://tools.cisco.com/security/center/publicationListing.x

Android Trojan Targets European Bank Customers
Cleafy: TeaBot Steals Credentials and SMS Texts From Victims to Use for Financial Fraud.
https://www.bankinfosecurity.com/android-trojan-targets-european-bank-customers-a-16570

****

Hints & Tips plus Security Awareness

CISA Resources to Reduce Ransomware Risk

June 24 at 11:00 a.m. Central, the total number of ransomware attacks quintupled globally over the last two years and are expected to rise 20 to 40 percent this year.
https://www.infosecinstitute.com/webinar/cisa-helps-you-fight-ransomware/?utm_source=marketing%20cloud&utm_medium=email%20blast&utm_campaign=infosec%20insights&utm_content=2021-06-04&crmid=0030y00002DsSD0AAN

Microsoft Patch Tuesday Fixes 6 In-The-Wild Exploits, 50 Flaws
In this month’s Patch Tuesday update, Microsoft issued fixes for 5 critical exploits and 45 vulnerabilities rated important in severity in Microsoft Windows, .NET Core, and Visual Studio, Microsoft Office, Microsoft Edge, SharePoint Server, Hyper-V, Visual Studio Code, and more. Microsoft researchers discovered a highly targeted malware campaign that has. https://threatpost.com/microsoft-patch-tuesday-in-the-wild-exploits/166724/

Scam Shields Up for Amazon Prime Day!
Amazon Prime Day -- days (plural), actually -- happens later this month and scammers have lined up a host of hacks, contricks, and frauds to catch out unwary shoppers. SCAMBUSTERS.
https://scambusters.org/primeday.html

How to spot a government impersonator scam
Scammers often disguise themselves as people working for the government and might pretend to offer help. But, really, they’re after your money or personal information. For Pride Month, the FTC wants the LGBTQ+ community to know about government imposter scams and how to avoid them.
https://www.consumer.ftc.gov/blog/2021/06/how-spot-government-impersonator-scam?utm_source=govdelivery

How to create a good and strong password
Want to keep your online accounts safe and secure?
https://cybernews.com/best-password-managers/how-to-create-a-strong-

password/?utm_source=newsletter&utm_medium=email&utm_campaign=CyberNewsLetter_Welcome
Creating a Large Company Security Stack on a Lean Company Budge
eBook; Cybersecurity practitioners know that threats are expanding, attacks are proliferating, and companies are more at risk than ever. The typical solution? To expand cybersecurity stacks to address new threats and techniques. Essentially, we've entered an arms race with malicious actors. Attackers find new, more dangerous and stealthier attack tactics, and we build higher walls, add more technologies, and expand our stacks to meet the challenge. https://go.cynet.com/hubfs/EBook-Creating-a-Large-Company-Security-Stack-on-a-Lean-Company-Budget.pdf

Hello, summer. Goodbye, scammers.
Summer is right around the corner. With things reopening, kids getting out of school, and days lasting longer, this summer promises, we hope, some much-needed relaxation, adventure, and a chance to reconnect with family and friends. Today, we're kicking off our summer safety series to share some thoughts on ways to make your summer season as enjoyable and safe as possible.
https://www.consumer.ftc.gov/blog/2021/06/hello-summer-goodbye-scammers?utm_source=govdelivery

DATA BREACH - Notification no-nos: What to avoid when alerting customers of a breach
Experts revealed to SC Media what they believe are some of the biggest errors companies can make when notifying the public of a breach, from revealing too little or too much, to scapegoating or downplaying the incident. https://www.scmagazine.com/home/security-news/data-breach/notification-no-nos-what-toavoidwhenalertingcustomersofabreach/?utm_source=newsletter&utm_medium=email&utm_campaign=SCUS_Newswire_{{%27now%27|date:%27%Y%m%d%27}}&hmSubId={{contact.cms_id_encrypted}}&email_hash={{contact.email|md5}}&oly_enc_id=0795J7353967J0E

CISA Releases Best Practice Guidance to Help Organizations Map Adversary Behavior to MITRE ATT&CK Framework
In partnership with Homeland Security Systems Engineering and Development Institute (HSSEDI), which worked with the MITRE ATT&CK team, this framework is an example of a successful collaboration by committed partners with a shared mission. https://us-cert.cisa.gov/best-practices-mitre-attckr-mapping

CISA suggests using ad blockers to fend off 'malvertising' – Securing your browser
The leading national agencies like CISA recommended ad blockers as a basic cybersecurity tool for everyone to fend off 'malvertising' – Securing your browser. https://www.hackread.com/cisa-suggests-using-ad-blockers-against-malvertising/

RANSOMWARE SERIES: BEST PRACTICES - Veam
Critical steps to evaluate your risk level, protect your business, and rapidly recover from data disasters.
https://www.ebulletinsresources.com/hubfs/D1/Storagepipe/Ransomware%20Series%20-%20Storagepipe%20and%20Veeam%20Best%20Practices%20%202021%20FINAL.pdf?hsCtaTracking=ae922145-fbe8-45ab-a32c-48caba8c8100%7C92e96fe6-9804-4660-8771-044ae498a1e3

****

News & Views

Is cyber insurance leading to an increase in ransom payments?
According to new research, ransomware victims are more likely to pay ransom demands by relying on their cyber insurance. According to a new report, in the first half of 2020, ransomware payments accounted for 41% of the total filed cyber-insurance claims. For example, in the recent Colonial Pipeline attack, the energy firm paid a $4.4 million ransom. It has since been revealed that Colonial Pipeline had a cyber-insurance protection policy covering them for at least £15 million, although it is unclear whether the firm utilized the policy. With more companies falling victim to ransomware attacks, does cyber-insurance policies mean that ransomware gangs are more likely to be paid off? https://threatpost.com/cyber-insurance-ransomware-payments/166580/

Stand up to cyberbullying
Pride Month is about connecting with and showing support for people in the LGTBQ+ community. It's also about standing up and protecting those we care for, so today we're talking about cyberbullying.
https://www.consumer.ftc.gov/blog/2021/06/stand-cyberbullying?utm_source=govdelivery

8.4B passwords posted online
A major leak of 8.4 billion passwords was posted on a forum popular with hackers, apparently compiled from previous breaches. The forum user who uploaded the text files is calling them "RockYou2021," after a 2009 data breach that involved more than 32 million passwords.
https://cybernews.com/security/rockyou2021-alltime-largest-password-compilation-leaked/

Can your MFA implementations stymie MFA bypass attacks?
Shay Nahari, Head of Red-Team services at CyberArk, says that they've been increasingly asked by customers to probe their multi-factor authentication (MFA) defenses, which lead them to pinpoint four main attack vectors used by threat actors to circumvent MFA controls, by exploiting: architectural and design flaws, insecure channels, side channel attacks and insufficient attack surface coverage.
https://www.helpnetsecurity.com/2021/06/09/mfa-bypass-attacks/

Lawyers doubling as PR reps can be a mistake, pro says
Handing off a cybersecurity incident response to lawyers often doesn't go well because "lawyers are not necessarily great communicators," says Jonathan Englert, founder of Australia-based PR company AndironGroup. The problem, Englert says, could be a narrative that is inaccurate or damages the company's reputation. https://ia.acs.org.au/article/2021/cyber-attack--who-ya-gonna-call-.html

Biometrics for banking and financial services market to reach $8.9 billion by 2026
The turn of next decade is expected to be more challenging for banks and financial institutions as security breaches become more sophisticated with technology advancements. Money laundering has become more widespread representing about 2%-5% of global GDP. One of the measures being actively pursued by banks is biometrics, since the technology assists in the creation of secure banking environment by reducing instances of identity fraud, establishing audit trail of transactions, and protecting financial data.
https://www.helpnetsecurity.com/2021/06/11/biometrics-for-banking-market/

What Are Practical Projects for Implementing Zero Trust?
Vendor marketing abuses the overloaded term “zero trust” to imply improved security. Security and risk management leaders must move beyond the hype and implement two key projects to reduce risk with least privileged access and adaptive security. https://www.gartner.com/doc/reprints?id=1-263IP35M&ct=210521&st=sb&utm_medium=email&_hsmi=129991323&_hsenc=p2ANqtz-8SZO2voKY5R6HtzIxjRmn1dR7dTQmS2PT1Tjx7CIVhbLjRLlY6Ab1dli5F6bBxHv3C7Y71ZoB0k8Mp43arVTS9ZOyqg&utm_content=129991323&utm_source=hs_automation

Cybersecurity Insurance Did NOT Cause the Ransomware Plague
The business pages have been full in recent months with tales of cyber extortion and ransomware. In an effort to try to explain these developments, some commentators have suggested that the availability of ransomware coverage under cyber insurance is a cause of the problem.
https://www.dandodiary.com/2021/06/articles/cyber-liability/cybersecurity-insurance-did-not-cause-the-ransomware-plague/

Microsoft Teams fixed serious flaw, researchers report
Cybersecurity company Tenable reports that a flaw in Microsoft Teams, which has since been patched, could have given hackers access to shared files and perhaps even control of Microsoft 365 accounts. "Given the number of access tokens this vulnerability exposes, there are likely to be other creative and serious potential attacks not explored in our proofs-of-concept," warns Tenable researcher Evan Grant.
https://www.darkreading.com/attacks-breaches/microsoft-teams-vulnerable-to-patch-workaround-researchers-report/d/d-id/1338583

Scam victims tell us their stories | Scamwatch
Scam victims tell us their stories. Investment scam: I lost $50 000 in fake online trading . Be suspicious of investment opportunities that promise a high return with little or no risk, and don't let anyone pressure you into making decisions about your money or. https://www.scamwatch.gov.au/get-help/real-life-stories/scam-victims-tell-us-their-stories

ICBA – Bank Agencies Coordinate Crypto Approach Amid Ransomware Escalation
Escalating attacks against critical infrastructure are bringing renewed focus to the role of cryptocurrencies in facilitating criminal activity, which has implications for community banks, ICBA’s Brian Laverdure writes in a new Main Street Matters post. https://www.icba.org/newsroom/blogs/main-street-matters---education/2021/06/16/crypto-chronicles-agencies-coordinate-crypto-approach-amid-ransomware-escalation?utm_campaign=NewsWatch%20Today&utm_medium=email&_hsmi=134324934&_hsenc=p2ANqtz-_zvX9qb2hzmbJEoZ_0wox4XgLwkPBMl4O6rPaz4w-amo4zYghqsP4hqMKc_tggn9-BiOR0gm3MVruSrwssHEzE3NqH-g&utm_content=134327316&utm_source=hs_email

****

"Ctrl -F" for The Board

2021 Cyberthreat Defense Report
https://www.isc2.org/-/media/ISC2/Research/Cyberthreat-Defense-Report/2021/CyberEdge-2021-CDR-Report-v10--ISC2-Edition.ashx?la=en&hash=60BC7C7969857E2FF07B714896F079EF5C9C1C39

C-suites adapt to ransomware as a cost of doing business
Tangible impacts to corporate earnings, combined with the multi-million dollar ransom payouts by Colonial Pipeline and JBS, demonstrate a reality that more and more in the cybersecurity community are beginning to acknowledge: Ransomware is a cost of doing business, grabbing the attention not just of security leaders, but the entire C-suite, boards, and even Wall Street investors.
https://www.scmagazine.com/home/security-news/ransomware/c-suites-adapt-to-ransomware-as-a-cost-ofdoingbusiness/?utm_source=newsletter&utm_medium=email&utm_campaign=SCUS_Newswire_{{%27now%27|date:%27%Y%m%d%27}}&hmSubId={{contact.cms_id_encrypted}}&email_hash={{contact.email|md5}}&oly_enc_id=0795J7353967J0E

Questions
Contact FIPCO’s Ken Shaurette at 800/722-3498 ext. 251 or email FIPCO IT Services for more information.

"Make Security Part of You and Your Institution's DNA!"

Threat Intelligence Newsletter: June 30, 2021

FIPCO®
IT Audit
Round Table
Discussions

If you would like to host an event, please contact: Amy Petersen

Upcoming Threat Intelligence Peer Group Discussions
None available at the current time

NIST's new ransomware framework up for public comment
The US National Institute of Standards and Technology is accepting comments through July 9 on its framework for dealing with ransomware. NIST's latest work is broken down into five sectors: "identify, protect, detect, respond and recover.” https://www.nist.gov/news-events/news/2021/06/ransomware-risk-management-preliminary-draft-nistir-8374-available-comment

****

Alerts & Warnings

Don’t send them money
Family emergency scams try to scare people into sending money to help a loved one in trouble. The fraud can play out in many ways, but the hustle is the same: the caller lies, tries to scare you, and rushes you to pay so you don’t have time to think twice or check things out before you send money. And once you do that, you’ll never get it back. https://www.consumer.ftc.gov/blog/2021/06/dont-send-them-money

VMSA-2021-0013 - VMware Tools, VMRC and VMware App Volumes updates addresses a local privilege escalation vulnerability (CVE-2021-21999)
Impacted Products: VMware Tools for Windows VMware Remote Console for Windows (VMRC for Windows) VMware App Volumes. Please see the advisory here: https://www.vmware.com/security/advisories/VMSA-2021-0013.html

****

Hints & Tips plus Security Awareness

Ransomware Prevention, Detection and Remediation
How quality XDR Can Stop Ransomware Before It Stops You…. https://go.cynet.com/hubfs/Cynet-Ransomware-Protection.pdf
If you'd like to know more contact FIPCO.

Why shaming and coaching employees isn't the best path
Phishing simulations and endless training sessions make "employees view the internal IT teams negatively, ultimately making it more challenging to get people on board with strategic initiatives," warns Sai Venkataraman, CEO of SecurityAdvisor. Venkataraman suggests that using the Golden Rule might get better results than shaming and coaching. https://www.helpnetsecurity.com/2021/06/23/shame-culture-security-posture/

10 tips for implementing governance frameworks
The COBIT® and ITIL governance frameworks are different, but are "excellent models to help create value in service-oriented IT organizations, if adopted correctly," writes Mark Thomas, president of Escoute, an IT governance company. Thomas provides 10 tips for implementing governance frameworks.
https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2021/leverage-cobit-and-itil-for-customer-centric-connected-and-collaborative-organizations

****

News & Views

US bill would require quick disclosure of cyberattacks
A bipartisan bill in the US Senate would require operators of digital security and critical infrastructure companies to report cyberattacks to the government within a day of their occurrence. A provision of the bill would immunize companies from lawsuits arising from the reporting requirements.
https://www.politico.com/news/2021/06/17/senate-bill-to-require-hack-reports-within-24-hours-and-punish-violators-495060

****

"Ctrl -F" for The Board

2021 Cyberthreat Defense Report

Questions
Contact FIPCO's Ken Shaurette at 800/722-3498 ext. 251 or email FIPCO IT Services for more information.

"Make Security Part of You and Your Institution's DNA!"

Threat Intelligence Newsletter: July 2, 2021

FIPCO®
IT Audit
Round Table
Discussions

If you would like to host an event, please contact: Amy Petersen

Upcoming Threat Intelligence Peer Group Discussions
None available at the current time

FFIEC releases Architecture, Infrastructure, and Operations Booklet
https://ithandbook.ffiec.gov/what%27s-new.aspx
The FFIEC members revised and renamed the Operations booklet to Architecture, Infrastructure, and Operations (AIO) to reflect the changing technological environment and increasing need for security and resilience, including architectural design, infrastructure implementation, and operation of information technology systems, and it provides examiners with fundamental examination expectations regarding architecture and infrastructure planning, governance and risk management, and operations of regulated entities. The new Handbook can be found at: https://ithandbook.ffiec.gov/it-booklets/architecture,-infrastructure,-and-operations.aspx

Federal agency releases ransomware assessment tool
The federal Cybersecurity and Infrastructure Security Agency said Wednesday it has introduced a ransomware module in its Cyber Security Evaluation Tool.
https://github.com/cisagov/cset/releases/tag/v10.3.0.0

****

Alerts & Warnings

Cobalt Strike Usage Explodes Among Cybercrooks
The legit security tool has shown up 161 percent more, year-over-year, in cyberattacks, having "gone fully mainstream...https://threatpost.com/cobalt-strike-cybercrooks/167368/
Can your antivirus and endpoint security defend against these types of an attack?
https://www.fipco.com/solutions/it-audit-security/xdr

TeaBot Trojan Steals Android Banking Credentials
There's a new Android banking trojan making the rounds overseas, but like other malware attacks in other countries, it won't take TeaBot Trojan long to reach the U.S. Still in early development, the goal of this one, called TeaBot, is stealing user credentials for fraudulent activities against financial institutions. It starts the device infection by posing as a legitimate package delivery service as the way to begin its costly malware infection.
https://www.sosdailynews.com/news.jspx?&articleid=DEC441BAB94E767BB54CD055905153DE&sx=79

Cobalt Strike Usage Explodes Among Cybercrooks
Cobalt strike usage among cybercriminals has increased by 161%, according to researchers at Proofpoint. Cobalt Strike is a legitimate, commercially available tool that is utilized by network penetration testers, however, it is abused by cybercriminals to conduct cyberattacks. Proofpoint tracked the year-over-year increase of the tool by analyzing the number…https://threatpost.com/cobalt-strike-cybercrooks/167368/

Leaked print spooler exploit lets Windows users remotely execute code as system on your domain controller
Kill this service immediately, An infosec firm accidentally published proof-of-concept code for a critical Windows print spooler remote code execution vuln that could lead to compromise of Active Directory domain controllers. https://www.theregister.com/2021/06/30/windows_print_spool_vuln_rce/

Looking At Chrome Extensions That Hijack Search — Spread Via Malvertising
In this blog post we discuss an ongoing malvertising campaign that pushes search hijacking browser extensions. We take a deep dive into the code of…
https://blog.confiant.com/looking-at-chrome-extensions-that-hijack-search-spread-via-malvertising-28ddc548463c

Russian RU Brute Force Campaign Advisory - ***BEWARE***
CISA strongly encourages users and administrators to review the Joint CSA for GTSS tactics, techniques, and procedures, as well as mitigation strategies.
https://media.defense.gov/2021/Jul/01/2002753896/-1/-1/1/CSA_GRU_GLOBAL_BRUTE_FORCE_CAMPAIGN_UOO158036-21.PDF

****

Hints & Tips plus Security Awareness

CISA Begins Cataloging Bad Practices that Increase Cyber Risk
While extensive guidance on cybersecurity "best practices" exists, additional perspective is needed. Ending the most egregious risks requires organizations to make a concerted effort to stop bad practices.
https://us-cert.cisa.gov/ncas/current-activity/2021/06/29/cisa-begins-cataloging-bad-practices-increase-cyber-risk

Is a Ransomware Attack a Reportable Data Breach?
One question that vexes security engineers, incident responders and lawyers is whether a ransomware attack constitutes a reportable data breach under any of the various data breach disclosure laws, regulations or other requirements. As with anything else in the law, the simple answer is, "it depends."
https://securityboulevard.com/2020/08/is-a-ransomware-attack-a-reportable-data-breach/

Operational Resiliency and the Future of Risk & Resiliency Management – GRC Red Flags
Firms globally and across industries are focusing on risk and resiliency. The organization has to maintain operations in the midst of uncertainty and change, and this is becoming a key regulatory requirement in some industries (e.g., financial services). This requires a holistic view into the objectives…
https://grc2020.com/event/operational-resiliency-and-the-future-of-risk-resiliency-management/?mc_cid=9302d8eef4&mc_eid=a6464752a9

CISA's CSET Tool Sets Sights on Ransomware Threat
CISA has released a new module in its Cyber Security Evaluation Tool (CSET): the Ransomware Readiness Assessment (RRA). CSET is a desktop software tool that guides network defenders through a step-by-step process to evaluate their cybersecurity practices on their networks. CSET—applicable to both information technology (IT) and industrial control system (ICS) networks—enables users to perform a comprehensive evaluation of their cybersecurity posture using many recognized government and industry standards and recommendations. https://us-cert.cisa.gov/ncas/current-activity/2021/06/30/cisas-cset-tool-sets-sights-ransomware-threat

****

News & Views

To pay or not to pay? That is the ransomware question
Government officials in the UK, US and elsewhere have kicked around the idea of laws prohibiting the payment of ransomware, but experts warn against unintended consequences. Then there's another consideration: "[N]o matter what legislation we put in place there's always clever accountants who will find their way around it," says F-Secure's Alan Melia, who helps companies deal with ransomware attacks.
https://www.verdict.co.uk/ransomware-payment-illegal/

Cisco routers come under attack, including a destructive hacktivist campaign
Cisco ASA routers and FTD firewalls are currently seeing exploitation attempts from threat actors and bug bounty hunters alike after proof of concept code was posted online last week.
https://therecord.media/cisco-devices-come-under-new-attacks-including-a-hacktivist-campaign/?utm_campaign=cyber-daily&utm_medium=email&_hsmi=137018509&_hsenc=p2ANqtz-85vJHAUmm356QiYKL_fGmmbp20btvE0q6vc-7_mlc-a_BGiXOYBGkFtH-dZMB7eEkllK_zqjNLO9RT39J7gARNEiRq1Q&utm_content=137018509&utm_source=hs_email

Sign-In Without A Password? The Pros And Cons Of The Alternatives
Using strong and unique passwords for every online account can be a frustrating, cumbersome, and time-consuming effort. Being human, the temptation to reuse passwords across multiple accounts surely exists. But in doing so, we know poor password hygiene can lead to cyberattacks, especially for accounts using the same password. Cyber history has shown us repeatedly that password reuse is very risky, yet we do it anyway. Now, the idea of passing on passwords to verify our identity are taking shape. But don't get in a hurry.
https://www.sosdailynews.com/news.jspx?&articleid=D01ADC77302F8DD4F98CFC2C3596CACE&sx=79

XDR: Security's new frontier
As enterprises transform their IT environment and workforce, finding the right security approach is critical for success. Without the proper protective measures in place, moving services to the cloud can introduce a great deal of risk. https://www.helpnetsecurity.com/2021/06/30/xdr-security/

Windows 11: Understanding the system requirements and the security benefits
Security is a big part of Windows 11, but so is delivering productivity and a good experience with all the security features turned on. https://www.techrepublic.com/article/windows-11-understanding-the-systemrequirementsandthesecuritybenefits/?ftag=TREa988f1c&bhid=78480402&mid=13421212&cid=712423569

Microsoft to Begin Sunsetting Internet Explorer Later This Year
On August 17, 2021, Microsoft will begin to sunset its Internet Explorer (IE) web browser as it plans to discontinue the service altogether by 2022. https://docs.microsoft.com/en-us/lifecycle/faq/internet-explorer-microsoft-edge

****

"Ctrl -F" for The Board

The Business Of Staying Safe Online
The road to keeping a business safe from cybercrime is littered with those having good intentions but poor execution. This can result from lack of insight into what data a company needs to protect most, and how valuable that data is to those looking to exploit it. Different organizations need different approaches to data protection and it's not a one size-fits-all scenario. Providing the right protection for the right data is vital and can help keep a business, well, in business…
https://www.sosdailynews.com/news.jspx?&articleid=7636732EE5861D3F5F4304974172EFC8&sx=79

Evolving Your Cybersecurity Through Cyber Maturity
With ever-increasing cyberattacks targeting high-profile businesses and enterprises, it's easy to understand why this has become a top concern among cybersecurity professionals.
https://www.isaca.org/resources/news-and-trends/newsletters/atisaca/2021/volume-19/evolving-your-cybersecurity-through-cyber-maturity?utm_source=isaca&utm_medium=email-internal&utm_campaign=newatisaca&utm_content=edmi_newatisaca_20210630&utm_term=article-evolvingcyberthrumaturity&cid=edmi_2007627&Appeal=EDMi&sp_rid=MTE4MTI5NDgxNzQwS0&sp_mid=33474784&spMailingID=33474784&spUserID=MTE4MTI5NDgxNzQwS0&spJobID=1965524514&spReportId=MTk2NTUyNDUxNAS2

Questions
Contact FIPCO's Ken Shaurette at 800/722-3498 ext. 251 or email FIPCO IT Services for more information.

"Make Security Part of You and Your Institution's DNA!"

Threat Intelligence Newsletter: July 9, 2021

FIPCO®
IT Audit
Round Table
Discussions

If you would like to host an event, please contact: Amy Petersen

Upcoming Threat Intelligence Peer Group Discussions
None available at the current time

****

Alerts & Warnings

Ahchoo! FluBot Banking Malware Spreads Through Europe, U.S. Likely Next
It may not be time to call the cyber doctor yet, but Proofpoint discovered a new malware virus is spreading rapidly across Europe. One lesson the coronavirus taught us is that virus can spread across borders like.
https://www.sosdailynews.com/news.jspx?&articleid=E0AAB9A346184D5FED98CD95F0FEC043&sx=79

Shocking Amazon Fake Review Scam Revealed In Data Breach
Yet another data security incident involving an ElasticSearch database happened earlier this year. More than 13 million records were made public without any encryption or password protection. But the real news here is how this data breach exposed a database used for fake reviews of products sold on Amazon. The data from over 200,000 Amazon users was compromised, including that of the vendors and reviewers involved in the scam. Security researchers from SafetyDetectives first discovered the database and it's currently unknown who's behind the product review scam.
https://www.sosdailynews.com/news.jspx?&articleid=F07F3CD4B04B10E467C34B338B391D02&sx=79

Fake Browser Updates Source Of Ransomware And Banking Malware
An all-out alarm reported by Surcuri finds bogus alerts circulating about the need to download the latest browser update. Although it's always recommended to keep software up to date, this report finds hackers are exploiting that call to action in a big way.
https://www.sosdailynews.com/news.jspx?&articleid=53145BB7E1358505ECA4883914955837&sx=79

Phishing attack targets DocuSign and SharePoint users
Researchers said most of the emails use COVID-19 as a way to dupe users into clicking on a bogus document. For example, the email will ask the user to review a "Covid 19 relief fund as approved by the board of directors." https://www.scmagazine.com/home/security-news/phishing-attack-targets-docusign-and-sharepoint-users/

****

Hints & Tips plus Security Awareness

Planning to Prevent Account Takeover
When planning an organization's security architecture, there has commonly been a focus on traditional approaches like managing firewalls and ensuring systems are patched. While these are critical components of any organization's best security practices, there have been several key areas of security planning that have been overlooked.
https://www.enzoic.com/planningtopreventaccounttakeover/?utm_medium=email&_hsmi=138581921&_hsenc=p2ANqtz8ZPyP6hdIfWqq0RjiCZEpWWeRjvw5kZ6wKdterXBCxbwnYLEKQ1YxXxHtlXgNnBoUi1BMWtf9g9vhgyUdKbNqD1N-Q&utm_content=138582948&utm_source=hs_email

****

News & Views

Zooming In On Identity Verification: Zoom Adds 2FA To Login Security
As its popularity grew, the widely used Zoom video conferencing app added a layer of login security to its user sign-in protocols.
https://www.sosdailynews.com/news.jspx?&articleid=888954C8A944D770D08DCD84DFB6C8C8&sx=79

In Case You Missed It: CSIAC Podcast – Entity Resolution for Cyber (Pt 1 & 2) - CSIAC
The foundational level of situation awareness lies in perception of the surrounding environment. In cyberspace, this relates to an ability to enumerate and identify elements of the cyber terrain, particularly, network-connected devices that are employed to accomplish a user's goals. These devices emit a plethora of signals in network traffic and server logs as they negotiate for services, but they do not share consistent features in those signals that make it straightforward to uniquely identify which hosts are active over a period of interest. This podcast presents a cyber Entity Resolution approach and blocking technique designed to bridge this gap. The technique is based on the construction and comparison of periodic snapshots of collections of "host segments," that are built up from multiple log files.
https://www.csiac.org/series/entity-resolution-for-cyber/

Questions
Contact FIPCO's Ken Shaurette at 800/722-3498 ext. 251 or email FIPCO IT Services for more information.

"Make Security Part of You and Your Institution's DNA!"

Threat Intelligence Newsletter: July 19, 2021

FIPCO®
IT Audit
Round Table
Discussions

If you would like to host an event, please contact: Amy Petersen

Upcoming Threat Intelligence Peer Group Discussions
None available at the current time

New StopRansomware.gov website – The U.S. Government's One-Stop Location to Stop Ransomware
The U.S. Government launched a new website to help public and private organizations defend against the rise in ransomware cases. StopRansomware.gov is a whole-of-government approach that gives one central location for ransomware resources and alerts. We encourage organizations to use this new website to understand the threat of ransomware, mitigate risk, and in the event of an attack, know what steps to take next. https://us-cert.cisa.gov/ncas/current-activity/2021/07/15/new-stopransomwaregov-website-us-governments-one-stop-location

****

Alerts & Warnings

Next Online PDF You Open can be a Part of Phishing Campaign
Stealing corporate credentials is a lucrative business in the underground markets. Threat actors have been found to go to various lengths to obtain those. Now, another group of cybercriminals has been observed impersonating Adobe online services and using fake notifications to lure their victims.
https://cyware.com/news/nextonlinepdfyouopencanbeapartofphishingcampaigne5879abe?_hsmi=78978938&_hsenc=p2ANqtz9Km3YwGxcmD8dzuqgMLlxnRtiB4ifn1MaykvU1FShkEvAUN_WINnuKiiGjGdIhfJYGDRsrhn03I6ZMrWXwfWLLJzILNw

Microsoft discovers critical SolarWinds zero-day under active attack
Only SolarWinds Serv-U Managed File Transfer and Serv-U Secure FTP—and by extension, the Serv-U Gateway, a component of those two products—are affected by this vulnerability, which allows attackers to remotely execute malicious code on vulnerable systems.
https://arstechnica.com/gadgets/2021/07/microsoft-discovers-critical-solarwinds-zero-day-under-active-attack/?_hsmi=78978938&_hsenc=p2ANqtz_EE8kOK_kQq_zRE9urThWF4qjYeaTPZtT0_lPAxS93DAeyUOc52kjsp7r7FH1m19IQiLmz9ScSlQLTabkFAb7VqWLw

****

Hints & Tips plus Security Awareness

VMware ESXi updates address authentication and denial of service vulnerabilities (CVE-2021-21994, CVE-2021-21995)
Please see the advisory here: https://www.vmware.com/security/advisories/VMSA-2021-0014.html

VMware ThinApp update addresses a DLL hijacking vulnerability (CVE-2021-22000)
Please see the advisory here: https://www.vmware.com/security/advisories/VMSA-2021-0015.html

Microsoft Patches 3 Under-Attack Windows Zero-Days:
Microsoft's embattled security response unit uses Patch Tuesday to respond to a new set of Windows zero-day attacks https://www.securityweek.com/microsoft-patches-3-under-attack-windows-zero-days

Five Days That Will Revolutionize Your Online Safety
Are you full of good intentions about your computer and online safety but never quite get around to doing all those things you know you should do, like changing passwords and security settings?
https://www.cisa.gov/sites/default/files/publications/Week1TipCard-%20508%20compliant.pdf

NO COST, Security & Privacy Metaframework
The SCF has the ambitious goal of providing FREE cybersecurity and privacy control guidance to cover the strategic, operational and tactical needs of organizations, regardless of its size, industry or country of origin. https://www.securecontrolsframework.com/

15 Types Of Cyber Attacks To Look Out For
Are you "cyber attack" conscious? What network security measures do you put in place to safeguard your business and critical data? https://robots.net/tech/15-types-of-cyber-attacks/

****

News & Views

Kaseya Ransomware Attack: Guidance and Resources
CISA has created a webpage to provide information and guidance for the recent ransomware attack against Kaseya customers that include managed service providers (MSPs) and customers of those MSPs. CISA encourages affected organizations to review Kaseya Ransomware Attack: Guidance for Affected MSPs and their Customers for more information. https://us-cert.cisa.gov/kaseya-ransomware-attack

Colorado becomes latest state to pass data privacy law
Colorado has become the third state, following in the footsteps of California and Virginia, to pass a comprehensive data privacy law that effectively forces companies to make changes to how they manage personally identifiable information online. The act, called the Colorado Privacy Act, was signed into law on July 7. https://www.zdnet.com/article/colorado-becomes-latest-state-to-pass-data-privacy-law/

HR should get ready for state-level privacy laws
States such as Colorado and Virginia are enacting privacy laws that will stretch IT, compliance and HR departments' ability to comply, write Zoe Argento and Philip Gordon of law firm Littler. "Human resources professionals cannot ignore state privacy laws, like the Colorado Privacy Act and the VACDPA, just because they do not apply to HR data," they write… https://www.jdsupra.com/legalnews/as-colorado-and-virginia-follow-1801587/

Be prepared for a national privacy law to materialize
A US privacy law could streamline the data collection process, but only if it takes precedence over the growing patchwork of state regulations, writes Philip Kushmaro of consent management platform Usercentrics. Kushmaro advises enterprises to be prepared because not being transparent with consumers "goes beyond fines; a bad reputation is harder to bounce back from."
https://www.cpomagazine.com/data-protection/the-future-of-data-privacy-consent-are-brands-ready-for-a-national-privacy-law

****

"Ctrl -F" for The Board

Is Cybersecurity Insurance For Me? What To Know (if you'd like more information reach out to Jeff Otteson jeffo@mbisllc.com at MBIS a subsidiary of the Wisconsin and Minnesota Bankers Associations for assistance)
The pandemic provided a catalyst for cyberattacks to spike in ways that had yet to be seen. According to a report by the Identity Theft Resource Center, when compared to the last quarter of 2020, the number of cybercrime victims is up 564% so far this year. For the right person or business, cybersecurity insurance can make a lot of sense. Help with recovering from a cyberattack is something everyone can use, especially with the chaos and financial losses that can follow.
https://www.sosdailynews.com/news.jspx?&articleid=48843306A95A1E35A841DEDB0592A89C&sx=79

FROM TECHNICAL ANALYST TO BUSINESS ENABLER:
What CISOs Must Have to Lead the Company…. https://info.processunity.com/rs/638-QKL-150/images/White-Paper-From-Technical-Analyst-To-Business-Enabler.pdf

Questions
Contact FIPCO's Ken Shaurette at 800/722-3498 ext. 251 or email FIPCO IT Services for more information.

"Make Security Part of You and Your Institution's DNA!"

Threat Intelligence Newsletter: July 26, 2021

FIPCO®
IT Audit
Round Table
Discussions

If you would like to host an event, please contact: Amy Petersen

Upcoming Threat Intelligence Peer Group Discussions
None available at the current time

****

Alerts & Warnings

Update Your Chrome Browser to Patch New Zero Day Bug Exploited in the Wild
Google has released Chrome 91.0.4472.164 for Windows, Mac, and Linux to fix seven security vulnerabilities, one of them a high severity zero-day vulnerability exploited in the wild… https://www.bleepingcomputer.com/news/security/google-patches-8th-chrome-zero-day-exploited-in-the-wild-this-year/

WifiDemon – iPhone Wifi bug exposed devices to remote attacks
Dubbed WifiDemon by researchers; the attack required the victim's wifi to be set on auto-join which is by default in iPhones… https://www.hackread.com/wifidemon-iphone-wifi-bug-remote-attacks/

This new password-stealing Windows malware is distributed via ads for cracked software
Cybersecurity company Bitdefender has discovered a new form of malware that is delivered to victims via advertisements that appear in search results. Bitdefender states that the malware is being used as a gateway for attackers to steal passwords, deliver additional malware, and install cryptocurrency miners. The malware targets Windows devices… https://www.zdnet.com/article/this-password-stealing-windows-malware-is-distributed-via-ads-in-search-results/

NPM Package Steals Passwords via Chrome's Account-Recovery Tool
A new widespread software supply-chain attack has been discovered by researchers, this time consisting of a password stealer harvesting credentials from Chrome on Windows systems via a tool called ChromePass. According to researchers, the campaign was discovered after professionals caught the malware stealing credentials, listening for incoming commands from the… https://threatpost.com/npm-package-steals-chrome-passwords/168004/

This new password-stealing Windows malware is distributed via ads for cracked software
Cybersecurity company Bitdefender has discovered a new form of malware that is delivered to victims via advertisements that appear in search results. Bitdefender states that the malware is being used as a gateway for attackers to steal passwords, deliver additional malware, and install cryptocurrency miners. The malware targets Windows devices… https://www.zdnet.com/article/this-password-stealing-windows-malware-is-distributed-via-ads-in-search-results/

****

Hints & Tips plus Security Awareness

Stop the Hidden Spy In Your Email
When an email lands in your inbox, you may think it's just for you, that the sender has no idea what you do with it, and that it's for your eyes only. Not so, SCAMBUSTERS https://scambusters.org/emailtracking.html
https://www.theverge.com/22288190/email-pixel-trackers-how-to-stop-images-automatic-download

Privacy Threat Modeling
The LINDDUN privacy engineering framework provides systematic support for the elicitation and mitigation of privacy threats in software systems. Its main strength is its combination of methodological guidance and privacy knowledge support… https://www.linddun.org/linddun

NIST SP800-47 Publication Managing the Security of Information Exchange
This publication focuses managing the protection of the information being exchanged or accessed before, during, and after the exchange rather than on any particular type of technology-based connection or information access or exchange method and thus provides guidance on identifying information exchanges, considerations for protecting exchanged information, and the agreement(s) needed to help manage protection of the exchanged information. Organizations are expected to tailor the guidance to meet specific organizational needs and requirements regarding the information exchange…
https://csrc.nist.gov/publications/detail/sp/800-47/rev-1/final

Preventing the Next Cybersecurity Attack with Effective Cloud Security Audits
The use of cloud services to support business needs has exponentially increased over the past years. Most companies have now moved from traditional IT environments to private or public cloud deployments to support IT, security and business needs.
The increase in cloud services usage comes with a great responsibility for cloud providers and cloud customers. Conducting proactive and regular security audits is necessary to secure these services…
https://www.isaca.org/resources/news-and-trends/newsletters/atisaca/2021/volume-22/preventing-the-next-cybersecurity-attack-with-effective-cloud-security-audits?utm_source=isaca&utm_medium=email-internal&utm_campaign=newatisaca&utm_content=edmi_newatisaca_20210721&utm_term=bau-article-cloudsecurityaudits&cid=edmi_2007826&Appeal=EDMi&sp_rid=MTE4MTI5NDgxNzQwS0&sp_mid=33528214&spMailingID=33528214&spUserID=MTE4MTI5NDgxNzQwS0&spJobID=1984707094&spReportId=MTk4NDcwNzA5NAS2

****

News & Views

Kaseya Ransomware Attack: Guidance and Resources
CISA has created a webpage to provide inform
A US privacy law could streamline the data collection process, but only if it takes precedence over the growing patchwork of state regulations, writes Philip Kushmaro of consent management platform Usercentrics. Kushmaro advises enterprises to be prepared because not being transparent with consumers "goes beyond fines; a bad reputation is harder to bounce back from…"
https://www.cpomagazine.com/data-protection/the-future-of-data-privacy-consent-are-brands-ready-for-a-national-privacy-law/

****

"Ctrl -F" for The Board

There's no excuse to be unprepared for a ransomware hit: Advanced Common Sense Advice
Legal and C-suite teams should make decisions ahead of time regarding possible cybersecurity worst-case scenarios, writes Alex Holden, chief information security officer at Hold Security. Holden notes the ISACA Ransomware Pulse Poll, in which about half of enterprises consider ransomware to be their biggest cyberthreat…
https://www.rsaconference.com/library/Blog/confronting-the-ransomware-crisis-advanced-common-sense-advice

Questions
Contact FIPCO's Ken Shaurette at 800/722-3498 ext. 251 or email FIPCO IT Services for more information.

"Make Security Part of You and Your Institution's DNA!"

Threat Intelligence Newsletter: July 30, 2021

FIPCO®
IT Audit
Round Table
Discussions

If you would like to host an event, please contact: Amy Petersen

Upcoming Threat Intelligence Peer Group Discussions
None available at the current time

****

Alerts & Warnings

Is someone tracking you? Signs that you may have been targeted by stalkerware
These are many indicators that stalkerware is potentially being used against you. We'll go through some of the common signs and learn whether it is actually safe to uninstall the malicious program… https://cybernews.com/editorial/is-someone-tracking-you-signs-that-you-may-have-been-targeted-by-stalkerware/?utm_source=newsletter&utm_medium=email&utm_campaign=CyberNewsLetter_spyware

Microsoft Rushes Fix for 'PetitPotam' Attack PoC
Microsoft rushed to release mitigations for a new exploit that forces remote Windows systems to reveal password hashes that can easily be cracked by malicious actors. The flaw lies in the Windows NT LAN Manager, according to the company, and has been dubbed PetitPotam. Microsoft has released an advisory that… https://threatpost.com/microsoft-petitpotam-poc/168163/

FakeSpy Data-Stealing App Returns, Now Using U.S.P.S. As Cover
Postal services around the globe are now being targeted by an Android malware that's back with a vengeance. FakeSpy is believed to be the spawn of a Chinese hacking group known as Roaming Mantis. This data stealing app first seen in 2017, has made a new and much improved debut. Originally targeting only postal services in South Korea and Japan, the vastly upgraded malware app now targets those services worldwide, including the U.S. Postal Service (U.S.P.S.)…
https://www.sosdailynews.com/news.jspx?&articleid=87E2A8AADBAEDFF1007E8D50FBC8D3B6&sx=79

Top Routinely Exploited Vulnerabilities
CISA, the Australian Cyber Security Centre (ACSC), the United Kingdom's National Cyber Security Centre (NCSC), and the U.S. Federal Bureau of Investigation (FBI) have released the Joint Cybersecurity Advisory Top Routinely Exploited Vulnerabilities, which details the top vulnerabilities routinely exploited by malicious actors in 2020 and those being widely exploited thus far in 2021…
https://uscert.cisa.gov/ncas/alerts/aa21-209a

Advisory PDF:
https://uscert.cisa.gov/sites/default/files/publications/AA21209A_Joint%20CSA_Top%20Routinely%20Exploited%20Vulnerabilities.pdf

Microsoft warns of credential-stealing NTLM relay attacks against Windows domain controllers
To ward off the attack known as PetitPotam, Microsoft advises you to disable NTLM authentication on your Windows domain controller…
https://www.techrepublic.com/article/microsoftwarnsofcredentialstealingntlmrelayattacksagainstwindowsdomaincontrollers/?ftag=TREa988f1c&bhid=78480402&mid=13454137&cid=712423569

Malware developers use new methods to escape detection
Malware developers are turning to unusual programming languages to hide their activities, report researchers from BlackBerry. "Malware authors are known for their ability to adapt and modify their skills and behaviors to take advantage of newer technologies," says BlackBerry executive Eric Milam, who also notes the "inherent lack of coverage from protective solutions." This is why there is a growing need for XDR (Extended Detection and Response Systems) that can correlate across uses, files, network and hosts – add in deception technology and the malware has a much lower potential for attackers to be successful.
https://www.zdnet.com/article/malware-developers-turn-to-exotic-programming-languages-to-thwart-researchers/

****

Hints & Tips plus Security Awareness

Ways To See If Your Data Has Been Stolen
With all the data breaches, whether by intrusion or accident lately, it's likely your information was exposed somehow to someone you didn't intend. After all, the marketing company Exactis, exposed hundreds of traits on us in 350 million records. Yahoo let out email addresses and passwords on billions of people, and of course who can forget the massive breach of Equifax just last year. There is a lot of information that gets leaked on us and the more the bad actors have on us, the more targeted their phishing campaigns can be. Checking on whether or not your data is available in the underground can help you mitigate any fraud or identity theft…
https://www.sosdailynews.com/news.jspx?&articleid=FAD22EBD9FF8E92FF0BA869DAB62463F&sx=79

7 Banking Fraud Myths Busted
A complimentary Independent Banker Magazine webinar with content by Harland Clarke, a Vericast Business…
https://event.webcasts.com/starthere.jsp?ei=1482352&tp_key=9c50db4b71&utm_medium=email&_hsmi=143030731&_hsenc=p2ANqtz8wGErTYYOisZkeTJUr18Ye3xsfh14RLsnlCgYCWGCXoKWtloRlHYsbB25EZlgcpwlgxx-0spODH3yfOUnj_T-ULqpXw&utm_content=143030731&utm_source=hs_email

****

News & Views

A Look At 2021 Hacking Trends Inherited From 2020

With the price tag for cybercrime set to hit $6 trillion globally this year, 2020 provided a massive and historic spike in cybercrime that continues today. The pandemic alone provided the environment for a cybercrime explosion. What we're now seeing are improvements to the cybercrimes of last year, making them more effective and devastating than ever. Cybersecurity experts find last year's attacks exposed weaknesses in our systems that continue to provide criminal opportunities today… https://www.sosdailynews.com/news.jspx?&articleid=D1C43F2EF20D838C7A251C245D8DD010&sx=79

Top Phishing Scams Continue To Improve And Grow

Much to our dismay, cybercrooks keep finding ways to better the phishing tools they have and find other ways to include new and sneakier methods of thievery. Organizations and individuals are targets and money, identities, credentials, and more are stolen from both every day. Even cyber-savvy users can get caught in phishing scams if they don't pay close attention to the signs and signals that something isn't quite right. Reviewing the most pervasive phishing scams is always recommended… https://www.sosdailynews.com/news.jspx?&articleid=E958B090105A4D4984D7C7F238486A47&sx=79

Law enforcement, CISA lobby for breach reporting requirement

At a Senate Judiciary hearing covering ransomware policy, federal agencies homed-in on requiring enterprise to report breaches… https://www.scmagazine.com/analysis/legislation/law-enforcement-cisa-lobbyforbreachreportingrequirement?utm_source=newsletter&utm_medium=email&utm_campaign=SCUS_Newswire_%7B%7B%27now%27%7Cdate%3A%27%25Y%25m%25d%27%7D%7D&hmSubId=%7B%7Bcontact.cms_id_encrypted%7D%7D&email_hash=%7B%7Bcontact.email%7Cmd5%7D%7D&oly_enc_id=0795J7353967J0E

Why "shame culture" tactics put IT in a bad light (that's the phish testing culture)

Sending fake phishing emails to see if employees can be tricked is likely counterproductive, argues systems administrator Scott Matteson. CEO Sai Venkataraman of SecurityAdvisor says such "shame culture" tactics tend to position "the internal IT teams negatively in the eyes of the organization's employees, making it more challenging to get people on board with strategic initiatives…" https://www.techrepublic.com/article/how-to-create-a-positive-and-effective-cybersecurity-environment-instead-of-a-shame-culture/

Discord under siege: chat service used to host, spread, and control malware

It is no wonder that popular social networks immediately find themselves in great demand by cybercriminals, too. For example, encrypted chat apps, such as Telegram, Signal, and Whatsapp, have been instrumental in dismantling authoritarian regimes and organizing uprisings. However, because of their private nature, cybercriminals exploit them to sell illegal goods… https://cybernews.com/security/discordundersiegechatserviceusedtohostspreadandcontrolmalware/?utm_source=newsletter&utm_medium=email&utm_campaign=CyberNewsLetter_26

****

"Ctrl -F" for The Board

Leveraging People in the Email Security Battle
Leveraging humans for detection makes it hard for the attackers to predict whether or not their malicious emails will be identified and using technology to automate response provides scale and speed in resolution… https://www.securityweek.com/leveraging-people-email-security-battle

Questions
Contact FIPCO's Ken Shaurette at 800/722-3498 ext. 251 or email FIPCO IT Services for more information.

"Make Security Part of You and Your Institution's DNA!"

Threat Intelligence Newsletter: August 6, 2021

FIPCO®
IT Audit
Round Table
Discussions

If you would like to host an event, please contact: Amy Petersen

Upcoming Threat Intelligence Peer Group Discussions
None available at the current time

InfraGard National Announces Key Partnership with CyberRisk Alliance & Launch of Critical Infrastructure Benchmark Survey
InfraGard National is thrilled to announce a key partnership with the CyberRisk Alliance (CRA), an influential information services company serving the cybersecurity community, which includes the Cybersecurity Collaborative, SC Media and InfoSec World. The partnership will employ CRA's diverse business intelligence platforms to deliver a series of cybersecurity resources and membership activities to you, including local, state and federal law enforcement entities, government agencies, and academic institutions.
After completing the survey, you will automatically receive a CIR score (out of 100) along with general guidance and comments based on your score…
https://cyberriskalliance.iad1.qualtrics.com/jfe/form/SV_81vxT1mIvV4jEl8?eType=EmailBlastContent&eId=8e1af10f-47d8-4d63-bbae-e59bd120bead
(survey should take about 10 minutes)

ABA Refreshes #BanksNeverAskThat Campaign for 2021
Registration is now open for banks of all sizes to participate in the second iteration of ABA's award-winning #BanksNeverAskThat anti-phishing campaign. Created on 2020 to help consumers fight phishing fraud, last October's #BanksNeverAskThat campaign saw nearly 1,700 banks participating. This year ABA hopes to recruit even more banks to join the industry-wide effort…
https://www.aba.com/advocacy/communityprograms/banksneveraskthat?utm_campaign=NEWSBYTES-20210802&utm_medium=email&utm_source=Eloqua

****

Alerts & Warnings

That email from Microsoft might be a clever ruse
About 43% of phishing attacks try to impersonate Microsoft, security solutions provider Barracuda reports after studying 12 million attacks. "Cybercriminals are getting sneakier about who they target with their attacks, often targeting employees outside the finance and executive teams, looking for a weak link in your organization," says Barracuda executive Don MacLennan… https://cio.economictimes.indiatimes.com/news/digital-security/it-staff-receive-upto-40-targeted-phishing-attacks-a-year-report/84848399

Microsoft labels latest phishing campaign "crafty"
Microsoft is warning clients of Office 365 of a "crafty" and "sneakier than usual" email phishing attack scheme, complete with spoofed sender addresses. The cybercriminals are spreading Microsoft branding and using SharePoint "in the display name to entice victims"… https://www.zdnet.com/article/microsoft-watch-out-for-this-sneakier-than-usual-phishing-attack/

Microsoft warns of NTLM relay attacks
Description: Microsoft released an advisory last week with a workout for recently discovered NTLM relay attacks. A tool, called PetitPotam, works against servers that enable NTLM authentication and Active Directory Certificate Services. An attacker could use this tool to abuse the Microsoft Encrypting File System Remote Protocol to authenticate to another server. An adversary could carry out this attack without any prior authentication. Microsoft and other security researchers advise disabling NTLM authentication on domain controllers. Users could also disable NTLM on any AD CS servers and NTLM for IIS AD CS servers… https://duo.com/decipher/microsoft-issue-guidance-for-mitigating-petitpotam-ntlm-relay-attack

Chipotle Emails Serve Up Phishing Lures
According to new information, a breach of Chipotle's restaurant email marketing service last month has lead to customers being targeted with phishing lures in seemingly legitimate emails that then harvested users' credentials. This attack mirrors earlier Nobelium attacks, according to researchers at Inky, who first reported that Chipotle's email vendor… https://threatpost.com/chipotle-serves-up-lures/168279/

NSA Warns Public Networks are Hacker Hotbeds
The NSA has warned that attackers are targeting teleworkers taking advantage of free public networks to steal corporate data that may be sensitive. The US National Security Agency offered advice to security teams that are seeking the best wireless practices to protect corporate networks and personal devices. According to the… https://threatpost.com/nsa-warns-public-networks-are-hacker-hotbeds/168268/

Vultur Malware Targeting Android Banking Customers
A new malware strain that has been discovered called Vultur and is targeting banking customers using invisible windows and keylogging to capture their banking data on Android phones… https://informationsecuritybuzz.com/expert-comments/vultur-malware-targeting-android-banking-customers/?_hsmi=78978938&_hsenc=p2ANqtz8e6tdlm8w5UInYpYGjvcF2z3Ypq4YjGLwAHCWgddwlVrylVvmkKUnV3hScePhI_7qjyN8Cz8XyC6_YgpuOGD8XUjeCQ

PayPal Shopping Alert! New Skim Scam Steals Your PayPal Payment Info
If you're holiday shopping, after holiday shopping, or just purchasing the everyday stuff, there's a new take on a skimming payment scam affecting PayPal users worldwide. There are 305 million active PayPal accounts globally since the end of last year, with almost 44% of those users in the U.S. This latest skim scam is popping up just in time to steal your gift giving spirit and your money, but being aware of it can help PayPal shoppers avoid becoming the next victim…
https://www.sosdailynews.com/news.jspx?&articleid=56209648C727C1019A77D6FE627FBCF9&sx=79

GEO-IP May Not Be of Much Use
A WSIC Special Agent caught a LexisNexis fraud investigation webinar with a "reformed cybercriminal" speaking. Discussed a technique he used, connecting via a SOCKS5 proxy to try to appear local, etc. Validated tactics observed in some ongoing fraud activity in Wisconsin (e.g. coming in from a SOCKS5 proxy in Wisconsin, so geo-ip isn't of much use)…
https://risk.lexisnexis.com/insightsresources/video/government-identity-fraud-summit

Phishing scheme targets unemployment insurance benefits and PII
Have you gotten an alarming text message about your unemployment insurance benefits from what seems to be your state workforce agency? You're not alone. Identity thieves are targeting millions of people nationwide with scam phishing texts aimed at stealing personal information, unemployment benefits, or both… https://www.consumer.ftc.gov/blog/2021/08/phishing-scheme-targets-unemployment-insurance-benefits-and-pii?utm_source=govdelivery

****

Hints & Tips plus Security Awareness

Questions to work through with a cloud security vendor
Vendors of compliance software should take security as seriously as you do, writes Dale Sanders of StarCompliance. Sanders outlines four areas to cover and suggests using a vendor that submits to independent audits because "it's a strong indication that they're likely committed to and prioritizing their own security as well as yours"… https://internationalbanker.com/technology/four-considerations-to-ensure-your-compliance-software-vendor-prioritizes-data-security/

Utility Services Scam
Jim Stickley talks with a targeted victim of a Utility Services Scam. She was lucky and hung up before they got her info, but her story points out just how easy it is for criminals to call you pretending to be from your gas and electric company!...
https://www.sosdailynews.com/news.jspx?&articleid=D527409DF64AB42FA8063A423038E2F7&sx=79

How to manage passwords:
Best practices and security tips, Too short, too complex, too frequently used, too many to remember: There are any number of problems with passwords. Individuals can use password managers to strike a balance between security and convenience. However, these services have their own security risks. This ebook takes a look at pros and the cons of password managers, password alternatives, how to pick a secure password, and more…
https://lgstatic.techrepublic.com/direct/whitepapers/TR_How_to_manage_passwordsV2.pdf

Social engineering goes automatic: new robocall bot on Telegram can trick you into giving up your password
Getting a call from a scammer pretending to be a tech support agent isn’t fun. It’s certainly tedious for the potential victim listening to someone trying to rob them blind by exploiting their goodwill. It’s probably even tedious for the scammer – calling hundreds of people each and every day can make scamming seem like actual work…
https://cybernews.com/security/newrobocallbotontelegramcantrickyouintogivingupyourpassword/?utm_source=newsletter&utm_medium=email&utm_campaign=CyberNewsLetter_27

10 BEST Ransomware Protection Solutions For Enterprises 2021
Ransomware Protection Solutions with features to select the best Ransomware Protection Software Tools as per your requirement…. If you’d like to get a demonstration of the top one, contact FIPCO for more information… https://www.softwaretestinghelp.com/ransomware-protection-solutions/

****

News & Views

Hackers leak full EA data after failed extortion attempt
The hackers who breached Electronic Arts last month have released the entire cache of stolen data after failing to extort the company and later sell the stolen files to a third-party buyer...
https://therecord.media/hackersleakfulleadataafterfailedextortionattempt/?_hsmi=78978938&_hsenc=p2ANqtzJb4AZ02O9QSJ2AEoY7IcAgXf5QEBXksujcUiV1DlqZNB9LckEE2VG5bNCH1lTZN7mRwh73oM6V59gJ4R9hI-l0QLgA

Ransomware Changes: DoppelPaymer Rebrands; Babuk Evolves
The ransomware landscape constantly changes, which can make it difficult to track which attackers are coming, going or simply rebranding. Glad we implemented leading edge Cynet360 XDR backed by world class threat intel and 24x7x365 monitoring… https://www.databreaches.net/ransomware-changes-doppelpaymer-rebrands-babuk-evolves/?_hsmi=78978938&_hsenc=p2ANqtz-9IzKgoNkJeI7tQ4-ZaBLyeWE4BITKdmIJohu-znunSQTA2fPm2WWj2RIF-0C1RP3Wzw52_H_vW40G-Itmqwib2UtoPtw

How IT Auditors Can Avoid Becoming Prey in the Corporate Jungle
“Survival of the fittest,” a phrase first coined by Herbert Spencer after reading Charles Darwin’s On the Origin of Species, describes what may be called the cardinal rule of the jungle. Darwin used it to describe the process of natural selection…
https://www.isaca.org/resources/newsandtrends/newsletters/atisaca/2021/volume-24/how-it-auditors-canavoidbecomingpreyinthecorporatejungle?utm_source=isaca&utm_medium=emailinternal&utm_campaign=newatisaca&utm_content=edmi_newatisaca_20210804&utm_term=bauarticleitaudnavcorpjungle&cid=edmi_2008017&Appeal=EDMi&sp_rid=MTE4MTI5NDgxNzQwS0&sp_mid=33563165&spMailingID=33563165&spUserID=MTE4MTI5NDgxNzQwS0&spJobID=2003231744&spReportId=MjAwMzIzMTc0NAS2

Spear phishing attacks underline how much dangerous phishing has gotten
Phishing is getting smarter. A type of social engineering attack in which the attacker uses fraudulent messages that are designed to fool the would-be victim into sharing sensitive information or clicking a particular link, phishing has long been part of life on the internet… https://www.hackread.com/spear-phishing-attacks-underline-danger/

****

"Ctrl -F" for The Board

Top Routinely Exploited Vulnerabilities of 2020 Be Prepared for 2021/22
This Joint Cybersecurity Advisory was coauthored by the U.S. Cybersecurity and Infrastructure Security Agency (CISA), the Australian Cyber Security Centre (ACSC), the United Kingdom's National Cyber Security Centre (NCSC), and the U.S. Federal Bureau of Investigation (FBI)…
https://uscert.cisa.gov/ncas/alerts/aa21-209a

True cybersecurity means centering policies on employee behavior, report says
Protecting systems from bad actors is essential, but all the firewalls in the world are useless against the modern hacker who targets human weaknesses instead of digital ones…
https://www.techrepublic.com/article/true-cybersecurity-means-centering-policies-on-employee-behavior-report-says/?ftag=TREa988f1c&bhid=78480402&mid=13462239&cid=712423569

Questions
Contact FIPCO's Ken Shaurette at 800/722-3498 ext. 251 or email FIPCO IT Services for more information.

"Make Security Part of You and Your Institution's DNA!"

Threat Intelligence Newsletter: August 13, 2021

FIPCO®
IT Audit
Round Table
Discussions

If you would like to host an event, please contact: Amy Petersen

Upcoming Threat Intelligence Peer Group Discussions
None available at the current time

CISA Launches New Joint Cyber Defense Collaborative
CISA is establishing the JCDC to integrate unique cyber capabilities across multiple federal agencies, many state and local governments, and countless private sector entities to achieve shared objectives. Specifically, the JCDC will: https://www.cisa.gov/news/2021/08/05/cisa-launches-new-joint-cyber-defense-collaborative?utm_campaign=RiskCyber-20210809&utm_medium=email&utm_source=Eloqua

****

Alerts & Warnings

Pegasus Spyware — A Zero Click Attacker
Spyware word is normal for a non-technical person. A technical person is aware of this. Spyware is software with malicious behavior. Around 90% of computers are infected with Spyware around the world.
https://medium.com/technology-hits/pegasus-spyware-a-zero-click-attacker-48a9872f887e

Microsoft patches actively exploited zero-day (CVE-2021-36948), more Print Spooler flaws
Microsoft’s August 2021 Patch Tuesday is pretty lightweight, through it covers a wide variety of Microsoft solutions. 44 CVE-numbered security holes have been plugged, seven of which are critical, and one is actively exploited (CVE-2021-36948).
https://www.helpnetsecurity.com/2021/08/10/cve-2021-36948-patch-tuesday/

Scammers Use Phone Hacking and Hijacking for Phishing
Smartphone hacking is big news these days. And it's not just the recent sensational news about Pegasus spyware. Phone hacking is everywhere, and it could be on your cell right now.
https://scambusters.org/phonehacking.html

FlyTrap Android Malware Used to Compromise Facebook Accounts
Thousands of Facebook accounts have reportedly been compromised by the Android malware since March. https://www.pcmag.com/news/flytrap-android-malware-used-to-compromise-facebook-accounts

Attackers Scanning for Microsoft Exchange ProxyShell Vulnerabilities
Threat actors are actively scanning for Microsoft Exchange ProxyShell vulnerabilities. Microsoft released fixes for the three vulnerabilities in April; advisories were published in May and July. Technical details about the flaws were disclosed at the Black Hat conference last week.
https://www.bleepingcomputer.com/news/microsoft/microsoft-exchange-servers-scanned-for-proxyshell-vulnerability-patch-now/

****

Hints & Tips plus Security Awareness

Citrix Releases Security Update for ShareFile Storage Zones Controller
Citrix has released a security update to address a vulnerability affecting Citrix ShareFile storage zones controller. An attacker can exploit this vulnerability to obtain access to sensitive information.
https://www.bleepingcomputer.com/news/microsoft/microsoft-exchange-servers-scanned-for-proxyshell-vulnerability-patch-now/

VulnHub Aim/Goal
To provide materials that allows anyone to gain practical 'hands-on' experience in digital security, computer software & network administration. https://www.vulnhub.com/about/

Important Security Update – ProxyShell
A new attack vector named ProxyShell was recently disclosed. ProxyShell is a Microsoft Exchange server vulnerability which provides an attacker with unauthenticated remote code execution (RCE) capabilities.
https://www.cynet.com/attacktechniqueshandson/cyopsimportantsecurityupdateproxyshell/?utm_medium=email&_hsmi=148485315&_hsenc=p2ANqtz8zt0HHw5VsmXlf7ZmpKR59UJUVR9TIipaly7oWlQFu7DSBGrv38300P1RkHoM8QNevVLVJVkP_X1Y5kx2SOUhrlax66Q&utm_content=148485315&utm_source=hs_email

****

News & Views

Ambitious criminals expose a million credit cards' info
Hackers have reportedly given away the information on more than a million credit cards on the dark web, affecting up to 500 banks, to promote their new criminal enterprise. Italian researchers say more than 50% of the cards are valid and "not yet identified as compromised." https://www.itpro.co.uk/security/cyber-crime/360534/cyber-criminals-leak-one-million-credit-cards-on-the-dark-web

Second FinCEN Exchange on Ransomware to Take Place in August
WASHINGTON—The Financial Crimes Enforcement Network (FinCEN) today announced it will convene a FinCEN Exchange in August 2021 with representatives from financial institutions, other key industry stakeholders, and federal government agencies to discuss ongoing concerns regarding ransomware, as well as efforts by the public and private sectors. The FinCEN Exchange will build upon FinCEN's November 2020 event on ransomware. FinCEN anticipates that this FinCEN Exchange will assist its government and private sector partners to inform next steps to address ransomware and focus resources to mitigate the threat. This announcement is part of a whole-of-government effort to combat ransomware.
https://www.fincen.gov/news/news-releases/second-fincen-exchange-ransomware-take-place-august

Can the public cloud become confidential?
It's been often said that the only two certain things in life are death and taxes. Over the past ten years, it seems data breaches can be added to this list. Can an organization really be completely safe – without fear of losing confidential or regulated data, company secrets, and (increasingly) proprietary algorithms and AI code? https://www.helpnetsecurity.com/2021/08/06/public-cloud-confidential/

Questions
Contact FIPCO's Ken Shaurette at 800/722-3498 ext. 251 or email FIPCO IT Services for more information.

"Make Security Part of You and Your Institution's DNA!"

Threat Intelligence Newsletter: September 7, 2021

FIPCO®
IT Audit
Round Table
Discussions

If you would like to host an event, please contact: Amy Petersen

Upcoming Threat Intelligence Peer Group Discussions
None available at the current time

****

Alerts & Warnings

Phishing campaign leverages legit DocuSign email notifications
Obfuscation techniques such as steganography can help the scanners circumvent security measures designed to prevent malicious attachments from being hosted on DocuSign's servers. https://www.scmagazine.com/analysis/cloud/phishingcampaignleverageslegitdocusignemailnotifications?utm_source=newsletter&utm_medium=email&utm_campaign=SCUS_Newswire_%7B%7B%27now%27%7Cdate%3A%27%25Y%25m%25d%27%7D%7D&hmSubId=%7B%7Bcontact.cms_id_encrypted%7D%7D&email_hash=%7B%7Bcontact.email%7Cmd5%7D%7D&oly_enc_id=0795J7353967J0E

Exchange Servers Under Active Attack via ProxyShell Bugs
A researcher at Black Hat revealed an entirely new attack surface that exists in Exchange. Threat actors are allegedly now exploiting servers vulnerable to the RCE bugs. According to researchers, Miscorosft Exchange servers are being actively exploited via ProxyShell, the name of the attack disclosed at Black Hat last week. https://threatpost.com/exchange-servers-attack-proxyshell/168661/

Unpatched Fortinet Bug Allows Firewall Takeovers
The OS command-injection bug, in the web application firewall (WAF) platform known as FortiWeb, will get a patch this week. https://threatpost.com/unpatched-fortinet-bug-firewall-takeovers/168764/

WARNING: Email from FTC Chair Lina Khan about Coronavirus money is fake
Scammers are impersonating FTC Chair Lina Khan in a new phishing scheme. The email says the FTC wants to send you Coronavirus relief funds and tells you to send some personal information, like your name, address, and date of birth. The FTC is not distributing Coronavirus economic stimulus or relief money to people. The email is a scam. Don't reply.
https://www.consumer.ftc.gov/blog/2021/08/warning-email-ftc-chair-lina-m-khan-about-coronavirus-money-fake

Threat Advisory: LockBit Ransomware Group Profile
LockBit ransomware was initially discovered in September 2019. Since then, the malware has been used in ransomware attacks against a range of industries located across the globe. With the evolution of ransomware operators and their tactics over the past few years, groups like the LockBit gang have implemented successful tactics from other groups to increase their success and/or profits. In the LockBit group's newest campaigns, they have rebranded themselves as "LockBit 2.0", a double-extortive Ransomware-As-A-Service (RaaS) operation.
https://www.herjavecgroup.com/herjavecgrouplockbit20ransomwareprofile/?mkt_tok=MjE1LUtKQi0wMDUAAAF_EvtCdjjnpODSL8XP9iEjcvxFphzoT0EHMpJYYyE9K30myWuhQkeZvvgKsRyhUywDkIyN5BpIS_CC6CvOtseNLWWZBYnfMtgK7gzr4n2Z

Microsoft Exchange vulnerabilities targeted in ProxyShell attacks
Researchers warn of LockFile ransomware and WannaMine crypto miners taking advantage of unpatched servers.
https://www.cybersecuritydive.com/news/microsoftexchangevulnerabilitiesproxyshell/605474/?utm_source=Sailthru&utm_medium=email&utm_campaign=Issue:%2020210824%20Cybersecurity%20Dive%20%5Bissue:36278%5D&utm_term=Cybersecurity%20Dive

LockFile Uses PetitPotam Attack to Target Domain Controllers
LockFile, a new ransomware group, has been discovered to be using the PetitPotam NTLM relay attack method. This attack was discovered last month that enables threat actors to take over a Windows domain completely. The LockFile ransomware group first appeared in the month of July.
https://www.infosecurity-magazine.com/news/new-lockfile-ransomware-petitpotam/

FBI Issues Ransomware Group Flash Alert
The FBI recently released a flash warning due to the recent activities of an organized cyber-criminal gang referred to as the OnePercent Group. In the alert, which was published on Monday, the FBI stated that the group has been targeting US companies since November 2020. OnePercent uses the threat emulation.
https://www.infosecurity-magazine.com/news/fbi-issues-ransomware-group-flash/

****

Hints & Tips plus Security Awareness

Excel is still a security headache after 30 years because of this one feature
Threat researcher explains why it's tricky to tell the difference between legitimate Excel Macros and ones that deliver malware.
https://www.techrepublic.com/article/excel-is-still-a-security-headache-after-30-years-because-of-this-one-feature/?ftag=TREa988f1c&bhid=78480402&mid=13476825&cid=712423569

In the event of a cyber incident, think like a lawyer
While security professionals may not be deeply involved in the legal aspects of a cyber incident, they have to be aware of attorney client privileges.
https://www.cybersecuritydive.com/news/legalincidentreportingcyberresponse/605103/?utm_source=Sailthru&utm_medium=email&utm_campaign=Issue:%202021-08-17%20Cybersecurity%20Dive%20%5Bissue:36135%5D&utm_term=Cybersecurity%20Dive

Moving to Windows 11 won't be that bad, probably
The changes from Windows 10 to Microsoft's latest OS aren't as deep as with previous migrations. Yet the shift gives CIOs an opportunity to ensure functionality and app compatibility.
https://www.ciodive.com/news/windows11migrationplansmicrosoft/605148/?utm_source=Sailthru&utm_medium=email&utm_campaign=Issue:%2020210818%20CIO%20Dive%20%5Bissue:36155%5D&utm_term=CIO%20Dive

How to Beat The $80m Gift Card Scammers
Hundreds of millions of dollars have been lost during the past few years to gift card scams.
https://scambusters.org/giftcard2.html

Kaseya Issues Patches for Two New 0-Day Flaws Affecting Unitrends Servers
U.S. technology firm Kaseya has released security patches to address two zero-day vulnerabilities affecting its Unitrends enterprise backup and continuity solution that could result in privilege escalation and authenticated remote code execution. The two weaknesses are part of a trio of.
https://thehackernews.com/2021/08/kaseyaissuespatchesfortwonew0day.html?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+TheHackersNews+%28The+Hackers+News++Cyber+Security+Blog%29&_m=3n.009a.2557.aa0ao086k1.1mfi

VMSA-2021-0014.1 - VMware
ESXi updates address authentication and denial of service vulnerabilities (CVE-2021-21994, CVE-2021-21995) Please see the updated advisory here:
https://www.vmware.com/security/advisories/VMSA-2021-0014.html

****

News & Views

New FFIEC Guidance for Access and Authentication

In response to an expanded cybersecurity threat landscape, the FFIEC just issued an update to agency expectations for access and authentication to financial institution products and systems. This update replaces both the 2005 and the 2011 authentication guidance, and has been extended beyond digital banking (ebanking) customers to include everyone and everything that might have […]
https://complianceguru.com/2021/08/newffiecguidanceforaccessandauthentication/?utm_medium=email&utm_content=150590918&utm_source=hs_email

Consider a non-human path to monitoring insider threats
It's important to give humans as much help as possible to protect an enterprise, writes Charisa Orwig, principal cybersecurity architect at Bank of the West. "Surround the human with protections and remove insider ability to create damage where possible by automating and implementing controls like access limits and required validations," Orwig argues in this commentary.
https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2021/the-non-human-path-to-an-effective-insider-threat-program

Why multifactor authentication is no longer near-foolproof
Hackers are finding ways around multifactor authentication systems that use single-use access codes sent to smartphones, observers say. In this article, Alexa Heah suggests stronger passwords and investigating hardware that plugs into devices to enable multifactor security.
https://designtaxi.com/news/415290/Hackers-Have-Learned-To-Bypass-Two-Factor-Security-What-Now/

Why most companies don't understand speed is vital to cybersecurity
In cybersecurity folk wisdom, frequent releases are scary and the foundation for security failure. Why is there this disconnect between cybersecurity superstition and reality?
https://www.cybersecuritydive.com/news/sppedsecuritydevsecops/605463/?utm_source=Sailthru&utm_medium=email&utm_campaign=Issue:%2020210824%20Cybersecurity%20Dive%20%5Bissue:36278%5D&utm_term=Cybersecurity%20Dive

Credential stuffing: the data availability problem
If data is the valuable asset locked away for safekeeping, credentials are key to opening the vault. For threat actors, the real value of credentials is that they offer access without trace.
https://www.cybersecuritydive.com/news/credentialstuffingdatabreach/605392/?utm_source=Sailthru&utm_medium=email&utm_campaign=Issue:%2020210824%20Cybersecurity%20Dive%20%5Bissue:36278%5D&utm_term=Cybersecurity%20Dive

JPMorgan Chase glitch let customers see other users' data
The breach, which lasted from May 24 to July 14, appears to have limited reach — seven customers in Montana, for example — although no details were available regarding potential impact in other states, or elsewhere.
https://www.bankingdive.com/news/jpmorgan-chase-glitch-let-customers-see-other-users-data/605383/?utm_source=Sailthru&utm_medium=email&utm_campaign=Issue:%202021-08-24%20Banking%20Dive%20%5Bissue:36247%5D&utm_term=Banking%20Dive

****

"Ctrl -F" for The Board

For sale: Access to your company network. Price: Less than you'd think
Access to secured networks is regularly sold on the Dark Web and 45% of those sales are less than $1,000.
https://www.techrepublic.com/article/for-sale-access-to-your-company-network-price-less-than-youd-think/?ftag=TREa988f1c&bhid=78480402&mid=13476825&cid=712423569

Cybersecurity falls to third on list of business risks
Business interruption is the leading corporate risk for this year, knocking cybersecurity out of the top spot, per the Allianz Risk Barometer. Cybersecurity fell to third place as the Delta variant vaulted the coronavirus pandemic into second place.
https://www.techdigest.tv/2021/08/cyber-breach-one-of-biggest-business-risks-in-2021.html

Questions
Contact FIPCO's Ken Shaurette at 800/722-3498 ext. 251 or email FIPCO IT Services for more information.

"Make Security Part of You and Your Institution's DNA!"

Threat Intelligence Newsletter: September 16, 2021

FIPCO® IT Audit Round Table Discussions

If you would like to host an event, please contact: Amy Petersen

Upcoming Threat Intelligence Peer Group Discussions
None available at the current time

Register Now to Participate in #BanksNeverAskThat
ABA has already seen over 1,100 bankers register for the second annual #BanksNeverAskThat campaign launch. What are you waiting for?
As the October 1 kick-off approaches, now is the time to get engaged and start preparing your bank's campaign to educate your customers on how to identify and avoid phishing scams.
https://www.aba.com/advocacy/community-programs/banksneveraskthat?utm_campaign=BNAT-Email3NotRegistered091021.html&utm_medium=email&utm_source=Eloqua&elqTrackId=244d7fd3cc2a4348ae4e5b4eca4f64b8&elq=277702937c0342d397c6d249e8864e7f&elqaid=26028&elqat=1&elqCampaignId=9252

****

Alerts & Warnings

Instagram Flaw Allows Public To Peek At Private Posts
Yet another reason for Instagram fans to question their online security has taken root. The Facebook-owned company made the “not-so-good-news” headlines due to a recent software flaw. The security flaw found on the photo-sharing app allowed anyone to view and comment on user posts without legitimately being a follower of their Instagram account. Despite the creepy feeling that anyone can see your photos and posts, the security bug can also lead to brute-force media ID’s, exposing users to further data vulnerability on the platform.
https://www.sosdailynews.com/news.jspx?&articleid=BE34D9814810D121326EE188807A7365&sx=79

"Dark Patterns": How Websites Trick You Into Spending
Have you ever kicked yourself after feeling tricked into spending more than you intended or buying something you probably didn't need?
https://scambusters.org/darkpattern.html

Microsoft warns of attacks targeting Office documents
Affecting Windows desktops and servers, the attacks exploit an MSHTML vulnerability by using specially crafted Microsoft Office documents.
https://www.techrepublic.com/article/microsoftwarnsofattackstargetingofficedocuments/?ftag=TREa988f1c&bhid=78480402&mid=13505369&cid=712423569

Microsoft: Attackers Exploiting Windows Zero-Day Flaw
Microsoft Corp. warns that attackers are exploiting a previously unknown vulnerability in Windows 10 and many Windows Server versions to seize control over PCs when users open a malicious document or visit a booby-trapped website. There is currently no official patch for the flaw, but Microsoft has released recommendations for mitigating the threat.
https://krebsonsecurity.com/2021/09/microsoft-attackers-exploiting-windows-zero-day-flaw/

Microsoft warns of credential phishing attack abusing open redirect links
So far, the ongoing phishing attack has utilized more than 350 unique domains to target Microsoft Office 365 users.
https://www.hackread.com/microsoft-credential-phishing-attack-open-redirect-links/

New 0-Day Attack Targeting Windows Users With Microsoft Office Documents
Microsoft on Tuesday, 9/7 warned of an actively exploited zero-day flaw impacting Internet Explorer that's being used to hijack vulnerable Windows systems by leveraging weaponized Office documents.
https://thehackernews.com/2021/09/new-0-day-attack-targeting-windows.html
REFER TO WORKAROUNDS AND MITIGATIONS in the Hints and Tips section.

TeaBot Trojan Steals Android Banking Credentials
There's a new Android banking trojan making the rounds overseas, but like other malware attacks in other countries, it won't take TeaBot Trojan long to reach the U.S. Still in early development, the goal of this one, called TeaBot, is stealing user credentials for fraudulent activities against financial institutions. It starts the device infection by posing as a legitimate package delivery service as the way to begin its costly malware infection.
https://www.cpomagazine.com/cyber-security/android-malware-named-teabot-banking-trojan-targets-sixty-banks-in-germany-spain-italy-belgium-and-the-netherlands/

UPS.com Used In Phishing Campaign Utilizing XSS Vulnerability
Be on the lookout for a creative UPS phishing campaign that is utilizing an XSS vulnerability in UPS.com to send fake and malicious 'Invoice' Word documents. The phishing scam impersonates a UPS message claiming there is an issue with the shipment and that it needs to be picked up by the customer. The cleaver part of the attack is the use of a XSS vulnerability in UPS.com to modify the site's regular page to look like a legitimate download page. Victims believe they were downloading a legitimate UPS shipping document when it was actually coming from a malicious site.
https://www.sosdailynews.com/news.jspx?&articleid=5B64BBC4FC767CBF6ACB47B3433C151D&sx=79

The Lender May be Real, but the Loan is a Scam - Watch out for "guaranteed" loans with upfront fees
BBB Scam Tracker is receiving reports of scammers masquerading as legitimate loan providers. These phony lenders guarantee a quick loan with no upfront fees. But victims who provide their banking information to the scammers are left in the negative.
https://www.bbb.org/article/newsreleases/16919bbbtipadvancefeeloanscams?utm_source=newsletter&utm_medium=email&utm_content=%26quot%3Bguaranteed%26quot%3B%20loans%20with%20upfront%20fees&utm_campaign=scam-alert

Your boss isn’t emailing you about a gift card
Did you get an email from your boss asking you for a favor? Does your boss need you to send gift cards to pay for an upcoming office party? Before you go out and pay up, ask yourself: is that really your boss? It could be a scammer trying to get your money.
https://www.consumer.ftc.gov/blog/2021/09/yourbossisntemailingyouaboutgiftcard?utm_source=govdelivery

Hackers dump login credentials of Fortinet VPN users in plain-text
Fortinet VPN users are urged to reset their passwords as the company has acknowledged the data to be legitimate.
https://www.hackread.com/hackersdumpfortinetvpnuserslogincredentials/?_hsmi=78978938&_hsenc=p2ANqtz-_IT4HMCRkGJj5rwIpfHTx_uEuLsXA4Xqm2TBroKB1S3lMWZwcgfO8YBFSgQ3pD_uWkszSn7raFDW6-ZcBMrH1uFI98Og

****

Hints & Tips plus Security Awareness

Microsoft, CISA urge use of mitigations and workarounds for Office document vulnerability
Microsoft said disabling the installation of all ActiveX controls in Internet Explorer mitigates the attack.
https://www.zdnet.com/article/microsoft-cisa-urge-use-of-mitigations-and-workarounds-for-office-documentvulnerability/?_hsmi=78978938&_hsenc=p2ANqtz92Ar7eonohBn9IxPAHRUahnZBT6Q7GflkMsclVH_JbluDsUKcmeo9_0WoCsgGwJXir7K7rQG_arHGa5Gg84RrOP-9KVw#ftag=RSSbaffb68

3 Ways to Keep Your Social Security Number Safe
Who really needs your social security number, NOT all that ask! Some businesses will ask for your Social Security number, but they don't really need it. Here is how to identify who you should share your Social Security number with.
https://videos.aarp.org/detail/video/6213670309001/3-ways-to-keep-your-social-security-number-safe

Google Android Security Update Patches 40 Vulnerabilities
Earlier this week, Google released its latest Android Security Bulletin, resolving a total of 40 vulnerabilities. The monthly update consisted of patches for seven flaws rated critical in nature. One of the security bugs tracked as CVE-2021-0687 patched this week affects Android 8.1, 9, 10, and 11. The most severe.
https://www.securityweek.com/google-android-security-update-patches-40-vulnerabilities

****

News & Views

Why a ban on ransom payments will not work
Those most impacted by an attack are motivated to pay. In some cases, it's not the victim company but its customers who want service restored.
https://www.cybersecuritydive.com/news/ransomwarepaymentextortionInstituteforSecurityandTechnology/605662/?utm_source=Sailthru&utm_medium=email&utm_campaign=Issue:%2020210830%20Cybersecurity%20Dive%20%5Bissue:36400%5D&utm_term=Cybersecurity%20Dive

Effective User-Centric Authentication is Critical for Modern Business
Over the past three decades, businesses around the world have been undergoing a rapid digital transformation. With more organizations moving both internal and front-facing operations to the cloud, Identity and Access Management (IAM) has become a paramount concern for many business executives.
https://www.herjavecgroup.com/cyber-playbook-effective-user-centric-authentication-is-critical-for-modern-business/?utm_source=Marketo&utm_medium=Email&utm_campaign=Digest%201835-2021-09-09T11:10:14.83104:00&mkt_tok=MjE1LUtKQi0wMDUAAAF_ahqgFYdbNSNX25qGA1P8Jd32ctTWeiTNJ6KRrgx3sjfjFI62D5YAGRJBQTaSa5r6N2u4OERQR8t8LPWLYMmUHtP1Jvz4X9ELnd0gnAGv

****

"Ctrl -F" for The Board

Shift to cyber resilience: 7 steps to a better security approach
Business interruption is the leading corporate risk for this year, knocking cybersecurity out of Shift to cyber resilience: 7 steps to a better security approach
If you sometimes feel like you are on a cybersecurity hamster wheel, running to fight off threats that never end, you are not alone. A recent report by IBM and the Ponemon Institute shows that many organizations are still running on that wheel to nowhere.
https://techbeacon.com/security/shiftcyberresilience7stepsbettersecurityapproach?utm_source=newsletter&utm_medium=email&utm_campaign=tbsecnewsletter40&utm_content=featured

Questions
Contact FIPCO's Ken Shaurette at 800/722-3498 ext. 251 or email FIPCO IT Services for more information.

"Make Security Part of You and Your Institution's DNA!"

Threat Intelligence Newsletter: September 23, 2021

FIPCO®
IT Audit
Round Table
Discussions

If you would like to host an event, please contact: Amy Petersen

Upcoming Threat Intelligence Peer Group Discussions
None available at the current time

****

Alerts & Warnings

The new maxtrilha trojan is being disseminated and targeting several banks
A new banking trojan dubbed maxtrilha (due to its encryption key) has been discovered in the last few days and targeting customers of European and South American banks.
https://securityaffairs.co/wordpress/122134/malware/maxtrilhabankingtrojan.html?utm_campaign=maxtrilhabankingtrojan&utm_medium=rss&_hsmi=78978938&_hsenc=p2ANqtzseAKJMfqbVd6HjBBfmbbC6zWUr02ndHj49himHGuH2ryehB470cwcvkEXBE1zXnasmoK3LnK1smoqjjrFhTIj8ctxWA&utm_source=rss

Tens of Thousands of Unpatched Fortinet VPNs Hacked via Old Security Flaw
A threat actor has leaked online access credentials for 87,000 Fortinet VPN devices that were apparently compromised using a vulnerability identified and patched two years ago.
https://www.securityweek.com/tensthousandsunpatchedfortinetvpnshackedoldsecurityflaw?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+securityweek+%28SecurityWeek+RSS+Feed%29&_hsenc=p2ANqtz9zJUxugZUrIa8Lxi8naUehdVxyzW08do0jf8PJrmR5oF0eJwFdgOLFVbRMEo6UE6PLOLVJUq5x-m-Am0-44njaZqXEOQ&_hsmi=78978938

Microsoft Patches Actively Exploited Windows Zero-Day Bug
In the most recent Patch Tuesday, Microsoft released fixes 66 CVEs, including an RCE bug under active attack. Three of the bugs that were patched in the update were rated critical. One of which has been under active attack for nearly two weeks. One of the other bugs included in.
https://threatpost.com/microsoft-patch-tuesday-exploited-windows-zero-day/169459/

Crooks switch focus to high income earners
People from all types of backgrounds can be sucked into terrifying scams - including professionals like medics, teachers, and businesspeople.
https://scambusters.org/professional.html

****

Hints & Tips plus Security Awareness

Microsoft patched an actively exploited Windows zero-day vulnerability.
In this month's Microsoft Patch Tuesday, Microsoft rolled out an update to patch the actively exploited zero-day in its MSHTML Platform, which came to light last week. The 8.8 rated flaw is a remote code execution vulnerability in MSHTML that leverages malware-laced Microsoft Office documents, with EXPMON researchers noting "the exploit uses logical flaws, so the exploitation is perfectly reliable." Also, in this month's Patch Tuesday, Microsoft addressed a publicly disclosed, but not actively exploited, a zero-day flaw in Windows DNS.
https://thehackernews.com/2021/09/microsoft-releases-patch-for-actively.html

Google addresses a new Chrome zero-day flaw actively exploited in the wild
Google Chrome 93.0.4577.82 for Windows, Mac, and Linux that addressed eleven security issues, including two zero-days actively exploited. Google released Chrome 93.0.4577.82 for Windows, Mac, and Linux that fixed eleven security issues, including.
https://securityaffairs.co/wordpress/122192/hacking/google-zero-day-10.html

Password managers are a necessary — yet vulnerable — last line of defense
The Passwordstate breach is forcing CISOs and researchers to review vendors and reassess security practices.
https://www.cybersecuritydive.com/news/passwordmanagementsecuritydefense/599518/?utm_source=Sailthru&utm_medium=email&utm_campaign=Issue:%2020210916%20Cybersecurity%20Dive%20%5Bissue:36758%5D&utm_term=Cybersecurity%20Dive

Microsoft announces passwordless authentication option for consumers
After offering the passwordless authentication option to enterprise customers in March 2021, Microsoft has now started rolling it out to its consumer segment of users.
https://www.helpnetsecurity.com/2021/09/16/microsoft-passwordless-authentication-consumers/

Companies must develop operational plan for ransomware recovery
In the face of more frequent and sophisticated attacks, companies need to identify their most critical assets and work to limit cyberattack fallout.
https://www.cybersecuritydive.com/news/companiesmustdevelopoperationalplanforransomwarerecovery/606698/?utm_source=Sailthru&utm_medium=email&utm_campaign=Issue:%2020210917%20Cybersecurity%20Dive%20%5Bissue:36785%5D&utm_term=Cybersecurity%20Dive

****

News & Views

REvil Ransomware Has Returned
The Malicious Group Is Back in Full Attack Mode and Is Leaking Data.
https://heimdalsecurity.com/blog/revilransomwarebackinbusiness/?_hsmi=78978938&_hsenc=p2ANqtzCKlCJ_2Xo7puOIApHvn4gR2BYAQRKkvbHTVu3lPgqBn0AsNOKf2OKQ9TZYZ0NAyatbboPWBVZUmxeUllJ3L70qNdfg

Attackers Impersonate DoT in Two-Day Phishing Scam
Threat actors allegedly impersonated the US Department of Transportation in a two-day phishing campaign, leveraging the recent $1 trillion infrastructure bill. The cyber attackers created new domains mimicking the real DoT site. The campaign combined a series of tactics, such as creating seemingly legitimate domains to evade security detections and.
https://threatpost.com/attackers-impersonate-dot-phishing-scam/169484/

Companies confident in cybersecurity despite growing threats: report
There's a perception of "safety in numbers," Beazley's survey found. "Time will tell if such high levels of confidence are well placed."
https://www.cybersecuritydive.com/news/beazleycyberinsurancetechnologyrisk/606683/?utm_source=Sailthru&utm_medium=email&utm_campaign=Issue:%2020210916%20Cybersecurity%20Dive%20%5Bissue:36758%5D&utm_term=Cybersecurity%20Dive

FFIEC Replaces, and Expands, the Operations Handbook - Updated AIO Guide:
Back in June of this year the FFIEC released an update to the 2004 Operations Handbook called Architecture, Infrastructure, and Operations (AIO). As the lengthier name implies, this was not simply an update, it also greatly expanded the scope of operations to include architecture and infrastructure principles and practices.
https://complianceguru.com/2021/09/ffiecreplacesandexpandstheoperationshandbook/?utm_medium=email&utm_content=159769385&utm_source=hs_email

The New FFIEC Architecture, Infrastructure, and Operations Booklet,
No cost vendor review of what changed, the booklet is new but there is really minimal that is NEW, mostly term, some consolidation and added focus on importance of infrastructure and security.
watch the recording, you can follow the link below. We have also included a link to download a copy of the slides.
Link to Recording: https://tandem.app/2021-ffiec-aio-vid
Link to Slide Deck: https://tandem.app/2021-ffiec-aio-pdf

****

"Ctrl -F" for The Board

Boards rethink incident response playbook as ransomware surges
Corporate boards are no longer rubber-stamping assurances from CIOs or CISOs but are bringing in outside experts, asking more questions and preparing for the risk of personal liability.
https://www.cybersecuritydive.com/news/boardsrethinkincidentresponseplaybookasransomwaresurges/606618/?utm_source=Sailthru&utm_medium=email&utm_campaign=Issue:%2020210916%20Cybersecurity%20Dive%20%5Bissue:36758%5D&utm_term=Cybersecurity%20Dive

Cybersecurity drills don't have to be 'fight or flight,' training creators say
Cyber training has followed "a very dangerous path," the co-founders of Hook Security said. But a humorous approach may turn things around.
https://www.cybersecuritydive.com/news/phishingtestworkforcecybersecuritytraining/606557/?utm_source=Sailthru&utm_medium=email&utm_campaign=Issue:%2020210915%20Cybersecurity%20Dive%20%5Bissue:36724%5D&utm_term=Cybersecurity%20Dive

Questions
Contact FIPCO’s Ken Shaurette at 800/722-3498 ext. 251 or email FIPCO IT Services for more information.

"Make Security Part of You and Your Institution's DNA!"

Threat Intelligence Newsletter: September 27, 2021

FIPCO®
IT Audit
Round Table
Discussions

If you would like to host an event, please contact: Amy Petersen

Upcoming Threat Intelligence Peer Group Discussions
None available at the current time

National Security Memorandum to Strengthen Nation's Cybersecurity Infrastructure
DHS's Cybersecurity and Infrastructure Security Agency (CISA), in coordination with the Department of Commerce's National Institute of Standards and Technology (NIST), developed preliminary cybersecurity performance goals based on nine categories of best practices.
https://www.cisa.gov/control-systems-goals-and-objectives

****

Alerts & Warnings

Watch out for Text Messages with Tempting Offers
Everyone loves a deal – including scammers. Con artists often offer too good to be true discounts in the hope that price-conscious consumers will jump on these "deals" without doing their research. Recently, BBB Scam Tracker has seen numerous reports of scammers impersonating well-known companies and offering COVID-19 themed discounts.
https://www.bbb.org/article/newsreleases/20913scamalertgreatdealonyourcablecouldbeatrick?utm_source=newsletter&utm_medium=email&utm_content=discount%20on%20your%20utility%20bills&utm_campaign=scam-alert

New Microsoft Scam Emails Bring Brand Impersonation Risk Into Focus
A new Microsoft scam may be landing in an inbox near you. Here's how to suss out fakes and stay out of trouble when handling branded emails.
https://www.graphus.ai/blog/newmicrosoftscamemailsbringbrandimpersonationriskintofocus/?utm_medium=Email&utm_source=Graphus&mkt_tok=NTk2LUlOWC03MDQAAAF_k6iiiPHWLS3y1MxcjmVyUCsu9ww6Cv7T7HsdPVtHaLPHGhyG48-j-cDfjFLV3Yxq6fvOOGRN6oq-zt8PeV8a34RJChugovkuz2wl-gGjZSXg

FBI and CISA offer Conti ransomware warning

The Cybersecurity and Infrastructure Security Agency and FBI released an advisory about the Conti ransomware on Wednesday.
https://www.scmagazine.com/news/ransomware/fbiandcisaoffercontiransomwarewarning?utm_source=newsletter&utm_medium=email&utm_campaign=SCUS_Newswire_%7B%7B%27now%27%7Cdate%3A%27%25Y%25m%25d%27%7D%7D&hmSubId=%7B%7Bcontact.cms_id_encrypted%7D%7D&email_hash=%7B%7Bcontact.email%7Cmd5%7D%7D&oly_enc_id=0795J7353967J0E

Scam Texts Target Struggling Renters With False Promises of Aid

Bogus rental assistance offers are ploys to steal money, personal information.
https://www.aarp.org/money/scams-fraud/info-2021/rental-assistance.html?intcmp=AE-FRDSC-MOR-R2-POS3

Threat Advisory: BlackMatter Ransomware Group Profile

BlackMatter Ransomware is a breakout ransomware group that became operational shortly after the shutdown of the REvil Ransomware and DarkSide Ransomware operations in late Summer 2021. Like DarkSide, this group has been very vocal and expressive with the press about their operation.
https://www.herjavecgroup.com/herjavecgroupblackmatterransomwareprofile/?utm_source=email&utm_medium=email&utm_campaign=BlackMatterProfile&utm_content=blog&utm_term=hg&mkt_tok=MjEDt-uOZPH8oml7qpiD5nPSHuxdAPdHXOSHkrQoIoeVG2LZ5f5ROjZ7NoF7DGLEIW2XpWIr1UOaiUrepuDmEWQ6m16b2DYruOxB7FwOr2vY

****

Hints & Tips plus Security Awareness

Phishing vs. Spear Phishing: What's the Difference?

Phishing vs. Spear phishing: What's the difference between the two and why is it important for the protection of your business?
https://www.graphus.ai/blog/phishingvsspearphishingwhatsthedifference/?utm_medium=Email&utm_source=Graphus&mkt_tok=NTk2LUlOWC03MDQAAAF_k6ig6Z9ZlMp4vIQKJWgO4p6CESt2XODJegHOWmU4qDkEGLYZgzMRixLOFE1HRdD5gFmycJJLtxTMiB05YJ1jHc2gjiclxmXL2kAtK3xHrVw

New Chrome Features Boost Your Browsing Security

We are always on the edge of our seats to see what new privacy and security settings Google comes up with for its massively used Chrome browsers. Perhaps wer are not on the edge of our seats, but there are some reportedly cool new features of version 92, that is already available.
https://www.sosdailynews.com/news.jspx?&articleid=A762CD13584BA5086DF31C01BB2BA532&sx=79

A security expert's guide to the top-exploited vulnerabilities

The biggest and baddest ransomware groups love an easy vulnerability.
https://www.cybersecuritydive.com/news/CISACVEmostcommonvulnerability20202021ransomware/604/

****

News & Views

Microsoft Warns Phishers Sneak In New Lures To Snag You
Detecting phishing is getting harder and harder as the days go by. Merely looking out for misspelled words, bad grammar, or unknown senders just isn't enough anymore. A popular way the phishers lure unsuspecting victims is using well-known business names and/or products and Microsoft Office 365 has been a popular one of late. As if they weren't hard enough to find anyway, Microsoft has recently warned of yet another one that is craftier at bypassing anti-phishing filters and succeeding at capturing user login credentials.
https://www.sosdailynews.com/news.jspx?&articleid=BE289A5F9A41321037B81B7CC390D826&sx=79

****

"Ctrl -F" for The Board

National Security Memorandum to Strengthen Nation's Cybersecurity Infrastructure
DHS's Cybersecurity and Infrastructure Security Agency (CISA), in coordination with the Department of Commerce's National Institute of Standards and Technology (NIST), developed preliminary cybersecurity performance goals based on nine categories of best practices.
https://www.cisa.gov/control-systems-goals-and-objectives

Questions
Contact FIPCO's Ken Shaurette at 800/722-3498 ext. 251 or email FIPCO IT Services for more information.

"Make Security Part of You and Your Institution's DNA!"

Threat Intelligence Newsletter: October 22, 2021

If you would like to host an event, please contact: [Amy Petersen]

Upcoming Threat Intelligence Peer Group Discussions
None available at the current time

CISA Releases Insider Risk Self-Assessment Tool
The Cybersecurity and Infrastructure Security Agency last week released an insider risk self-assessment tool to help organizations gauge their vulnerability to an insider threat. The tool is a downloadable PDF that asks users questions about their existing enterprise, focusing on program management, personnel and training, and data collection and analysis. CISA noted that the tool collects no data or personal information and allows users to receive scores that evaluate their immunity to insider threat incidents. https://www.cisa.gov/publication/insider-risk-self-assessment-tool?utm_campaign=RiskCyber-20211004&utm_medium=email&utm_source=Eloqua

ABA Launches Refreshed #BanksNeverAskThat Anti-Phishing Campaign
As part of Cybersecurity Awareness Month in October, ABA today launched its award-winning anti-phishing campaign #BanksNeverAskThat. Created in 2020 to help consumers fight phishing fraud, last year's #BanksNeverAskThat campaign... https://www.aba.com/advocacy/community-programs/banksneveraskthat

****

Alerts & Warnings

LinkedIn URLs are being hijacked for phishing
Is it time to ban shortened URLs? https://www.techradar.com/news/linkedin-urls-are-being-hijacked-for-phishing

Apache patches an actively exploited vulnerability for its HTTP Server product
On Thursday, the Apache Software Foundation released additional security updates for its HTTP Server product to remediate what it says is an "incomplete fix" for an actively exploited path traversal and remote code execution flaw that it patched earlier this week. Apache HTTP Server is an open-source, cross-platform web server that powers approximately 25% of websites worldwide.
https://thehackernews.com/2021/10/new-patch-released-for-actively.html

Microsoft reports three critical vulnerabilities, a fourth 'high'™ vulnerability actively exploited
This month's batch of more than 70 vulnerabilities includes three critical RCEs and a fourth privilege elevation vulnerability found in the Win32k process. https://www.scmagazine.com/news/patch-management/microsoft-reports-three-critical-vulnerabilities-a-fourth-high-vulnerability-actively-exploited?utm_source=newsletter&utm_medium=email&utm_campaign=SCUS_Newswire_%7B%7Bnow%7Cdate%3A%25Y%25m%25d%7D%7D&hmSubId=%7B%7Bcontact.cms_id_encrypted%7D%7D&email_hash=%7B%7Bcontact.email%7Cmd5%7D%7D&mkt_tok=MTg4LVVOWi02NjAAAAGAGBFjD9RIY7D8ymgxRJ2f4sbAnUjSBFZ9CPLPyQWB0NVV5_Nm9IOIBIraEW8APp6HMGaTRXJreDcyA9HIRSn30xLtL_zDzYTKvdivoQ

The ad blocker that injects ads
Deceptive ad injection is a growing concern on the internet today, affecting many people browsing the web. And while the concept isn't new (Google stated it was the most common complaint amongst Chrome users back in 2015), just like with other online threats, bad actors are constantly refining their techniques.
https://www.imperva.com/blog/the-ad-blocker-that-injects-ads/?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+Imperviews+%28Imperva+Cyber+Security+Blog%29&_hsenc=p2ANqtz-_P1ORBKIrYGR8ot28pIoY2w88AmvI2gledKXsFbTZEMYMbGQLeSVb9OAYULWeqeSBNnr3KN61mzuPIRHB7B7B6i3bH7A&_hsmi=78978938

Users have bad security habits. What can businesses do?
"As strange as it sounds, in the case of a security incident in the enterprise, you can't blame the user...".
https://www.cybersecuritydive.com/news/bitdefender-user-security-behavior-remote-work/608209/?utm_source=Sailthru&utm_medium=email&utm_campaign=Issue:%202021-10-14%20Cybersecurity%20Dive%20%5Bissue:37361%5D&utm_term=Cybersecurity%20Dive

CISA, FBI, and NSA Release Joint Cybersecurity Advisory on Blackmatter Ransomware
CISA, the Federal Bureau of Investigation (FBI), and the National Security Agency (NSA) have released joint Cybersecurity Advisory (CSA): BlackMatter Ransomware. https://us-cert.cisa.gov/ncas/current-activity/2021/10/18/cisa-fbi-and-nsa-release-joint-cybersecurity-advisory-blackmatter

Phishing campaign uses manipulated Excel spreadsheets
Security company Morphisec is warning of a phishing campaign, apparently from a Russia-based group, that emails Microsoft Excel spreadsheets with embedded macros, then uses a variety of tactics to persuade users to activate them. https://www.zdnet.com/article/this-particularly-dangerous-phishing-attack-features-a-weaponized-excel-file/

Zero-day hackers are working feverishly
Hacks involving zero-day vulnerabilities are arriving faster than ever, HP Wolf Security reports. The groups perpetuating these attacks are becoming full-fledged organizations, buoyed by success in obtaining ransoms, says ThreatModeler CEO Archie Agarwal. https://securityboulevard.com/2021/10/attackers-weaponizing-zero-days-at-record-pace/

****

Hints & Tips plus Security Awareness

NSA & CISA Guide on VPN Security
The US National Security Agency (NSA) and the Cybersecurity and Infrastructure Security Agency (CISA) have jointly released a guide to virtual private network (VPN) security. The guide offers advice for choosing a VPN as well as details for secure deployment. https://www.govinfosecurity.com/nsa-cisa-release-vpn-security-guidance-a-17640 , https://media.defense.gov/2021/Sep/28/2002863184/-1/-1/0/CSI_SELECTING-HARDENING-REMOTE-ACCESS-VPNS-20210928.PDF

Windows 11: Tips on installation, security and more (no cost PDF)
Windows 11, Microsoft's newest major release of its operating system and the successor to Windows 10, rolls out to eligible devices on Oct. 5. How do you know if your PC can run Windows 11? How do you install it on a Mac or virtual machine? Find the answers to these questions and more in this no cost PDF ebook. https://www.techrepublic.com/resource-library/whitepapers/windows-11-tips-on-installation-security-and-more-free-pdf/?ftag=TREa988f1c&bhid=78480402&mid=13535917&cid=712423569

Apache fixes actively exploited web server zero-day
The Apache Software Foundation has released on Monday a security patch to address a vulnerability in its HTTP Web Server project that has been actively exploited in the wild. https://therecord.media/apache-fixes-actively-exploited-web-server-zero-day/?_hsmi=78978938&_hsenc=p2ANqtz-_qz4NTRNBBOtRdxH9mIJyynGXUesizc3QmR6HpaQ-6SD8kWwLWkc-Rm1OGeg6Hy55SKz1ROkyQObADVdaaFB9SutH10Q

How You Can Help Seniors Avoid Scams
Scams targeting seniors affect nearly everyone, not just the victims. Many of us are either in that age group or have relatives who are. The financial and emotional distress that follows overflows into entire families and communities… https://scambusters.org/seniors.html Consumer Reports 5 Ways to Stop Senior Scams: https://www.consumerreports.org/elder-fraud/ways-to-stop-senior-citizen-scams/

Three kinds of phish: What distinguishes the best phishing campaigns and how to avoid falling for them
What distinguishes the best phishing campaigns and how to avoid falling for them…
https://www.itproportal.com/features/three-kinds-of-phish-what-distinguishes-the-best-phishing-campaigns-and-how-to-avoid-falling-for-them/?utm_source=SmartBrief&utm_medium=email&utm_campaign=79B375AA-AA0B-4881-99A1-64F0F9BDBE17&utm_content=CE4F2507-42FC-40C9-928B-2F362BDC9753&utm_term=d6f5ac02-1e66-435e-bd3b-c146f0284875

How to Prepare for Ransomware Attacks
Ransomware attacks continue to increase, using techniques that are growing more and more sophisticated and targeted. Security and risk management leaders need to look beyond just the endpoints to help protect the organization from ransomware. https://www.gartner.com/doc/reprints?id=1-27EBINO8&ct=210909&st=sb&mkt_tok=NzUwLURRSC01MjgAAAF_-XVBYypH0lUMCzOfa6shkBrEd3qI-i8Bz4OkVMyCdbo7uYLvDmgVgxmqGVJL0f5nl6YuilpKvPdVU4pw66Gz3_ipmohfcmHLnugVtJKlnOjz_AY

Spot a Scam to Stop a Scam!
Millions of Americans are victimized by frauds and scams every year. Too often the damage doesn't stop with their bank accounts. Experiencing fraud at the hands of a stranger, or even someone who is known and trusted, can lead to emotional trauma and other harmful effects. Join us for a series of virtual events aimed at fighting fraud in the Heartland. Learn how to spot and stop scams, protect your identity and your pocketbook, and find out where to get help and build resilience if you or a loved one has been victimized. Registration required… https://aarp.cvent.com/events/lecture-fraud-in-the-heartland-the-original-internet-godfather/event-summary-c9db72e3d528452e9dbf7f308d16c52b.aspx

Password Auditing Tool L0phtCrack Released as Open Source:
Password auditing and recovery tool L0phtCrack has been released as open source and the project is looking for both maintainers and contributors... https://www.securityweek.com/password-auditing-tool-l0phtcrack-released-open-source

Design Phishing Tests for Teaching, Not Tricking
Running phishing tests is a proven way to improve employees' cybersecurity awareness and behavior, but using misleading tactics to simulate malicious attacks could damage employee morale, according to new research. https://www.shrm.org/ResourcesAndTools/hr-topics/technology/pages/design-phishing-tests-teaching-not-tricking.aspx

Amazon impersonators: what you need to know
Has Amazon contacted you to confirm a recent purchase you didn't make or to tell you that your account has been hacked? According to the FTC's new Data Spotlight, since July 2020, about one in three people who have reported a business impersonator scam say the scammer pretended to be Amazon. https://www.consumer.ftc.gov/blog/2021/10/amazon-impersonators-what-you-need-know?utm_source=govdelivery

Keeping older adults safe from scams
As our annual report to Congress makes clear, the safety of older consumers in the marketplace is a priority for the FTC. Protecting Older Consumers 2020 – 2021: A Report of the Federal Trade Commission summarizes the agency's ongoing law enforcement efforts, new research results, and extensive outreach aimed at keeping older adults safe from scams including those related to the COVID-19 pandemic. https://www.consumer.ftc.gov/blog/2021/10/keeping-older-adults-safe-scams?utm_source=govdelivery

****

News & Views

Scheming Scam Alert! These Top Scams Are Heading Your Way
This year's top scams are bigger and better than ever. Phishing scams hit new heights during the pandemic and show no signs of slowing down. The FBI's Internet Crime Complaint Center (IC3) received over 2.1 million complaints from scam victims last year. The most common reports were about imposter scams, but that's just the tip of the iceberg. The FTC finds that last year, the financial cost of these fraudulent scams was more than $3.3 billion. Most scams are...
https://www.sosdailynews.com/news.jspx?&articleid=B6545CF9660AB8755DC9199E21A3AFB6&sx=79

Cybercriminals Use Interactsh Tool for Vulnerability Validation
Cybercriminals are known to exploit open-source tools for their nefarious purposes and advantage. Recently, researchers have observed active exploits abusing an open-source service known as Interactsh. https://cyware.com/news/cybercriminals-use-interactsh-tool-for-vulnerability-validation-68ea5acd?_hsmi=78978938&_hsenc=p2ANqtz-9CEEKAjrTxI3iDc1MyXrz5nYJl7p53xqhaXt6beL0srUQvDGHosBFVvfSsalc8vLt4UoRy6BbM5uWVyb8QcXY2EQhFmw

****

"Ctrl -F" for The Board

Execs say they're ready for an attack, but are they?
After surveying C-suite executives, CloudBees found that more than 9 in 10 consider themselves ready to handle a ransomware attack. But a follow-up question tells a different story: 64% say they aren't sure exactly whom to call after a cyberattack. https://www.techradar.com/news/most-execs-say-they-dont-know-who-to-call-when-security-issues-come-up?utm_source=SmartBrief&utm_medium=email&utm_campaign=79B375AA-AA0B-4881-99A1-64F0F9BDBE17&utm_content=31ECAB8E-C6FE-4BAB-9EEE-86588B9FD9A7&utm_term=d6f5ac02-1e66-435e-bd3b-c146f0284875

Questions
Contact FIPCO’s Ken Shaurette at 800/722-3498 ext. 251 or email FIPCO IT Services for more information.

"Make Security Part of You and Your Institution's DNA!"

Threat Intelligence Newsletter: October 29, 2021

FIPCO®
IT Audit
Round Table
Discussions

If you would like to host an event, please contact: Amy Petersen

Upcoming Threat Intelligence Peer Group Discussions
None available at the current time

Wednesday, November 3rd, (1:00 PM – 2:00 PM ET) Overview of the Architecture, Infrastructure, and Operations Booklet
This webinar will provide an overview of the changes and content of the AIO booklet.
https://onlinexperiences.com/Launch/QReg/ShowUUID=C38FB0C9-24DA-4989-B240-64852BC8E55F&LangLocaleID=1033

Wednesday, November 3rd, (2:15 PM – 3:15 PM ET) Webinar on new FFIEC Authentication Guidance
This webinar will provide an overview of the new FFIEC Guidance on Authentication and Access to Financial Institution Services and Systems, which was published in August 2021. This new FFIEC Authentication Guidance sets forth examples of effective authentication and access risk management principles and practices.
https://onlinexperiences.com/Launch/QReg/ShowUUID=56FB8549-B678-4397-8AE8-CB3607B302B0&LangLocaleID=1033

****

Alerts & Warnings

BBB: Wrong Number? Don't Even Text Back
A new text message scam seems so innocent that it's tempting to reply. But con artists are using phony "wrong number" texts to lure victims into conversation and falling for a scam.
https://www.bbb.org/all/spotascam/howtospotaphonytextmessage?utm_source=newsletter&utm_medium=email&utm_content=fake%20text%20messages&utm_campaign=scam-alert

Fake Websites Trick Travelers Into Airport Security Pass Scam
Fake airport security websites are tricking travelers into revealing personal details for identity theft or stealing money by demanding fee payments. https://scambusters.org/airportsecurity.html

****

Hints & Tips plus Security Awareness

New breach has researchers questioning value of VPNs
Quickfox, a free virtual private network that connects browsers from outside China to that country's websites, has exposed the personal information of more than a million users, researchers say. Some maintain that VPNs have outlived their usefulness because they are "doorways to private sensitive internal networks and are sitting there exposed to the world for any miscreant to try to break through," as ThreatModeler CEO Archie Agarwal puts it. https://threatpost.com/vpn-exposes-data-1m/175612/

CAPTCHA Used as Bait For Growing Number Of Email Scams
Most of us are familiar with the funky CAPTCHA verification window that occasionally pops-up when esigning onto a website. CAPTCHA systems lend a level of credibility to those of us asked to verify online that we're human and not a bot. Seeing it makes us feel better about the site being more secure than others. After all, only a 100% legitimate website or service would dare use CAPTCHA, right? Wrong. This now Google-owned service has become a favorite bait for scammers who want you to believe they're legitimate, and it's working big-time.
https://www.sosdailynews.com/news.jspx?&articleid=1C10AD8C88CF339F89876721FEDCF193&sx=79

How to automate configuration review
Configuration management can be challenging. IT teams can become overwhelmed between various standards, compliance requirements, and security options. As the popularity of remote work grows, so does the complexity of implementing secure configurations.
https://www.helpnetsecurity.com/2021/10/28/how-to-automate-configuration-review/

Online Banking Smishing Scam
Text message scams are on the rise and in this Today Show segment, Jim Stickley demonstrates how easy it is from criminals to perform these attacks. Most people receive legitimate text alerts from their financial institution so a malicious text can be very believable. DON'T CLICK EVER. Simply open your mobile app or open a browser and sign into your account. If there is a real fraud alert, you will be notified once you are logged in.
https://www.sosdailynews.com/news.jspx?&articleid=2CE07759E8769CD625937DEDD21B3FF6&sx=79

****

News & Views

SolarWinds hackers, Nobelium, once again strike global IT supply chains, Microsoft warns
Microsoft released an advisory yesterday warning that the hackers behind the SolarWinds attacks are back at it again, targeting at least 140 global resellers and technology service providers in global IT supply chains. The group, known as Nobelium, is of Russian origin and has pivoted to software and cloud service…
https://www.zdnet.com/article/solarwinds-hacking-group-nobelium-is-now-targeting-the-global-it-supply-chain-microsoft-warns/

Cookie Theft Malware Used to Hijack YouTube Accounts
Google says it has disrupted phishing attacks in which threat actors were attempting to use cookie theft malware to hijack YouTube accounts and abuse them to promote cryptocurrency scams.
https://www.securityweek.com/cookietheftmalwareusedhijackyoutubeaccounts?_hsmi=78978938&_hsenc=p2ANqtz_sC2UOSl6fTQ_Azv7LvUOsg9p0noA9kDtIB7wmbiTrJDzxbEtGBXS4BEKPfbziyntGmhhwD2BNsPey2PXMUXk74RROMA

Why deepfake videos are a threat on many levels
Avani Desai, president of Schellman & Company, tackles the subject of threats posed by deepfakes—videos doctored by artificial intelligence to misrepresent the subject. "Researchers and tech giants are focusing on developing tools for exposing fakes, but malicious attackers are getting savvier," Desai writes.
https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2021/taking-fakeness-to-new-depths-with-ai-alterations-the-dangers-of-deepfake-videos

****

"Ctrl -F" for The Board

Wednesday, November 3rd, (1:00 PM – 2:00 PM ET) Overview of the Architecture, Infrastructure, and Operations Booklet
This webinar will provide an overview of the changes and content of the AIO booklet.
https://onlinexperiences.com/Launch/QReg/ShowUUID=C38FB0C9-24DA-4989-B240-64852BC8E55F&LangLocaleID=1033

Wednesday, November 3rd, (2:15 PM – 3:15 PM ET) Webinar on new FFIEC Authentication Guidance
This webinar will provide an overview of the new FFIEC Guidance on Authentication and Access to Financial Institution Services and Systems, which was published in August 2021. This new FFIEC Authentication Guidance sets forth examples of effective authentication and access risk management principles and practices.
https://onlinexperiences.com/Launch/QReg/ShowUUID=56FB8549-B678-4397-8AE8-CB3607B302B0&LangLocaleID=1033

Questions
Contact FIPCO's Ken Shaurette at 800/722-3498 ext. 251 or email FIPCO IT Services for more information.

"Make Security Part of You and Your Institution's DNA!"

Threat Intelligence Newsletter: November 9, 2021

FIPCO®
IT Audit
Round Table
Discussions

If you would like to host an event, please contact: Amy Petersen

Upcoming Threat Intelligence Peer Group Discussions
None available at the current time

****

Alerts & Warnings

SEO Poisoning Used to Distribute Ransomware (SEO = Search Engine Optimization)
This tactic — used to distribute REvil ransomware and the SolarMarker backdoor — is part of a broader increase in such attacks in recent months, researchers say. https://www.darkreading.com/attacks-breaches/seo-poisoning-used-to-distribute-ransomware?_hsmi=78978938&_hsenc=p2ANqtz-9ctaXHiPRdXf1--25hHTGc_WC4Wge_GVhpCUvOsDQ993WD4___lCIb6xrKVpJqd1lJUZtn-e2ksk7wd9f38H4cLufpTLQ

Google patches zero-day vulnerability, and others, in Android
Google has issued security patches for the Android Operating System. In total, the patches address 39 vulnerabilities. There are indications that one of the patched vulnerabilities may be under limited, targeted exploitation. https://blog.malwarebytes.com/exploits-and-vulnerabilities/2021/11/google-patches-zero-day-vulnerability-and-others-in-android/?_hsmi=78978938&_hsenc=p2ANqtz-9ikK6lTJvbvyAqajWo5I6-cXp6yfTcRRMy9icLCpG5ltX5Cr6rz6KA3awmH5qhM7DDQw1HxoPKjfyn4ujEpyYJZVY5Rw

Google releases emergency fix to plug zero day hole in Chrome
The emergency release comes a mere three days after Google's previous update that plugged another 19 security loopholes… https://www.welivesecurity.com/2021/09/27/google-releases-emergency-fix-plug-zero-day-hole-chrome/

Reducing the Significant Risk of Known Exploited Vulnerabilities
Addresses vulnerabilities that establishes specific timeframes for federal civilian agencies to remediate vulnerabilities that are being actively exploited by known adversaries. To support this Directive, CISA has established a catalog of relevant vulnerabilities. https://www.cisa.gov/known-exploited-vulnerabilities-catalog

HelloKitty Ransomware Adds New Extortion Tactics
Distributed Denial-of-service (DDoS) Attacks Were Added to the Malicious Actors' Arsenal. https://heimdalsecurity.com/blog/hellokitty-ransomware-adds-new-extortion-tactics/?_hsmi=78978938&_hsenc=p2ANqtz-_kKZJlYi7r4Et-DZzHYQQXbXirlOx1YJIYJSW-onPJbRArCKj0Y1lHLjf2-nmoVaSNu4FB2w397HVqqow24NmD_QgLRw

Credit card skimmer evades Virtual Machines
There are many techniques threat actors use to slow down analysis or, even better, evade detection. Perhaps the most popular method is to detect virtual machines commonly used by security researchers and sandboxing solutions. https://blog.malwarebytes.com/threat-intelligence/2021/11/credit-card-skimmer-evades-virtual-machines/?_hsmi=78978938&_hsenc=p2ANqtz-8csLSBaj8oFxLWs4T9AwtHa6QIXLVgqWST7jUShZ4RxVz-MxalNx5DA31EehuT3fj3aM_k-iq7X0gsNKEYrgKGFjH0yQ

****

Hints & Tips plus Security Awareness

This open season, is that really the health insurance you're looking for?
With the 2022 health insurance open enrollment season just around the corner (November 1 - December 15, 2021), now is the time to think about changes to your health coverage. But before you do, make sure any plan you're considering actually gives you the coverage you seek. Dishonest companies sometimes market medical discount plans or health plans with limited insurance benefits, as comprehensive health insurance. And sometimes they just lie about the "health plans" they offer. https://www.consumer.ftc.gov/blog/2021/11/open-season-really-health-insurance-youre-looking?utm_source=govdelivery

What to do if your online order never arrives — and how to get your money back
Shopping online is oh-so-convenient. Haven't we all bought stuff online when we could easily run to the store (figuratively, of course) and be back home in less than 30 minutes? Because reputable online businesses want happy, returning customers, they make returning something almost as simple as buying it. But what if a seller won't give you a refund even though you qualify for it? Or what if you ordered something and never got it? https://www.consumer.ftc.gov/blog/2021/11/what-do-if-your-online-order-never-arrives-and-how-get-your-money-back?utm_source=govdelivery

How to Steer Clear of Fake Review Scams
The Internet has brought us competitive shopping choices beyond anything we could have imagined 10 years ago. But that very situation has also delivered a lucrative opportunity for scammers -- fake reviews. The scam started with payments to freelancers for one-off commentaries and spread through free or discounted products or refunds for online buyers and, later, influencers paid to review and recommend. Some were no doubt genuine assessments and, for those that weren't, we didn't know any better. https://scambusters.org/fakereview.html https://www.consumerreports.org/online-shopping/online-shopping-scams-how-to-steer-clear/

Tabletop Exercises Focused on Individual, Organizational, and Community Resilience
EARTH EX has become the largest resilience exercise in history, with participation from all corporate and government sectors, individuals, families, and communities in more than 40 nations. And there is no cost to participate. https://eiscouncil.org/earth-ex/

****

News & Views

Holiday Shopping Disruption Beckons as Retail Bot Attacks Surge 13%
Security experts expressed concern over potential disruptions to the upcoming holiday shopping season after retail bot attacks were observed to have increased. Experts found that there was a double-digit year-on-year increase in bot driver cyberattacks in 2021. Imperva released a report titled State of Security Within eCommerce that revealed that… https://www.infosecurity-magazine.com/news/holiday-disruption-retail-bot/

Top 10 ways attackers are increasing pressure on their ransomware victims to pay
Sophos researchers have detailed how ransomware attackers are implementing a wide range of ruthless pressure tactics to persuade victims to pay the ransom.
https://www.helpnetsecurity.com/2021/11/04/attackers-pressure-ransomware-victims/

What's at stake in a credential stuffing attack
Attackers gain a network foothold by using stolen credentials under the guise of an authenticated trusted employee or third party. https://www.cybersecuritydive.com/news/whats-at-stake-in-a-credential-stuffing-attack/605807/

****

"Ctrl -F" for The Board

Ransomware Gangs Target Corporate Financial Activities
The Federal Bureau of Investigation has released a warning detailing how ransomware gangs are threatening to tank share prices for publicly held companies. According to the FBI, the new extortion tactic consists of cybercriminals targeting businesses when they are approaching significant and time-sensitive financial events, such as quarterly earnings reports… https://threatpost.com/ransomware-corporate-financial/175940/

Questions
Contact FIPCO’s Ken Shaurette at 800/722-3498 ext. 251 or email FIPCO IT Services for more information.

"Make Security Part of You and Your Institution's DNA!"

Threat Intelligence Newsletter: November 12, 2021

FIPCO®
IT Audit
Round Table
Discussions

If you would like to host an event, please contact: Amy Petersen

Upcoming Threat Intelligence Peer Group Discussions
None available at the current time

FFIEC Industry Outreach Webinar with the Financial Crimes Enforcement Network (FinCEN) on Ransomware Trends
https://fdicevents.webex.com/webappng/sites/fdicevents/meeting/info/87a84f33a091423eafaae724acde4bce?siteurl=fdicevents&MTID=m105d0b6ae5d0069065ca97d214c5e3a6

Direct Link:
https://fdicevents.webex.com/webappng/sites/fdicevents/meeting/download/87a84f33a091423eafaae724acde4bce?siteurl=fdicevents&MTID=m105d0b6ae5d0069065ca97d214c5e3a6

Event PW: 74JtnKsF36J
Event #: 2763 224 5851

****

Alerts & Warnings

Microsoft: Password spraying attacks are proliferating
Microsoft's Detection and Response Team is warning about an uptick in password spraying attacks, which are attempts to gain entry by using common passwords. These are the opposite of brute force attacks, which identify one account and hit it with hundreds or even thousands of passwords.
https://tech.co/news/microsoft-password-spraying

Zero-Days Under Attack: Microsoft Plugs Exchange Server, Excel Holes:
Microsoft said the two under-attack vulnerabilities exist in Microsoft Exchange Server and Microsoft Excel, two widely deployed products in the Windows ecosystem. Or have an XDR solution like Cynet360 from FIPCO in place makes zero day attacks less a worry.
https://www.securityweek.com/zero-days-under-attack-microsoft-plugs-exchange-server-excel-holes

New Android Spyware Poses Pegasus-Like Threat
Researchers have uncovered new Android spyware that boasts similar capabilities to the controversial NSO Group’s Pegasus spyware. The software, called PhoneSpy, is a mobile surveillance tool that has already stolen data and tracked the activity of targets in South Korea. The spyware is disguising itself as legitimate lifestyle apps. PhoneSpy…
https://threatpost.com/new-android-spyware-poses-pegasus-like-threat/176155/

Beware These Top 10 Online Holiday Shopping Scams
With pandemic scares still buzzing around and so many of us pressed for time, more Americans than ever will be doing most or all of their holiday shopping online this year.
https://scambusters.org/holidayshopping.html

Magniber ransomware gang now exploits Internet Explorer flaws in attacks
The Magniber ransomware gang is now using two Internet Explorer vulnerabilities and malicious advertisements to infect users and encrypt their devices.
https://www.bleepingcomputer.com/news/security/magniber-ransomware-gang-now-exploits-internet-explorer-flaws-in-attacks/?_hsmi=78978938&_hsenc=p2ANqtz-8W8HXDfJFhyoI9zQfGnDsO04KZwfg-rS-wfVCADu88dkgd9LRiGxrz6NMr45bG1jFxb5EsQ8Z6yfQmm7r8ZtRk-j6FlA

****

Hints & Tips plus Security Awareness

Looking for alternatives for your holiday shopping?
You’ve probably heard: this holiday season, it might be harder to find the gifts you’re looking for. So, many of us might be looking for alternatives, like buying gifts locally — or maybe from online marketplaces or sites you find through your social media accounts, online ads, or by searching online. If that might be you heading online, here are some things you can do to avoid a scam or negative experience.
https://www.consumer.ftc.gov/blog/2021/11/looking-alternatives-your-holiday-shopping?utm_source=govdelivery

****

News & Views

"Elevated privileges" are a problem in cybersecurity
Far too many employees of enterprises "are given elevated privileges on systems that have little to nothing to do with their day-to-day jobs," writes Brandon Blankenship, a cybersecurity consultant at ProCircular. Blankenship cites key individuals who might serve as vacation backups or do various jobs as a manner of course. https://www.thegazette.com/columns/cyber-security-and-the-principle-of-least-privilege/

****

"Ctrl -F" for The Board

FFIEC Industry Outreach Webinar with the Financial Crimes Enforcement Network (FinCEN) on Ransomware Trends

Ransomware incidents can severely affect business processes and leave organizations without the data they need to serve their customers. Malicious actors have adjusted their ransomware tactics over time to include pressuring victims for payment by threatening to release stolen data if victims refuse to pay, and by publicly naming and shaming victims as secondary forms of extortion. The monetary value of ransom demands has also increased. These ransomware incidents have become more destructive and impactful. This webinar will highlight current ransomware trends, and recently updated FFIEC statements about cyber preparedness and operational resilience as they relate to ransomware. This webinar will also include an overview of FinCEN's analysis of recent ransomware-related incidents.

Audio Bridge
Dial in Line:
+1-415-527-5035 US Toll

Access code:
2760 928 8643

Attendee Passcode:
85638456

Questions
Contact FIPCO's Ken Shaurette at 800/722-3498 ext. 251 or email FIPCO IT Services for more information.

"Make Security Part of You and Your Institution's DNA!"

Threat Intelligence Newsletter: December 3, 2021

FIPCO® IT Audit Round Table Discussions

If you would like to host an event, please contact: Becky Schowalter

Upcoming Threat Intelligence Peer Group Discussions
None available at the current time

****

Alerts & Warnings

HTML smuggling targets Banking industry
Microsoft reported HTML smuggling, which spread via email, had been extensively targeting banking organizations. Microsoft described the attack that surfaced in the early half of this month as "a highly evasive malware delivery technique". The attack uses genuine HTML5 and Javascript features to obfuscate its true actions. https://cyberdaily.securelayer7.net/html-smuggling-targets-banking-industry/

APT ACTORS EXPLOITING NEW IDENTIFIED VULNERABILITY IN - 'ManageEngine ADSelfServices Plus'
This joint advisory is the result of analytic efforts between the Federal Bureau of Investigation (FBI), United States Coast Guard Cyber Command (CGCYBER), and the Cybersecurity and Infrastructure Security Agency (CISA) to highlight the cyber threat associated with active exploitation of a newly identified vulnerability (CVE-2021-40539) in ManageEngine ADSelfService Plus—a self-service password management and single sign-on solution. https://pitstop.manageengine.com/portal/en/community/topic/adselfservice-plus-6114-security-fix-release

New Windows 10 zero-day gives admin rights, gets unofficial patch
Unofficial patches have been released to protect Windows users from a local privilege escalation (LPE) zero-day vulnerability in the Mobile Device Management Service impacting Windows 10, version 1809 and later. https://www.bleepingcomputer.com/news/security/new-windows-10-zero-day-gives-admin-rights-gets-unofficial-patch/?_hsmi=78978938&_hsenc=p2ANqtz-8LUml0UXVBh54nstSCWsmDS0t7qBASGvPgQOUyjORJFL735wDqYgyuqPQl_aE9nO_LfY-ikabTjG_ukC5Emn5HsP8bTA

Info-stealing trojan installed on millions of Android devices
More than 9 million Android devices have downloaded and installed dozens of games from the Huawei AppGallery that have a trojan designed to collect information, according to analysts.
https://www.scmagazine.com/news/cybercrime/info-stealing-trojan-installed-on-millions-of-android-devices?mkt_tok=MTg4LVVOWi02NjAAAAGBClL6bqCdjCLmGclqPh0r_w7-MUT43Oq9IqG8eJXfZGkxuD9fma-zGolWb_nkc44_iTHVFNRbUffB6el8s3kEb9Bpbkhwt6-mQF0tPA

Be Aware of Social Security Scams: Spread the word.
Share your knowledge of Social Security-related scams. Post on social media using the hashtag #SlamtheScam to share your experience and warn others. Visit oig.ssa.gov/scam for more information. Please also share with your friends and family.
https://links.ssa.gov/l/eyJhbGciOiJIUzI1NiJ9.eyJidWxsZXRpbl9saW5rX2lkIjoxMDUsInVyaSI6ImJwMjpjbGljayIsImJ1bGxldGluX2lkIjoiMjAyMTExMzAuNDk1Njk5NzEiLCJ1cmwiOiJodHRwczovL29pZy5zc2EuZ292L3NjYW0vP3V0bV9jYW1wYWlnbj1vaWctc2NhbS0yMiZ1dG1fY29udGVudD1vaWctc2NhbS1wYWdlJnV0bV9tZWRpdW09ZW1haWwmdXRtX3NvdXJjZT1nb3ZkZWxpdmVyeSJ9.szCO7SpZ_fwEpGzlco-_QazoeoVg9kNk3gUV4-gxsxw/s/1801829115/br/121969520320-l

Critical Wormable Security Flaw Found in Several HP Printer Models
Cybersecurity researchers on Tuesday disclosed eight-year-old security flaws affecting 150 different multifunction printers (MFPs) from HP Inc that could be potentially abused by an adversary to take control of vulnerable devices, pilfer sensitive information, and infiltrate enterprise networks to mount other attacks. https://thehackernews.com/2021/11/critical-wormable-security-flaw-found.html

The Emotet malware is now being spread via fake Adobe Windows App Installer packages.
Last month, the Emotet malware resurfaced after law enforcement shut down its infrastructure ten months ago. https://www.bleepingcomputer.com/news/security/emotet-now-spreads-via-fake-adobe-windows-app-installer-packages/

****

Hints & Tips plus Security Awareness

CISA Releases Incident and Vulnerability Response Playbooks
The Cybersecurity and Infrastructure Security Agency (CISA) has released two cybersecurity playbooks that focus specifically on incident and vulnerability response. https://www.securityweek.com/cisa-releases-incident-and-vulnerability-response-playbooks

5 IT risk assessment frameworks compared
Formal risk assessment methodologies can help take guesswork out of evaluating IT risks if applied appropriately. Here is real-world feedback on using COBIT, OCTAVE, FAIR, NIST RMF, and TARA.
https://www.csoonline.com/article/2125140/it-risk-assessment-frameworks-real-world-experience.html

Small businesses urged to protect their customers from card skimming
With Black Friday and Cyber Monday quickly approaching, the UK National Cyber Security Centre (NCSC) is urging small online shops to protect their customers from card skimming cyber criminals.
https://www.helpnetsecurity.com/2021/11/23/online-shops-card-skimming/

****

News & Views

New rule requires banks to report cybersecurity incidents
Financial regulators in the US will require banks to report serious cybersecurity incidents within 36 hours, beginning April 1. The notification requirement covers any incident that could disrupt operational viability or financial sector stability, such as a sizable distributed-denial-of-service attack. https://techcrunch.com/2021/11/19/us-banks-report-cybersecurity-incidents/

Why cybersecurity training needs a post-pandemic overhaul
COVID-19 may have ushered in the rise of remote work (either temporarily or permanently) but not all organizations were prepared to manage a fully remote workforce and the cybersecurity challenges that come with it. https://www.helpnetsecurity.com/2021/11/23/employees-cybersecurity-training/

What are people reporting at DoNotCall.gov? (FTC)
In the past 18 years of the National Do Not Call Registry, those of you signed up for the registry (244 million phone numbers right now) have reported millions upon millions of unwanted sales calls over the years. Here's a quick look at what you've reported this year at DoNotCall.gov about the calls you're getting. https://www.consumer.ftc.gov/blog/2021/11/what-are-people-reporting-donotcallgov?utm_source=govdelivery

****

"Ctrl -F" for The Board

US government looks to improve detection of cyberattacks
Jen Easterly, director of the Cybersecurity and Infrastructure Security Agency, says the US must improve visibility and modernize systems to address cyberthreats. "We're working to really centralize visibility to improve detection of incidents across federal government networks," she says. https://www.meritalk.com/articles/cisas-easterly-visibility-modernization-are-keys-to-cybersecurity/

Ransomware costs go far beyond price of ransom
The IBM Security Cost of a Data Breach Report 2021 finds that ransomware attacks cost organizations $4.62 million, on average, not including the cost of the ransom itself, if paid. The cost cited in the report includes response costs and lost business due to attacks. https://securityintelligence.com/cost-of-data-breach-bottom-line/

Questions
Contact FIPCO's Ken Shaurette at 800/722-3498 ext. 251 or email FIPCO IT Services for more information.

"Make Security Part of You and Your Institution's DNA!"

Threat Intelligence Newsletter: December 13, 2021

FIPCO® IT Audit Round Table Discussions

If you would like to host an event, please contact: Becky Schowalter

Upcoming Threat Intelligence Peer Group Discussions
None available at the current time

****

Alerts & Warnings

SURGE IN UNEMPLOYMENT INSURANCE SCAMS SPARKS GOVERNMENT WARNING
Unemployment insurance has been a boon for millions during the pandemic. But it's also been a boon for scammers. Government sources says there's been a big surge in fraudulent claims and innocent people could be the victims. https://scambusters.org/unemploymentinsurance.html

How Criminals Are Using Synthetic Identities for Fraud
Organizations must improve their cybersecurity protocols to detect fraudulent identities and make sure they're safeguarding their consumers' personal information. Synthetic identity fraud was already a problem before the COVID-19 pandemic shifted spending and work online, but it is becoming a bigger problem now as criminals take advantage of looser rules around credit and the sheer amount of personal information exposed via data breaches. https://www.darkreading.com/edge-articles/how-criminals-are-using-synthetic-identities-for-fraud?_mc=NL_DR_EDT_DR_daily_20211204&cid=NL_DR_EDT_DR_daily_20211204&elq_mid=107905&elq_cid=36315893

DNA testing center admits to breach affecting SSNs, banking info of more than 2 million people
DNA Diagnostics Center said it discovered the breach on August 6 but noted that hackers had access from May 24 to July 28. A DNA testing company has reported a data breach that leaked the personal information -- including Social Security Numbers and banking information -- of more than 2 million people, according to a notification letter the company is sending out to those affected.
https://www.zdnet.com/article/dna-testing-center-admits-to-breach-affecting-ssns-banking-info-of-more-than-2-million-people/

Scammers are tricking more people into buying gift cards
According to the newest Data Spotlight, 40,000 people reported losing a whopping $148 million in gift cards to scammers during the first nine months of 2021. Those are staggering numbers which have increased each year for the past several years… https://www.consumer.ftc.gov/blog/2021/12/scammers-are-tricking-more-people-buying-gift-cards?utm_source=govdelivery

Microsoft is raising SaaS prices, and other vendors will, too
The more value and tools vendors offer through SaaS, the more they can justify cost increases. Experts believe price hikes will become an annual tradition in the SaaS space. https://www.ciodive.com/news/Microsoft-saas-office-price-increases/611210/?utm_source=Sailthru&utm_medium=email&utm_campaign=Issue:%202021-12-10%20CIO%20Dive%20%5Bissue:38525%5D&utm_term=CIO%20Dive

****

Hints & Tips plus Security Awareness

USB Devices the Common Denominator in All Attacks on Air-Gapped Systems
A new study of 17 malware frameworks shows threat actors always use USB drives to sneak malware into air-gapped environments and then steal data from there. Cyberattacks on air gapped systems, including the sophisticated and dangerous 2010 Stuxnet attack that crippled a uranium enrichment facility, all have one thing in common: a USB stick. https://www.darkreading.com/attacks-breaches/usb-devices-common-denominator-in-all-attacks-on-air-gapped-systemsd?_mc=NL_DR_EDT_DR_daily_20211207&cid=NL_DR_EDT_DR_daily_20211207&elq_mid=107937&elq_cid=36315893

5 Ways to Keep Fraudsters at Bay Over the Holidays
Organizations want to focus on customer satisfaction and increased revenues during the holiday shopping season. Here are some smart security and fraud protections to keep in mind. Simply put, there is a lot of money at stake during this peak shopping season. Not surprisingly, attackers and fraudsters are keenly aware of this. They hone their skills and target their efforts to maximize their financial gain by maximizing customer losses. https://www.darkreading.com/edge-articles/5-ways-to-keep-fraudsters-at-bay-over-the-holidays?_mc=NL_DR_EDT_DR_daily_20211207&cid=NL_DR_EDT_DR_daily_20211207&elq_mid=107937&elq_cid=36315893

Six Ways Small Businesses Can Overcome Supply Chain Challenges
It's common knowledge that supply chain issues are currently widespread and affecting many industries. For small businesses, whether you have a retail outlet or an e-commerce store, it can be a challenge to keep popular items stocked and deal with impatient customers. https://www.darkreading.com/edge-articles/5-ways-to-keep-fraudsters-at-bay-over-the-holidays?_mc=NL_DR_EDT_DR_daily_20211207&cid=NL_DR_EDT_DR_daily_20211207&elq_mid=107937&elq_cid=36315893

UPDATE – New Proposed Cyber Incident Notification Rules Finalized
Currently, financial institutions are required to report a cyber event to their primary federal regulator under very specific circumstances. This requirement dates back to GLBA, Appendix B to Part 364 and states that FI incident response plans (IRP's) should contain procedures for: "Notifying its primary Federal regulator as soon as possible when the institution becomes…
https://complianceguru.com/2021/12/update-new-proposed-cyber-incident-notification-rules-finalized/?utm_medium=email&utm_content=192305688&utm_source=hs_email

****

News & Views

Is the security of legacy IT providers prompting a confidence crisis?
Research commissioned by CrowdStrike found security professionals are losing confidence in providers like Microsoft amid the rise in supply chain attacks. Microsoft has thoughts.
https://www.cybersecuritydive.com/news/is-the-security-of-legacy-it-providers-prompting-a-confidence-crisis/611167/?utm_source=Sailthru&utm_medium=email&utm_campaign=Issue:%202021-12-08%20Cybersecurity%20Dive%20%5Bissue:38461%5D&utm_term=Cybersecurity%20Dive

Why the C-Suite Doesn't Need Access to All Corporate Data
If zero trust is to work properly, then it must apply to everyone. To review, the key to the zero-trust framework is the principle of least privilege, which is the notion that all users are provided with the minimum level of access required to complete a task. Likewise, users should only be granted access to a particular app, system, or network when they need access. https://www.darkreading.com/vulnerabilities-threats/why-the-c-suite-doesn-t-need-access-to-all-corporate-data?_mc=NL_DR_EDT_DR_daily_20211207&cid=NL_DR_EDT_DR_daily_20211207&elq_mid=107937&elq_cid=36315893

US Military Has Acted Against Ransomware Groups: Report
The US military has taken offensive action against ransomware groups, said Gen. Paul Nakasone, head of US Cyber Command and director of the National Security Agency (NSA), according to new reports.
https://www.darkreading.com/threat-intelligence/us-military-has-acted-against-ransomware-groups-report?_mc=NL_DR_EDT_DR_daily_20211207&cid=NL_DR_EDT_DR_daily_20211207&elq_mid=107937&elq_cid=36315893

Bot Friday? A third of online Black Friday Shoppers were fake, new study reveals
New data released today by global Cybersecurity company CHEQ revealed that bots and fake users made up 35.7% of all online shoppers this Black Friday. Among the forms of fake traffic uncovered by CHEQ were malicious scrapers and crawlers, sophisticated botnets, fake accounts, click farms and proxy users as well as a host of illegitimate users committing eCommerce-related fraud. https://www.prnewswire.com/news-releases/bot-friday-a-third-of-online-black-friday-shoppers-were-fake-new-study-reveals-301437278.html

Canada Charges Its "Most Prolific Cybercriminal"
A 31-year-old Canadian man has been arrested and charged with fraud in connection with numerous ransomware attacks against businesses, government agencies and private citizens throughout Canada and the United States. Canadian authorities describe him as "the most prolific cybercriminal we've identified in Canada," but so far they've released few other details about the investigation or the defendant. Helpfully, an email address and nickname apparently connected to the accused offer some additional clues.
https://krebsonsecurity.com/2021/12/canada-charges-its-most-prolific-cybercriminal/

Widespread ‘Smishing’ Campaign Defrauds Iranian Android Users
Attackers are impersonating the Iranian government in a widespread SMS phishing campaign that is defrauding thousands of Android users by installing malware on their devices that can steal their credit card data and siphon money from financial accounts. https://threatpost.com/smishing-campaign-iranian-android-users/176679/

Clearview AI to be Fined $22.6m for Breaching UK Data Protection Laws
American facial recognition company Clearview AI faces a fine of just over £17m ($22.6m) for alleged “serious breaches” of the UK’s data protection laws. The UK’s Information Commissioner’s Office (ICO) announced the planned penalty yesterday and issued a provisional notice to Clearview to stop processing personal data taken from UK residents and to delete any such data in its possession.
The announcement follows a joint investigation by the ICO and the Office of the Australian Information Commissioner (OAIC), which found Clearview AI in breach of Australian privacy laws.
https://threatpost.com/smishing-campaign-iranian-android-users/176679/

Federal government looks to standardize zero-trust
The Department of Homeland Security's Cybersecurity and Infrastructure Security Agency is moving toward a zero-trust environment and a risk-based approach to cybersecurity. The agency is working on the incorporation of zero-trust into NIST Special Publication 800-53 standards.
https://federalnewsnetwork.com/ask-the-cio/2021/12/zero-trust-cloud-security-pushing-cisa-to-rethink-its-approach-to-cyber-services/

Security, GRC and Audits: Avoiding the Findings
Audits and regulatory examinations are inevitable in the financial industry. Audit findings don’t need to be, but as banking services grow more sophisticated and compete at fever pitch, you might find yourself postponing that risk assessment meeting to focus on your new digital banking platform release. Maybe the new release... https://discover.jackhenry.com/fintalk/security-grc-and-audits-avoiding-the-findings?utm_campaign=FinTalk&utm_medium=email&_hsmi=192348938&_hsenc=p2ANqtz-9PHA1v-vQAd8lpruZQX_kzOG9QSVHSisGlije77SKlFI0hqmgY8Hk4IWmdjKdQHDL_rgq4_YsaqjAnTCA3J7z9DuAyKg&utm_content=192348938&utm_source=hs_email

The Virginia Consumer Data Protection Act, the Colorado Privacy Act, and the Draft Connecticut Privacy Legislation: An Overview and Practical Guide
Just when organizations start to feel comfortable with the California Consumer Privacy Act (CCPA), as amended by the California Privacy Rights Act (CPRA), this year we saw the passage of two new comprehensive privacy laws in Virginia and Colorado and nearly another in Connecticut. This article discusses the Virginia Consumer Data Protection Act (VCDPA) and the Colorado Privacy Act (CoPA) and identifies parallels and differences between these statutes and other privacy laws. The article also discusses the pending comprehensive privacy law in Connecticut – we anticipate its passage in the near future. https://www.natlawreview.com/article/virginia-consumer-data-protection-act-colorado-privacy-act-and-draft-connecticut?utm_source=Robly.com&utm_medium=email&utm_campaign=2021-12-08Cybersecurity+Legal+News&utm_content=f1f2eab83e2347962507a6be67696310

****

"Ctrl -F" for The Board

Bosses are reluctant to spend money on cybersecurity. Then they get hacked
Preventing a cyberattack is more cost effective than reacting to one - but many boardrooms still aren't willing to free up budget. https://www.zdnet.com/article/too-many-bosses-are-reluctant-to-spend-money-on-cybersecurity-then-they-get-hacked/?utm_source=Sailthru&utm_medium=email&utm_campaign=Issue:%202021-12-07%20Cybersecurity%20Dive%20%5Bissue:38443%5D&utm_term=Cybersecurity%20Dive#ftag=RSSbaffb68

A month after 'malicious' cyberattack, a small Colorado utility still doesn't have all systems back online
Delta-Montrose Electric Association is still working to restore its payment and billing systems. Security experts say the recovery time points to a need for better backups.
https://www.cybersecuritydive.com/news/malicious-cyberattack-colorado-utility-recovery/611048/?utm_source=Sailthru&utm_medium=email&utm_campaign=Issue:%202021-12-07%20Cybersecurity%20Dive%20%5Bissue:38443%5D&utm_term=Cybersecurity%20Dive

The ransomware threat landscape has changed: here's how defenders must adapt
Cybersecurity professionals once imagined that their adversaries were criminal gangs who operated within a shadowy underworld, trading secrets and malicious code on clandestine hacker forums.
https://www.cybersecuritydive.com/spons/the-ransomware-threat-landscape-has-changed-heres-how-defenders-must-adap/610815/

Questions
Contact FIPCO’s Rob Foxx at 800-722-3498 ext. 249 or email FIPCO IT Services for more information.

"Make Security Part of You and Your Institution's DNA!"

Threat Intelligence Newsletter: December 17, 2021

FIPCO®
IT Audit
Round Table
Discussions

If you would like to host an event, please contact: Becky Schowalter

Upcoming Threat Intelligence Peer Group Discussions
None available at the current time

****

Alerts & Warnings

Log4Shell Explained

Log4j is an open-source logging framework distributed by Apache group that is widely used by well-known public services and roughly one third of the world's webservers. On December 9, 2021, an RCE (Remote Code Execution) vulnerability was disclosed within the log4j package (CVE- 2021-44228) which allows an attacker to execute arbitrary code on machines which utilize the logging functionality of log4j package which give the vulnerability its common name: Log4Shell. https://www.cynet.com/log4shell

Chinese, Iranian State Hackers Exploiting Log4j Flaw

Chinese and Iranian state actors are exploiting the recently disclosed "Log4Shell" vulnerability that has sparked chaos across the tech world, cybersecurity firm Mandiant warned late Tuesday.
https://www.securityweek.com/chinese-iranian-state-hackers-exploiting-log4j-flaw-mandiant

New TSA PreCheck Scam Seeks to Collect Your Personal and Credit Card Details

Doing one of the best jobs impersonating a website ever seen, this new scam attempts to take those renewing or initially signing up through a believable process that most would fall for.
https://blog.knowbe4.com/new-tsa-precheck-scam-seeks-to-collect-your-personal-and-credit-card-details

Cloud outages raise question on how to architect for resiliency

AWS uptime briefly wobbled Wednesday, an incident unrelated to last week's hours-long outage. For long-term business resilience against provider disruption, the answer may be rearchitecting workloads.
https://www.ciodive.com/news/AWS-outage-iaas-resiliency/611607/?utm_source=Sailthru&utm_medium=email&utm_campaign=Issue:%202021-12-16%20CIO%20Dive%20%5Bissue:38650%5D&utm_term=CIO%20Dive

Cuba ransomware targets critical infrastructure, steals $44M in payments

The threat actors compromised at least 49 organizations across the financial, government, healthcare, manufacturing, and information technology sectors.
https://www.cybersecuritydive.com/news/cuba-ransomware-fbi-critical-infrastructure/610984/?utm_source=Sailthru&utm_medium=email&utm_campaign=Newsletter%20Weekly%20Roundup:%20Cybersecurity%20Dive:%20Daily%20Dive%2012-11-2021&utm_term=Cybersecurity%20Dive%20Weekender

Kronos Suffers Ransomware Attack, Expects Full Restoration to Take 'Weeks'

Customers advised to adopt alternative internal processes to support the affected human resources services.
https://www.darkreading.com/attacks-breaches/kronos-suffers-ransomware-attack-expects-full-restoration-to-take-weeks-?_mc=NL_DR_EDT_DR_daily_20211214&cid=NL_DR_EDT_DR_daily_20211214&elq_mid=108060&elq_cid=36315893

Lack of Patching Leaves 300,000 Routers at Risk for Attack

Hundreds of thousands of routers produced by a Latvian network hardware firm MikroTik are still vulnerable to at least one of four vulnerabilities that are over a year old. These vulnerabilities are most likely being used by attackers as their operational infrastructure. Approximately 94% of the 2 million routers deployed.
https://www.oodaloop.com/briefs/2021/12/10/lack-of-patching-leaves-300000-routers-at-risk-for-attack/

****

Hints & Tips plus Security Awareness

How to spot, stop, and report post-disaster scams

If you or someone you know has been affected by the devastating series of tornadoes that roared across Kentucky, Illinois, Tennessee, Arkansas, and Missouri, coping with the aftermath is never easy. But when scammers target people just trying to recover, it can be even worse. Here are ways to help you and your neighbors avoid common post-disaster scams.
https://www.consumer.ftc.gov/blog/2021/12/how-spot-stop-and-report-post-disaster-scams?utm_source=govdelivery

What CISOs need to know on securing against ransomware

Security experts hail cybersecurity basics as the best defense against ransomware — regular patching, multifactor authentication and, maybe most importantly, information sharing.
https://www.cybersecuritydive.com/trendline/securing-against-ransomware/214/?utm_source=CSD&utm_medium=InlineDec16&utm_campaign=Horizon3.ai&utm_content=ad-SPONSORED_CONTENT&utm_term=38042

Why Cloud Storage Isn't Immune to Ransomware

Cloud security is a shared responsibility. which sometimes leads to security gaps and complexity in risk management.
https://www.darkreading.com/attacks-breaches/why-cloud-storage-isn-t-immune-to-ransomware?_mc=NL_DR_EDT_DR_daily_20211216&cid=NL_DR_EDT_DR_daily_20211216&elq_mid=108123&elq_cid=36315893

Combat Misinformation by Getting Back to Security Basics
One volley of fake news may land, but properly trained AI can shut down similar attempts at their sources. https://www.darkreading.com/attacks-breaches/combat-misinformation-by-getting-back-to-security-basics?_mc=NL_DR_EDT_DR_daily_20211215&cid=NL_DR_EDT_DR_daily_20211215&elq_mid=108090&elq_cid=36315893

Actively Exploited Microsoft Zero-Day Allows App Spoofing, Malware Delivery
Microsoft has addressed a recently discovered vulnerability that was exploited in the wild to deliver Emotet, Trickbot, and other botnets via fake applications. The vulnerability was included in the company's December Patch Tuesday, along with five other publicly known bugs and seven critical security vulnerabilities. In total, this month's security. https://www.oodaloop.com/briefs/2021/12/15/actively-exploited-microsoft-zero-day-allows-app-spoofing-malware-delivery/

****

News & Views

Cyber Risk Institute Updates Cybersecurity Profile
The Cyber Risk Institute—a coalition of financial institutions and trade associations including the American Bankers Association—has updated its Financial Services Cybersecurity Profile. The profile—which ABA helped develop and which is intended to help financial institutions reduce the overall time spent on cyber risk compliance—is currently being implemented by many institutions and is accepted by the regulatory community.
https://bankingjournal.aba.com/2021/12/cyber-risk-institute-updates-cybersecurity-profile-2/?utm_source=eloqua&utm_medium=email&utm_campaign=newsbytes&utm_content=NEWSBYTES-20211215

Microsoft is raising SaaS prices, and other vendors will, too
The more value and tools vendors offer through SaaS, the more they can justify cost increases. Experts believe price hikes will become an annual tradition in the SaaS space.
https://www.ciodive.com/news/Microsoft-saas-office-price-increases/611210/?utm_source=Sailthru&utm_medium=email&utm_campaign=Newsletter%20Weekly%20Roundup:%20CIO%20Dive:%20Daily%20Dive%2012-11-2021&utm_term=CIO%20Dive%20Weekender

Crypto execs push for tailored regulation, but not a rush to judgment
At stake, they said in a Wednesday hearing on Capitol Hill, is the U.S.'s leadership in the field.
https://www.bankingdive.com/news/crypto-execs-push-for-tailored-regulation-but-not-a-rush-to-judgment/611183/?utm_source=Sailthru&utm_medium=email&utm_campaign=Newsletter%20Weekly%20Roundup:%20Banking%20Dive:%20Daily%20Dive%2012-11-2021&utm_term=Banking%20Dive%20Weekender

Inside Ireland's Public Healthcare Ransomware Scare
The accounting firm PricewatersCoopers recently published lessons learned from the disruptive and costly ransomware attack in May 2021 on Ireland's public health system. The unusually candid post-mortem found that nearly two months elapsed between the initial intrusion and the launching of the ransomware. It also found affected hospitals had tens of thousand of outdated Windows 7 systems, and that the health system's IT administrators failed to respond to multiple warning signs that a massive attack was imminent.
https://krebsonsecurity.com/2021/12/inside-irelands-public-healthcare-ransomware-scare/

****

"Ctrl -F" for The Board

Data is an asset. Treat it as such.

If a company loses its data or if its data is compromised, it could significantly damage the business in terms of financial performance, brand reputation or loss of customers.

https://www.ciodive.com/spons/data-is-an-asset-treat-it-as-such/610892/

'War for talent' rises toward top of C-suite risks for 2022

The ability to attract and retain top talent jumped to the second spot in a ranking of business risks, up from No. 8 a year ago, according to a global survey.

https://www.ciodive.com/news/talent-war-rises-toward-top-business-risks-2022/611447/?utm_source=Sailthru&utm_medium=email&utm_campaign=Issue:%202021-12-14%20CIO%20Dive%20%5Bissue:38577%5D&utm_term=CIO%20Dive

Questions

Contact FIPCO’s Rob Foxx at 800-722-3498 ext. 249 or email FIPCO IT Services for more information.

"Make Security Part of You and Your Institution's DNA!"

Threat Intelligence Newsletter: December 23, 2021

FIPCO® IT Audit Round Table Discussions

If you would like to host an event, please contact: Becky Schowalter

Upcoming Threat Intelligence Peer Group Discussions
None available at the current time

****

Alerts & Warnings

Google Finds 35,863 Java Packages Using Defective Log4j
The sheer scale and impact of the crisis became a bit clearer this week with Google's open-source team reporting that a whopping 35,863 Java packages in Maven Central are still using defective versions of Log4j library.
https://www.securityweek.com/google-finds-35863-java-packages-using-defective-log4j

Conti Ransomware Gang Has Full Log4Shell Attack Chain
According to new reports, the sophisticated Russia-based Conti ransomware group has become the first group to weaponize Log4j2 with a full attack chain. Last week, the group became the first professional cybercrime group to adopt the Log4Shell vulnerability and has since built up a holistic attack chain, according to researchers.
https://threatpost.com/conti-ransomware-gang-has-full-log4shell-attack-chain/177173/

Meta Acts Against 7 Entities Found Spying on 50,000 Users
The parent company of Facebook and Instagram has warned some 50,000 account holders they are targets of surveillance.
https://www.darkreading.com/threat-intelligence/meta-acts-against-7-entities-found-spying-on-50-000-users?_mc=NL_DR_EDT_DR_daily_20211220&cid=NL_DR_EDT_DR_daily_20211220&elq_mid=108166&elq_cid=36315893

FBI says hackers are actively exploiting this flaw on ManageEngine Desktop Central servers
The FBI has issued an advisory regarding a vulnerability in the Zoho ManageEngine Desktop Central that is being actively exploited by advanced cyberattackers. According to the warning, the flaw has been exploited to install malware since late October.
https://www.oodaloop.com/briefs/2021/12/21/fbi-says-hackers-are-actively-exploiting-this-flaw-on-manageengine-desktop-central-servers/

VISHING DRIVES SURGE IN CELL PHONE SCAMS
Vishing is a phishing scam but uses your phone rather than emails or texts. And with 298 million Americans using these devices, they've become a prime target for the tricksters.
https://scambusters.org/vishing2.html

Researchers Uncover New Coexistence Attacks On Wi-Fi and Bluetooth Chips
Cybersecurity researchers have demonstrated a new attack technique that makes it possible to leverage a device's Bluetooth component to directly extract network passwords and manipulate traffic on a Wi-Fi chip, putting billions of electronic devices at risk of stealthy attacks.
https://thehackernews.com/2021/12/researchers-uncover-new-coexistence.html?_m=3n%2e009a%2e2634%2eod0ao445rz%2e1odc

TSA Precheck
If you're flying away for Christmas or New Year breaks, be on your guard and watch out for phishing emails and websites pretending to be the TSA PreCheck airport security service, complete with lookalike logos. Check our recent report on this scam at https://scambusters.org/airportsecurity.html

Researchers Disclose Unpatched Vulnerabilities in Microsoft Teams Software
Microsoft said it won't be fixing or is pushing patches to a later date for three of the four security flaws uncovered in its Teams business communication platform earlier this March.
https://thehackernews.com/2021/12/researchers-disclose-unpatched.html?_m=3n%2e009a%2e2638%2eod0ao445rz%2e1ogq

Active Directory Bugs Could Let hackers Take Over Windows Domain Controllers
Microsoft is urging customers to patch two security vulnerabilities in Active Directory domain controllers that it addressed in November following the availability of a proof-of-concept (PoC) tool on December 12.
https://thehackernews.com/2021/12/active-directory-bugs-could-let-hackers.html?_m=3n%2e009a%2e2637%2eod0ao445rz%2e1ofo

****

Hints & Tips plus Security Awareness

5 Ways to Keep Fraudsters at Bay Over the Holidays
Organizations want to focus on customer satisfaction and increased revenues during the holiday shopping season. Here are some smart security and fraud protections to keep in mind.
https://www.darkreading.com/edge-articles/5-ways-to-keep-fraudsters-at-bay-over-the-holidays?_mc=NL_DR_EDT_DR_daily_20211218&cid=NL_DR_EDT_DR_daily_20211218&elq_mid=108163&elq_cid=36315893

****

News & Views

Dear Congress: It's Complicated. Please Consider This When Crafting New Cybersecurity Legislation
As mandatory reporting bills work their way through the halls of Congress, what should businesses do to prepare for this pending legislation?
https://www.darkreading.com/risk/dear-congress-it-s-complicated-please-consider-this-when-crafting-new-cybersecurity-legislation?_mc=NL_DR_EDT_DR_daily_20211217&cid=NL_DR_EDT_DR_daily_20211217&elq_mid=108144&elq_cid=36315893

Zero Trust Shouldn’t Mean Zero Trust in Employees
Some think zero trust means you cannot or should not trust employees, an approach that misses the mark and sets up everyone for failure.
https://www.darkreading.com/endpoint/zero-trust-shouldn-t-mean-zero-trust-in-employees?_mc=NL_DR_EDT_DR_daily_20211221&cid=NL_DR_EDT_DR_daily_20211221&elq_mid=108198&elq_cid=36315893

UK Cyber Cops Share 225 Million Passwords with Breach Site
UK cyber investigators have share 225 million stolen passwords with a popular data breach checking website, offering it the ability to significantly expand its reach. HaveIBeenPwned is a tool for the public that allows individuals to easily check if their phone, email, or password has been involved in a data breach.
https://ooda.us1.list-manage.com/track/click?u=f16e84831246ee66e1d9f6eab&id=d253d09cff&e=158fb74005

The Need for Artificial Intelligence Governance
Artificial intelligence, and more specifically machine learning, is being deployed in the insurance space in some very exciting ways — from assessing underwriting risks to determining pricing to evaluating claims. But with these advances come sizable risks, some of which are already surfacing.
https://www.nbcnews.com/tech/security/bitcoin-crypto-exchange-hacks-little-anyone-can-do-rcna7870

****

"Ctrl -F" for The Board

Crypto exchanges keep getting hacked, and there’s little anyone can do
It’s not just lucky investors getting rich from crypto. Hackers have made off with billions of dollars in virtual assets in the past year by compromising some of the cryptocurrency exchanges that have emerged during the bitcoin boom.
https://www.nbcnews.com/tech/security/bitcoin-crypto-exchange-hacks-little-anyone-can-do-rcna7870

Cloud computing has won. But we still don’t know what that means
There’s little doubt that cloud computing is now the absolutely dominant force across enterprise computing. Most companies have switched from buying their own hardware and software to renting both from vendors who host their services in vast anonymous data centers around the globe.
https://www.zdnet.com/article/cloud-computing-has-won-but-we-still-dont-know-what-that-means/

The True Cost Of Rising Cyber Threats, According To A Cybersecurity CFO
Every security product in the last 20 years has been built to identify attacks after they have been executed. Look no further than then one of the hottest categories in cybersecurity — endpoint detection and response (EDR) — to see the proof.
https://www.forbes.com/sites/deep-instinct/2021/11/29/the-true-cost-of-rising-cyber-threats-according-to-a-cybersecurity-cfo/?sh=44114715f332

Fed Observes 'Unprecedented Decline' in In-Person Payments during COVID
Payment behavior "changed sharply in 2020 with the COVID-19 pandemic," the Federal Reserve said today in a new research brief. In-person card payments exhibited an "unprecedented decline" in 2020, with the number of these payments falling by 11.7 billion—the first one-year decline of in-person card payments ever seen in the Fed's data. Meanwhile, remote card payments increased by 8.7 billion, the largest on-year increase ever observed.
https://bankingjournal.aba.com/2021/12/fed-observes-unprecedented-decline-in-in-person-payments-during-covid/?utm_source=eloqua&utm_medium=email&utm_campaign=newsbytes&utm_content=NEWSBYTES-20211223

Why MFA, Why Now
In the last year, we've seen federal agencies, cyber insurance providers, and more require MFA to be implemented to remain compliant and accessible. Salesforce is the latest to require an MFA solution for their own homegrown solution enabled for uninterrupted access. These events are reiterating the importance of having a scalable IAM strategy in place. Webinar 30 Minutes on Jan 12, 2022, 11AM CST
https://www.brighttalk.com/webcast/14899/524030?player-preauth=zXerQNCJNDKAVfA8sCd%2ByYLzcHlRL6Vsz0IZ3fLF8ZY%3D&utm_source=brighttalk-promoted&utm_medium=email&utm_term=Audience290672&utm_campaign=AUD-11639&utm_content=2021-12-22

Questions
Contact FIPCO's Rob Foxx at 800-722-3498 ext. 249 or email FIPCO IT Services for more information.

"Make Security Part of You and Your Institution's DNA!"

Threat Intelligence Newsletter: December 30, 2021

FIPCO®
IT Audit
Round Table
Discussions

If you would like to host an event, please contact: Becky Schowalter

Upcoming Threat Intelligence Peer Group Discussions
None available at the current time

****

Alerts & Warnings

5+ Common Job Scams in 2021
Job scams have always existed in one way or another, be it in the form of a fake job ad in the newspaper, on TV, or on the radio. But with more and more people turning to the internet to find jobs, job scams have both moved online and become more frequent. According to the FBI's Internet Crime Complaint Center, 16,012 people reported being victims of employment scams in 2020, with losses amounting to more than $59 million. https://novoresume.com/career-blog/job-scams

Payment by gift card? It's a scam!
Gift cards are popular and convenient … and not just for gifts. Con artists have latched onto gift cards as a convenient form of payment in their scams. In a 2021 AARP survey, nearly 1 in 3 adults said they or someone they know had been asked at some point to purchase a gift card to pay a bill, fee or some other debt or obligation or to claim a prize. https://www.aarp.org/money/scams-fraud/gift-card-payment/?CMP=EMC-CSN-NLC-OTH-FWN_NEWS_DEC29_NATIONAL-1090501-1426503-12292021_section_two_bullet3_LNK-6037456&encparam=a2kbABDTs8aki3KrMaMg9C%2f8GD2Ftx%2bE8fs%2fPojRO%2bU%3d

Beware of Robocalls, Texts and Emails Promising COVID-19 Cures or Stimulus Payments
As of Dec. 14, the Federal Trade Commission (FTC) had logged nearly 657,000 consumer complaints related to COVID-19 and stimulus payments, 73 percent of them involving fraud or identity theft. These scams have cost consumers $636.7 million, with a median loss of $400. https://www.aarp.org/money/scams-fraud/info-2020/coronavirus.html?CMP=EMC-CSN-NLC-OTH-FWN_NEWS_DEC29_NATIONAL-1090501-1426503-12292021_section_one_body_LNK-6037456&encparam=a2kbABDTs8aki3KrMaMg9C%2f8GD2Ftx%2bE8fs%2fPojRO%2bU%3d

TIKTOK SCAMS PUT YOUNGSTERS AT RISK
With a claimed active user base of one billion, social media site TikTok is a big hit with the younger generations. But they're also one of the age groups most likely to fall for con tricks, which keeps TikTok scammers busy. https://scambusters.org/tiktok.html

****

Hints & Tips plus Security Awareness

7 Steps for Navigating a Zero-Trust Journey
Don't think of zero trust as a product. Think of it as "how you actually practice security."
https://www.darkreading.com/edge-slideshows/7-steps-for-navigating-a-zero-trust-journey-?_mc=NL_DR_EDT_DR_daily_20211230&cid=NL_DR_EDT_DR_daily_20211230&elq_mid=108290&elq_cid=36315893

****

News & Views

7 of the Most Impactful Cybersecurity Incidents of 2021
There was a lot to learn from breaches, vulnerabilities, and attacks this year.
https://www.darkreading.com/attacks-breaches/6-of-the-most-impactful-cybersecurity-incidents-of-2021?_mc=NL_DR_EDT_DR_daily_20211227&cid=NL_DR_EDT_DR_daily_20211227&elq_mid=108247&elq_cid=36315893

What's In Store for Nation State Cyber Activity in 2022?
As 2021 winds down, online cybersecurity journals and cyber experts are providing their cyber threat forecasts for the new year. Ransomware, cloud security, supply chain attacks, and of course critical infrastructure are common themes in many of these prognostications.
https://www.oodaloop.com/archive/2021/12/27/whats-in-store-for-nation-state-cyber-activity-in-2022/

Shutterfly reports ransomware incident
Shutterfly, a digital photography company, has reported a ransomware attack that occurred on Sunday. Shutterfly confirmed that portions of the Lifetouch and BorrowLenses business were affected. The company also experienced interruptions with Groovebook manufacturing offices, and corporate systems due to the attack. Shutterfly stated that it had contacted law enforcement...
https://www.oodaloop.com/briefs/2021/12/28/us-halves-isolation-time-for-asymptomatic-covid-infection/

NY Man Pleads Guilty in $20 Million SIM Swap Theft
Nicholas Truglia, a 24-year-old New York resident, has pleaded guilty of helping to steal more than $20 million worth of cryptocurrency from a technology executive names Michael Terpin. Terpin is a cryptocurrency investor who co-founded the first angel investor group for bitcoin. Truglia was a member of a group that... https://www.oodaloop.com/cyber/2021/12/29/ny-man-pleads-guilty-in-20-million-sim-swap-theft/

****

"Ctrl -F" for The Board

Average IT salary reaches 6 figures. What's next for technology hiring?
The shift to remote work is spurring a "normalizing of compensation rates" across locations, Randstad research found. https://www.ciodive.com/news/randstad-IT-salaries-report/593929/?utm_source=Sailthru&utm_medium=email&utm_campaign=Issue:%202021-12-29%20Top%20CIO%20Trends%20%5Bissue:38739%5D&utm_term=CIO%20Dive%20-%20All%20daily%20%2B%20Weekender%20Subscribers

What cyber insurance CEOs want to see from customers
Insurers joined high-profile CEOs at the White House summit last week to discuss how to improve national cybersecurity. For one insurance CEO, the industry needs three points of improvement. https://www.cybersecuritydive.com/news/white-house-tech-summit-cyber-insurance/605845/?utm_source=Sailthru&utm_medium=email&utm_campaign=Issue:%202021-12-29%20Top%20Cybersecurity%20Trends%20%5Bissue:38799%5D&utm_term=Cybersecurity%20Dive%20%2B%20Weekender

Questions
Contact FIPCO's Rob Foxx at 800-722-3498 ext. 249 or email FIPCO IT Services for more information.

"Make Security Part of You and Your Institution's DNA!"

Threat Intelligence Newsletter: January 11, 2022

FIPCO®
IT Audit
Round Table
Discussions

If you would like to host an event, please contact: Becky Schowalter

Upcoming Threat Intelligence Peer Group Discussions
None available at the current time

****

Alerts & Warnings

Don't trade personal info for coupons
Everyone loves a good deal, and scammers know it. Counterfeit coupons are popular way for scammers to steal your identity and money. Motives and methods vary, but phony coupons often mean serious losses for retailers, consumers, or both
https://www.bbb.org/article/news-releases/22318-bbb-scam-alert-fake-retail-coupons-hit-social-media?utm_source=newsletter&utm_medium=email&utm_content=Read%20our%20other%20tips%20for%20avoiding%20phony%20coupons.%C2%A0&utm_campaign=scam-alert

FTC threatens enforcement on firms lax about Log4j vulnerability
The FTC warning underscores a commitment by federal regulators to ensure a more secure environment for enterprise and consumer software, according to legal experts and industry analysts.
https://www.cybersecuritydive.com/news/ftc-enforcement-companies-log4j/616683/?utm_source=Sailthru&utm_medium=email&utm_campaign=Issue:%202022-01-05%20Cybersecurity%20Dive%20%5Bissue:38945%5D&utm_term=Cybersecurity%20Dive

LastPass Users Warned After Suspicious Login Attempts From Strange Locations
LastPass users have been alerted to a potential cybersecurity risk on the platform that may have compromised passwords, payment cards, and other sensitive data. LastPass, a password management app, detected suspicious login attempts almost immediately, and was able to take action against the unauthorized access. https://www.forbes.com/sites/dollar-general/2021/12/17/lessons-learned-for-the-future-of-retail/?sh=3584d6c7a66e

UK’s Defence Academy hit by cyberattack which caused ‘significant’ damage
The UK’s Defence Academy reportedly suffered from a cyberattack last year that inflicted significant damage to the institution, says a retired high-ranking officer. Air Marshal Edward Stringer stated that the attack was likely launched by a hostile foreign state such as Russia or China.
https://www.oodaloop.com/briefs/2022/01/04/uks-defence-academy-hit-by-cyberattack-which-caused-significant-damage/

Data Skimmer Hits 100+ Sotheby’s Real-Estate Websites
A data-skimming attack has hit over 100 Sotheby’s real estate websites in a supply chain attack abusing a weaponized cloud video player. According to Palo Alto Networks’ Unit 42 division, all of the compromised sites belonged to Sotheby’s and no other companies were impacted.
https://threatpost.com/data-skimmer-sothebys-real-estate-websites/177347/

Fire at vital tech factory could worsen global computer chip shortage
A fire at a plant in Berlin, Germany owned by ASML Holding could worsen the global computer chip shortage as the plant is the sole provider of a vital technology used to manufacture computer chips.
https://www.newscientist.com/article/2303316-fire-at-vital-tech-factory-could-worsen-global-computer-chip-shortage/

Big US banks are slowly embracing cloud services like AWS, Azure, and GCP, after hesitating for years due to regulation, cyberattacks, and old infrastructure
Michael W. Lucas made big plans to take a trip around the world in March 2020. He arranged to travel from his home in Detroit to Tokyo, then attend conferences in Hong Kong and Bangalore, India, before making a final stop in Paris. https://www.oodaloop.com/technology/2022/01/04/big-us-banks-are-slowly-embracing-cloud-services-like-aws-azure-and-gcp-after-hesitating-for-years-due-to-regulation-cyberattacks-and-old-infrastructure/

Why Card Stacking Loans Could Be a Costly Scam
You need money but you can't imagine where it's going to come from. So, you approach a loan company that has the answer: Take on lots of credit cards and max them out for cash or to pay debts.
https://scambusters.org/cardstacking.html

****

Hints & Tips plus Security Awareness

The CISO as Sustaining Force: Helping Infosec Staff Beat Burnout
To protect their staffers, leaders should focus on identifying and alleviating root causes of burnout.
https://www.darkreading.com/careers-and-people/the-ciso-as-sustaining-force-helping-infosec-staff-beat-burnout?_mc=NL_DR_EDT_DR_daily_20220103&cid=NL_DR_EDT_DR_daily_20220103&elq_mid=108299&elq_cid=36315893

T-Mobile confirms SIM swapping attacks led to breach
T-Mobile recently confirmed a data breach that was caused by SIM swapping attacks, according to the T-Mo Report. T-Mo Report, a block tracking T-Mobile, obtained internal reports that showed data was leaked from a subset of customers. According to the report, some individuals had their customer proprietary network information leaked https://www.zdnet.com/article/t-mobile-confirms-sim-swapping-attacks-led-to-breach/

****

News & Views

NCUA OKs crypto partnerships for credit unions
"Financial services has always been 'adapt or die,'" Kyle Hauptman, the regulator's vice chair, told CoinDesk. "I don't want credit unions to go the way of Blockbuster Video because we, the regulators, prevented innovation." https://www.bankingdive.com/news/ncua-oks-crypto-partnerships-for-credit-unions/616624/?utm_source=Sailthru&utm_medium=email&utm_campaign=Issue:%202022-01-04%20Banking%20Dive%20%5Bissue:38887%5D&utm_term=Banking%20Dive

Mobile Application Security: 2021's Breaches
Many of last year's largest app breaches could have been prevented with testing, training, and the will to take app security seriously.
https://www.darkreading.com/application-security/mobile-application-security-2021-s-breaches?_mc=NL_DR_EDT_DR_daily_20220105&cid=NL_DR_EDT_DR_daily_20220105&elq_mid=108340&elq_cid=36315893

****

"Ctrl -F" for The Board

Intelligent Information Capture: Fintechs vs Traditional Banks
While financial institutions started to automate and digitize more than a decade ago, the changing preferences for digitization of services and communication changed faster than offers. This created an opportunity that FinTechs embraced and pressure for traditional banks to remain relevant.
Webinar Jan 25th 10AM CST https://www.brighttalk.com/webcast/13689/524758?player-preauth=WLYxJCqo4mn6TgswWxN58gaF0x6QBBYdABxuaOc5WsA%3D&utm_source=brighttalk-promoted&utm_medium=email&utm_term=Audience295052&utm_campaign=AUD-11711&utm_content=2022-01-4

Gartner: 12 technology trends for 2022 and beyond
The way back toward sustainable profits and expansion starts with technology investments as CIOs are expected to create resilient IT organizations. https://www.ciodive.com/news/gartner-strategic-trends-2022/608315/?utm_source=Sailthru&utm_medium=email&utm_campaign=Issue:%202022-01-03%20CIO%20Dive%20%5Bissue:38741%5D&utm_term=CIO%20Dive

Multiple buyers, hybrid work drive software spending through 2022
A pandemic-era wave of software deployment was aimed at solving urgent gaps for businesses. Apps that automated staff onboarding or facilitated online collaboration let companies keep running through the lockdown phase. https://www.ciodive.com/news/enterprise-software-buying-trends-2022/607399/?utm_source=Sailthru&utm_medium=email&utm_campaign=Issue:%202022-01-03%20CIO%20Dive%20%5Bissue:38741%5D&utm_term=CIO%20Dive

Questions
Contact FIPCO's Rob Foxx at 800-722-3498 ext. 249 or email FIPCO IT Services for more information.

"Make Security Part of You and Your Institution's DNA!"

Threat Intelligence Newsletter: January 20, 2022

FIPCO®
IT Audit
Round Table
Discussions

If you would like to host an event, please contact: Donna Stanger

Upcoming Threat Intelligence Peer Group Discussions
None available at the current time

****

Alerts & Warnings

Norton 360 Now Comes With a Cryptominer
Norton 360, one of the most popular antivirus products on the market today, has installed a cryptocurrency mining program on its customers' computers.
https://krebsonsecurity.com/2022/01/norton-360-now-comes-with-a-cryptominer/

Partially Unpatched VMware Bug Opens Door to Hypervisor Takeover
ESXi version 7 users are still waiting for a full fix for a high-severity heap-overflow security vulnerability, but Cloud Foundation, Fusion and Workstation users can go ahead and patch.
https://threatpost.com/unpatched-vmware-bug-hypervisor-takeover/177428/?utm_source=Sailthru&utm_medium=email&utm_campaign=Issue:%202022-01-07%20Cybersecurity%20Dive%20%5Bissue:39012%5D&utm_term=Cybersecurity%20Dive

Phishing lures await in Google Docs comments
Despite the increased use of productivity tools in the enterprise, email remains a favored attack vector for bad actors because credentials for platforms like Slack are less sought-after by cybercriminals. Attackers often initiate attacks from compromised email accounts.
https://www.ciodive.com/news/phishing-google-docs-impersonation/616932/?utm_source=Sailthru&utm_medium=email&utm_campaign=Issue:%202022-01-11%20CIO%20Dive%20%5Bissue:39046%5D&utm_term=CIO%20Dive

Google Drive, OneDrive top cloud apps for malware delivery: report
Netskope's findings are based on blocked malware, so the hacker's attempts to get a user to open a malicious download were initially successful.
https://www.cybersecuritydive.com/news/netskope-cloud-malware-delivery/617061/?utm_source=Sailthru&utm_medium=email&utm_campaign=Issue:%202022-01-12%20Cybersecurity%20Dive%20%5Bissue:39098%5D&utm_term=Cybersecurity%20Dive

Cloud Apps Replace Web as Source for Most Malware Downloads
Two-thirds of all malware distributed to enterprise networks last year originated from cloud apps such as Google Drive, OneDrive, and numerous other cloud apps, new research shows.
https://www.darkreading.com/cloud/cloud-apps-replace-web-as-source-for-most-malware-downloads?_mc=NL_DR_EDT_DR_daily_20220112&cid=NL_DR_EDT_DR_daily_20220112&elq_mid=108481&elq_cid=36315893

New Cyberattack Campaign Uses Public Cloud Infrastructure to Spread RATs
An attack campaign detected in October delivers variants of Nanocore, Netwire, and AsyncRATs to target user data.
https://www.darkreading.com/cloud/new-campaign-uses-public-cloud-infrastructure-to-spread-rats?_mc=NL_DR_EDT_DR_daily_20220113&cid=NL_DR_EDT_DR_daily_20220113&elq_mid=108497&elq_cid=36315893

5 Painful Scams: Obituary Pirates, LGBTQ+ Extortion & More
We're only a couple of weeks into 2022 and scammers are already busy. In this week's Snippets issue, we highlight some of the scams that are active right now.
https://scambusters.org/obituarypirate.html

****

Hints & Tips plus Security Awareness

Fire at vital tech factory could worsen global computer chip shortage
A fire at a plant in Berlin, Germany owned by ASML Holding could worsen the global computer chip shortage as the plant is the sole provider of a vital technology used to manufacture computer chips.
https://www.newscientist.com/article/2303316-fire-at-vital-tech-factory-could-worsen-global-computer-chip-shortage/

****

News & Views

5 banking trends to watch in 2022
A reversal on in-office work from Goldman Sachs may represent a pivot point in the acceptance of remote policies. But other narratives, such as small-scale niche M&A, mark a continuation from 2021.
https://www.bankingdive.com/news/5-banking-trends-2022-crypto-cannabis-office-return-merger-acquisition-regulatory-pitfall-innovation/611181/?utm_source=Sailthru&utm_medium=email&utm_campaign=Newsletter%20Weekly%20Roundup:%20Banking%20Dive:%20Daily%20Dive%2001-08-2022&utm_term=Banking%20Dive%20Weekender

5 trends shaping enterprise SaaS use in 2022
How companies buy software is changing as more line-of-business managers adopt tools outside of the CIO's purview and businesses rethink their must-haves.
https://www.ciodive.com/news/5-saas-trends-2022/616780/?utm_source=Sailthru&utm_medium=email&utm_campaign=Issue:%202022-01-07%20CIO%20Dive%20%5Bissue:38993%5D&utm_term=CIO%20Dive

What happens if threat data isn't shared?
Companies with mature cybersecurity organizations have vested interest in understanding their adversaries and cyberthreats. There's always the chance another organization uncovered a threat pertinent to someone else. What happens if the data isn't shared?
https://www.cybersecuritydive.com/news/information-sharing-threat-intelligence-analysis-cybersecurity/599319/?utm_source=Sailthru&utm_medium=email&utm_campaign=Issue:%202022-01-11%20Cybersecurity%20Dive%20%5Bissue:39056%5D&utm_term=Cybersecurity%20Dive

****

"Ctrl -F" for The Board

How to hire and recruit a CISO
High turnover means organizations are always on the lookout for new cybersecurity leadership, but what exactly are companies looking for in a CISO? The cybersecurity talent shortage is well-analyzed but less discussed is the search for CISOs with the right expertise and skills to lead a company's cybersecurity programs and team.
https://www.cybersecuritydive.com/news/CISO-hire-recruit/616600/?utm_source=Sailthru&utm_medium=email&utm_campaign=Newsletter%20Weekly%20Roundup:%20Cybersecurity%20Dive:%20Daily%20Dive%2001-08-2022&utm_term=Cybersecurity%20Dive%20Weekender

5 analyst predictions for how the CIO role will change in 2022
Companies will scrutinize CIOs' ability to deliver financial results, flexibility, and an effective hybrid work strategy. The tech leaders who spent 2021 focused on business acceleration will now be tasked with guiding business transformation.
https://www.ciodive.com/news/5-tech-predictions-2022/616485/?utm_source=Sailthru&utm_medium=email&utm_campaign=Newsletter%20Weekly%20Roundup:%20CIO%20Dive:%20Daily%20Dive%2001-08-2022&utm_term=CIO%20Dive%20Weekender

Questions
Contact FIPCO’s Rob Foxx at 800-722-3498 ext. 249 or email FIPCO IT Services for more information.

"Make Security Part of You and Your Institution's DNA!"

Threat Intelligence Newsletter: January 26, 2022

FIPCO®
IT Audit
Round Table
Discussions

If you would like to host an event, please contact: Donna Stanger

Upcoming Threat Intelligence Peer Group Discussions
None available at the current time

****

Alerts & Warnings

Social Media Platforms Remain a Force Multiplier for Information-Based Threats
A recent report published by The Washington Post revealed how China is aggressively using advanced software to surveil popular social media sites such as Twitter and Facebook, among others, in order to monitor the activities of and collect information against Western government officials and journalists.
https://www.oodaloop.com/archive/2022/01/12/social-media-platforms-remain-a-force-multiplier-for-information-based-threats/

Fashion giant Moncler confirms data breach after ransomware attack
Italian luxury fashion giant Moncler confirmed that they suffered a data breach after files were stolen by the AlphV/BlackCat ransomware operation in December and published today on the dark web.
https://www.bleepingcomputer.com/news/security/fashion-giant-moncler-confirms-data-breach-after-ransomware-attack/?_hsmi=78978938&_hsenc=p2ANqtz-_E9vqpEuTQ6JSMUniDeF-jnaGPm8yhw6WOlF1zJjYgBiW0GrYQs-V_PBttsaeSTb0oT-UKZDM7ypR7G85JpjXm0lGh3A

‘Zero-Click’ Zoom Vulnerabilities Could Have Exposed Calls
Most hacks require the victim to click on the wrong link or open the wrong attachment. But as so-called zero-click vulnerabilities—in which the target does nothing at all—are exploited more and more, Natalie Silvanovich of Google's Project Zero bug-hunting team has worked to find new examples and get them fixed before attackers can use them. Her list now includes Zoom, which until recently had two alarming, interactionless flaws lurking inside.
https://news.hitb.org/content/zero-click-zoom-vulnerabilities-could-have-exposed-calls?_hsmi=78978938&_hsenc=p2ANqtz-_f0K9L4V9Ew_TwtYGVItu-Jobs0uhRTdDH1P2_Z2vSeDgXsUOkl7no_GLflJ4g27JSdG0FQhwHiYmvtDkzlcyOI2VfZA

The Chaos Ransomware Can Be Ravaging
A ransomware builder called Chaos is still actively under development. The fourth version has recently been observed being improved, as identified in underground forums as well as code leaks in other community sites.
https://blog.qualys.com/vulnerabilities-threat-research/2022/01/17/the-chaos-ransomware-can-be-ravaging?_hsmi=78978938&_hsenc=p2ANqtz-_FTbLjsYXAmzdPr-H2OudTUfNM8L3923kLg8ln3rQGlllOl4ogozDm5A2ttCWHihsuTQNOptSZUCvwQOFrMBKVTp6Ksg

Researchers Bypass SMS-based Multi-Factor Authentication Protecting Box Accounts
Cybersecurity researchers have disclosed details of a now-patched bug in Box's multi-factor authentication (MFA) mechanism that could be abused to completely sidestep SMS-based login verification.
https://thehackernews.com/2022/01/researchers-bypass-sms-based-multi.html?_m=3n%2e009a%2e2656%2eod0ao445rz%2e1ow8

****

Hints & Tips plus Security Awareness

How Can I Get A Scam Refund After Being Conned?
If you've been defrauded via a con trick or unauthorized use of your money and credit accounts, you may be able to get a scam refund. But it's not easy, especially since every organization has different rules.The most important thing is to report the crime immediately. Then, follow some of the actions suggested in this week's issue. Not every scam victim is a loser. Some get all or part of their money back. But that can depend on knowing how and where to get a scam refund.
https://scambusters.org/scamrefund.html

Feds want businesses to report cyberattacks — the agency doesn't matter
The FBI's Bryan Vorndran compared a cyberattack to a house robbery: Law enforcement assists with attack response while CISA is representative of an alarm company tasked with prevention.
https://www.cybersecuritydive.com/news/fbi-cisa-incident-response/617193/?utm_source=Sailthru&utm_medium=email&utm_campaign=Issue:%202022-01-18%20Cybersecurity%20Dive%20%5Bissue:39186%5D&utm_term=Cybersecurity%20Dive

Microsoft: This new browser feature is 'huge step forward' against zero-day threats
The latest Edge beta introduces a new browsing mode in Edge "where the security of your browser takes priority". For admins who fear web-based attacks on desktop systems via the browser, this feature gives them the option to "mitigate unforeseen active zero days". Enabling this mode can be configured, so that important sites and line-of-business applications "continue to work as expected,"
https://www.zdnet.com/article/microsoft-says-its-new-browser-feature-is-huge-step-forward-against-zero-day-threats/?_hsmi=78978938&_hsenc=p2ANqtz-9lgsG9EZmJLm04GJf9i6jizE15mZVEFTEaB3org4qWZT93ErXMuGDCHdKevzFpb0wXqczhCq-TxETDjhQF7gYRY_wFMg#ftag=RSSbaffb68

High-Severity Vulnerability in 3 WordPress Plugins Affected 84,000 Websites
Researchers have disclosed a security shortcoming affecting three different WordPress plugins that impact over 84,000 websites and could be abused by a malicious actor to take over vulnerable sites.
https://thehackernews.com/2022/01/high-severity-vulnerability-in-3.html?_hsmi=78978938&_hsenc=p2ANqtz-__8n4w-zEuACKypoo2M_CrBe3Vm4hmXhEmd2jzh2_JA9MiVD93ayHWKURuLcsIWvDurbKVASkxx-mV_8ruyIiE8lv9kQ

Backdoor RAT for Windows, macOS, and Linux went undetected until now
Researchers have uncovered a never-before-seen backdoor malware written from scratch for systems running Windows, macOS, or Linux that remained undetected by virtually all malware scanning engines.
https://arstechnica.com/information-technology/2022/01/backdoor-for-windows-macos-and-linux-went-undetected-until-now/?_hsmi=78978938&_hsenc=p2ANqtz-8MFIobpjeF8sNR0GQ2h7dmFQmhvX5PZX8rTYiCVggGog5-HMHxX-lVEFACd07MVi1oWzhLwfXP8-6h5xlKLNHlmH4Btw

****

News & Views

ATMs may have peaked in 2019, research finds
A Euromonitor International executive predicts the once-revolutionary dispensers may be gone within 25 years — a consequence of reduced demand and higher costs for servicing the machines.
https://www.bankingdive.com/news/atms-may-have-peaked-in-2019-research-finds/616872/?utm_source=Sailthru&utm_medium=email&utm_campaign=Newsletter%20Weekly%20Roundup:%20Banking%20Dive:%20Daily%20Dive%2001-15-2022&utm_term=Banking%20Dive%20Weekender

4 ways the CIO can help stem the Great Resignation
CIOs can take an active role in creating a positive environment that breeds loyalty, both within their organization and across the company.
https://www.ciodive.com/news/tech-executive-great-resignation-sharon-mandell/616937/?utm_source=Sailthru&utm_medium=email&utm_campaign=Newsletter%20Weekly%20Roundup:%20CIO%20Dive:%20Daily%20Dive%2001-15-2022&utm_term=CIO%20Dive%20Weekender

Russia Takes Down REvil Ransomware Operation, Arrests Key Members
Timing of the move has evoked at least some skepticism from security experts about the country's true motives.
https://www.darkreading.com/threat-intelligence/russia-takes-down-revil-ransomware-operation-arrests-key-members?_mc=NL_DR_EDT_DR_daily_20220118&cid=NL_DR_EDT_DR_daily_20220118&elq_mid=108586&elq_cid=36315893

Safari 15 vulnerability leaks users' identity and website history
Discovered and detailed Jan. 14 by researchers at FingerprintJs Inc., the vulnerability relates to Safari 15's implementation of the IndexedDB application programming interface. IndexedDB is a browser API for client-side storage designed to hold significant amounts of data and is found in many browsers.
https://siliconangle.com/2022/01/17/safari-15-vulnerability-leaks-users-identity-website-history/?_hsmi=78978938&_hsenc=p2ANqtz--f7nWbAXAyKsBKpeUtI76TGFXeMvhQoCXtKqTfdfKmG78ELa6tXwrri4f9kxS55bv8CkAgJ63z-DhdzG6EBEWebk8Fqg

IRS Will Soon Require Selfies for Online Access
If you created an online account to manage your tax records with the U.S.
Internal Revenue Service (IRS), those login credentials will cease to work later this year. The agency says that by the summer of 2022, the only way to log in to irs.gov will be through ID.me, an online identity verification service that requires applicants to submit copies of bills and identity documents, as well as a live video feed of their faces via a mobile device.
https://krebsonsecurity.com/2022/01/irs-will-soon-require-selfies-for-online-access/

****

"Ctrl -F" for The Board

The Great Resignation: Existential Crisis or Once in a Generation Opportunity?
Workers are reconsidering where, how and why they work. Should SMBs fight the changing tide or embrace it? Hear a discussion on how to make the most of the new approach to working. Webinar January 27th 2022, 12:00PM CST
https://www.brighttalk.com/webcast/19036/525683?player-preauth=vY02%2B0sVWfztgJfvB%2BbroN2NGvdwwzV2y1kKUhHDVVA%3D&utm_source=brighttalk-promoted&utm_medium=email&utm_term=Audience299284&utm_campaign=AUD-11754&utm_content=2022-01-14

Biden Memo Orders Cybersecurity Improvements
The memo requires that national security systems "employ the same network cybersecurity measures as those required of federal civilian networks," per Biden's May 2021 executive order. It also gives new powers to the National Security Agency to oversee cybersecurity improvements, and the agency will also now collect reports on incidents affecting national security systems.
https://www.databreachtoday.com/biden-memo-orders-cybersecurity-improvements-a-18346?rf=2022-01-20_ENEWS_ACQ_DBT__Slot1_ART18346&mkt_tok=MDUxLVpYSS0yMzcAAAGCF2JqPh1SlFCRWyKHzywFUQbuLwBWNb_3ZXQq2f7h48nE8iBWomBEmeo4pNDdOWgz0_bKEgIWh3-0-1GlKDZMYZsefAW50fnMd72fsVCswJdgyFdlqA

Questions
Contact FIPCO's Rob Foxx at 800-722-3498 ext. 249 or email FIPCO IT Services for more information.

"Make Security Part of You and Your Institution's DNA!"

Threat Intelligence Newsletter: January 31, 2022

FIPCO®
IT Audit
Round Table
Discussions

If you would like to host an event, please contact: Donna Stanger

Upcoming Threat Intelligence Peer Group Discussions
None available at the current time

****

Alerts & Warnings

Malicious app on Google Play drops banking malware on users' devices
Pradeo's researchers discovered a malicious mobile application called 2FA Authenticator distributed on Google Play and installed by 10K+ users.
https://blog.pradeo.com/vultur-malware-dropper-google-play?utm_campaign=Newsletter&utm_medium=email&_hsmi=202235015&_hsenc=p2ANqtz--PfTV9ijBbkZPEJhS7Q7VfiEnvTD321l2nAXFX6jSgTZHD0bKm65AOL2HHlrNa-YNMxC924p9k9qksTZECExZZVQJ0xg&utm_content=202235015&utm_source=hs_email

Microsoft warns about this phishing attack that wants to read your emails
The potentially malicious app, dubbed 'Upgrade', asks users to grant it OAuth permissions that would allow attackers to create inbox rules, read and write emails and calendar items, and read contacts, according to Microsoft Security Intelligence.
https://www.zdnet.com/article/microsoft-warns-about-this-phishing-attack-that-wants-to-read-your-emails/

Log4j raises cyber risk for public finance entities, Fitch warns
Local agencies and critical sites face increased operational and financial risk as the vulnerability opens organizations to ransomware or other malicious activity. https://www.cybersecuritydive.com/news/fitch-ratings-log4j-finance/617353/?utm_source=Sailthru&utm_medium=email&utm_campaign=Issue:%202022-01-20%20Cybersecurity%20Dive%20%5Bissue:39247%5D&utm_term=Cybersecurity%20Dive

DHS warns local authorities, critical infrastructure providers over potential Russia threat
As tensions rise over a possible incursion into the Ukraine, federal authorities say Russia may launch direct cyberattacks against targets in the U.S.
https://www.cybersecuritydive.com/news/dhs-critical-infrastructure-government-warnings/617670/?utm_source=Sailthru&utm_medium=email&utm_campaign=Issue:%202022-01-25%20Cybersecurity%20Dive%20%5Bissue:39338%5D&utm_term=Cybersecurity%20Dive

Fraud Is On the Rise, and It's Going to Get Worse
The acceleration of the digital transformation resulted in a surge of online transactions, greater adoption of digital payments, and increased fraud.
https://www.darkreading.com/edge-articles/fraud-is-on-the-rise-and-its-going-to-get-worse?_mc=NL_DR_EDT_DR_daily_20220122&cid=NL_DR_EDT_DR_daily_20220122&elq_mid=108675&elq_cid=36315893

Millions of Routers, IoT Devices at Risk as Malware Source Code Surfaces on GitHub
"BotenaGo" contains exploits for more than 30 vulnerabilities in multiple vendor products and is being used to spread Mirai botnet malware, security vendor says.
https://www.darkreading.com/vulnerabilities-threats/source-code-for-malware-targeting-millions-of-routers-iot-devices-uploaded-to-github?_mc=NL_DR_EDT_DR_daily_20220127&cid=NL_DR_EDT_DR_daily_20220127&elq_mid=108752&elq_cid=36315893

McAfee Bug Can Be Exploited to Gain Windows SYSTEM Privileges
McAfee has recently patched two different high-severity bugs in its Agent component that could be used by attackers to escalate privileges, including up to SYSTEM. The bugs could also allow attackers to achieve arbitrary code execution and perform other malicious actions.
https://threatpost.com/mcafee-bug-windows-system-privileges/177857/

****

Hints & Tips plus Security Awareness

The Science of Cybersecurity: Best Practices in the New Normal
As organizations adapted quickly to large-scale WFH policies, CISOs and cybersecurity leaders must work in parallel to address new and heightened cyber risks to meet evolving business demands. As you navigate this new workforce dynamic, how you help to protect employees, critical data, and intellectual property requires a new way of thinking. Webinar February 8th @ 2:00PM
https://www.brighttalk.com/webcast/8887/526462?player-preauth=YhcVxdw%2FC%2BAShailFBcockOpP9SmDs66a%2Fw%2B3bamHPE%3D&utm_source=brighttalk-promoted&utm_medium=email&utm_term=Audience301989&utm_campaign=AUD-11831&utm_content=2022-01-23

3 CIO strategies to improve vendor management
CIOs must leverage new technologies to improve vendor relationships, free up bandwidth and proactively manage vendors and contracts.
https://www.ciodive.com/news/vendor-management-technology-CIO/617458/?utm_source=Sailthru&utm_medium=email&utm_campaign=Issue:%202022-01-21%20CIO%20Dive%20%5Bissue:39243%5D&utm_term=CIO%20Dive

Semiconductors expected to be in tight supply throughout 2022
Suppliers are working to ramp up production, but many planned capacity projects are not expected to be operational until 2023 at the earliest.
https://www.ciodive.com/news/semiconductor-tight-supply-shortage-2022/617563/?utm_source=Sailthru&utm_medium=email&utm_campaign=Issue:%202022-01-25%20CIO%20Dive%20%5Bissue:39307%5D&utm_term=CIO%20Dive

Are You Prepared to Defend Against a USB Attack?
Recent "BadUSB" attacks serve as a reminder of the big damage that small devices can cause.
https://www.darkreading.com/vulnerabilities-threats/are-you-prepared-to-defend-against-a-USB-attack-?_mc=NL_DR_EDT_DR_daily_20220125&cid=NL_DR_EDT_DR_daily_20220125&elq_mid=108702&elq_cid=36315893

****

News & Views

Biden gives defense, intel agencies 180 days to apply MFA, encryption
The White House's memorandum builds on past requirements to bolster U.S. cyber standards. This time, the administration is targeting agencies that handle classified intelligence.
https://www.cybersecuritydive.com/news/biden-memo-cyber-defense-intel-mfa-encryption/617425/?utm_source=Sailthru&utm_medium=email&utm_campaign=Issue:%202022-01-20%20Cybersecurity%20Dive%20%5Bissue:39247%5D&utm_term=Cybersecurity%20Dive

It's time to focus on critical infrastructure systems security
Cyber-physical systems rely on legacy infrastructure and new, vulnerability-filled assets. The recipe has created an ideal attack surface for malicious actors.
https://www.cybersecuritydive.com/news/critical-infrastructure-security/617561/?utm_source=Sailthru&utm_medium=email&utm_campaign=Issue:%202022-01-24%20Cybersecurity%20Dive%20%5Bissue:39306%5D&utm_term=Cybersecurity%20Dive

U.S. banks close 2,927 branches in 2021, a 38% jump
Wells Fargo, with 267, reported more net closures than any other bank in the U.S., followed by U.S. Bank at 257. However, Huntington Bank reported the greatest proportion of shrinkage at 16%, S&P Global reported.
https://www.bankingdive.com/news/us-banks-close-2927-branches-in-2021-a-38-jump/617594/?utm_source=Sailthru&utm_medium=email&utm_campaign=Issue:%202022-01-24%20Banking%20Dive%20%5Bissue:39295%5D&utm_term=Banking%20Dive

End Users Remain Organizations' Biggest Security Risk
Yet they're showing signs of improvement across several important areas, a Dark Reading survey reveals.
https://www.darkreading.com/edge-threat-monitor/despite-rise-of-third-party-concerns-end-users-still-the-biggest-security-risk?_mc=NL_DR_EDT_DR_daily_20220122&cid=NL_DR_EDT_DR_daily_20220122&elq_mid=108675&elq_cid=36315893

****

"Ctrl -F" for The Board

U.S. Bank, Truist scale down overdraft fees
U.S. Bank is increasing from $5 to $50 the amount by which accounts can go negative before triggering an overdraft fee and is instituting a 24-hour grace period. Truist, meanwhile, is unveiling two overdraft-free accounts this summer.
https://www.bankingdive.com/news/us-bank-truist-scale-down-overdraft-fees/617442/?utm_source=Sailthru&utm_medium=email&utm_campaign=Issue:%202022-01-20%20Banking%20Dive%20%5Bissue:39237%5D&utm_term=Banking%20Dive

Long-term projects to drive IT spending growth in 2022
With talent scarce, companies need more outsourcing and managed services to execute multiyear projects, Gartner says.
https://www.ciodive.com/news/IT-spending-2022-services-Gartner/617388/?utm_source=Sailthru&utm_medium=email&utm_campaign=Issue:%202022-01-21%20CIO%20Dive%20%5Bissue:39243%5D&utm_term=CIO%20Dive

How CIOs can shape customer experience
A sweeping shift to digital operations means CIOs now touch more critical components of a business and their influence can ripple all the way down to CX.
https://www.ciodive.com/news/CIO-customer-experience-enterprise/617673/?utm_source=Sailthru&utm_medium=email&utm_campaign=Issue:%202022-01-26%20CIO%20Dive%20%5Bissue:39333%5D&utm_term=CIO%20Dive

4 Ways to Develop Your Team's Cyber Skills
Organizations need to invest in professional development — and then actually make time for it.
https://www.darkreading.com/careers-and-people/4-ways-to-develop-your-team-s-cyber-skills?_mc=NL_DR_EDT_DR_daily_20220121&cid=NL_DR_EDT_DR_daily_20220121&elq_mid=108658&elq_cid=36315893

Questions
Contact FIPCO’s Rob Foxx at 800-722-3498 ext. 249 or email FIPCO IT Services for more information.

"Make Security Part of You and Your Institution's DNA!"

Threat Intelligence Newsletter: February 04, 2022

If you would like to host an event, please contact: Donna Stanger

Upcoming Threat Intelligence Peer Group Discussions
None available at the current time

****

Alerts & Warnings

Cyberthreat trends to watch in 2022
Cybercriminals are finding ways to manipulate corporate data, and for that problem, there really is no end in sight. https://www.ciodive.com/news/cyber-threat-trends-2022/618131/?utm_source=Sailthru&utm_medium=email&utm_campaign=Issue:%202022-02-02%20CIO%20Dive%20%5Bissue:39495%5D&utm_term=CIO%20Dive

In 2022, you can no longer afford to ignore credential security
Credentials are among the most sought-after targets by hackers due to the low risk and high rewards. If today's cybersecurity landscape was the Wild West, credentials would be more valuable than every bank, train and stagecoach combined. https://www.cybersecuritydive.com/spons/in-2022-you-can-no-longer-afford-to-ignore-credential-security/617421/

More Security Flaws Found in Apple's OS Technologies
Apple's latest updates included fixes for two zero-day flaws, several code execution bugs, and vulnerabilities that allowed attackers to bypass its core security protections.
https://www.darkreading.com/vulnerabilities-threats/more-security-flaws-found-in-apple-s-OS-technologies?_mc=NL_DR_EDT_DR_daily_20220131&cid=NL_DR_EDT_DR_daily_20220131&elq_mid=108799&elq_cid=36315893

Millions of Routers, IoT Devices at Risk as Malware Source Code Surfaces on GitHub
"BotenaGo" contains exploits for more than 30 vulnerabilities in multiple vendor products and is being used to spread Mirai botnet malware, security vendor says. https://www.darkreading.com/vulnerabilities-threats/source-code-for-malware-targeting-millions-of-routers-iot-devices-uploaded-to-github?_mc=NL_DR_EDT_DR_daily_20220131&cid=NL_DR_EDT_DR_daily_20220131&elq_mid=108799&elq_cid=36315893

How Phishers Are Slinking Their Links Into LinkedIn
If you received a link to LinkedIn.com via email, SMS or instant message, would you click it? Spammers, phishers and other ne'er-do-wells are hoping you will, because they've long taken advantage of a marketing feature on the business networking site which lets them create a LinkedIn.com link that bounces your browser to other websites, such as phishing pages that mimic top online brands (but chiefly Linkedin's parent firm Microsoft). https://krebsonsecurity.com/2022/02/how-phishers-are-slinking-their-links-into-linkedin/

Unsecured AWS server exposed 3TB in airport employee records
The SafetyDirectives cybersecurity team reported on Monday that a server belonging to Securitas was left unsecured, resulting in the exposure of 3TB in airport employee records. Securitas is based in Stockholm, Sweden and provides on-site guarding, electronic security solutions, fire and safety services, and risk management services. https://www.zdnet.com/article/unsecured-aws-server-exposed-airport-employee-records-3tb-in-data/

****

Hints & Tips plus Security Awareness

Debunking Ransomware's Biggest Myths
Ransomware is today's biggest cybersecurity threat for businesses of all sizes. This session will separate ransomware fact from fiction. Ransomware is today's biggest cybersecurity threat for CISOs. Hackers from around the globe are cashing in on this lucrative "business" and it is showing no sign of slowing down. With click-bait swirling around the internet, it is challenging to separate fact from fiction.
https://www.brighttalk.com/webcast/19203/528560?player-preauth=YhcVxdw%2FC%2BAShailFBcockOpP9SmDs66a%2Fw%2B3bamHPE%3D&utm_source=brighttalk-promoted&utm_medium=email&utm_term=Audience306906&utm_campaign=AUD-11966&utm_content=2022-02-1

Cybersecurity tool trends to watch in 2022
For enterprises, the security priority remains doing more with less and finding tools that offer greater areas of coverage and integration. https://www.cybersecuritydive.com/news/cybersecurity-tool-trends-2022/617845/?utm_source=Sailthru&utm_medium=email&utm_campaign=Issue:%202022-01-27%20Cybersecurity%20Dive%20%5Bissue:39401%5D&utm_term=Cybersecurity%20Dive

7 Privacy Tips for Security Pros
According to a recent survey from Cisco, some 90% of security pros now consider privacy a mission-critical business imperative. In fact, 90% of responding security pros say their customers would not buy from them if they did not adequately protect their data. Detecting and responding to threats and assessing and managing risk has become a core area of responsibility for security pros.
https://www.darkreading.com/risk/7-privacy-tips-for-security-pros-?_mc=NL_DR_EDT_DR_daily_20220203&cid=NL_DR_EDT_DR_daily_20220203&elq_mid=108865&elq_cid=36315893

****

News & Views

Survey: Cyber Fraud Tops List of Bank Concerns about Global Economy
A new survey from TD Bank and Strategic Treasurer found that 81% of bank respondents see cyber fraud as the top concern with respect to the global economy. The survey of more than 250 banks and corporate finance departments found that 57% of all corporate respondents—and 81% of banks—ranked cyber fraud as the top concern. https://bankingjournal.aba.com/2022/01/survey-cyber-fraud-tops-list-of-bank-concerns-about-global-economy/?utm_source=eloqua&utm_medium=email&utm_campaign=newsbytes&utm_content=NEWSBYTES-20220131

Why Security Pros Are Frustrated With Cloud Security
Companies are struggling to keep up with cloud security, with 55% of security professionals believing at least half their time is wasted, in part because security event data is of uneven quality, which leads to false positives, according to a new report. https://www.darkreading.com/cloud/why-security-pros-are-frustrated-with-cloud-security?_mc=NL_DR_EDT_DR_daily_20220203&cid=NL_DR_EDT_DR_daily_20220203&elq_mid=108865&elq_cid=36315893

****

"Ctrl -F" for The Board

CIO involvement in security grows as CEOs target risk reduction
Half of CIOs are prioritizing security management this year, as CEOs push for IT and data security upgrades to reduce corporate risk, which included responses from almost 1,000 heads of IT and 250 line of business participants. https://www.ciodive.com/news/cio-cyber-security-2022-expectations/617900/?utm_source=Sailthru&utm_medium=email&utm_campaign=Issue:%202022-01-28%20CIO%20Dive%20%5Bissue:39399%5D&utm_term=CIO%20Dive

GDPR regulators crack down on data processing as companies struggle with privacy compliance
Almost four years into GDPR, it took regulators time to find their footing to pursue violations.
https://www.cybersecuritydive.com/news/gdpr-data-privacy-chief-privacy-security-officer/617936/?utm_source=Sailthru&utm_medium=email&utm_campaign=Issue:%202022-01-31%20Cybersecurity%20Dive%20%5Bissue:39460%5D&utm_term=Cybersecurity%20Dive

The Looming CISO Mental Health Crisis — and What to Do About It, Part 1
The security team is hardly the only group under pressure. Other corporate functions, and other executives, must meet elevated and sometimes unrealistic expectations. But what makes the CISO position unique is its relative newness; most jobs in a modern organization have been around for decades, so they're fairly well-defined. https://www.darkreading.com/edge-articles/the-looming-ciso-mental-health-crisis-and-what-to-do-about-it-part-1?_mc=NL_DR_EDT_DR_daily_20220129&cid=NL_DR_EDT_DR_daily_20220129&elq_mid=108794&elq_cid=36315893

Questions
Contact FIPCO’s Rob Foxx at 800-722-3498 ext. 249 or email FIPCO IT Services for more information.

"Make Security Part of You and Your Institution's DNA!"

Threat Intelligence Newsletter: February 14, 2022

FIPCO®
IT Audit
Round Table
Discussions

If you would like to host an event, please contact: Donna Stanger

Upcoming Threat Intelligence Peer Group Discussions
None available at the current time

****

Alerts & Warnings

FBI Releases Warning on Potential Cyber Attacks During Winter Olympics
The Federal Bureau of Investigation last week released a Private Industry Notification to warn entities associated with the February 2022 Beijing Winter Olympics and March 2022 Paralympics that malicious cyber actors could use a broad range of cyber activities to disrupt these events.
https://www.ic3.gov/Media/News/2022/220131.pdf?utm_source=eloqua&utm_medium=email&utm_campaign=riskcyberbulletin&utm_content=RiskCyber-20220207

Conflict over Ukraine raises cyber risk for US enterprises
A diplomatic standoff with Russia threatens to drag U.S. companies and critical infrastructure into wider security crisis that could echo NotPetya. https://www.cybersecuritydive.com/news/ukraine-russia-cyber-threat/618084/?utm_source=Sailthru&utm_medium=email&utm_campaign=Newsletter%20Weekly%20Roundup:%20Cybersecurity%20Dive:%20Daily%20Dive%2002-05-2022&utm_term=Cybersecurity%20Dive%20Weekender

Linux Malware on the Rise
Ransomware, cryptojacking, and a cracked version of the penetration-testing tool Cobalt Strike have increasingly targeted Linux in multicloud infrastructure, report states.
https://www.darkreading.com/cloud/linux-malware-on-the-rise-including-illicit-use-of-cobalt-strike?_mc=NL_DR_EDT_DR_daily_20220210&cid=NL_DR_EDT_DR_daily_20220210&elq_mid=108975&elq_cid=36315893

This malware is reading your email just 30 minutes after infecting your PC
An old malware called Qbot is still targeting Windows PCs and other devices with new nefarious efficiency. Although the malware first emerged in 2007, it remains a threat to Windows users.
https://www.zdnet.com/article/this-malware-is-reading-your-email-30-minutes-after-the-first-infection/

****

Hints & Tips plus Security Awareness

What You Need to Know About CPRA in 2022: Your Questions Answered
Although the California Privacy Rights Act of 2020 (CPRA) will not go into full effect until January 1, 2023, businesses are expected to start complying with the law's obligations for gathering and maintaining consumer personal information as early as 1, 2022.
https://www.brighttalk.com/webcast/17963/516183?player-preauth=YhcVxdw%2FC%2BAShailFBcockOpP9SmDs66a%2Fw%2B3bamHPE%3D&utm_source=brighttalk-promoted&utm_medium=email&utm_term=Audience309878&utm_campaign=AUD-08634&utm_content=2022-02-6

Ransomware: Is Your Sensitive Data Protected, or Will You Have to Pay Up?
Are ransomware attacks out of control, or are security teams unprepared? The last two years have certainly seen an uptick in ransomware attacks. However, most organizations forced to pay their cyber bullies are victims of lax security practices. https://www.brighttalk.com/webcast/17963/516629?player-preauth=YhcVxdw%2FC%2BAShailFBcockOpP9SmDs66a%2Fw%2B3bamHPE%3D&utm_source=brighttalk-promoted&utm_medium=email&utm_term=Audience309349&utm_campaign=AUD-08634&utm_content=2022-02-5

Talk to the board, not just IT, about ransomware
The spread of fast-moving cyberattacks accelerates the need for rapid, clear communication between end-users, security teams and the board. https://www.cybersecuritydive.com/news/board-ransomware-discussions/618291/?utm_source=Sailthru&utm_medium=email&utm_campaign=Issue:%202022-02-04%20Cybersecurity%20Dive%20%5Bissue:39580%5D&utm_term=Cybersecurity%20Dive

3 tactics shaping ransomware mitigation in 2022
Though businesses have become more confident in preventing ransomware attacks, confronting risk is an internal commitment. https://www.cybersecuritydive.com/news/ransomware-prevention/617966/?utm_source=Sailthru&utm_medium=email&utm_campaign=Issue:%202022-02-04%20Cybersecurity%20Dive%20%5Bissue:39580%5D&utm_term=Cybersecurity%20Dive

7 Privacy Tips for Security Pros
How best to integrate privacy into your organization's security program.
https://www.darkreading.com/risk/7-privacy-tips-for-security-pros-?_mc=NL_DR_EDT_DR_daily_20220204&cid=NL_DR_EDT_DR_daily_20220204&elq_mid=108888&elq_cid=36315893

CISA Tells Organizations to Patch CVEs Dating Back to 2014
The US government has added eight more vulnerabilities to a list of CVEs that federal agencies are required to patch, called the Known Exploited Vulnerabilities Catalog. The list was first launched by the Cybersecurity and Infrastructure Security Agency in November 2021. https://www.infosecurity-magazine.com/news/cisa-patch-cves-dating-back-to-**2014/**

****

News & Views

Apache tells US Senate committee the Log4j vulnerability could take years to resolve

While a software bill of materials could improve supply chain security, users still download vulnerable versions of software. https://www.cybersecuritydive.com/news/apache-senate-log4j-years/618567/?utm_source=Sailthru&utm_medium=email&utm_campaign=Issue:%202022-02-09%20Cybersecurity%20Dive%20%5Bissue:39672%5D&utm_term=Cybersecurity%20Dive

Hackers Went Wild in 2021 — Every Company Should Do These 5 Things in 2022

Practical steps companies can take to defend their critical infrastructure and avoid the financial and reputational damage that could result from a breach. https://www.darkreading.com/attacks-breaches/hackers-went-wild-in-2021-every-company-should-do-these-5-things-in-2022?_mc=NL_DR_EDT_DR_daily_20220204&cid=NL_DR_EDT_DR_daily_20220204&elq_mid=108888&elq_cid=36315893

Phishing Simulation Study Shows Why These Attacks Remain Pervasive

Email purportedly from human resources convinced more than one-fifth of recipients to click, the majority of whom did so within an hour of receiving the fraudulent message. https://www.darkreading.com/threat-intelligence/simulation-shows-why-phishing-attacks-continue-to-dominate?_mc=NL_DR_EDT_DR_daily_20220204&cid=NL_DR_EDT_DR_daily_20220204&elq_mid=108888&elq_cid=36315893

****

"Ctrl -F" for The Board

OCC Announces Virtual Workshops for Community Bank Directors

The OCC announced the February through May schedule for the agency's series of virtual workshops for boards of directors of community national banks and federal savings associations. The examiner-led workshops cover risk governance, credit risk, operational risk and directorship success. https://occ.gov/news-issuances/news-releases/2022/nr-occ-2022-11.html?utm_source=eloqua&utm_medium=email&utm_campaign=newsbytes&utm_content=NEWSBYTES-20220208

5 tech workforce trends for 2022

Shifting job descriptions, hybrid work strategies and worker mobility will shape tech labor dynamics this year. https://www.ciodive.com/news/tech-workforce-trends-2022-labor/617171/?utm_source=Sailthru&utm_medium=email&utm_campaign=Issue:%202022-02-04%20CIO%20Dive%20%5Bissue:39574%5D&utm_term=CIO%20Dive

Questions
Contact FIPCO's Rob Foxx at 800-722-3498 ext. 249 or email FIPCO IT Services for more information.

"Make Security Part of You and Your Institution's DNA!"

Threat Intelligence Newsletter: February 23, 2022

FIPCO®
IT Audit
Round Table
Discussions

If you would like to host an event, please contact: Becky Schowalter

Upcoming Threat Intelligence Peer Group Discussions
None available at the current time

****

Alerts & Warnings

FBI warns criminals are using fake QR codes to scam users
Cybercriminals could use altered Quick Response (QR) codes to steal personal and financial information of unsuspecting customers, the FBI warns.
https://abcnews.go.com/Politics/fbi-warns-criminals-fake-qr-codes-scam-users/story?id=82371866

VMware Issues Security Patches for High-Severity Flaws Affecting Multiple Products
VMware on Tuesday patched several high-severity vulnerabilities impacting ESXi, Workstation, Fusion, Cloud Foundation, and NSX Data Center for vSphere that could be exploited to execute arbitrary code and cause a denial-of-service (DoS) condition.
https://thehackernews.com/2022/02/vmware-issues-security-patches-for-high.html?_m=3n%2e009a%2e2677%2eod0ao445rz%2e1pf2

Spanish Police Arrest SIM Swappers Who Stole Money from Victims Bank Accounts
Spain's National Police Agency, the Policía Nacional, said last week it dismantled an unnamed cybercriminal organization and arrested eight individuals in connection with a series of SIM swapping attacks that were carried out with the goal of financial fraud.
https://thehackernews.com/2022/02/spanish-police-arrest-sim-swappers-who.html?_m=3n%2e009a%2e2675%2eod0ao445rz%2e1pd4

FBI Warns of BlackByte Ransomware Attacks on Critical Infrastructure
The BlackByte ransomware has been used in attacks on at least three critical infrastructure sectors in the United States, the Federal Bureau of Investigation (FBI) and the U.S. Secret Service (USSS) warn in a joint advisory.
https://www.securityweek.com/fbi-warns-blackbyte-ransomware-attacks-critical-infrastructure?_hsmi=78978938&_hsenc=p2ANqtz-8WGwkAsRcXMy7nGCsjA1X5Ctq2DJf92y4qjUE-qfJXZwrzDoY0m84zA2LUlsvVcvZmj8_92ztAuY-cOp-FK0DUylTyMg

A new Google Chrome zero-day vulnerability is being actively exploited
Chrome 98.0.4758.102 for Windows, Mac, and Linux has been published to address a high-severity zero-day flaw exploited by malicious attackers in attacks.
https://david-artykov.medium.com/a-new-google-chrome-zero-day-vulnerability-is-being-actively-exploited-68f1c94c4dec

Red Cross Hack Linked to Iranian Influence Operation?
A network intrusion at the International Committee for the Red Cross (ICRC) in January led to the theft of personal information on more than 500,000 people receiving assistance from the group. KrebsOnSecurity has learned that the email address used by a cybercriminal actor who offered to sell the stolen ICRC data also was used to register multiple domain names the FBI says are tied to a sprawling media influence operation originating from Iran.
https://krebsonsecurity.com/2022/02/red-cross-hack-linked-to-iranian-influence-operation/

Linux Malware on the Rise
Ransomware, cryptojacking, and a cracked version of the penetration-testing tool Cobalt Strike have increasingly targeted Linux in multicloud infrastructure, report states. With Linux frequently used as the basis for cloud services, virtual-machine hosts, and container-based infrastructure, attackers have increasingly targeted Linux environments with sophisticated exploits and malware.
https://www.darkreading.com/cloud/linux-malware-on-the-rise-including-illicit-use-of-cobalt-strike?_mc=NL_DR_EDT_DR_daily_20220215&cid=NL_DR_EDT_DR_daily_20220215&elq_mid=109068&elq_cid=36315893

****

Hints & Tips plus Security Awareness

Be Flexible About Where People Work — But Not on Data Privacy
If your policies don't keep up with your work models, your company's sensitive information could be at risk. Return-to-workplace dates may still be in flux, but it's clear that hybrid and remote work is here to stay.
https://www.darkreading.com/edge-articles/be-flexible-on-where-people-work-but-not-on-data-privacy?_mc=NL_DR_EDT_DR_daily_20220216&cid=NL_DR_EDT_DR_daily_20220216&elq_mid=109131&elq_cid=36315893

7 Privacy Tips for Security Pros

Privacy and security, while often viewed through separate management lenses, go hand-in-hand. And privacy is increasingly becoming a key element of many security strategies. According to a recent survey from Cisco, some 90% of security pros now consider privacy a mission-critical business imperative. In fact, 90% of responding security pros say their customers would not buy from them if they did not adequately protect their data. Detecting and responding to threats and assessing and managing risk has become a core area of responsibility for security pros.

https://www.darkreading.com/risk/7-privacy-tips-for-security-pros-?_mc=NL_DR_EDT_DR_daily_20220211&cid=NL_DR_EDT_DR_daily_20220211&elq_mid=109008&elq_cid=36315893

****

News & Views

Facebook Agrees to Pay $90 Million to Settle Decade-Old Privacy Violation Case

Meta Platforms has agreed to pay $90 million to settle a lawsuit over the company's use of cookies to allegedly track Facebook users' internet activity even after they had logged off from the platform.

https://thehackernews.com/2022/02/facebook-agrees-to-pay-90-million-to.html?_m=3n%2e009a%2e2677%2eod0ao445rz%2e1pfk

France Rules That Using Google Analytics Violates GDPR Data Protection Law

French data protection regulators on Thursday found the use of Google Analytics a breach of the European Union's General Data Protection Regulation (GDPR) laws in the country, almost a month after a similar decision was reached in Austria.

https://thehackernews.com/2022/02/france-rules-that-using-google.html?_m=3n%2e009a%2e2675%2eod0ao445rz%2e1pdt

Google moves to make Android apps more private

Google's plan to limit data tracking on its Chrome browser has been extended to cover apps on its Android-based smartphones.

https://www.bbc.com/news/technology-60403963

Three-Quarters of Ransomware Payments Linked to Russia

Around three-quarters (74%) of ransomware revenue resulted from attacks associated with Russia in 2021, according to a new report by blockchain investigations and analytics company Chainalysis. The researchers found that more than $400m worth of cryptocurrency went to ransomware strains “highly likely” to be affiliated with Russia in some way last year.

https://www.infosecurity-magazine.com/news/three-quarters-ransomware-payments/

****

"Ctrl -F" for The Board

Financial Crimes Enforcement Network Makes Ransomware a Priority
FinCEN is currently in the midst of enacting new regulations under the Anti-Money Laundering Act of 2020 (AML Act), which will seek to address threats, such as corruption and anti-terrorism, while also taking a proactive approach against crimes tied to ransomware, digital assets, and strategic corruption.
https://www.lexblog.com/2022/02/14/financial-crimes-enforcement-network-makes-ransomware-a-priority/?_hsmi=203237365&_hsenc=p2ANqtz-_yKo0ot3aJP2WA8ABfVV5MLl4MyM3QAejuTyYg9n0XlD1TTz6TdY39pj6BpqhfgHoabsUSIX3JpJVQCO1s85SIIWUUYw

What CISOs Should Tell the Board About Log4j
It's time for a reset with the board of directors. Very few have a dedicated, board-level cybersecurity committee, which means cybersecurity isn't viewed as a critical executive function.
https://www.darkreading.com/attacks-breaches/what-cisos-should-tell-the-board-about-log4j?_mc=NL_DR_EDT_DR_daily_20220216&cid=NL_DR_EDT_DR_daily_20220216&elq_mid=109131&elq_cid=36315893

Questions
Contact FIPCO’s Rob Foxx at 800-722-3498 ext. 249 or email FIPCO IT Services for more information.

"Make Security Part of You and Your Institution's DNA!"

Threat Intelligence Newsletter: February 28, 2022

FIPCO®
IT Audit
Round Table
Discussions

If you would like to host an event, please contact: Becky Schowalter

Upcoming Threat Intelligence Peer Group Discussions
None available at the current time

****

Alerts & Warnings

New Data-Wiping Malware Discovered on Systems in Ukraine
Researchers were scrambling to analyze a newly discovered piece of data-wiping malware found in the wild.
https://www.darkreading.com/attacks-breaches/new-data-wiping-malware-discovered-on-systems-in-ukraine?_mc=NL_DR_EDT_DR_daily_20220224&cid=NL_DR_EDT_DR_daily_20220224&elq_mid=109273&elq_cid=36315893

CISA Warns of New Malware Framework Used by Russian 'Sandworm' Hacking Team
Russian General Staff Main Intelligence Directorate (GRU) hacking team appears to have swapped its VPNFilter malware platform for the so-called Cyclops Blink malware framework.
https://www.darkreading.com/vulnerabilities-threats/cisa-warns-of-new-malware-framework-employed-by-infamous-sandworm-hacking-team?_mc=NL_DR_EDT_DR_daily_20220224&cid=NL_DR_EDT_DR_daily_20220224&elq_mid=109273&elq_cid=36315893

9 Ransomware Trends: More Leaks, Higher Ransom Payments
By Nearly Every Measure, Ransomware Attacks Got Worse in 2021, Researchers Report
https://www.databreachtoday.com/9-ransomware-trends-more-leaks-higher-ransom-payments-a-18519?rf=2022-02-19__ACQ_DBT__Slot1_ART18519&mkt_tok=MDUxLVpYSS0yMzcAAAGCsb5Ngq9ktQjc2FnCyTHIo1lB91NKhdL2Nkb91InC26IHtFXLPWP1mjBFOwjVlDQsO3kjgV8XHud9INu19kt7-dvfqwOqZ2gBFZn5Eyuc6j8_kjHNmA

Samsung Shattered Encryption on 100M Phones
Samsung reportedly shipped 100 million smartphones containing botched encryption, including models ranging from the 2017 Galaxy S8 to last year's Galaxy S21.
https://threatpost.com/samsung-shattered-encryption-on-100m-phones/178606/

Almost 100,000 new mobile banking Trojan strains detected in 2021
Mobile malware used to be relatively rare. Now, the focus has pivoted from PCs to our handsets.
https://www.zdnet.com/article/almost-100000-new-mobile-banking-trojans-detected-in-2021/

Iranian Hackers Targeting VMware Horizon Log4j Flaws to Deploy Ransomware
A "potentially destructive actor" aligned with the government of Iran is actively exploiting the well-known Log4j vulnerability to infect unpatched VMware Horizon servers with ransomware.
https://thehackernews.com/2022/02/iranian-hackers-targeting-vmware.html?_m=3n%2e009a%2e2679%2eod0ao445rz%2e1ph7

****

Hints & Tips plus Security Awareness

Hidden Costs of a Data Breach
Don't consider just the initial costs. Hidden factors include remediation, revenue loss, reputational harm, national security — even human life.
https://www.darkreading.com/attacks-breaches/hidden-costs-of-a-data-breach?_mc=NL_DR_EDT_DR_daily_20220223&cid=NL_DR_EDT_DR_daily_20220223&elq_mid=109232&elq_cid=36315893

The 7 Most Critical Risks to Your Sensitive Data in 2022 & How to Tackle Them
Modern organizations continue to embrace the convenience of hybrid work, but a lack of control over cloud apps introduces risks to sensitive data. A new Palo Alto Networks research, which analyzes data from more than 1,000 enterprises, reveals the top cybersecurity risks and modern trends that put organizations at the risk of attack, data breaches, and non-compliance.
https://www.databreachtoday.com/webinars/live-webinar-today-7-most-critical-risks-to-your-sensitive-data-in-w-3733?user_email=rfoxx@fipco.com&rf=2022-02-24_ENEWS_ACQ_DBT___Slot2_WEB3733&mkt_tok=MDUxLVpYSS0yMzcAAAGCy5yI33f62zOTbA2yU7tnwGmuFmShXbZfLEjULadwVNKuSbJqnTKm4a75KKRuHJvlUHdQVrQkTlJ3jfarW3V0ngWPQPFAxZCsLfedV-oc-JnrY53g3Q

****

News & Views

Russia Could Use Cryptocurrency to Blunt the Force of U.S. Sanctions
Russian companies have many cryptocurrency tools at their disposal to evade sanctions, including a so-called digital ruble and ransomware.
https://www.nytimes.com/2022/02/23/business/russia-sanctions-cryptocurrency.html?utm_source=Sailthru&utm_medium=email&utm_campaign=Issue:%202022-02-24%20Cybersecurity%20Dive%20%5Bissue:39990%5D&utm_term=Cybersecurity%20Dive

Rail transit vulnerable to cyberattacks, experts say
Transit networks are a target of criminal and state actors intent on disrupting operations.
https://www.cybersecuritydive.com/news/rail-transit-cyberattacks/619123/?utm_source=Sailthru&utm_medium=email&utm_campaign=Issue:%202022-02-23%20Cybersecurity%20Dive%20%5Bissue:39956%5D&utm_term=Cybersecurity%20Dive

Banks, late to the game, double down on the cloud
Top bank CEOs migrate faster to stay agile, competitive, secure and relevant.
https://www.ciodive.com/news/banks-cloud-fortune-500/618652/?utm_source=Sailthru&utm_medium=email&utm_campaign=Newsletter%20Weekly%20Roundup:%20CIO%20Dive:%20Daily%20Dive%2002-19-2022&utm_term=CIO%20Dive%20Weekender

Why Passwordless Is at an Impasse
Many widely used business applications aren't built to support passwordless login because identity and authentication remain siloed.
https://www.darkreading.com/operations/why-passwordless-is-at-an-impasse?_mc=NL_DR_EDT_DR_daily_20220224&cid=NL_DR_EDT_DR_daily_20220224&elq_mid=109273&elq_cid=36315893

IRS: Selfies Now Optional, Biometric Data to Be Deleted
The U.S. Internal Revenue Service (IRS) said Monday that taxpayers are no longer required to provide facial scans to create an account online at irs.gov. In lieu of providing biometric data, taxpayers can now opt for a live video interview with ID.me, the privately-held Virginia company that runs the agency's identity proofing system.
https://krebsonsecurity.com/2022/02/irs-selfies-now-optional-biometric-data-to-be-deleted/

****

"Ctrl -F" for The Board

How to Prepare Your Business for the Latest Cyber Threats
In 2020, nearly half (47%) of companies were impacted by scammers and identity theft. With more business being done online, companies are increasingly opening themselves up to cybersecurity risk – and for fintech companies, that risk is especially significant.
https://www.cybersecuritydive.com/events/how-to-prepare-your-business-for-the-latest-cyber-webinar-2pm-et-feb-24-2022-cybersecurity-dive/?utm_source=Sailthru&utm_medium=email&utm_campaign=Issue:%202022-02-24%20Cybersecurity%20Dive%20%5Bissue:39990%5D&utm_term=Cybersecurity%20Dive

Flex work in 2022 may mean chucking your title
Where Citi became 2021's poster bank for hybrid schedules, UBS is looking to streamline by making employees known more for their functions than by their place in a pecking order.
https://www.bankingdive.com/news/flex-work-in-2022-may-mean-chucking-your-title/619118/?utm_source=Sailthru&utm_medium=email&utm_campaign=Issue:%202022-02-18%20Banking%20Dive%20%5Bissue:39877%5D&utm_term=Banking%20Dive

More Orgs Suffered Successful Phishing Attacks in 2021 Than in 2020
Threat actors maintained their relentless attacks on enterprise end users for yet another year, new study shows.
https://www.darkreading.com/attacks-breaches/more-orgs-experienced-a-successful-phishing-attack-in-2021-than-year-before?_mc=NL_DR_EDT_DR_daily_20220224&cid=NL_DR_EDT_DR_daily_20220224&elq_mid=109273&elq_cid=36315893

If the Cloud Is More Secure, Then Why Is Everything Still Broken?
The sooner we discover sources of risk, the better equipped we will be to create effective
https://www.darkreading.com/cloud/if-the-cloud-is-more-secure-then-why-is-everything-still-broken-?_mc=NL_DR_EDT_DR_daily_20220222&cid=NL_DR_EDT_DR_daily_20220222&elq_mid=109204&elq_cid=36315893

Enterprises Look Beyond Antivirus Software for Remote Workers
Priorities are shifting, with growing emphasis on endpoint detection and response (EDR) software and multifactor authentication (MFA), a recent survey of IT professionals shows.
https://www.darkreading.com/tech-trends/enterprises-require-more-mfa-less-antivirus-for-remote-workers?_mc=NL_DR_EDT_DR_daily_20220222&cid=NL_DR_EDT_DR_daily_20220222&elq_mid=109204&elq_cid=36315893

Questions
Contact FIPCO’s Rob Foxx at 800-722-3498 ext. 249 or email FIPCO IT Services for more information.

"Make Security Part of You and Your Institution's DNA!"

Threat Intelligence Newsletter: March 4, 2022

FIPCO®
IT Audit
Round Table
Discussions

If you would like to host an event, please contact: [Becky Schowalter]

Upcoming Threat Intelligence Peer Group Discussions
None available at the current time

****

Alerts & Warnings

U.S. banks prepare for cyber attacks after latest Russia sanctions
U.S. banks are preparing for retaliatory cyber attacks after Western nations slapped a raft of stringent sanctions on Russia for invading Ukraine, cyber experts and executives said. Tensions between Russia and the West escalated on Saturday as the United States and its allies moved to block some Russian banks from the SWIFT international payment system and placed curbs on the Russian central bank's international reserves.
https://www.oodaloop.com/technology/2022/03/01/u-s-banks-prepare-for-cyber-attacks-after-latest-russia-sanctions/

Destructive Malware Targeting Organizations in Ukraine
Leading up to Russia's unprovoked attack against Ukraine, threat actors deployed destructive malware against organizations in Ukraine to destroy computer systems and render them inoperable.
https://www.cisa.gov/uscert/ncas/alerts/aa22-057a#:~:text=Technical%20Details%20%20%20%20Name%20%20,%20%20SentinelLabs%20%207%20more%20rows%20

100 Million Samsung Galaxy Phones Affected with Flawed Hardware Encryption Feature
A group of academics from Tel Aviv University have disclosed details of now-patched "severe" design flaws affecting about 100 million Android-based Samsung smartphones that could have resulted in the extraction of secret cryptographic keys.
https://thehackernews.com/2022/02/100-million-samsung-galaxy-phones.html?_m=3n%2e009a%2e2685%2eod0ao445rz%2e1pm0

Fake gaming apps on Microsoft Store drop Electron Bot malware
The malware boasts diverse capabilities, including SEO poisoning, where cybercriminals create infected websites and use SEO tactics to ensure these sites appear prominently in search results.
https://www.hackread.com/fake-game-app-microsoft-store-electron-bot-malware/?_hsmi=78978938&_hsenc=p2ANqtz-8QQ9JieNH4jmB7Prf46j90B3bapkmFVtbDD1O7A_mFU3whkFvwFi0uVZ6hES4gLaSuqGPCxV14cRH4sqTkKhCxAG_7lg

Experts Fear Surge in Romance and Cybercurrency Scams
With overall scam losses running at a 10-year high, consumer experts are expressing increasing concern about an alarming rise in cybercurrency and romance scams.
https://scambusters.org/experts.html

Healthcare Org Hit By Two Ransomware Gangs At Once
Two competing threat groups both deployed ransomware on the victim’s network. One was the Russia-linked Conti while the other, Karma, counts Russian IP addresses among its top five targets.
https://www.forbes.com/sites/leemathews/2022/02/28/healthcare-org-hit-by-two-ransomware-gangs-at-once/?ss=cybersecurity&sh=4a40e8a521de

****

Hints & Tips plus Security Awareness

7 Steps to Take Right Now to Prepare for Cyberattacks by Russia
US-led sanctions on Russia for its invasion of Ukraine earlier this week have sparked considerable concern about retaliatory and spillover cyberattacks from the region on US organizations and those based in other allied nations.
https://www.darkreading.com/threat-intelligence/7-steps-to-take-right-now-to-prepare-for-cyberattacks-by-russia?_mc=NL_DR_EDT_DR_daily_20220303&cid=NL_DR_EDT_DR_daily_20220303&elq_mid=109410&elq_cid=36315893

CISO Checklist for Offboarding Security Staff
The Great Resignation strikes cybersecurity teams, too. Here's a checklist for CISOs to ensure security is retained even when security staff is not. The Great Resignation hits every company hard, but it can be terrifying when your security pros leave in droves. There are more than the obvious risks at stake, and CISOs must manage them all. A checklist can help ensure mistakes aren't made and regrets aren't expensive.
https://www.darkreading.com/edge-articles/ciso-checklist-for-offboarding-security-staff?_mc=NL_DR_EDT_DR_daily_20220303&cid=NL_DR_EDT_DR_daily_20220303&elq_mid=109410&elq_cid=36315893

****

News & Views

Hackers Try to Target European Officials to Get Info on Ukrainian Refugees, Supplies
Details of a new nation-state sponsored phishing campaign have been uncovered setting its sights on European governmental entities in what's seen as an attempt to obtain intelligence on refugee and supply movement in the region.
https://thehackernews.com/2022/03/hackers-try-to-hack-european-officials.html?_m=3n%2e009a%2e2687%2eod0ao445rz%2e1pns

Anonymous Hacker Group Targets Russian State Media
Hacker group Anonymous claimed responsibility on Monday for disrupting the work of websites of pro-Kremlin Russian media in protest of the invasion of Ukraine. The group targeted the websites of state news agencies TASS and RIA Novosti, as well as taking over websites of newspapers Kommersant and Izvestiya and Forbes Russia magazine.
https://www.securityweek.com/anonymous-hacker-group-targets-russian-state-media?_hsmi=78978938&_hsenc=p2ANqtz--rA0mKdu1Pz_8AUof9XBfWOZVfq4kOjn5aLtpA1YuwAZeS2-8A4yKvllvW7sUCLH97Sf5AmM4SyKkQq_vD5HLzZr5seg

Toyota to Close Japan Plants After Suspected Cyberattack
The plants will shut down on March 1st, halting about a third of the company's global production. Toyota doesn't know how long the 14 plants will be unplugged.
https://threatpost.com/toyota-to-close-japan-plants-after-suspected-cyberattack/178686/

Moscow Exchange Downed by Cyber-Attack
The website for the Moscow Stock Exchange was offline and inaccessible on Monday. A crowdsourced community of hackers endorsed by Kyiv officials has claimed responsibility for the outage. The Ukraine IT Army posted a message on Telegram that it had taken just five minutes to render the site inaccessible.
https://www.infosecurity-magazine.com/news/moscow-exchange-cyber-attack/

****

"Ctrl -F" for The Board

Bitcoin jumps back above $40,000 as Russians switch to crypto
Hong Kong (CNN Business)Cryptocurrency prices are climbing after Russia's ruble sank to another record low and Moscow was hit with new sanctions. As of 5:25 a.m. ET on Tuesday, bitcoin had jumped 13% over the last 24 hours to $43,163, according to cryptocurrency tracker CoinDesk. Other cryptocurrencies moved higher, too. Ethereum climbed 10% Tuesday to reach $2,878. Dogecoin rose nearly 6% to about 13 cents apiece.
https://edition.cnn.com/2022/03/01/investing/bitcoin-price-russia-ruble-intl-hnk/index.html

Questions
Contact FIPCO's Rob Foxx at 800-722-3498 ext. 249 or email FIPCO IT Services for more information.

"Make Security Part of You and Your Institution's DNA!"

Threat Intelligence Newsletter: March 11, 2022

FIPCO®
IT Audit
Round Table
Discussions

If you would like to host an event, please contact: Becky Schowalter

Upcoming Threat Intelligence Peer Group Discussions
None available at the current time

****

Alerts & Warnings

WATCH OUT FOR THESE 5 UKRAINE SCAMS THAT COULD BE ON THEIR WAY HERE
The military situation in Ukraine is moving quickly -- and so are crooks using the name of the country to pull off scams. Fraudsters will twist the name of Ukraine into well-known scam disguises in the coming weeks. The conflict in Ukraine may seem a long way from your doorstep but you can be sure, in at least one way, your security is likely to be threatened: by scammers!
https://scambusters.org/ukraine.html

FBI Alert: Ransomware Attacks Hit Critical Infrastructure Organizations
The FBI issued a warning this week that the RagnarLocker ransomware has infected some 52 organizations in manufacturing, energy, financial services, government, and information technology so far this year.
https://www.darkreading.com/attacks-breaches/fbi-alert-ransomware-attacks-hit-critical-infrastructure-organizations?_mc=NL_DR_EDT_DR_daily_20220310&cid=NL_DR_EDT_DR_daily_20220310&elq_mid=109565&elq_cid=36315893

Russia-Ukraine crisis replaces Covid as top risk to global supply chains, Moody's says
Covid-19 drove global supply chains to the breaking point, causing shortages and sending prices skyrocketing. Just as the pandemic has calmed down, Russia's invasion of Ukraine threatens to further scramble those fragile supply chains. Russia is a major producer of commodities, everything from oil and natural gas to palladium and wheat.
https://www.oodaloop.com/technology/2022/03/04/russia-ukraine-crisis-replaces-covid-as-top-risk-to-global-supply-chains-moodys-says/

****

Hints & Tips plus Security Awareness

SEC pushes for tougher cybersecurity disclosure rules
Companies would need to report breaches within four days under the proposed rules.
https://www.cybersecuritydive.com/news/sec-cyber-
disclosure/620143/?utm_source=Sailthru&utm_medium=email&utm_campaign=Issue:%202022-03-
10%20Cybersecurity%20Dive%20%5Bissue:40299%5D&utm_term=Cybersecurity%20Dive

The state of cybersecurity in 2022
As the transition to remote work stirred organizations away from a traditional network perimeter, CISOs have seen cyberattack records shatter. Now as international conflicts spill into the cyber domain, prioritizing core enterprise vulnerabilities is more important than ever.
https://www.ciodive.com/trendline/cybersecurity/106/?utm_source=CSD&utm_medium=NL2March7&ut
m_campaign=Hyperproof&utm_content=ad-CUSTOM_TOP&utm_term=40185

9 Essentials for Global CISOs During Russia's Ukraine War
As Russia's invasion of Ukraine continues, what should CISOs and security teams be doing to ensure that their organizations stay protected?
https://www.databreachtoday.com/9-essentials-for-global-cisos-during-russias-ukraine-war-a-
18656?rf=2022-03-
04_ENEWS_ACQ_DBT__Slot1_ART18656&mkt_tok=MDUxLVpYSS0yMzcAAAGC9M40bfvn_q4MFM2x6KHK
R5GAeL2L_4ckq8phFAUG2ezcLChJaI1JCXov0-J7Kh2ri6yC2YFtIfAkRNRov73xd-n4qXg4OHtKTlTiDK6svn-
htiL7HA

Russia eyes sanctions workarounds in energy, gold, crypto
The harsh sanctions imposed on Russia and the resulting crash of the ruble have the Kremlin scrambling to keep the country’s economy running. For Vladimir Putin, that means finding workarounds to the Western economic blockade even as his forces continue to invade Ukraine.
https://www.oodaloop.com/technology/2022/03/02/russia-eyes-sanctions-workarounds-in-energy-gold-
crypto/

****

News & Views

Cyber risk to US utilities seen as limited as Biden sets red line
Critical infrastructure is on high alert, but — at least for now — the conflict in Europe could signal a lull in utility ransomware attacks.
https://www.cybersecuritydive.com/news/Russia-ukraine-utility-
cyberattack/619819/?utm_source=Sailthru&utm_medium=email&utm_campaign=Newsletter%20Weekly
%20Roundup:%20Cybersecurity%20Dive:%20Daily%20Dive%2003-05-
2022&utm_term=Cybersecurity%20Dive%20Weekender

It's time to pay back technical debt
A breaking point is fast approaching for companies that quickly migrated technology in the pandemic. Companies around the world adopted new technology to support remote workers and fast-tracked digital product releases in response to the pandemic.
https://www.ciodive.com/news/technical-debt-payoff-enterprise-IT/619953/?utm_source=Sailthru&utm_medium=email&utm_campaign=Issue:%202022-03-09%20CIO%20Dive%20%5Bissue:40245%5D&utm_term=CIO%20Dive

Internet Backbone Giant Lumen Shuns .RU
Lumen Technologies, an American company that operates one of the largest Internet backbones and carries a significant percentage of the world's Internet traffic, said today it will stop routing traffic for organizations based in Russia. Lumen's decision comes just days after a similar exit by backbone provider Cogent, and amid a news media crackdown in Russia that has already left millions of Russians in the dark about what is really going on with their president's war in Ukraine.
https://krebsonsecurity.com/2022/03/internet-backbone-giant-lumen-shuns-ru/

Made in Beijing: The Plan for Global Market Domination
The FBI's Office of Private Sector, Counterintelligence Division and Training Division present this 30-minute film entitled Made in Beijing: The Plan for Global Market Domination. In the world of global adversaries, the People's Republic of China stands at the forefront with its sustained and brazen campaign of industrial espionage, posing the single greatest threat to our freedom, national security, and economic vitality.
https://www.youtube.com/watch?v=GdapE82GceA&t=1s

****

"Ctrl -F" for The Board

Ukraine war tests cyber insurance exclusions
Enterprise customers should expect higher premiums and more restrictive underwriting criteria.
https://www.ciodive.com/news/cyber-insurance-ukraine-war-exclusions/619785/?utm_source=Sailthru&utm_medium=email&utm_campaign=Issue:%202022-03-04%20CIO%20Dive%20%5Bissue:40155%5D&utm_term=CIO%20Dive

WhatsApp scandal's specter rises again
Citi, Goldman Sachs and HSBC all warned, in their annual reports, that the SEC and CFTC are investigating banks' record-keeping of communications through private platforms.
https://www.bankingdive.com/news/whatsapp-citi-goldman-sachs-hsbc-deutsche-bank-jpmorgan-chase-sec-cftc/619609/?utm_source=Sailthru&utm_medium=email&utm_campaign=Newsletter%20Weekly%20Roundup:%20Banking%20Dive:%20Daily%20Dive%2003-05-2022&utm_term=Banking%20Dive%20Weekender

Credit unions buy Wisconsin, Arkansas banks
The moves to acquire Commerce State Bank and HomeBank bring to three the number of bank tie-ups with credit unions within a week.
https://www.bankingdive.com/news/credit-unions-buy-wisconsin-arkansas-banks/619814/?utm_source=Sailthru&utm_medium=email&utm_campaign=Issue:%202022-03-07%20Banking%20Dive%20%5Bissue:40186%5D&utm_term=Banking%20Dive

Medical debt is having a significant impact on consumer credit
The CFPB released a new report that found medical debt is having a significant impact on consumer credit. Our findings suggest that roughly 43 million Americans have medical debt on their credit reports, and as of June 2021, that debt totals around $88 billion.
https://www.consumerfinance.gov/data-research/research-reports/medical-debt-burden-in-the-united-states/

Questions
Contact FIPCO's Rob Foxx at 800-722-3498 ext. 249 or email FIPCO IT Services for more information.

"Make Security Part of You and Your Institution's DNA!"

Threat Intelligence Newsletter: March 18, 2022

FIPCO®
IT Audit
Round Table
Discussions

If you would like to host an event, please contact: Becky Schowalter

Upcoming Threat Intelligence Peer Group Discussions
None available at the current time

****

Alerts & Warnings

SEC Issues Proposal on Cyber Risk Management, Incident Reporting
A new proposal by the Securities and Exchange Commission today would create new requirements for public companies regarding the disclosure of cybersecurity incidents.
https://bankingjournal.aba.com/2022/03/sec-issues-proposal-on-cyber-risk-management-incident-reporting/?utm_source=eloqua&utm_medium=email&utm_campaign=compliancebulletin&utm_content=COMPLIANCE-20220314

Instagram accounts hijacked with fake copyright infringement notifications
A new phishing scheme targeting popular accounts on Instagram is gaining momentum. The e-mail claims that you have just 24 hours (in some versions it's 48 hours) to appeal and provides a "Review complaint" button. If you click it, you end up on a convincing phishing page, where fraudsters put an image saying they care very much about copyright protection and offer you a link to "Appeal."
https://usa.kaspersky.com/blog/instagram-hijack-new-wave/17354/?utm_source=newsletter&utm_medium=email&utm_content=explains%20Kaspersky&utm_campaign=scam-alert

Multiple Security Flaws Discovered in Popular Software Package Managers
Multiple security vulnerabilities have been disclosed in popular package managers that, if potentially exploited, could be abused to run arbitrary code and access sensitive information, including source code and access tokens, from compromised machines.
https://thehackernews.com/2022/03/multiple-security-flaws-discovered-in.html?_m=3n%2e009a%2e2693%2eod0ao445rz%2e1pt4

Mobile Threats Skyrocket
A new report shows an explosion of zero-day attacks and malware focused on mobile devices just as companies adopted widespread bring-your-own device policies.
https://www.darkreading.com/endpoint/mobile-threats-skyrocket?_mc=NL_DR_EDT_DR_daily_20220316&cid=NL_DR_EDT_DR_daily_20220316&elq_mid=109696&elq_cid=36315893

****

Hints & Tips plus Security Awareness

Scammers Up Their Game Using Advanced Technology
Technology has changed our lives dramatically -- but not always for the benefit of consumers. Scammers are also using advanced devices and programming schools to step up their game. They may still rely mostly on old, long-established con tricks, but advances in technology and their skills have changed the game -- for the worse.
https://scambusters.org/technology.html

Microsoft the No. 1 Most-Spoofed Brand in Phishing Attacks
New Barracuda Networks data shows attackers sent some 3 million emails from around 12,000 pilfered accounts.
https://www.darkreading.com/vulnerabilities-threats/microsoft-the-1-most-spoofed-brand-in-phishing-attacks?_mc=NL_DR_EDT_DR_daily_20220317&cid=NL_DR_EDT_DR_daily_20220317&elq_mid=109734&elq_cid=36315893

Fireside Chat | 10 Trends That Will Shape the Fraud Landscape in 2022
Many organizations face an upward battle when detecting and preventing fraud. Consumers continue to migrate to digital channels and while organizations are benefiting from this transition, it comes at a price. Where transactions occur, fraudsters follow, seeking out new vulnerabilities to exploit. Thursday, Mar. 31, 2022 11:30 AM EDT
https://www.databreachtoday.com/webinars/fireside-chat-10-trends-that-will-shape-fraud-landscape-in-2022-w-3811?user_email=rfoxx@fipco.com&rf=2022-03-16_ENEWS_ACQ_DBT__Slot7_WEB3811&mkt_tok=MDUxLVpYSS0yMzcAAAGDMmNZVA8sw-Y-_yfVQ1ywFnjFWZaThbhuwgToH_8NzOOPnR5XQHVwRRrFNBKcNGzz2tN-1c8bphvxstTOrX0p6CHBC4BcSUFGCO9sGzNiIdGGBugBiQ

****

News & Views

Biden orders government to study digital dollar, other cryptocurrency risks
U.S. President Joe Biden signed an executive order on Wednesday requiring the government to assess the risks and benefits of creating a central bank digital dollar, as well as other cryptocurrency issues, the White House said. Bitcoin surged on the news as the administration's holistic and deliberative approach calmed market fears about an immediate regulatory crackdown on cryptocurrencies. In midday trading, bitcoin rose 9.1% to $42,280, on track for its largest percentage gain since Feb. 28.
https://www.reuters.com/business/finance/biden-orders-government-study-digital-dollar-other-cryptocurrency-risks-2022-03-09/

Kronos ransomware attack raises questions of vendor liability
The December ransomware attack against workforce management company Ultimate Kronos Group hindered the ability of its customers to process payrolls. The attack, which has far-reaching ramifications, has stakeholders looking for who is to blame.
https://www.cybersecuritydive.com/news/kronos-ransomware-attack-lawsuits/620184/?utm_source=Sailthru&utm_medium=email&utm_campaign=Issue:%202022-03-14%20Cybersecurity%20Dive%20%5Bissue:40348%5D&utm_term=Cybersecurity%20Dive

U.S. officials wonder: Where are Russia's much-feared cyberattacks?
Putin has bragged about his nation's digital warriors and the U.S. is bracing for their arrival. There's a particularly unnerving scenario for a Russian cyberattack casting its shadow in the head of an American politician who oversees intelligence issues. Mark Warner leads the Senate intelligence committee, which gets him regular intelligence briefings and better-than-average access to U.S. state secrets. The Virginia Democrat has been voicing his concern at recent public events about the risk of a cyberattack striking a NATO country, potentially broadening the Ukraine war.
https://www.cbc.ca/news/world/where-are-russian-cyberattacks-1.6384951

****

"Ctrl -F" for The Board

IT workers most likely to quit, Gartner finds
Technology is at the center of worker attrition concerns, as talent woes hamper transformation and company growth. CIOs kicked off 2022 with large IT budgets and big plans for digital transformation. One constant pain point holding them back is the ability to attract and retain talent, as IT skills remain in high demand across industry verticals.
https://www.ciodive.com/news/IT-talent-retention-challenges-2022/620259/?utm_source=Sailthru&utm_medium=email&utm_campaign=Issue:%202022-03-15%20CIO%20Dive%20%5Bissue:40352%5D&utm_term=CIO%20Dive

What the Newly Signed US Cyber-Incident Law Means for Security
Bipartisan cybersecurity legislation comes amid increased worries over ransomware, and fears of cyberattacks from Russia in the wake of its invasion of Ukraine.
https://www.darkreading.com/attacks-breaches/new-cyber-incident-law-not-a-national-breach-law-but-a-major-first-step?_mc=NL_DR_EDT_DR_daily_20220317&cid=NL_DR_EDT_DR_daily_20220317&elq_mid=109734&elq_cid=36315893

How Pen Testing Gains Critical Security Buy-in and Defense Insight
It's more important than ever for companies to challenge their defenses, learning about new gaps and opportunities for improvement along the way.
https://www.darkreading.com/edge-articles/how-pen-testing-gains-critical-security-buy-in-and-defense-insight?_mc=NL_DR_EDT_DR_daily_20220317&cid=NL_DR_EDT_DR_daily_20220317&elq_mid=109734&elq_cid=36315893

Russia's war with Ukraine could permanently reshape the global supply chain
Companies will no longer be able to separate business from geopolitics, and the global supply chain will never be the same. Francis Fukuyama, the American political scientist who once described the collapse of the Soviet Union as the "end of history," suggested that Russia's invasion of Ukraine might be called "the end of the end of history." He meant that Vladimir Putin's aggression signals a rollback of the ideals of a free Europe that emerged after 1991. Some observers suggest it may kick off a new Cold War, with an Iron Curtain separating the West from Russia.
https://www.fastcompany.com/90731234/russias-war-with-ukraine-could-permanently-reshape-the-global-supply-chain

Questions
Contact FIPCO's Rob Foxx at 800-722-3498 ext. 249 or email FIPCO IT Services for more information.

"Make Security Part of You and Your Institution's DNA!"

Threat Intelligence Newsletter: March 25, 2022

FIPCO®
IT Audit
Round Table
Discussions

If you would like to host an event, please contact: Becky Schowalter

Upcoming Threat Intelligence Peer Group Discussions
None available at the current time

****

Alerts & Warnings

Whitehouse FACT SHEET: Act Now to Protect Against Potential Cyberattacks
The Biden-Harris Administration has warned repeatedly about the potential for Russia to engage in malicious cyber activity against the United States in response to the unprecedented economic sanctions we have imposed. There is now evolving intelligence that Russia may be exploring options for potential cyberattacks.
https://www.whitehouse.gov/briefing-room/statements-releases/2022/03/21/fact-sheet-act-now-to-protect-against-potential-cyberattacks/
Related White house press release: https://www.youtube.com/watch?v=biwoDSgEbag

A Closer Look at the LAPSUS$ Data Extortion Group
Microsoft and identity management platform Okta both this week disclosed breaches involving LAPSUS$, a relatively new cybercrime group that specializes in stealing data from big companies and threatening to publish it unless a ransom demand is paid. Here's a closer look at LAPSUS$, and some of the low-tech but high-impact methods the group uses to gain access to targeted organizations.
https://krebsonsecurity.com/2022/03/a-closer-look-at-the-lapsus-data-extortion-group/

HubSpot Data Breach Ripples Through Cryptocurrency Industry
A rogue employee working at HubSpot – used by more than 135,000 (and growing) customers to manage marketing campaigns and on-board new users – has been fired over a breach that zeroed in on the company's cryptocurrency customers, the company confirmed on Friday the 18th of March.
https://threatpost.com/hubspot-data-breach-crytocurrency-industry/179086/?_hsmi=78978938&_hsenc=p2ANqtz-8lCYBXsBTscyIcnCPQTfMw-CzHP3AYAnwpvbnPsL_e8ag9qkLJfB7cGIqKZ3HvyuGWINSjAjJwI5HSMXsyNp3-9yqJEg

A new rootkit comes to an ATM near you
It’s not unusual to hear about malware created to affect automated teller machines (ATMs). Malware can be planted at the ATM’s PC or its network, or attackers could launch a Man-in-the-Middle (MiTM) attack. Recently, a new rootkit, which the Mandiant Advanced Practices team have named CAKETAP, was found targeting Oracle Solaris systems running on ATM switch servers. This rootkit is a Unix kernel module that performs several malicious tasks to aid attackers—Mandiant tracks it as UNC2891 (aka LightBasin)—in conducting fraudulent ATM transactions.
https://blog.malwarebytes.com/cybercrime/2022/03/a-new-rootkit-comes-to-an-atm-near-you/?_hsmi=78978938&_hsenc=p2ANqtz-_AEumWQ7seh1bnTpUeDtqmcxwW6c3kxjplOfzvzhTS940fE_hg1GOkUZaxHfa4y64VnbkO8sTEwSL9kwW_IIUwlS43Eg

Accounts Drained By Zelle Smishing Scam
From time to time, scammers come up with a new tactic using new technology, new events, or whatever they can to continue tricking us into giving up our personal or confidential information. Over the past few years and with the increasing use of texting and SMS messaging, a newer one in the bag of tricks has been coined as “smishing.” Because it’s text, it often catches people off guard and causes them to react quickly, which is exactly what you shouldn’t do.
https://www.sosdailynews.com/news.jspx?&articleid=14A03A19BCD46C6002714E1DF9A0EA80&sx=26446

New Browser-in-the Browser (BITB) Attack Makes Phishing Nearly Undetectable
A novel phishing technique called browser-in-the-browser (BitB) attack can be exploited to simulate a browser window within the browser in order to spoof a legitimate domain, thereby making it possible to stage convincing phishing attacks. According to penetration tester and security researcher, who goes by the handle mrd0x on Twitter, the method takes advantage of third-party single sign-on (SSO) options embedded on websites such as "Sign in with Google" (or Facebook, Apple, or Microsoft).
https://thehackernews.com/2022/03/new-browser-in-browser-bitb-attack.html?_m=3n%2e009a%2e2699%2eod0ao445rz%2e1pzc

****

Hints & Tips plus Security Awareness

Cyber Risk Institute Updates Cybersecurity Profile
The Cyber Risk Institute—a coalition of financial institutions and trade associations including the American Bankers Association—has added an extension to its Cybersecurity Profile to address cloud security. The profile extension provides guidance to financial institutions and cloud service providers on commonly understood responsibilities related to cloud deployment.
https://bankingjournal.aba.com/2022/03/cyber-risk-institute-updates-cybersecurity-profile-3/?utm_source=eloqua&utm_medium=email&utm_campaign=newsbytes&utm_content=NEWSBYTES-20220324

6 Reasons Not to Pay Ransomware Attackers
Paying a ransom might appear to be the best option, but it comes with its own costs. Victims of ransomware attacks face the excruciating choice of either paying off their attackers or risking considerable disruption in attempting to restore encrypted data on their own or — as is often the case — with the help of an incident response firm.
https://www.darkreading.com/attacks-breaches/-6-reasons-not-to-pay-ransomware-attackers?_mc=NL_DR_EDT_DR_daily_20220324&cid=NL_DR_EDT_DR_daily_20220324&elq_mid=109815&elq_cid=36315893&sp_eh=72a861290e89658b5ada8de6a8a9c12b185e8e45329503691618392cbd15751b

Block Those Scam Calls, Spam Calls, and Robocalls Now!
Scam calls are costing Americans $30 billion a year, with one in every five of us having lost money to phone crooks. In this week's issue, we'll explain the simple steps you need to take to block most calls, or what to do if you want to stop them almost completely. Plus, we have three new scam alerts to help keep you out of the clutches of crooks.
https://scambusters.org/scamcall.html

10 College Scams and How to Beat Them
Student loan repayments are due to start again on May 1 (unless there's another pause) and college scammers are ready to cash in. But the fake debt relief they offer in return for payment is just the tip of a recent surge in con tricks targeting students. They also face blackmail threats, digital download scams, and even being tricked into taking courses backed by false promises.
https://scambusters.org/collegescam2.html

****

News & Views

How the War in Ukraine Is Further Disrupting Global Supply Chains
The invasion of Ukraine by Russia and sanctions imposed on it for doing so and new pandemic-related shutdowns in China are the latest events to rock global supply chains. Combined with the China-U.S. trade war and other pandemics- and climate-related disruptions, it is certain to accelerate the movement by Western companies to reduce their dependency on China for components and finished goods and on Russia for transportation and raw materials and to lead to more localized, or regional, sourcing strategies.
https://www.oodaloop.com/technology/2022/03/18/how-the-war-in-ukraine-is-further-disrupting-global-supply-chains/

****

"Ctrl -F" for The Board

FDIC: Banks Reporting More Sophisticated Cyber Attacks Since Start of Pandemic
Since the start of the pandemic, banks have reported more sophisticated cyber attacks, said Lisa Arquette, associate director of the FDIC's anti-money laundering and cyber fraud division at an industry event today. The more sophisticated attacks are the result of several factors, Arquette said, including an increase in bank employees working remotely and more customers accessing digital banking services.
https://bankingjournal.aba.com/2022/03/fdic-banks-reporting-more-sophisticated-cyber-attacks-since-start-of-pandemic/?utm_source=eloqua&utm_medium=email&utm_campaign=newsbytes&utm_content=NEWSBYTES-20220322

Podcast: What Banks Need to Know about Russia Sanctions Compliance
In the wake of Russia's invasion of Ukraine, western governments have imposed unprecedented financial sanctions on individuals, businesses, banks and governments in Russia, Belarus and Russian-occupied areas of Ukraine. With new sanctions continuing to be announced and a rolling series of compliance deadlines, the latest episode of the ABA Banking Journal Podcast
https://bankingjournal.aba.com/2022/03/podcast-what-banks-need-to-know-about-the-russia-sanctions/?utm_source=eloqua&utm_medium=email&utm_campaign=newsbytes&utm_content=NEWSBYTES-20220324

Kronos ransomware attack raises questions of vendor liability
A cyberattack with supply chain and legal consequences has stakeholders considering contract minutiae. The December ransomware attack against workforce management company Ultimate Kronos Group hindered the ability of its customers to process payrolls. The attack, which has far-reaching ramifications, has stakeholders looking for who is to blame.
https://www.cybersecuritydive.com/news/kronos-ransomware-attack-lawsuits/620184/?utm_source=Sailthru&utm_medium=email&utm_campaign=Issue:%202022-03-24%20Cybersecurity%20Dive%20%5Bissue:40621%5D&utm_term=Cybersecurity%20Dive

Questions
Contact FIPCO's Rob Foxx at 800-722-3498 ext. 249 or email FIPCO IT Services for more information.

"Make Security Part of You and Your Institution's DNA!"

Threat Intelligence Newsletter: April 1, 2022

FIPCO®
IT Audit
Round Table
Discussions

If you would like to host an event, please contact: Becky Schowalter

Upcoming Threat Intelligence Peer Group Discussions
None available at the current time

****

Alerts & Warnings

CISA Warns of Ongoing Cyber Attacks Targeting Internet-Connected UPS Devices
The U.S. Cybersecurity and Infrastructure Security Agency (CISA) and the Department of Energy (DoE) are jointly warning of attacks against internet-connected uninterruptible power supply (UPS) devices by means of default usernames and passwords.
https://thehackernews.com/2022/03/cisa-warns-of-ongoing-cyber-attacks.html?_m=3n%2e009a%2e2706%2eod0ao445rz%2e1q68

What are the biggest ransomware trends facing US businesses?
The US alone accounted for more than two-thirds (67.6%) of all ransomware attacks worldwide last year as the nation logged almost 421.5 million hits – a 98% rise year-on-year, according to a new report by cybersecurity firm SonicWall.
https://www.insurancebusinessmag.com/us/news/cyber/what-are-the-biggest-ransomware-trends-facing-us-businesses-399176.aspx?utm_source=GA&e=amVmZm9AbWJpc2xsYy5jb20&utm_medium=20220329&utm_campaign=IBAW-Cyber-Inverted-20220329&utm_content=5E6BF6FA-507D-4BE3-9DF6-5535E55A258A&tu=5E6BF6FA-507D-4BE3-9DF6-5535E55A258A

Cyber extortion surges 78% as 'ransomware as a service' spreads
Most companies require a recovery period of more than a month following a ransomware attack, Palo Alto Networks found. The average ransomware payment to cybercriminals surged 78% last year to $541,010, fueled in part by the rapid spread of ransomware as a service (RaaS) business models that reduce barriers to entry for cyber extortionists, Palo Alto Networks said.
https://www.cybersecuritydive.com/news/Ransomware-cyber-extortion-palo-alto/621144/?utm_source=Sailthru&utm_medium=email&utm_campaign=Issue:%202022-03-30%20Cybersecurity%20Dive%20%5Bissue:40744%5D&utm_term=Cybersecurity%20Dive

Hackers Gaining Power of Subpoena Via Fake "Emergency Data Requests"
There is a terrifying and highly effective "method" that criminal hackers are now using to harvest sensitive customer data from Internet service providers, phone companies and social media firms. It involves compromising email accounts and websites tied to police departments and government agencies, and then sending unauthorized demands for subscriber data while claiming the information being requested can't wait for a court order because it relates to an urgent matter of life and death.
https://krebsonsecurity.com/2022/03/hackers-gaining-power-of-subpoena-via-fake-emergency-data-requests/

Google Chrome Bug Actively Exploited as Zero-Day
The internet giant issued an update for the bug, which is found in the open-source V8 JavaScript engine. Google has updated its Stable channel for the desktop version of Chrome, to address a zero-day security vulnerability that's being actively exploited in the wild.
https://threatpost.com/google-chrome-bug-actively-exploited-zero-day/179161/

Shutterfly Discloses Data Breach After Conti Ransomware Attack
Online retail and photography manufacturing platform Shutterfly has disclosed a data breach that exposed employee information after threat actors stole data during a Conti ransomware attack.
https://informationsecuritybuzz.com/expert-comments/shutterfly-discloses-data-breach-after-conti-ransomware-attack/?_hsmi=78978938&_hsenc=p2ANqtz-_RLODS_kRuxig10kvn_gTvPL99pQMC3smPH7Nrkk-nOGXJyB84YTBmjk8kwyrIKaVLY9Ti1Qm4Me_UzjyVSimAHf1R8w

Malware Downloads From Harmless Word Document
You have heard it over and over and likely, your reaction is "Yes, I know. Don't enable macros in Microsoft documents or spreadsheets." Well, don't plug your ears or turn away, but you're about to hear it again…only for a new reason. Some who have less than great intentions have figured out a way to get those macros enabled using a seemingly harmless Microsoft Word document (.doc). So now, even if you have them disabled by default, someone has found a way to get those enabled for you; like it or not.
https://www.sosdailynews.com/news.jspx?&articleid=5EE745589E43C47A8C19033FFC8B3EBD&sx=26446

****

Hints & Tips plus Security Awareness

Optimize Your Third-Party Risk Management Program
Third Party Risk is a top concern for organizations as external partnerships and technologies become more complex, and cybercriminals become more sophisticated in attacks that exploit the supply chain. Webinar 4/5/22 2PM CDT
https://www.brighttalk.com/webcast/19315/535750?player-preauth=YhcVxdw%2FC%2BAShailFBcockOpP9SmDs66a%2Fw%2B3bamHPE%3D&utm_source=brighttalk-promoted&utm_medium=email&utm_term=Audience331561&utm_campaign=AUD-12415&utm_content=2022-03-24

Conducting a Risk Assessment
Risk Assessments are mandatory for passing your audits and protecting your business from serious threats. Not understanding the process can lead to complications and incomplete audits. Webinar 4/13/22 1PM CDT
https://www.brighttalk.com/webcast/18933/537038?player-preauth=YhcVxdw%2FC%2BAShailFBcockOpP9SmDs66a%2Fw%2B3bamHPE%3D&utm_source=brighttalk-promoted&utm_medium=email&utm_term=Audience335960&utm_campaign=AUD-12000&utm_content=2022-03-28

How Do I Demonstrate the ROI of My Security Program?
Security teams must shift away from saying no, align security initiatives to business goals, and report metrics in a way business leaders can understand.
https://www.darkreading.com/edge-ask-the-experts/how-do-i-demonstrate-the-roi-of-my-security-program?_mc=NL_DR_EDT_DR_daily_20220326&cid=NL_DR_EDT_DR_daily_20220326&elq_mid=109841&elq_cid=36315893&sp_eh=72a861290e89658b5ada8de6a8a9c12b185e8e45329503691618392cbd15751b

Unlocking the Mystery of VPN's: Why You Need One
You may have heard about VPN's (Virtual Private Network) more often lately, even popping up in TV ads for VPN service providers. What's behind the sudden surge of VPN's and why would you want or need one? For those who use WiFi internet connections at home or work, for shopping, banking, or just plain fun, VPN's provide a layer of security that WiFi cannot. Although free public WiFi is found most everywhere, it's long been a favorite for hackers because there is virtually no online security offered when using it.
https://www.sosdailynews.com/news.jspx?&articleid=14C2195807D26E1B4F834A3AC5193FC7&sx=26446

****

News & Views

Could Gaming Close the Cyberskills Gap?
Wicked6 has the look and feel of an e-sports competition. There are a variety of games and skill levels for the competitors, and lots of action to follow for the spectators. You can even buy some pretty sweet swag.
https://www.darkreading.com/edge-articles/could-gaming-close-the-cyberskills-gap-?_mc=NL_DR_EDT_DR_daily_20220326&cid=NL_DR_EDT_DR_daily_20220326&elq_mid=109841&elq_cid=36315893&sp_eh=72a861290e89658b5ada8de6a8a9c12b185e8e45329503691618392cbd15751b

Researchers Hack Remote Keyless System of Honda Vehicles
The attack is possible because of a vulnerability in the car manufacturer's remote keyless system (CVE-2022-27254) that appears to impact all Honda Civic (LX, EX, EX-L, Touring, Si, and Type R) models between 2016 and 2020.
https://www.securityweek.com/researchers-hack-remote-keyless-system-honda-vehicles

****

"Ctrl -F" for The Board

How Pen Testing Gains Critical Security Buy-in and Defense Insight
Sometimes stepping into hackers' shoes is the only way to truly guard against them. That's why so many organizations include penetration testing in their cybersecurity posture. In fact, 85% of cybersecurity pros reporting that they pen test at least once a year.
https://www.darkreading.com/edge-articles/how-pen-testing-gains-critical-security-buy-in-and-defense-insight?_mc=NL_DR_EDT_DR_daily_20220326&cid=NL_DR_EDT_DR_daily_20220326&elq_mid=109841&elq_cid=36315893&sp_eh=72a861290e89658b5ada8de6a8a9c12b185e8e45329503691618392cbd15751b

HR Alone Can't Solve the Great Resignation
Here's how IT teams and decision-makers can step up to support the workforce. Creating a culture of feedback and introducing automation can mitigate burnout, inspire employees, and reduce turnover. The Great Resignation has one clear cause: employee burnout. In a recent survey, more than half of employees said they feel burned out, and more than two-thirds say the feeling has increased since the onset of the pandemic. Given these common sentiments, it's no surprise workers are quitting their jobs in droves in search of (what they hope are) greener pastures at other companies.
https://www.darkreading.com/careers-and-people/hr-alone-can-t-solve-the-great-resignation-?_mc=NL_DR_EDT_DR_daily_20220328&cid=NL_DR_EDT_DR_daily_20220328&elq_mid=109846&elq_cid=36315893&sp_eh=72a861290e89658b5ada8de6a8a9c12b185e8e45329503691618392cbd15751b

Cyber (re)insurers limit exposure to ransomware
Ransomware continues to shape the cyber risk landscape, explained Dwic roundtable panellists
https://www.insurancetimes.co.uk/news/cyber-reinsurers-limit-exposure-to-ransomware/1440718.article?_hsmi=203237365&_hsenc=p2ANqtz-8F73MVzwmJw-HHODpmNGkrZoXUbF2LJibjZKiS49i0LmaRp8ZNmKxw-qwEE_Z6O4OgFLkSS4wSU5roSFoiv0R-Ijv_vw

Questions
Contact FIPCO’s Rob Foxx at 800-722-3498 ext. 249 or email FIPCO IT Services for more information.

"Make Security Part of You and Your Institution's DNA!"

Threat Intelligence Newsletter: April 8, 2022

FIPCO®
IT Audit
Round Table
Discussions

If you would like to host an event, please contact: Ngina Ali

Upcoming Threat Intelligence Peer Group Discussions
None available at the current time

****

Alerts & Warnings

Apple's Zero-Day Woes Continue
Two new bugs in macOS and iOS disclosed this week add to the growing list of zero-days the company has rushed to patch over the past year. Apple's expanding footprint in enterprise organizations appears to have made its technologies a growing focus area for security researchers.
https://www.darkreading.com/vulnerabilities-threats/apple-s-zero-day-woes-continue?_mc=NL_DR_EDT_DR_daily_20220404&cid=NL_DR_EDT_DR_daily_20220404&elq_mid=109954&elq_cid=36315893&sp_eh=72a861290e89658b5ada8de6a8a9c12b185e8e45329503691618392cbd15751b

Beware of These 5 Tax Scams
Fraudsters are out in full force as Tax Day approaches. Use this list to keep your company's employees informed on what to watch out for this year. Tax Day may be on April 18, but cybercriminals and scammers have been at it for the past several months trying to dupe taxpayers.
https://www.darkreading.com/remote-workforce/5-tax-scams-to-watch-out-for-before-tax-day-?_mc=NL_DR_EDT_DR_daily_20220405&cid=NL_DR_EDT_DR_daily_20220405&elq_mid=109979&elq_cid=36315893&sp_eh=72a861290e89658b5ada8de6a8a9c12b185e8e45329503691618392cbd15751b

Notification of Engaging in Crypto-Related Activities
All FDIC-supervised institutions that intend to engage in, or that are currently engaged in, any activities involving or related to crypto assets (also referred to as "digital assets") should notify the FDIC. FDIC-supervised institutions are requested to provide information described in this letter. The FDIC will review the information and provide relevant supervisory feedback.
https://www.fdic.gov/news/financial-institution-letters/2022/fil22016.html?source=govdelivery&utm_medium=email&utm_source=govdelivery#letter

Russia threatens ‘grave consequences’ over Cyberattacks, blames U.S.
Russia signaled Tuesday that it’s becoming increasingly aggravated by cyberattacks targeting the country, which have come from numerous directions in response to its unprovoked assault on Ukraine. In a statement, reported on by outlets including Reuters and the Russian news agency Tass, Russia’s foreign ministry pledged to uncover the sources of the recent “cyber aggression” and hold those sources responsible.
https://venturebeat.com/2022/03/29/russia-threatens-grave-consequences-over-cyberattacks-blames-u-s/

U.S. warned firms about Russia’s Kaspersky software day after invasion
The U.S. government began privately warning some American companies the day after Russia invaded Ukraine that Moscow could manipulate software designed by Russian cybersecurity company Kaspersky to cause harm, according to a senior U.S. official and two people familiar with the matter.
https://www.reuters.com/technology/exclusive-us-warned-firms-about-russias-kaspersky-software-day-after-invasion-2022-03-31/

TrickBot Malware Adds New Tricks To Evade Antivirus Solutions
Word to the wise: If you’re keeping tabs on TrickBot malware and look away for a hot minute, new additions to its arsenal could happen. In this latest version, TrickBot’s operators added antivirus evasion techniques to its long list of cyber-tricks. With a history of 100 identified variations to date, how TrickBot evolves next has experts wondering what tomorrow’s new tricks will bring. TrickBot first earned its notorious reputation as a banking trojan and evolved over time to its current iteration.
https://www.sosdailynews.com/news.jspx?&articleid=F4F50E01E55AF8745029D226A324A3BC&sx=26446

****

Hints & Tips plus Security Awareness

Incident Response Webinar | Best Practices to Prevent, Detect, & Respond
Businesses are often ill-prepared to deal with ransomware incidents. Especially if an attacker has masqueraded as a privileged user—you may not know they’re doing any damage until it’s too late. Every organization needs a well-defined, battle-tested incident response plan to combat ransomware. In this webinar, ethical hacker and Chief Security Scientist, Joseph Carson, will help you build one.
Webinar Wednesday, Apr. 13, 2022 Noon CST
https://www.databreachtoday.com/webinars/live-webinar-key-steps-ransomware-incident-response-plan-w-3849?user_email=rfoxx@fipco.com&rf=2022-04-02__ACQ_DBT__Slot6_WEB3849&mkt_tok=MDUxLVpYSS0yMzcAAAGDidLK9pj3eGujr81Dedcc-m43wz-2IEtkMrEKL5GW2LEa4FXcHXKolkjNa-p9UONPY8BQs-gfNVIDN5VxkUWRR_6LLdiRDhdl8StenV6pnMzL7krtOQ

INTO THE DARK WEB WHERE CROOKS AND SCAMMERS HANG OUT
Scam victims, consumer groups, and law enforcement agencies often talk about the dark web. But what exactly is it, and why might it be a dangerous place to visit? Put simply, the term refers to pages and content that aren't indexed by search engines. In other words, dark web pages won't show up when you google a particular topic.
https://scambusters.org/darkweb.html

****

News & Views

Results Overview: 2022 MITRE ATT&CK Evaluation – Wizard Spider and Sandworm Edition
To think about it simply, this MITRE ATT&CK Evaluation measured protection capabilities of 30 endpoint protection solutions. Two key measurements that are generated from the testing are Overall Detection and Overall Protection.
https://thehackernews.com/2022/04/results-overview-2022-mitre-att.html

5 tech workforce trends for 2022
Shifting job descriptions, hybrid work strategies and worker mobility will shape tech labor dynamics this year.
https://www.ciodive.com/news/tech-workforce-trends-2022-labor/617171/?utm_source=Sailthru&utm_medium=email&utm_campaign=Issue:%202022-04-07%20CIO%20Dive%20%5Bissue:40906%5D&utm_term=CIO%20Dive

Microsoft Details New Security Features for Windows 11
Security features to come include a TPM-like security processor for protecting artifacts that a computer uses during the secure boot-up process, as well as a control for blocking unsigned and untrusted apps.
https://www.darkreading.com/remote-workforce/microsoft-details-new-security-features-for-windows-11?_mc=NL_DR_EDT_DR_daily_20220406&cid=NL_DR_EDT_DR_daily_20220406&elq_mid=109989&elq_cid=36315893&sp_eh=72a861290e89658b5ada8de6a8a9c12b185e8e45329503691618392cbd15751b

****

"Ctrl -F" for The Board

Companies Going to Greater Lengths to Hire Cybersecurity Staff
Employers are desperately seeking to fill cybersecurity positions. The number of available cybersecurity jobs coupled with accelerated attrition due to the Great Resignation has led to companies offering ridiculously high salaries, a bevy of benefits, and free training and certifications to woo candidates. Even so, the candidate pool is limited. Employers are exploring ways to help applicants fill in the gaps in their experience so that they can be hired.
https://www.darkreading.com/edge-articles/accelerating-onto-the-on-ramp-for-cybersecurity-jobs?_mc=NL_DR_EDT_DR_daily_20220402&cid=NL_DR_EDT_DR_daily_20220402&elq_mid=109944&elq_cid=36315893&sp_eh=72a861290e89658b5ada8de6a8a9c12b185e8e45329503691618392cbd15751b

Questions
Contact FIPCO's Rob Foxx at 800-722-3498 ext. 249 or email FIPCO IT Services for more information.

"Make Security Part of You and Your Institution's DNA!"

Threat Intelligence Newsletter: April 14, 2022

FIPCO®
IT Audit
Round Table
Discussions

If you would like to host an event, please contact: Ngina Ali

Upcoming Threat Intelligence Peer Group Discussions
None available at the current time

****

Alerts & Warnings

Thousands of Android users downloaded this password-stealing malware disguised as anti-virus from Google Play
Cybersecurity researchers at Check Point have identified six different fraudulent anti-virus applications that have since been removed from the Google Play store. The applications are parading as tools that help to protect users from cybercrime, however, they actually deliver malware to steal passwords, bank details, and other personal information.
https://www.zdnet.com/article/these-android-users-wanted-to-protect-their-phones-from-hackers-instead-they-downloaded-malware/

Did you get a text from your own number? That's a scam
Scammers are always thinking up ways to put a new spin on their criminal tricks. This time, they're sending spam texts to you — from your own phone number. They've changed (spoofed) the caller ID to look like they're messaging you from your number, but the shock of getting a text from yourself is bound to get your attention — which is what they're after.
https://consumer.ftc.gov/consumer-alerts/2022/04/did-you-get-text-your-own-number-thats-scam?utm_source=govdelivery

New Octo Banking Trojan Spreading via Fake Apps on Google Play Store
A number of rogue Android apps that have been cumulatively installed from the official Google Play Store more than 50,000 times are being used to target banks and other financial entities. The rental banking trojan, dubbed Octo, is said to be a rebrand of another Android malware called ExobotCompact, which, in turn, is a "lite" replacement for its Exobot predecessor, Dutch mobile security firm ThreatFabric said in a report shared with The Hacker News.
https://thehackernews.com/2022/04/new-octo-banking-trojan-spreading-via.html?_m=3n%2e009a%2e2713%2eod0ao445rz%2e1qc4

BUYING CHEAP ONLINE COURSES COULD LAND YOU IN COURT
Online courses have never been so cheap and easy to access, and with many of us spending more time at home, website classes and streaming tuition are enjoying a huge surge in popularity. But you may be shocked to learn that much of what's on offer online are illegal copies, sales of which are threatening the livelihood of providers and could be putting buyers at risk.
https://scambusters.org/onlinecourse.html

Scan This: There's Danger in QR Codes
The same qualities that make QR codes so valuable make them a legitimate threat to enterprise (and personal) cybersecurity.
https://www.darkreading.com/omdia/scan-this-there-s-danger-in-qr-codes?_mc=NL_DR_EDT_DR_daily_20220411&cid=NL_DR_EDT_DR_daily_20220411&elq_mid=110060&elq_cid=36315893&sp_eh=72a861290e89658b5ada8de6a8a9c12b185e8e45329503691618392cbd15751b

****

Hints & Tips plus Security Awareness

Windows Autopatch Aims to Make Patch Tuesday 'Just Another Tuesday' for Enterprises
Microsoft this week announced Windows Autopatch, a new automatic updates service for Windows 10 and 11 Enterprise E3 customers that will manage all software, firmware, driver, and enterprise app updates. The new feature ensures that Windows and Office products on enrolled endpoints are automatically updated, at no additional cost, helping admins more easily manage the security updates rolled out on the second Tuesday of every month.
https://www.securityweek.com/windows-autopatch-aims-make-patch-tuesday-just-another-tuesday-enterprises

Facebook Messenger's 'Dangerous' New Update—Why You Should Be Concerned
Despite multiple warnings that Meta's new update is a dangerous step in the wrong direction, the company announced plans to bring about end-to-end encryption to its Facebook Messenger and Instagram platforms. The plans were first announced in 2019, but have been plagued with technical challenges, meaning that the global rollout is not expected until 2023. Meta has battled regulatory policies to achieve its encryption goals.
https://www.forbes.com/sites/zakdoffman/2022/04/09/apple-iphone-google-android-and-windows-10-11-users-given-reason-to-quit-facebook-messenger/?sh=522becc5703f

****

News & Views

'The big one is coming': tech giant's stark Russia warning
The chief technology officer of $US50 billion ($67 billion) cybersecurity giant CrowdStrike has warned that Russia is still likely to launch large-scale cyberattacks against the West in response to sanctions and accusations of war crimes. Although doomsday predictions about Russian retaliation have so far proved

wide of the mark, Australian Mike Sentonas said cyberwarfare had still played a major role in the campaign, starting with early attempts by Moscow to destabilise its target Ukraine.
https://www.oodaloop.com/technology/2022/04/11/the-big-one-is-coming-tech-giants-stark-russia-warning/

Semiconductors expected to be in tight supply throughout 2022
Semiconductor producers don't expect shortages to improve in the near term as soaring demand and a backlog of orders constrains supply. Increasing use of chips in everything from automobiles to appliances means more businesses across industries are competing for limited supply. Suppliers are working furiously to ramp up production, announcing plans for new factories and billions of dollars worth of capital expenditures.
https://www.ciodive.com/news/semiconductor-tight-supply-shortage-2022/617563/?utm_source=Sailthru&utm_medium=email&utm_campaign=Issue:%202022-04-11%20CIO%20Dive%20%5Bissue:40977%5D&utm_term=CIO%20Dive

****

"Ctrl -F" for The Board

SEC Breach Disclosure Rule Makes CISOs Assess Damage Sooner
Rule Would Force Firms to Disclose 'Material Cybersecurity Incidents' in 4 Days. A proposed rule requiring publicly traded companies to disclose a breach within four days of deeming it material will force CISOs to determine the consequences of cyberattacks sooner
https://www.databreachtoday.com/sec-breach-disclosure-rule-makes-cisos-assess-damage-sooner-a-18875?rf=2022-04-11_ENEWS_ACQ_DBT__Slot1_ART18875&mkt_tok=MDUxLVpYSS0yMzcAAAGDuEZl89rmKLjtLSNf7St0zyR1js5wsAY9AkfU3yCesjzPK48_b65E9n0Lo-BQPOv8KtPVD-1w5EoYt9BuwPS5JUWdBzCcSaQI_V9j31LJ0gUAJVQX1Q

What You Need to Know About PCI DSS 4.0's New Requirements
The updated security payment standard's goal is to “address emerging threats and technologies and enable innovative methods to combat new threats” to customer payment information, the PCI Security Standards Council says.
https://www.darkreading.com/edge-articles/what-s-new-in-pci-dss-4-0-for-authentication-requirements-?_mc=NL_DR_EDT_DR_daily_20220409&cid=NL_DR_EDT_DR_daily_20220409&elq_mid=110039&elq_cid=36315893&sp_eh=72a861290e89658b5ada8de6a8a9c12b185e8e45329503691618392cbd15751b

2 years later: What's next in security for the pandemic-era workforce
Organizations can expect the return-to-work model to stress a corporate infrastructure that has languished in recent years. When businesses left the office in 2020, they left security strategies — long relied upon — behind.
https://www.ciodive.com/news/hybrid-cyber-security-strategy/622075/?utm_source=Sailthru&utm_medium=email&utm_campaign=Issue:%202022-04-14%20CIO%20Dive%20%5Bissue:41077%5D&utm_term=CIO%20Dive

Questions
Contact FIPCO’s Rob Foxx at 800-722-3498 ext. 249 or email FIPCO IT Services for more information.

"Make Security Part of You and Your Institution's DNA!"

Threat Intelligence Newsletter: April 22, 2022

If you would like to host an event, please contact: Ngina Ali

Upcoming Threat Intelligence Peer Group Discussions
None available at the current time

****

Alerts & Warnings

Cybercriminals Trick Victims into Transferring Funds to "Reverse" Instant Payments
Cybercriminals are targeting victims by sending text messages with what appear to be bank fraud alerts asking if the customer initiated an instant money transfer using digital payment applications (apps). Once the victim responds to the alert, the cybercriminal then calls from a number which appears to match the financial institution's legitimate 1-800 support number. Under the pretext of reversing the fake money transfer, victims are swindled into sending payment to bank accounts under the control of the cyber actors.
https://www.ic3.gov/Media/Y2022/PSA220414?_hsmi=210059059&_hsenc=p2ANqtz74wUJGmgIQXi8jeT2QoT0W_MJre5O_z6572C7a_y3bqLVABfE8etdLS-ebJgDbBVHa9JRXFwjPklRRTLzAXtAw7ptjg

Phishing emails targeting LinkedIn accounts are on the rise. Here's what to watch out for.
LinkedIn users are being urged to watch out for suspicious emails because the professional networking website is one of the most popular brands targeted by cyber criminals in phishing attacks. According to cybersecurity researchers at Check Point, who analysed phishing emails sent during the first three months of this year, over half of all phishing attacks (52%) attempted to leverage LinkedIn.
https://www.zdnet.com/article/phishing-emails-targeting-linkedin-accounts-are-on-the-rise-heres-what-to-watch-out-for/

Emergency Security Update For 3.2 Billion Google Chrome Users—Attacks Underway
Google has now released three emergency, out-of-band, security updates for the Chrome browser in as many weeks. What's more this one, like the first, is to fix a high-severity zero-day vulnerability that is already being exploited by attackers.
https://www.forbes.com/sites/daveywinder/2022/04/17/emergency-security-update-for-32-billion-google-chrome-users-attacks-underway/?sh=7698385236a5

TAX DEBT RELIEF SCAMMERS CHARGE $25,000 - FOR NOTHING!

Maybe you've never heard of the IRS tax debt relief program called Offer in Compromise (OIC). But scammers certainly have. They claim they can use it to have the IRS slash your tax debt to "pennies on the dollar" but they want you to pay upfront for their so-called service, which more than likely won't save you a dime.
https://scambusters.org/taxdebt.html

New Twitter Scam Involves Hacking Verified Accounts To Post Fake NFT Links

TheNextWeb reports that many hackers are taking over several verified accounts on the platform (the ones with the blue checkmark), all to post malicious links targeting the Moonbirds NFT project. The NFT project, as per the report, has raked in over $290 million in sales across platforms like Looksrare and OpenSea. In order to steal, the hackers hijack a verified Twitter account, tweet out a malicious link. This link is made to trick people into thinking they're going to get a Moonbirds NFT, they're just sending their crypto payments straight into the hackers' wallets.
https://www.techtimes.com/articles/274464/20220419/new-twitter-scam-involves-hacking-verified-accounts-post-fake-nft.htm?_hsmi=210059059&_hsenc=p2ANqtz-8CQbiIiU-VgdrSKdn0UTf9EOQkXN8AFVkp4igA5XMD_5GXl0OuvljE5KqKhj1nFb_ZrisJf5f05lI1wbtK5ifAHjRrNA

FBI Warns: Ransomware Victims Threatened By Attacker Phone Calls

The FBI recently released a warning about ransomware victims being threatened by phone calls from their attackers. These attack groups want their ransom demand paid and are willing to escalate their threat tactics to do it. One of the best answers for victims of such an attack is having data backup systems that restore data and entirely avoid paying a ransom. But now, the FBI finds businesses who do so are being threatened by phone calls from attackers who demand their ransom be paid, regardless of data backups. The FBI has known about these incidents since February of 2020, as part of monitoring the escalation of ransomware tactics. They believe these menacing phone calls are yet another example of escalating cyberthreats.
https://www.sosdailynews.com/news.jspx?&articleid=3A58DF3B96B2F0F83149B60CB767B7C4&sx=26446

Getting To Know You. New Android Spyware Infiltrates Mobile Messaging Apps

No one wants to think their smartphone is also a spying device, but a recent discovery found a new Android spyware is finding a home on mobile devices. This new spyware is the latest version since first being detected in 2017, and it has gone through many improvements since then. The spyware, called Android/SpyC23.A and the hacking group behind it, have a history of using surveillance malware and both are well-known to the cybersecurity community worldwide. The spy group behind the threat, APT-C-23, is known for spying efforts in the Middle East and experts believe it’s just a matter of time before it’s unleashed in the US and other locations.
https://www.sosdailynews.com/news.jspx?&articleid=D8E2BBCAD5F1A1ADCDC4871C1E9D001E&sx=26446

****

Hints & Tips plus Security Awareness

Creating a Security Culture Where People Can Admit Mistakes

In cybersecurity, user error is the symptom, not the disease. A healthy culture acknowledges and addresses the underlying causes of lapses.
https://www.darkreading.com/remote-workforce/creating-a-security-culture-where-people-can-admit-mistakes?_mc=NL_DR_EDT_DR_daily_20220419&cid=NL_DR_EDT_DR_daily_20220419&elq_mid=110188&elq_cid=36315893&sp_eh=72a861290e89658b5ada8de6a8a9c12b185e8e45329503691618392cbd15751b

Top Phishing Scams Continue To Improve And Grow
Much to our dismay, cybercrooks keep finding ways to better the phishing tools they have and find other ways to include new and sneakier methods of thievery. Organizations and individuals are targets and money, identities, credentials, and more are stolen from both every day. Even cyber-savvy users can get caught in phishing scams if they don’t pay close attention to the signs and signals that something isn’t quite right. Reviewing the most pervasive phishing scams is always recommended because an educated user can be the best tool against the many forms that phishing takes.
https://www.sosdailynews.com/news.jspx?&articleid=E958B090105A4D4984D7C7F238486A47&sx=26446

****

News & Views

Conti’s Ransomware Toll on the Healthcare Industry
Conti — one of the most ruthless and successful Russian ransomware groups — publicly declared during the height of the COVID-19 pandemic that it would refrain from targeting healthcare providers. But new information confirms this pledge was always a lie, and that Conti has launched more than 200 attacks against hospitals and other healthcare facilities since first surfacing in 2018 under its earlier name, “Ryuk.”
https://krebsonsecurity.com/2022/04/contis-ransomware-toll-on-the-healthcare-industry/

****

"Ctrl -F" for The Board

Curating Intentional Remote or Hybrid Workforce Policies
The COVID-19 pandemic has radically changed the way we work. What many businesses thought initially would be a months-long foray into remote work has now become the new norm. Increasingly remote or hybrid workforces present unprecedented challenges for employers.
https://www.brighttalk.com/webcast/19422/536673?player-preauth=YhcVxdw%2FC%2BAShailFBcockOpP9SmDs66a%2Fw%2B3bamHPE%3D&utm_source=brighttalk-promoted&utm_medium=email&utm_term=Audience342534&utm_campaign=AUD-12525&utm_content=2022-04-14

Security professionals are burned out. Here are 5 ways to help them.
Addressing the causes of burnout requires a top-down approach that better aligns security teams with the rest of the business. Data and expert insight shows there's no single cause to burnout. Lack of talent, too much time in meetings, too many manual tasks, too little training, the ever-changing threat landscape, and misalignment between security staff and company leadership all play a part.
https://www.cybersecuritydive.com/news/cyber-security-burn-out/621245/?utm_source=Sailthru&utm_medium=email&utm_campaign=Issue:%202022-04-19%20Cybersecurity%20Dive%20%5Bissue:41144%5D&utm_term=Cybersecurity%20Dive

Questions
Contact FIPCO’s Rob Foxx at 800-722-3498 ext. 249 or email FIPCO IT Services for more information.

"Make Security Part of You and Your Institution's DNA!"

Threat Intelligence Newsletter: April 29, 2022

If you would like to host an event, please contact: Ngina Ali

Upcoming Threat Intelligence Peer Group Discussions
None available at the current time

****

Alerts & Warnings

Cyber Conflict Overshadowed a Major Government Ransomware Alert
The FBI warns that ransomware targets are no longer predictably the biggest, richest organizations, and that attackers have leveled up to victimize organizations of all sizes. As the cyber dimension of the Ukraine conflict erupted, demonstrating the ungoverned and unstable nature of full-on cyberwar, a parallel ransomware alert from the US government got comparatively scant coverage. But it, too, merits attention.
https://www.darkreading.com/attacks-breaches/cyber-conflict-overshadowed-a-major-government-ransomware-alert-here-s-the-attention-it-deserves?_mc=NL_DR_EDT_DR_daily_20220427&cid=NL_DR_EDT_DR_daily_20220427&elq_mid=110339&elq_cid=36315893&sp_eh=72a861290e89658b5ada8de6a8a9c12b185e8e45329503691618392cbd15751b

HHS warns providers of 'exceptionally aggressive' ransomware group
The Hive group practices double extortion — demanding payment to free data it has encrypted while also threatening to release the unencrypted data publicly, often by selling it on "name and shame" dark web sites, according to the department.
https://www.cybersecuritydive.com/news/hhs-hive-ransomware-warning/622500/?utm_source=Sailthru&utm_medium=email&utm_campaign=Issue:%202022-04-25%20Cybersecurity%20Dive%20%5Bissue:41278%5D&utm_term=Cybersecurity%20Dive

Tenet says 'cybersecurity incident' disrupted hospital operations
According to WPTV, a local news outlet in Florida, telephone service and some IT systems at at least two Tenet hospitals in the West Palm Beach area went offline starting last Wednesday. The station reported

doctors and nurses were using paper charts and having to leave the hospitals to use their phones because they weren't functional inside.
https://www.cybersecuritydive.com/news/tenet-cyberattack-hospital-operations/622728/?utm_source=Sailthru&utm_medium=email&utm_campaign=Issue:%202022-04-27%20Cybersecurity%20Dive%20%5Bissue:41350%5D&utm_term=Cybersecurity%20Dive

T-Mobile Breached Again; Lapsus$ Behind the Attack
The U.S. telecom carrier T-Mobile has confirmed that the Lapsus$ ransomware group has breached its internal network by compromising employee accounts, according to multiple media reports. But, it says, hackers did not steal any sensitive customer or government information during the incident.
https://www.databreachtoday.com/t-mobile-breached-again-lapsus-behind-attack-a-18956?rf=2022-04-25_ENEWS_ACQ_DBT__Slot1_ART18956&mkt_tok=MDUxLVpYSS0yMzcAAAGEAF95JTtOeWqikQ8WJsgyGc-kH_hC3TnpX8QyCLA5ZbLbp4OcYOfDdxz_jl7AB52E1Haf_ZEoDZyRCFvsHpgKyoylUbcPtyixpbadjSQMYhaJmHdGA

A $600,000 Reminder to Not Save Your Passwords on Post-It Notes
A security analyst in Pinellas Park, Florida (about a 15-minute drive from our office in downtown St. Petersburg) was arrested for stealing well over half a million dollars in cryptocurrency from a client. But unlike many other crypto theft cases, this incident isn't the result of a complex cyber attack or even a phishing scam. The way this cybercriminal carried out this theft is far simpler to explain and even easier to prevent…
https://www.oodaloop.com/technology/2022/04/21/a-600000-reminder-to-not-save-your-passwords-on-post-it-notes/

****

Hints & Tips plus Security Awareness

3 Ways We Can Improve Cybersecurity
To better manage risks, companies can concentrate on resilience, sharing information to protect from cyber threats, and making the cybersecurity tent bigger by looking at workers with nontraditional skill sets. As we look ahead, there are many reasons for optimism in cybersecurity. Defenders are maturing in their approach, we're getting better at articulating cyber threats in the language of business risk, and we're continually improving cross-sector collaboration.
https://www.darkreading.com/vulnerabilities-threats/3-ways-we-can-improve-cybersecurity?_mc=NL_DR_EDT_DR_daily_20220422&cid=NL_DR_EDT_DR_daily_20220422&elq_mid=110274&elq_cid=36315893&sp_eh=72a861290e89658b5ada8de6a8a9c12b185e8e45329503691618392cbd15751b

Adversaries Look for 'Attackability' When Selecting Targets
A large number of enterprise applications are affected by the vulnerability in Log4j, but adversaries aren't just looking for the most common applications. They are looking for targets that are easier to exploit and/or have the biggest payoff.
https://www.darkreading.com/edge-threat-monitor/adversaries-look-for-attackability-when-selecting-targets?_mc=NL_DR_EDT_DR_daily_20220423&cid=NL_DR_EDT_DR_daily_20220423&elq_mid=110277&elq_cid=36315893&sp_eh=72a861290e89658b5ada8de6a8a9c12b185e8e45329503691618392cbd15751b

****

News & Views

OCC orders crypto bank Anchorage to revamp AML program
The Office of the Comptroller of the Currency (OCC) ordered Anchorage Digital Bank on Thursday to overhaul its anti-money laundering (AML) program and hire a Bank Secrecy Act (BSA) officer after the regulator said it found failures in the firm's AML and BSA compliance program.
https://www.bankingdive.com/news/occ-orders-crypto-bank-anchorage-to-revamp-aml-program/622558/?utm_source=Sailthru&utm_medium=email&utm_campaign=Issue:%202022-04-22%20Banking%20Dive%20%5Bissue:41175%5D&utm_term=Banking%20Dive

FTC action to stop illegal marketing robocalls
The Federal Trade Commission yesterday announced it has taken action against Voice over Internet Protocol (VoIP) service provider VoIP Terminator, Inc., a related company, and the firms' owner for assisting and facilitating the transmission of millions of illegal prerecorded telemarketing robocalls, including those they knew or should have known were scams, to consumers nationwide. Many of the calls originated overseas, and related to the COVID-19 pandemic, with the defendants allegedly failing to act as a gatekeeper to stop the calls from entering the country.
https://www.bankersonline.com/topstory/170664

10 Signs of a Good Security Leader
Strong leadership can lead to motivated and loyal employees. Here's what that looks like. These signs don't merely apply to security leaders — they apply to all leaders. So how can organizations know and appreciate when they have a strong security leader in place? Here are the top 10 signs.
https://www.darkreading.com/edge-articles/10-signs-of-a-good-security-leader?_mc=NL_DR_EDT_DR_daily_20220423&cid=NL_DR_EDT_DR_daily_20220423&elq_mid=110277&elq_cid=36315893&sp_eh=72a861290e89658b5ada8de6a8a9c12b185e8e45329503691618392cbd15751b

10 Signs of a Poor Security Leader
Weak leadership can demotivate and demoralize the security workforce. Here's what to look out for. Many businesses are concerned about attrition — and for good reason. Few fields feel this pressure more acutely than the security field. While companies cannot control the tight labor market, they can control some of the factors that cause employees to leave.
https://www.darkreading.com/edge-articles/10-signs-of-a-poor-security-leader

****

"Ctrl -F" for The Board

Merchants prioritize fraud prevention as fraud costs, impact to businesses rise
While the nature of fraud-related challenges stayed fairly consistent over the past year, the severity each challenge presents to merchants has increased. In particular, identifying and responding to emerging fraud attacks, updating fraud risk models and effectively managing fraud while expanding into new sales channels have become markedly more difficult for merchants to overcome.
https://www.cybersecuritydive.com/spons/merchants-prioritize-fraud-prevention-as-fraud-costs-impact-to-businesses/620499/

Banks face ‘tight deadline’ under new cyber notification rule

Starting May 1, banks in the U.S. will be required to notify their primary federal regulator of a cybersecurity incident within 36 hours, a tight turnaround time that could be challenging for some institutions.

https://www.cybersecuritydive.com/news/banks-cyber-reporting-rule/622486/?utm_source=Sailthru&utm_medium=email&utm_campaign=Issue:%202022-04-22%20Cybersecurity%20Dive%20%5Bissue:41260%5D&utm_term=Cybersecurity%20Dive

Questions

Contact FIPCO’s Rob Foxx at 800-722-3498 ext. 249 or email FIPCO IT Services for more information.

"Make Security Part of You and Your Institution's DNA!"

Threat Intelligence Newsletter: May 9, 2022

FIPCO® IT Audit Round Table Discussions

If you would like to host an event, please contact: Ngina Ali

Upcoming Threat Intelligence Peer Group Discussions
None available at the current time

****

Alerts & Warnings

Attacker Breach 'Dozens' of GitHub Repos Using Stolen OAuth Tokens
GitHub shared the timeline of breaches in April 2022, this timeline encompasses the information related to when a threat actor gained access and stole private repositories belonging to dozens of organizations. GitHub revealed details tied to last week's incident where hackers, using stolen OAuth tokens, downloaded data from private repositories. "We do not believe the attacker obtained these tokens via a compromise of GitHub or its systems because the tokens in question are not stored by GitHub in their original, usable formats," said Mike Hanley, chief security officer, GitHub.
https://threatpost.com/github-repos-stolen-oauth-tokens/179427/

Intuit Sued After Hackers Stole Crypto from Customers
Intuit customers sued the company after its email marketing service was hacked. A class-action lawsuit was filed against Intuit, a software company, after its email marketing service was hacked and cyber criminals stole cryptocurrencies from Trezor users. The hackers deployed a phishing attack on March 26 and gained entry into the crypto wallets that are sold by Trezor, a Czech company, according to a federal lawsuit filed in the U.S. District Court, Northern District of California in San Jose, California.
https://www.thestreet.com/investing/cryptocurrency/intuit-sued-after-hackers-stole-crypto-from-customers

As If Stealing Your $$ Isn't Enough, BRATA Malware Wipes Out Your Data Too
Attacks by BRATA financial malware have finally made their way to the U.S., among other countries. Victims of the improved BRATA (Brazilian Remote Access Android) malware are finding a cruel twist to its

attacks. BRATA not only steals a victim’s money, but cleans their device of any personal data stored there. It’s a mean-spirited component of this trojan malware, but BRATA criminals might add “it’s nothing personal.”
https://www.sosdailynews.com/news.jspx?&articleid=C0A6F35DF62E643B9E18CBDD72CA7431&sx=26446

Social Media Quizzes Make You The Villain And The Victim
If you want your product to get any type of attention, you can bet that social media is a place to put it. You know that game Wordle that’s all the rage? You likely hadn’t heard about it until your friends started sharing their results on social media. And when you see one of those cute little quizzes that compares you to a Disney Villain, you might be giving up more than your latest Wordle score, should you decide to play that game.
https://www.sosdailynews.com/news.jspx?&articleid=1587E570932E0C4D4CB84DFF66F04EF4&sx=26446

****

Hints & Tips plus Security Awareness

What To Know About The Top 15 Exploited Vulnerabilities
A recent joint cybersecurity advisory from U.S and allied cybersecurity authorities identified the top exploited vulnerabilities and exposures (CVEs) of last year. Out of the 15 vulnerabilities that made the list, it is interesting to see 11 of the 15 are from 2021. There are 4 other vulnerabilities identified in 2020 and earlier that are routinely exploited. Read our post to see the complete list of vulnerabilities, plus what you need to know about them to help reduce your organization's cyber risk.
https://media.defense.gov/2022/Apr/27/2002984949/-1/-1/1/JOINT_CSA_2021_ROUTINELY_EXPLOITED_CVES_20220427.PDF?utm_medium=email&_hsmi=212006767&_hsenc=p2ANqtz--B2IbD-F41YuADV9lGvvAsL2sQItbL-gyfXHsrsMhtjYfXwhWvWLEA_8fo-EjWMXHOVdqKOfJcbw_5UEJEMcT3TH85xA&utm_content=212006767&utm_source=hs_email

You Can Now Ask Google to Remove Your Phone Number, Email or Address from Search Results
Google said this week it is expanding the types of data people can ask to have removed from search results, to include personal contact information like your phone number, email address or physical address. The move comes just months after Google rolled out a new policy enabling people under the age of 18 (or a parent/guardian) to request removal of their images from Google search results.
https://krebsonsecurity.com/2022/04/you-can-now-ask-google-to-remove-your-phone-number-email-or-address-from-search-results/

Massive New Security Update For 3.2 Billion Chrome Users Confirmed
Google Chrome security has experienced a busy past few weeks and there is no sign of slowing down. Just days after two emergency fixes for vulnerabilities being exploited in the wild and a record number of Chromium zero-days across 2021 was announced, Google has released another massive security update that applies to billions of Chrome users. The new update that will take Google Chrome to version 101.0.4951.41 fixes more than 30 security vulnerabilities across Windows, Mac, and Linux devices.
https://www.oodaloop.com/briefs/2022/05/02/massive-new-security-update-for-3-2-billion-chrome-users-confirmed/

6 Best Data Security Practices You Can Start Today

Given the dramatic increases in the volume and frequency of data theft due to breaches and the increased threat of cyberattacks resulting from current conflicts, organizations worldwide are prioritizing tactical and strategic efforts to shore up their data security. Here are six best practices you can implement right now to improve your security posture and protect the sensitive personal data for which you are responsible.
https://www.imperva.com/blog/6-best-data-security-practices-you-can-start-today/?_hsmi=78978938&_hsenc=p2ANqtz-_lWyIXUZZoiJbf-RLlTX6K1ab2256zG2aWt4i_Dpg_Dn5FHOOOn84dgKBFFeFihjR_PGPaApH-gXjrshqGZCUJj41q7A

NIST Releases Updated Cybersecurity Guidance for Managing Supply Chain Risks

The National Institute of Standards and Technology (NIST) on Thursday released an updated cybersecurity guidance for managing risks in the supply chain, as it increasingly emerges as a lucrative attack vector. "It encourages organizations to consider the vulnerabilities not only of a finished product they are considering using, but also of its components — which may have been developed elsewhere — and the journey those components took to reach their destination," NIST said in a statement.
https://thehackernews.com/2022/05/nist-releases-updated-guidance-for.html?_m=3n%2e009a%2e2732%2eod0ao445rz%2e1qso

****

News & Views

Directorate of Enforcement seizes $725 million from Xiaomi India

India's anti-money laundering agency, the Directorate of Enforcement (ED), has seized assets worth ₹5551.27 crore (around $725 million) from Xiaomi India after it found the company had broken foreign exchange laws. In 2014, the company began operations in India and is alleged to have commenced the illegal activity in 2015. The ED claimed that Xiaomi India remitted foreign currency to three off-shore entities under the guise of royalties, with one of those including a company within the Xiaomi group, whilst the others were US-based.
https://www.zdnet.com/home-and-office/networking/directorate-of-enforcement-seizes-725-million-from-xiaomi-india/

Mobile health apps leak sensitive data through APIs, report finds

All of the apps were found to be vulnerable to API attacks, and some allowed access to electronic health records (EHRs). The 30 apps collectively expose 23 million mobile health users to attacks, Knight reported. Of the 30 apps tests, 77% contained hardcoded API keys, of which some do not expire, according to the report, and 7% had hardcoded usernames and passwords.
https://www.fiercehealthcare.com/tech/mobile-health-apps-leak-sensitive-data-through-apis-report-finds

****

"Ctrl -F" for The Board

What cyber insurance companies want from clients
Insurers evaluate how a company leverages technology and what internal standards are in place to manage risk. Cyberattacks are a fact of life. Every organization — in fact, anyone with an internet account — has been targeted in some manner, from a phishing email to DDoS website attacks to malicious account takeovers. Just as a company purchases insurance to protect from physical theft and other potential loss and damages, organizations need to add protection against the financial aftermath of a cyberattack.
https://www.ciodive.com/news/cyber-insurance-IT-demands/622966/?utm_source=Sailthru&utm_medium=email&utm_campaign=Issue:%202022-05-02%20CIO%20Dive%20%5Bissue:41425%5D&utm_term=CIO%20Dive

Majority of banks paid ransom for cyberattacks last year
Cloud computing company VMware says its most recent report has found a drastic increase of destructive cyberattacks, with 74% of businesses interviewed experiencing one or more ransomware attacks in the last year. Its report, 2022 Modern Bank Heist, is an annual look into the experiences of top financial and security leaders regarding cybercriminal cartels and offers insights on the shift of defensive methods.
https://securitybrief.co.nz/story/majority-of-banks-paid-ransom-for-cyberattacks-last-year

Questions
Contact FIPCO's Rob Foxx at 800-722-3498 ext. 249 or email FIPCO IT Services for more information.

"Make Security Part of You and Your Institution's DNA!"

Threat Intelligence Newsletter: May 20, 2022

FIPCO®
IT Audit
Round Table
Discussions

If you would like to host an event, please contact: Ngina Ali

Upcoming Threat Intelligence Peer Group Discussions
None available at the current time

****

Alerts & Warnings

College Shuts Down Due to Cost of Ransomware Attack
The "financial burden" of a December 2021 cyberattack and the aftereffects of the COVID-19 pandemic forced 157-year-old Lincoln College in Illinois to cease operations on Friday, its president, David Gerlach, says. The decision to terminate operations, which was decided in a vote by the board of trustees, has been sent to the Illinois Department of Higher Education and the Higher Learning Commission, Gerlach says.
https://www.databreachtoday.com/college-shuts-down-due-to-cost-ransomware-attack-a-19051?rf=2022-05-11_ENEWS_ACQ_DBT__Slot1_ART19051&mkt_tok=MDUxLVpYSS0yMzcAAAGEUsVFTV0UaL6S8wRC7tNKK7t2drE36EV7814eL8m_QuLIgKCRJNQ7tVS5Qn3GkLBw0X4xF1UQY-bE_Dxh4E1gBfn706394QJstkHOc7nLEJ5iM4lRdg

DEA Investigating Breach of Law Enforcement Data Portal
The U.S. Drug Enforcement Administration (DEA) says it is investigating reports that hackers gained unauthorized access to an agency portal that taps into 16 different federal law enforcement databases. KrebsOnSecurity has learned the alleged compromise is tied to a cybercrime and online harassment community that routinely impersonates police and government officials to harvest personal information on their targets.
https://krebsonsecurity.com/2022/05/dea-investigating-breach-of-law-enforcement-data-portal/

British Man Charged With Hacking US Bank Computers, Stealing Millions
UK citizen Idris Dayo Mustapha, 32, faces criminal charges including unauthorized computer intrusion, securities fraud, wire fraud, and other crimes for hacking into US banks, resulting in $5 million in loses. The 10-count complaint was made public yesterday and revealed that Mustapha used phishing tactics and other means to obtain user credentials between January 2011 and March 2018. The complaint also stated that Mustapha gained access to US-based computers, including those belonging to financial institutions, to steal money from online bank accounts and securities brokerage accounts.
https://www.infosecurity-magazine.com/news/british-charged-hacking-us-bank/

Cryptocurrency hype spawns email attacks, FBI says
An increasing number of recent business email compromise complaints involve the use of cryptocurrency, according to the FBI's Internet Crime Complaint Center. Business email compromise scams continue to grow and evolve, according to the FBI's Internet Crime Complaint Center. Between July 2019 and December 2021, IC3 reported a 65% increase in global exposed losses, partly due to the increase in virtual business as a result of the pandemic.
https://gcn.com/cybersecurity/2022/05/cryptocurrency-hype-spawns-email-attacks-fbi-says/366705/

Kaspersky uncovers fileless malware inside Windows event logs
Kaspersky has made an unprecedented discovery that could have serious consequences for Windows operating systems and its users. Kaspersky released information about its findings on May 4, detailing how hackers were able to place shellcode into Windows event logs for the first time ever. This means that threat actors were able to hide Trojans in the documents as file-less malware. The malware campaign leveraged techniques such as commercial penetration testing suites and anti-detection wrappers, according to Kaspersky. There were two Trojans deployed for the last stage, which allowed it to gain further access into the system. Kaspersky explained how the Trojans were delivered via two different methods, HTTP network communications and engagement with the named pipes.
https://www.oodaloop.com/briefs/2022/05/10/kaspersky-uncovers-fileless-malware-inside-windows-event-logs/

BBB Scam Alert: How to spot a phony discount when buying CBD online
Cannabidiol (CBD), an active ingredient of cannabis, is now legal in many US states and Canadian provinces. If you want to try it, watch out for scams. BBB Scam Tracker received dozens of reports from frustrated consumers who thought they bought discounted CBD online but ended up with hundreds of dollars in credit card charges.
https://www.bbb.org/article/scams/24164-bbb-scam-alert-trying-cbd-watch-out-for-tricky-free-trial-offers?utm_source=newsletter&utm_medium=email&utm_content=See%20the%20full%20article%20for%20victim%20reports&utm_campaign=scam-alert

Spoofing SaaS Vanity URLs for Social Engineering Attacks
Many SaaS applications offer what's known as vanity URLs — customizable web addresses for landing pages, file-sharing links, etc. While vanity URLs provide a custom, easy-to-remember link, Varonis Threat Labs discovered that some applications do not validate the legitimacy of the vanity URL's subdomain but instead only validate the URI.
https://www.varonis.com/blog/url-spoofing

US, allies blame Russia for Viasat cyberattack
The Five Eyes and other EU authorities linked Russia to a series of web defacement, DDoS and destructive wiper attacks in the weeks leading up to the Ukraine invasion. The EU and U.K. set off a series of formal condemnations that blamed Russia for the wave of malicious attacks preceding the Ukraine invasion. U.S. and European officials had warned for months about the potential use of cyber as means of asymmetric

attack against military, government and critical infrastructure targets in Ukraine as well as Western allies linked the conflict.
https://www.cybersecuritydive.com/news/viasat-cyber-russia-satellite/623560/?utm_source=Sailthru&utm_medium=email&utm_campaign=Newsletter%20Weekly%20Roundup:%20Cybersecurity%20Dive:%20Daily%20Dive%2005-14-2022&utm_term=Cybersecurity%20Dive%20Weekender

When Your Smart ID Card Reader Comes With Malware
Millions of U.S. government employees and contractors have been issued a secure smart ID card that enables physical access to buildings and controlled spaces, and provides access to government computer networks and systems at the cardholder's appropriate security level. But many government employees aren't issued an approved card reader device that lets them use these cards at home or remotely, and so turn to low-cost readers they find online. What could go wrong?
https://krebsonsecurity.com/2022/05/when-your-smart-id-card-reader-comes-with-malware/

Vulnerabilities found in Bluetooth Low Energy gives hackers access to numerous devices
Cybersecurity researchers at NCC Group have found a critical flaw in Bluetooth Low Energy (BLE) receivers. The flaw may grant cyber criminals access to a range of devices, including phones, laptops, cars, and houses. NCC Group details how BLE uses proximity to authenticate that the user is within a close distance to the device. As part of NCC Group's research, it was able to fake this proximity. Therefore, the flaw does not only affect organizations and businesses, but the average consumer as well. The issue may not be easily patchable either, and may affect millions of people.
https://www.oodaloop.com/briefs/2022/05/18/vulnerabilities-found-in-bluetooth-low-energy-gives-hackers-access-to-numerous-devices/

****

Hints & Tips plus Security Awareness

Why iPhone Owners Should Consider Using an Antivirus
When they unleash their campaigns, cybercriminals don't differentiate between device type or OS. For example, FluBot operators – who typically target Android users – will switch to platform-agnostic methods like phishing if they catch iOS users in their net. Security has become an essential aspect for all mobile netizens out there, regardless of phone model. In this post, we take a look at three distinct threats iPhone users face every day to understand why it's important to use a dedicated security solution.
https://www.bitdefender.com/blog/hotforsecurity/why-iphone-owners-should-consider-using-an-antivirus/?_hsmi=78978938&_hsenc=p2ANqtz-8VJqGuMKdqYOrk7xY8hoC7wWS8JPxpcmomRjTWYX2dtLjlpr95x-E_1SNZ2okTMXRx6Dk7BsiYRd-y5XWVqRCQpI8bIw

Vanity URLs Could Be Spoofed for Social Engineering Attacks
Attackers could abuse the vanity subdomains of popular cloud services such as Box.com, Google, and Zoom to mask attacks in phishing campaigns. Vanity links created by companies to add their brand to well-known cloud services could become a useful vector for phishing attacks and a way to better fool victims, researchers warn.
https://www.darkreading.com/cloud/vanity-urls-could-be-spoofed-for-social-engineering-attacks?_mc=NL_DR_EDT_DR_daily_20220512&cid=NL_DR_EDT_DR_daily_20220512&elq_mid=110651&elq_cid=36315893&sp_eh=72a861290e89658b5ada8de6a8a9c12b185e8e45329503691618392cbd15751b

NIST Issues Guidance for Addressing Software Supply-Chain Risk

Amid ongoing software supply-chain jitters, the US' top tech division is offering a finalized, comprehensive cybersecurity control framework for managing risk. The National Institute of Standards and Technology (NIST) has updated its cybersecurity guidance for addressing software supply-chain risk, offering tailored sets of suggested security controls for various stakeholders. View NIST publication here https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161r1.pdf Software supply-chain attacks rocketed to the top of the enterprise worry list last year as the SolarWinds and Log4Shell incidents sent shockwaves through the IT security community.
https://www.darkreading.com/risk/nist-guidance-software-supply-chain-risk?_mc=NL_DR_EDT_DR_daily_20220506&cid=NL_DR_EDT_DR_daily_20220506&elq_mid=110541&elq_cid=36315893&sp_eh=72a861290e89658b5ada8de6a8a9c12b185e8e45329503691618392cbd15751b

Live Masterclass | The Cost of Password Authentication Failures

Ponemon Institute's recent report highlights that most organizations do not have an enterprise-wide strategy for reducing the risk of authentication failures. So, what happens to the significant cost to businesses when organizations are unable to verify user ID due to weaknesses in the authentication processes? Tuesday June 8th 1:00 PM CST
https://www.databreachtoday.com/webinars/live-masterclass-cost-password-authentication-failures-w-3582?user_email=rfoxx@fipco.com&rf=2022-05-17_ENEWS_ACQ_DBT___Slot5_WEB3582&mkt_tok=MDUxLVpYSS0yMzcAAAGEcat0fXeV6Pj6xgSK4nAtImSfDDlXdPcIrG0Lqj_759kedMhn441JSqBH8oGcA8fRDpq-YenEDQYO5z6OXdbMtkrV-BIU1BvunNXJre2kjAYF0hsIKw

How to Protect Your Data When Ransomware Strikes

Ransomware is not a new attack vector. In fact, the first malware of its kind appeared more than 30 years ago and was distributed via 5.25-inch floppy disks. To pay the ransom, the victim had to mail money to a P.O. Box in Panama. Fast forward to today, affordable ransomware-as-a-service (RaaS) kits are available on the dark web for anyone to purchase and deploy and attackers have an infinite number of channels available to them to infiltrate organizations as a result of reliance on cloud and mobile technologies.
https://thehackernews.com/2022/05/how-to-protect-your-data-when.html?_m=3n%2e009a%2e2742%2eod0ao445rz%2e1r28

****

News & Views

Enterprise Mobile Threats

NIST's National Cybersecurity Center of Excellence released an infographic identifying 12 enterprise mobile threats including the installation of unauthorized applications, the remote misuse of device sensors, device compromise by brute-force attacks and more. Download the infographic.
https://www.nccoe.nist.gov/sites/default/files/2022-04/12-MobileThreats%28FINAL%29.pdf?utm_source=eloqua&utm_medium=email&utm_campaign=riskcyberbulletin&utm_content=RiskCyber-20220509
Access additional resources, including the Mobile Threat Catalog, via the NCCoE's Mobile Device Security page.
https://www.nccoe.nist.gov/mobile-device-security?utm_source=eloqua&utm_medium=email&utm_campaign=riskcyberbulletin&utm_content=RiskCyber-20220509

Colonial Pipeline faces nearly $1M in penalties as federal regulator discloses violations

The Transportation Department's pipeline safety regulator scrutinized control room management, which may have contributed to the fuel disruptions from the 2021 ransomware attack.
https://www.cybersecuritydive.com/news/colonial-pipeline-ransomware-fines/623335/?utm_source=Sailthru&utm_medium=email&utm_campaign=Newsletter%20Weekly%20Roundup:%20Cybersecurity%20Dive:%20Daily%20Dive%2005-07-2022&utm_term=Cybersecurity%20Dive%20Weekender

Your Phone May Soon Replace Many of Your Passwords

Apple, Google and Microsoft announced this week they will soon support an approach to authentication that avoids passwords altogether, and instead requires users to merely unlock their smartphones to sign in to websites or online services. Experts say the changes should help defeat many types of phishing attacks and ease the overall password burden on Internet users, but caution that a true passwordless future may still be years away for most websites.
https://krebsonsecurity.com/2022/05/your-phone-may-soon-replace-many-of-your-passwords/

****

"Ctrl -F" for The Board

Security Stuff Happens: What Do You Do When It Hits the Fan?

Breaches can happen to anyone, but a well-oiled machine can internally manage and externally remediate in a way that won't lead to extensive damage to a company's bottom line. (Part 1 of a series.)
https://www.darkreading.com/vulnerabilities-threats/security-stuff-happens-what-do-you-do-when-it-hits-the-fan-

Security Stuff Happens: What Will the Public Hear When You Say You've Been Breached?

Security vendors know their products have blind spots. They know that there are areas of the attack surface they cannot protect. Despite this, vendors continue to make promises on which they cannot deliver. That's why companies large and small continue to experience intrusions,
https://www.darkreading.com/vulnerabilities-threats/security-stuff-happens-what-will-the-public-hear-when-you-say-you-ve-been-breached-?_mc=NL_DR_EDT_DR_daily_20220506&cid=NL_DR_EDT_DR_daily_20220506&elq_mid=110541&elq_cid=36315893&sp_eh=72a861290e89658b5ada8de6a8a9c12b185e8e45329503691618392cbd15751b

Security Stuff Happens: Where Do You Go From Here?

Even when cybersecurity investigations after an incident are ongoing and you won't have all the answers upfront, it's still important to communicate what you can as early as possible and as often as possible. Communication is integral to successful incident response and the endurance of a brand's reputation.
https://www.darkreading.com/vulnerabilities-threats/security-stuff-happens-where-do-you-go-from-here-

How much has the semiconductor shortage cost?

In its first quarter results the company said Covid-19 lockdowns in Shanghai and Russia's war in Ukraine were "further increasing supply chain risk and contributing to inflationary pressures", exacerbating the shortage. Pat Gelsinger, CEO of Intel, said: "In the supply chain, lockdowns in Shanghai and the war in Ukraine have demonstrated more than ever that the world needs more resilient and more geographically balanced semiconductor manufacturing. "The chip shortage cost the US economy $240bn last year, and we

expect the industry will continue to see challenges until at least 2024 in areas like foundry capacity and tool availability."
https://www.oodaloop.com/technology/2022/05/05/how-much-has-the-semiconductor-shortage-cost/

Gen Z wants jobs in tech, but retention questions linger
A generation waiting in the wings. A corporate world eager to fill tech talent vacancies. Culture and compensation can make or break the deal for the rising IT talent class. Gen Z, or those born after 1997, according to Pew Research, represents a pool of largely untapped, incoming talent. Three in every 10 members of Gen Z say software developer is the role they are most interested in after graduating college, according to a survey of 1,000 people between the ages of 19-24 conducted by CloudBees.
https://www.ciodive.com/news/gen-z-tech-talent-retention/607859/?utm_source=Sailthru&utm_medium=email&utm_campaign=Issue:%202022-05-13%20CIO%20Dive%20%5Bissue:41732%5D&utm_term=CIO%20Dive

Questions
Contact FIPCO's Rob Foxx at 800-722-3498 ext. 249 or email FIPCO IT Services for more information.

"Make Security Part of You and Your Institution's DNA!"

Threat Intelligence Newsletter: June 3, 2022

FIPCO®
IT Audit
Round Table
Discussions

If you would like to host an event, please contact: Ngina Ali

Upcoming Threat Intelligence Peer Group Discussions
None available at the current time

****

Alerts & Warnings

CISA Issues Emergency Directive and Releases Advisory Related to VMware Vulnerabilities
CISA has issued Emergency Directive (ED) 22-03 and released a Cybersecurity Advisory (CSA) in response to active and expected exploitation of multiple vulnerabilities in the following VMware products: VMware Workspace ONE Access (Access), VMware Identity Manager (vIDM), VMware vRealize Automation (vRA), VMware Cloud Foundation, vRealize Suite Lifecycle Manager.
https://www.cisa.gov/uscert/ncas/current-activity/2022/05/18/cisa-issues-emergency-directive-and-releases-advisory-related

Multiple Governments Buying Android Zero-Days for Spying: Google
At least eight governments around the world have purchased a package of Android zero-day exploits from a company called Cytrox and are using them to install spyware on targets' mobile phones. The development highlights the sophistication of off-the-shelf surveillance offerings, according to a recent report. At least eight governments around the world have purchased a package of Android zero-day exploits from a company called Cytrox and are using them to install spyware on targets' mobile phones. The development highlights the sophistication of off-the-shelf surveillance offerings, according to a recent report.
https://www.darkreading.com/attacks-breaches/google-android-0-days-multiple-governments-spying?_mc=NL_DR_EDT_DR_daily_20220524&cid=NL_DR_EDT_DR_daily_20220524&sp_aid=110865&elq_cid=36315893&sp_eh=72a861290e89658b5ada8de6a8a9c12b185e8e45329503691618392cbd15751b&utm_source=eloqua&utm_medium=email&utm_campaign=DR_NL_Dark%20Reading%20Daily_05.24.22&sp_cid=45015&utm_content=DR_NL_Dark%20Reading%20Daily_05.24.22

U.S. Cybersecurity Agency 'Strongly Urges' You Patch These 75 Actively Exploited Flaws
The U.S. Cybersecurity & Infrastructure Security Agency (CISA) has added a total of 75 security vulnerabilities, all known to be actively exploited, to its 'significant risk' listing in just three days this week. So serious is the risk of attack exposure by these exploited vulnerabilities, some of which reach back many years, CISA warns that federal civilian executive branch (FCEB) agencies must ensure they are patched by the middle of June.
https://www.forbes.com/sites/daveywinder/2022/05/26/us-cybersecurity-agency-strongly-urges-you-patch-these-75-actively-exploited-flaws/?sh=65780e186381

Microsoft Office zero day leaves researchers scrambling over the holiday weekend
The company warns a successful attack could allow an attacker to install programs, delete data or create new accounts. The Cybersecurity and Infrastructure Security Agency urged administrators and users to review Microsoft's guidance on a workaround to the Follina vulnerability, which affects the Microsoft Support Diagnostic Tool in Windows.
https://www.ciodive.com/news/microsoft-office-zero-day/624638/?utm_source=Sailthru&utm_medium=email&utm_campaign=Issue:%202022-06-01%20CIO%20Dive%20%5Bissue:42123%5D&utm_term=CIO%20Dive

Russia, backed by ransomware gangs, actively targeting US, FBI director says
The FBI is laser focused on preventing a destructive attack, FBI Director Christopher Wray said. The agency, meanwhile, helped to disrupt a 2021 Iran-backed attack against Boston Children's Hospital.
https://www.cybersecuritydive.com/news/fbi-wray-russia-targeting-us/624790/?utm_source=Sailthru&utm_medium=email&utm_campaign=Issue:%202022-06-02%20Cybersecurity%20Dive%20%5Bissue:42185%5D&utm_term=Cybersecurity%20Dive

Big Cyber Hits on GM, Chicago Public Schools, & Zola Showcase the Password Problem
It has been a week of data breach news, with General Motors, Chicago Public Schools, and wedding-planner startup Zola all reeling from the exposure of customers' personal information. In the latter's case, customers were also riffed for stored funds and suffered fraudulent payment-card charges.
https://www.darkreading.com/attacks-breaches/big-cyber-hits-gm-chicago-public-schools-zola-password-problem?_mc=NL_DR_EDT_DR_daily_20220527&cid=NL_DR_EDT_DR_daily_20220527&sp_aid=110947&elq_cid=36315893&sp_eh=72a861290e89658b5ada8de6a8a9c12b185e8e45329503691618392cbd15751b&utm_source=eloqua&utm_medium=email&utm_campaign=DR_NL_Dark%20Reading%20Daily_05.27.22&sp_cid=45064&utm_content=DR_NL_Dark%20Reading%20Daily_05.27.22

Zero-Click Zoom Bug Allows Code Execution Just by Sending a Message
Google has disclosed a nasty set of six bugs affecting Zoom chat that can be chained together for MitM and RCE attacks, no user interaction required. A vulnerability chain discovered in Zoom's chat functionality can be exploited to allow zero-click remote code execution (RCE), threat hunters have revealed.
https://www.darkreading.com/application-security/zero-click-zoom-bug-allows-remote-code-execution-by-sending-a-message?_mc=NL_DR_EDT_DR_daily_20220531&cid=NL_DR_EDT_DR_daily_20220531&sp_aid=110971&elq_cid=36315893&sp_eh=72a861290e89658b5ada8de6a8a9c12b185e8e45329503691618392cbd15751b&utm_source=eloqua&utm_medium=email&utm_campaign=DR_NL_Dark%20Reading%20Daily_05.31.22&sp_cid=45085&utm_content=DR_NL_Dark%20Reading%20Daily_05.31.22

Costa Rica May Be Pawn in Conti Ransomware Group's Bid to Rebrand, Evade Sanctions
Costa Rica's national health service was hacked sometime earlier this morning by a Russian ransomware group known as Hive. The intrusion comes just weeks after Costa Rican President Rodrigo Chaves declared a state of emergency in response to a data ransom attack from a different Russian ransomware gang — Conti. Ransomware experts say there is good reason to believe the same cybercriminals are behind both attacks, and that Hive has been helping Conti rebrand and evade international sanctions targeting extortion payouts to cybercriminals operating in Russia.
https://krebsonsecurity.com/2022/05/costa-rica-may-be-pawn-in-conti-ransomware-groups-bid-to-rebrand-evade-sanctions/

Study Warns That Shadow Code on External JavaScript Libraries Pose a Serious Supply Chain Risk
Israeli cybersecurity firm Source Defense analyzed the supply chain risk posed by shadow code on third- and fourth-party scripts on major businesses' websites. Third-party scripts and open source JavaScript libraries assist development teams in adding advanced functionality to web applications without writing or maintaining code.
https://www.cpomagazine.com/cyber-security/study-warns-that-shadow-code-on-external-javascript-libraries-pose-a-serious-supply-chain-risk/

****

Hints & Tips plus Security Awareness

FDIC Publishes 2022 Risk Review
The 2022 Risk Review expands coverage of risks from prior reports by examining operational risk to banks from cyber threats and illicit activity and climate-related financial risks to banking organizations. Monitoring these risks is among the FDIC's top priorities.
https://www.fdic.gov/analysis/risk-review/2022-risk-review.html?source=govdelivery&utm_medium=email&utm_source=govdelivery

CISA Releases FY21 Risk and Vulnerability Analysis
The Cybersecurity and Infrastructure Security Agency last week released the analysis and infographic detailing the findings from the 112 risk and vulnerability assessments conducted in fiscal year 2021 across multiple sectors. The analysis details a sample attack path comprising 11 successive actions a cyber threat actor could take to compromise an organization with weaknesses that are representative of those CISA observed in FY21 RVAs.
https://www.cisa.gov/sites/default/files/publications/FY21-RVA-Analysis_508c.pdf?utm_source=eloqua&utm_medium=email&utm_campaign=riskcyberbulletin&utm_content=RiskCyber-20220523

6 Scary Tactics Used in Mobile App Attacks
Mobile attacks have been going on for many years, but the threat is rapidly evolving as more sophisticated malware families with novel features enter the scene. Mobile platforms are increasingly under threat as criminal and nation-state actors look for new ways to install malicious implants with advanced capabilities on iPhone and Android devices.
https://www.darkreading.com/application-security/6-scary-tactics-used-in-mobile-app-attacks?_mc=NL_DR_EDT_DR_daily_20220523&cid=NL_DR_EDT_DR_daily_20220523&sp_aid=110842&elq_cid=36315893&sp_eh=72a861290e89658b5ada8de6a8a9c12b185e8e45329503691618392cbd15751b&utm_source=eloqua&utm_medium=email&utm_campaign=DR_NL_Dark%20Reading%20Daily_05.23.22&sp_cid=45003&utm_content=DR_NL_Dark%20Reading%20Daily_05.23.22

That Money-Saving Discount Offer May Be a Scam
Discounts. Don't you just love them? They're spread all over the Internet for all manner of purchases and you start to feel disappointed if you don't get one. But when it comes to online discounts, all is not what it seems. You could still end up paying more than you need to for that supposed bargain. With a discount, you're supposed to get a reduction on a regular price for an item or service. Or you may see them linked to supposed money savings for medications or household bills.
https://scambusters.org/discount.html

Spring Cleaning Checklist for Keeping Your Devices Safe at Work
Implement zero-trust policies for greater control, use BYOD management tools, and take proactive steps such as keeping apps current and training staff to keep sensitive company data safe and employees' devices secure. Mobile workers are productive and often essential to a business's success, but it puts an immense amount of pressure on IT to protect the company's corporate apps and data while maintaining worker privacy.
https://www.darkreading.com/endpoint/spring-cleaning-checklist-for-keeping-your-devices-safe-at-work?_mc=NL_DR_EDT_DR_daily_20220527&cid=NL_DR_EDT_DR_daily_20220527&sp_aid=110947&elq_cid=36315893&sp_eh=72a861290e89658b5ada8de6a8a9c12b185e8e45329503691618392cbd15751b&utm_source=eloqua&utm_medium=email&utm_campaign=DR_NL_Dark%20Reading%20Daily_05.27.22&sp_cid=45064&utm_content=DR_NL_Dark%20Reading%20Daily_05.27.22

6 Steps to Ensure Cyber Resilience
To minimize the impact of cyber incidents, organizations must be pragmatic and develop a strategy of resilience for dealing with break-ins, advanced malware, and data theft. The frequency and severity of cyber threats are escalating and will continue to get stronger as cybercriminals pivot from one target to the next to maximize profit potential. Sooner or later, an attack will be successful. This presents a huge risk for businesses that lack sufficient cyber-resiliency preparation to stop the spread and recover quickly.
https://www.darkreading.com/attacks-breaches/6-steps-to-ensure-cyber-resilience?_mc=NL_DR_EDT_DR_daily_20220531&cid=NL_DR_EDT_DR_daily_20220531&sp_aid=110971&elq_cid=36315893&sp_eh=72a861290e89658b5ada8de6a8a9c12b185e8e45329503691618392cbd15751b&utm_source=eloqua&utm_medium=email&utm_campaign=DR_NL_Dark%20Reading%20Daily_05.31.22&sp_cid=45085&utm_content=DR_NL_Dark%20Reading%20Daily_05.31.22

Act Now: Leveraging PCI Compliance to Improve Security
Let the threat landscape guide your company's timeline for complying with new data security standards for credit cards. Use the phase-in time to improve security overall — security as a process — not just comply with new standards. In March, the PCI Council released the latest update to its Data Security Standard (DSS).
https://www.darkreading.com/risk/act-now-leveraging-pci-compliance-to-improve-security?_mc=NL_DR_EDT_DR_daily_20220531&cid=NL_DR_EDT_DR_daily_20220531&sp_aid=110971&elq_cid=36315893&sp_eh=72a861290e89658b5ada8de6a8a9c12b185e8e45329503691618392cbd15751b&utm_source=eloqua&utm_medium=email&utm_campaign=DR_NL_Dark%20Reading%20Daily_05.31.22&sp_cid=45085&utm_content=DR_NL_Dark%20Reading%20Daily_05.31.22

Live Masterclass | The Cost of Password Authentication Failures
Ponemon Institute's recent report highlights that most organizations do not have an enterprise-wide strategy for reducing the risk of authentication failures. So, what happens to the significant cost to businesses when organizations are unable to verify user ID due to weaknesses in the authentication processes? Here are the results of this ground-breaking study examining how authentication challenges and organization misalignments are directly affecting the security posture of organizations, digital

transformation initiatives, and current hard-money business loss. Webinar Tuesday June 28 2022 @ 1:00 PM CST
https://www.google.com/search?q=2pm+edt+to+central+time&rlz=1C1GCEU_enUS970US970&oq=2pm+edt+to+ce&aqs=chrome.1.69i57j0i512l2j0i22i30l4j0i390l3.8647j0j7&sourceid=chrome&ie=UTF-8

CISA Adds 75 Flaws to Known Vulnerability Catalog in 3 Days
The U.S. Cybersecurity and Infrastructure Security Agency added 75 flaws to its catalog of known exploited software vulnerabilities. The vulnerabilities were disclosed as part of three separate batches on three consecutive days - it released batches of 21, 20 and 34 vulnerabilities
https://www.databreachtoday.com/cisa-adds-75-flaws-to-known-vulnerability-catalog-in-3-days-a-19170?rf=2022-05-31_ENEWS_ACQ_DBT__Slot3_ART19170&mkt_tok=MDUxLVpYSS0yMzcAAAGEucZaYn3GPn8zqWvgD99Kx8Np66YsyuycpLbrxMt17hf73oBfpUZBrCvnfRkP6ez4MpRBiaTwehllc0hpAJ9RSbS-whhn5hKu87XzSJSiw2h4WphRMg

****

News & Views

Is your kid using education technology? Read on
Whether in class or at home, kids are probably using technology to do their schoolwork. But have you ever wondered what information that technology is gathering from your kid? The FTC has, and today issued a policy statement that put ed tech on notice: Kids shouldn’t have to give up their privacy rights to do their schoolwork or go to class remotely. In other words, ed tech companies: You can’t require parents and schools to agree to the comprehensive surveillance of children for kids to use those learning tools.
https://consumer.ftc.gov/consumer-alerts/2022/05/your-kid-using-education-technology-read?utm_source=govdelivery

Threat Actors Are Stealing Data Now to Decrypt When Quantum Computing Comes
The technique, called store-now, decrypt later (SNDL), means organizations need to prepare now for post-quantum cryptography. Although quantum computing is years away from commercial availability, business leaders, CIOs, and CISOs need to act now to prepare for the technology's inevitable ability to crack RSA-encrypted data. Failure to start adopting a post-quantum cryptography (PQC) strategy will put all existing encrypted data assets at risk of exposure, according to a stark warning from key technical cryptography experts.
https://www.darkreading.com/edge-articles/threat-actors-are-stealing-data-now-to-decrypt-when-quantum-computing-comes?_mc=NL_DR_EDT_DR_daily_20220521&cid=NL_DR_EDT_DR_daily_20220521&sp_aid=110831&elq_cid=36315893&sp_eh=72a861290e89658b5ada8de6a8a9c12b185e8e45329503691618392cbd15751b&utm_source=eloqua&utm_medium=email&utm_campaign=DR_NL_Dark%20Reading%20Daily_05.21.22&sp_cid=44998&utm_content=DR_NL_Dark%20Reading%20Daily_05.21.22

6 Things You Need To Know About Crypto
Despite being around for roughly 13 years and currently in the midst of a market crash, crypto feels like it’s still in a goldrush phase. As hopeful investors pile in with dreams of making big money, many still lack any real knowledge about what they’re getting into. A survey by software developer Oxford Risk last year found more than a third of investors had little or no understanding of the sector when they first got involved. And, with more than 2 million UK adults now holding crypto, according to figures from the

Financial Conduct Authority (FCA), there could be significant gaps in the nation’s collective crypto knowledge.
https://www.forbes.com/uk/advisor/investing/cryptocurrency/6-things-you-need-to-know-about-crypto/

Feds remain in the dark as ransomware disclosure lags
Peters in July 2021 launched an investigation into the role cryptocurrencies play in ransomware. The probe was announced after a series of devastating ransomware attacks on key industries, including the May 2021 attack on Colonial Pipeline, followed weeks later by a ransomware attack on meat supplier JBS USA and the July ransomware attack against IT monitoring firm Kaseya.
https://www.cybersecuritydive.com/news/senate-ransomware-cisa/624369/?utm_source=Sailthru&utm_medium=email&utm_campaign=Issue:%202022-05-27%20Cybersecurity%20Dive%20%5Bissue:42085%5D&utm_term=Cybersecurity%20Dive

Scammer Behind $568M International Cybercrime Syndicate Gets 4 Years
The 14th defendant behind The Infraud Organization contraband marketplace has been sentenced, this time for one count of racketeering. Stolen identities, compromised credit-card data, computer malware, and more were collected and sold by The Infraud Organization, a transnational cybercrime syndicate — and the Department of Justice estimates the activity cost victims more than $568 million.
https://www.darkreading.com/attacks-breaches/scammer-568m-cybercrime-4-years?_mc=NL_DR_EDT_DR_daily_20220531&cid=NL_DR_EDT_DR_daily_20220531&sp_aid=110971&elq_cid=36315893&sp_eh=72a861290e89658b5ada8de6a8a9c12b185e8e45329503691618392cbd15751b&utm_source=eloqua&utm_medium=email&utm_campaign=DR_NL_Dark%20Reading%20Daily_05.31.22&sp_cid=45085&utm_content=DR_NL_Dark%20Reading%20Daily_05.31.22

****

"Ctrl -F" for The Board

Cyber Insurers Raise Rates Amid a Surge in Costly Hacks
Insurers significantly increased premiums for cyber coverage over the course of 2021, as a string of high-profile attacks and government action helped boost demand for products, data collected by industry bodies shows. Direct-written premiums collected by the largest U.S. insurance carriers in 2021 swelled by 92% year-over-year, according to information submitted to the National Association of Insurance Commissioners, an industry watchdog, and compiled by ratings firms.
https://www.wsj.com/articles/cyber-insurers-raise-rates-amid-a-surge-in-costly-hacks-11652866200?page=1&mod=djemCybersecruityPro&tpl=cy

Enterprises rarely follow advice to never pay ransoms
Ransomware foists a difficult choice on executives and very few leave business operations in limbo to test a best practice. Payments incentivize ransomware threat actors and reinforce their use of malware for financial gain. Executives often approve ransomware payments because it works, but the benefits are short-lived. “If they’ve come in and owned you, so to speak, and you pay them, they’re likely to do it again because you’ve just taught them that you’re willing to pay. It’s a matter of if, not when,” said Charles Jacco, principal at KPMG’s cybersecurity advisory practice.
https://www.cybersecuritydive.com/news/ransomware-payments-executives-kaspersky/623811/?utm_source=Sailthru&utm_medium=email&utm_campaign=Newsletter%20Weekly%20Roundup:%20Cybersecurity%20Dive:%20Daily%20Dive%2005-21-2022&utm_term=Cybersecurity%20Dive%20Weekender

Forget technology: Talent is the key to modernization
Competition for digital skills remains a major headache — and the solution may be an HR rethink. Modernization, it turns out, is really a people problem. The solutions may require CIOs and other tech leaders to forge stronger working relationships with HR departments, and to adopt more of an HR mindset regarding workforce planning.
https://www.ciodive.com/news/tech-talent-crunch-modernization-MIT-CIO/624755/?utm_source=Sailthru&utm_medium=email&utm_campaign=Issue:%202022-06-03%20CIO%20Dive%20%5Bissue:42192%5D&utm_term=CIO%20Dive

C-Suite Special Report: Insider Risk – What Your Security Team Wishes You Knew
Executives are required to make "data-driven" decisions; Metrics, Objectives & Key Results (OKRs), Key Performance Indicators (KPIs) – however you define being data-driven – to measure security program effectiveness, and frame their conversations to the board, partners, and company at large. Yet, there is a fundamental disconnect in security's ability to communicate risk to the executives, which in turn results in gaping missed opportunities for proactively making strategic and growth-oriented decisions. Webinar Wednesday June 22 2022 @ 1:00 PM CST
https://www.databreachtoday.com/webinars/c-suite-special-report-insider-risk-what-your-security-team-wishes-you-w-3972?user_email=rfoxx@fipco.com&rf=2022-05-30_ENEWS_ACQ_DBT__Slot2_WEB3972&mkt_tok=MDUxLVpYSS0yMzcAAAGEtJ_1JNxBUaT1H_Nk4h8EkII8rE6vvThrvFtdb0I97FzP5FlrvVuAeD1vwxjdkCeRZVguaAGykRiV8ZY36Qwal9KXGXb9CU08blshW_bEqdw_r1-TtQ

Questions
Contact FIPCO's Rob Foxx at 800-722-3498 ext. 249 or email FIPCO IT Services for more information.

"Make Security Part of You and Your Institution's DNA!"

Threat Intelligence Newsletter: June 13, 2022

FIPCO® IT Audit Round Table Discussions

If you would like to host an event, please contact: Ngina Ali

Upcoming Threat Intelligence Peer Group Discussions
None available at the current time

****

Alerts & Warnings

Actively Exploited Atlassian Zero-Day Bug Allows Full System Takeover
A remote code execution (RCE) vulnerability in all versions of the popular Confluence collaboration platform can be abused in credential harvesting, cyber espionage, and network backdoor attacks. Recent research has suggested that modern ransomware operations run much like legitimate businesses. Both have a management structure, different teams specializing in different aspects of the operation, and they outsource work when necessary.
https://www.darkreading.com/cloud/actively-exploited-atlassian-zero-day-bug-full-system-takeover?_mc=NL_DR_EDT_DR_daily_20220608&cid=NL_DR_EDT_DR_daily_20220608&sp_aid=111122&elq_cid=36315893&sp_eh=72a861290e89658b5ada8de6a8a9c12b185e8e453295036916183 92cbd15751b&utm_source=eloqua&utm_medium=email&utm_campaign=DR_NL_Dark%20Reading%20Daily_06.08.22&sp_cid=45166&utm_content=DR_NL_Dark%20Reading%20Daily_06.08.22

10 Most Prolific Banking Trojans Targeting Hundreds of Financial Apps with Over a Billion Users
10 of the most prolific mobile banking trojans have set their eyes on 639 financial applications that are available on the Google Play Store and have been cumulatively downloaded over 1.01 billion times. Of the 639 apps tracked, 121 are based in the U.S., followed by the U.K. (55), Italy (43), Turkey (34), Australia (33), France (31), Spain (29), and Portugal (27).
https://thehackernews.com/2022/06/10-most-prolific-banking-trojans.html?_m=3n%2e009a%2e2755%2eod0ao445rz%2e1rds

New Android malware SMSFactory detailed
Tens of thousands of Android device users across eight countries have been under attack from the new SMSFactory malware that unknowingly subscribes victims to premium services, BleepingComputer reports. Most of the over 165,000 Android users have been targeted by SMSFactory between May 2021 and May

2022 were reported in Russia, Brazil, Argentina, Turkey, and Ukraine, said Avast researchers, who noted that a variant of the malware also features contact list exfiltration capabilities
https://www.scmagazine.com/brief/threat-intelligence/new-android-malware-smsfactory-detailed?_hsmi=78978938&_hsenc=p2ANqtz-_jYuTCuOr6ZJKHQ8J9USJkOLDCNtSB7D-06FsMg9UOgsDaOGy6n7sl3UTIjC5ZOes0RqrLAzZkKI8T2LpL1ttUMeBfbQ

Data Breach at Shields Health Care Group Impacts 2 Million Patients
Shields Health Care Group has informed roughly two million individuals of a cybersecurity incident that potentially impacted their personal data. The Massachusetts-based firm provides management and imaging services to more than 50 healthcare partners and facilities throughout New England. In a data breach notice published on their website, Shields said the incident was identified on March 28, 2022, but the intrusion actually happened between March 7 and March 21.
https://www.securityweek.com/data-breach-shields-health-care-group-impacts-2-million-patients?_hsmi=78978938&_hsenc=p2ANqtz--_cGVhacWQfGvb7dT3eHsOLh8oeZ0_-30cwwji8BgGohrmw24SnkbiSoWfjXHg7_1lqn0feYNvD4zBHTccSG1Q2Anzpg

****

Hints & Tips plus Security Awareness

For Ransomware, Speed Matters
Someone interested in putting together a ransomware campaign has to consider several factors. The LockBit group touts its speed over competing families to attract potential buyers for its ransowmare-as-a-service.
https://www.darkreading.com/edge-threat-monitor/for-ransomware-speed-matters?_mc=NL_DR_EDT_DR_daily_20220604&cid=NL_DR_EDT_DR_daily_20220604&sp_aid=111073&elq_cid=36315893&sp_eh=72a861290e89658b5ada8de6a8a9c12b185e8e45329503691618392cbd15751b&utm_source=eloqua&utm_medium=email&utm_campaign=DR_NL_Dark%20Reading%20Daily_06.04.22&sp_cid=45136&utm_content=DR_NL_Dark%20Reading%20Daily_06.04.22

Biometric Data Offers Added Security — But Don't Lose Sight of These Important Risks
With rising fraud, businesses are seeking authentication methods that are security- and user-friendly. But with that comes a few complications. Biometric authentication, such as face ID, voice biometrics, fingerprints, or some combination thereof, is becoming an essential part of the cybersecurity toolbox as organizations try to block adversaries from taking over online accounts and to prevent fraud.
https://www.darkreading.com/edge-articles/biometric-data-offers-added-security-and-risks?_mc=NL_DR_EDT_DR_daily_20220604&cid=NL_DR_EDT_DR_daily_20220604&sp_aid=111073&elq_cid=36315893&sp_eh=72a861290e89658b5ada8de6a8a9c12b185e8e45329503691618392cbd15751b&utm_source=eloqua&utm_medium=email&utm_campaign=DR_NL_Dark%20Reading%20Daily_06.04.22&sp_cid=45136&utm_content=DR_NL_Dark%20Reading%20Daily_06.04.22

We're Still Creating No Good, Very Bad Passwords; Time To Up Our Game
Yep, we're still doing it. What's that, you ask? Unfortunately, the collective "we" are still creating as Alexander may say, terrible, horrible, no good, very bad passwords. At the beginning of each year, there are lists of the worst passwords used the previous year. As if 2020 didn't bring enough chaos and disappointment, our password choices also left a lot to be desired. So, let's revisit those and toss in a few reminders about how to create good ones.
https://www.sosdailynews.com/news.jspx?&articleid=409D3411CA91DFA1CC294351F4DFA676&sx=26446

Protect Against On-site Social Engineering
Social engineering is a method of using human interaction to convince people to break their normal security processes. It can utilize technology, but that isn't necessary in order to reach a goal. It's been around since the beginning of time and although it has a modern name, it really is just a game for hackers. When people hear the term Social Engineering, it's likely they think of email Phishing attacks. While remote social engineering attacks are extremely popular, what people often forget is that on-site social engineering attacks can be just as dangerous and in many cases, just as easy for a criminal to pull off.
https://www.sosdailynews.com/news.jspx?&articleid=6DCB697DC39E4E05C4CE7CC5F8666FB1&sx=26446

****

News & Views

Will the United States Enact a National Data Privacy Law?
In the aftermath of massive data breaches that have exposed the personal identifiable and financial information of millions of people around the globe, it became clear that there has beena need for legally-mandated data protection. Europe leapt to the forefront, implementing its General Data Protection Regulation (GDPR), a comprehensive law that empowered European citizens to have substantial control on how organizations used, processed, and stored their information. In addition, the GDPR created a regulatory framework mandating how companies went about ensuring data privacy protection and setting costly fines for those that fell out of compliance.
https://www.oodaloop.com/archive/2022/06/07/will-the-united-states-enact-a-national-data-privacy-law/

A third of organizations hit by ransomware were forced to close temporarily or permanently
A recent survey reveals many organizations close either temporarily or permanently after a ransomware attack. Learn more about how you can protect your business ransomware attacks. A successful ransomware attack can devastate an organization. And even paying the ransom doesn't mean your company won't suffer lasting damage. A report released Tuesday by security provider Cybereason looks at the impact of ransomware on many organizations and offers advice on how to defend yourself against these types of attacks.
https://www.techrepublic.com/article/organizations-hit-by-ransomware-shut-down/

****

"Ctrl -F" for The Board

Banking for Z next generation
More than 10,000 baby boomers are turning 65 every day, and over the next 20 to 30 years, an estimated $68 trillion of wealth will transfer to their children. The landscape of financial customers is changing as millennials and Gen Z'ers age (and as Gen Z influences the decisions of their parents in Gen X).
https://bankingjournal.aba.com/2022/06/banking-for-z-next-generation/?utm_source=eloqua&utm_medium=email&utm_campaign=newsbytes&utm_content=NEWSBYTES-20220607

Crypto framework would define SEC, CFTC oversight purview

Crypto oversight has been a focus for lawmakers, regulators and digital-asset professionals for months. Several crypto executives who testified on Capitol Hill in December said the U.S.’s approach to regulating the space will determine the nation’s status as a leader in the field.

https://www.bankingdive.com/news/crypto-framework-would-define-sec-cftc-oversight-purview/625044/?utm_source=Sailthru&utm_medium=email&utm_campaign=Issue:%202022-06-07%20Banking%20Dive%20%5Bissue:42250%5D&utm_term=Banking%20Dive

Communication Is Key to CISO Success

A panel of CISOs at the RSA Conference outlined what a successful first 90-day plan looks like, and it boiled down to effective communication and listening. RSA CONFERENCE – San Francisco – A trio of high-powered CISOs talked about the first 90 days in their roles, and whether the aim was getting board of directors' buy-in or building rank-and-file credibility, they all said how they communicated was what mattered the most.

https://www.darkreading.com/careers-and-people/communication-is-key-to-ciso-success?_mc=NL_DR_EDT_DR_daily_20220607&cid=NL_DR_EDT_DR_daily_20220607&sp_aid=111107&elq_cid=36315893&sp_eh=72a861290e89658b5ada8de6a8a9c12b185e8e45329503691618392cbd15751b&utm_source=eloqua&utm_medium=email&utm_campaign=DR_NL_Dark%20Reading%20Daily_06.07.22&sp_cid=45154&utm_content=DR_NL_Dark%20Reading%20Daily_06.07.22

Questions

Contact FIPCO’s Rob Foxx at 800-722-3498 ext. 249 or email FIPCO IT Services for more information.

"Make Security Part of You and Your Institution's DNA!"

Threat Intelligence Newsletter: June 17, 2022

FIPCO®
IT Audit
Round Table
Discussions

If you would like to host an event, please contact: Ngina Ali

Upcoming Threat Intelligence Peer Group Discussions
None available at the current time

****

Alerts & Warnings

China State-Sponsored Cyber Actors Exploit Network Providers and Devices
CISA, the NSA and the FBI last week released a joint cybersecurity advisory that outlines cyber actors sponsored by the People's Republic of China continue to exploit publicly known vulnerabilities to establish a broad network of compromised infrastructure across public and private sectors, including telecommunications companies and network service providers.
http://app.response.aba.com/e/er?utm_source=eloqua&utm_medium=email&utm_campaign=riskcyberbulletin&utm_content=RiskCyber-20220613&s=1527&lid=36618&elqTrackId=c45dd487301f470faf795a3acc7aa0eb&elq=c62d4b0284324347b82d8e27955fffe3&elqaid=27651&elqat=1

CISA Recommends Organizations Update to the Latest Version of Google Chrome
The US Cybersecurity and Infrastructure Agency (CISA) Friday urged users and administrators to update to a new version of Chrome that Google released last week to fix a total of seven vulnerabilities in its browser. In an advisory, Google described four of the flaws — three of which were reported to the company by external researchers — as presenting a high risk for organizations.
https://www.darkreading.com/vulnerabilities-threats/cisa-encourages-organizations-to-updated-to-latest-chrome-version?_mc=NL_DR_EDT_DR_daily_20220614&cid=NL_DR_EDT_DR_daily_20220614&sp_aid=111198&elq_cid=36315893&sp_eh=72a861290e89658b5ada8de6a8a9c12b185e8e45329503691618392cbd15751b&utm_source=eloqua&utm_medium=email&utm_campaign=DR_NL_Dark%20Reading%20Daily_06.14.22&sp_cid=45218&utm_content=DR_NL_Dark%20Reading%20Daily_06.14.22

24+ Billion Credentials Circulating on the Dark Web in 2022 — So Far
Passwordless technology may be one of the most hyped categories in cybersecurity at the moment, but the reality on the ground is that passwords are still widely entrenched — and wildly insecure. Some 24.6

billion complete sets of usernames and passwords are currently in circulation in cybercriminal marketplaces as of this year, a report has found.
https://www.darkreading.com/vulnerabilities-threats/24-billion-credentials-circulate-dark-web-2022?_mc=NL_DR_EDT_DR_daily_20220616&cid=NL_DR_EDT_DR_daily_20220616&sp_aid=111225&elq_cid=36315893&sp_eh=72a861290e89658b5ada8de6a8a9c12b185e8e45329503691618392cbd15751b&utm_source=eloqua&utm_medium=email&utm_campaign=DR_NL_Dark%20Reading%20Daily_06.16.22&sp_cid=45238&utm_content=DR_NL_Dark%20Reading%20Daily_06.16.22

This new Android malware bypasses multi-factor authentication to steal your passwords
A newly discovered form of Android malware steals passwords, bank details and cryptocurrency wallets from users – and it does so by bypassing multi-factor authentication protections. The malware has been detailed by cybersecurity researchers at F5 Labs, who've dubbed it MaliBot. It's the latest in a string of powerful malware targeting Android users.
https://www.zdnet.com/article/this-new-android-malware-bypasses-multi-factor-authentication-to-steal-your-passwords/

Fake Update Ads Steal Your Passwords
We know the cyber-cheats are always out there using every trick in the book to steal our money, identities and whatever else they can get their hands on. So, the next time you're alerted to a software update, especially one appearing in an online ad, it's time to step back and take a closer look before tapping "Download."
https://www.sosdailynews.com/news.jspx?&articleid=0B50E6F30A08CB3EB11216A9F462BB96&sx=26446

****

Hints & Tips plus Security Awareness

How Information Security Teams Can Help Reduce Stress and Burnout
Work across the organization and take practical steps to ease user stress — prioritize user productivity by offering the right tools to avoid shadow IT and cultivate a transparent security culture. Remember the security team, too, and automate as many processes as possible.
https://www.darkreading.com/careers-and-people/how-information-security-teams-can-help-reduce-stress-and-burnout?_mc=NL_DR_EDT_DR_daily_20220616&cid=NL_DR_EDT_DR_daily_20220616&sp_aid=111225&elq_cid=36315893&sp_eh=72a861290e89658b5ada8de6a8a9c12b185e8e45329503691618392cbd15751b&utm_source=eloqua&utm_medium=email&utm_campaign=DR_NL_Dark%20Reading%20Daily_06.16.22&sp_cid=45238&utm_content=DR_NL_Dark%20Reading%20Daily_06.16.22

Cybersecurity: Why It's Not Just an 'IT Problem'
Far too many companies think that backups and cyber insurance will see them through a cybersecurity breach, says Mark Sangster of Adlumin. He shares his advice to enterprise security leaders who want to treat cybersecurity as the business risk it is.
https://www.databreachtoday.com/cybersecurity-its-just-it-problem-a-19210?rf=2022-06-10_ENEWS_ACQ_DBT___Slot5_ART19210&mkt_tok=MDUxLVpYSS0yMzcAAAGE7USr0nndxFFALXN6fZbPUAKE-567ykk27NS4t_dS21FBUS_5yD9s9hEaaHeuSkGZ_2wYVn0DKbfNreWTVk-HrLZzWHxlhGqGO5ytyhjTrZuU5Y8lSw

Oversharing On Social Media: If Opportunity Knocks, Know When Not To Answer
Sharing online can be irresistible, especially when quizzes, surveys and other fun opportunities allow your voice to be heard. It's important to note that bad actors are constantly trolling social media sites for

personal information. One of their biggest allies are the viral social media quizzes and surveys that pop-up on sites like Facebook. They give hackers gold nuggets of information that can be used for future cyberattacks. With online quizzes and oversharing providing the fuel for an attack, knowing it’s avoidable to begin with is perhaps most disturbing of all.
https://www.sosdailynews.com/news.jspx?&articleid=C89525B3FD3FE318B7543541104C350B&sx=26446

****

News & Views

Thousands Arrested in Global Raids on Social-Engineering Scammers
Interpol says it busted fraudsters who were operating call centers for romance scams, get-rich-quick schemes, and more. Interpol has announced that a coordinated, global law-enforcement effort has led to the arrest of 2,000 individuals and the seizure of more than $50 million in illicit funds stolen through a variety of social-engineering scams.
https://www.darkreading.com/threat-intelligence/thousands-arrested-global-raids-social-engineering-scammers?_mc=NL_DR_EDT_DR_daily_20220616&cid=NL_DR_EDT_DR_daily_20220616&sp_aid=111225&elq_cid=36315893&sp_eh=72a861290e89658b5ada8de6a8a9c12b185e8e45329503691618392cbd15751b&utm_source=eloqua&utm_medium=email&utm_campaign=DR_NL_Dark%20Reading%20Daily_06.16.22&sp_cid=45238&utm_content=DR_NL_Dark%20Reading%20Daily_06.16.22

Researchers Block Two Million Extortion Emails Daily
Security researchers at Proofpoint have warned users to be aware of extortion scams after announcing that they block millions of these emails every day. Proofpoint released a new blog post claiming that on average, it blocks a million extortion emails every 24 hours.
https://www.infosecurity-magazine.com/news/researchers-two-million-extortion/

A Microsoft Office 365 Feature Could Help Ransomware Hackers Hold Cloud Files Hostage
A "dangerous piece of functionality" has been discovered in Microsoft 365 suite that could be potentially abused by a malicious actor to ransom files stored on SharePoint and OneDrive and launch attacks on cloud infrastructure.
https://thehackernews.com/2022/06/a-microsoft-office-365-feature-could.html?_m=3n%2e009a%2e2762%2eod0ao445rz%2e1rji

****

"Ctrl -F" for The Board

Comprehensive, Easy Cybersecurity for Lean IT Security Teams Starts with XDR
Breaches don't just happen to large enterprises. Threat actors are increasingly targeting small businesses. In fact, 43% of data breaches involved small to medium-sized businesses. But there is a glaring discrepancy. Larger businesses typically have the budget to keep their lights on if they are breached. Most small businesses (83%), however, don't have the financial resources to recover if they are a victim of an attack.
https://thehackernews.com/2022/06/comprehensive-easy-cybersecurity-for.html?_m=3n%2e009a%2e2761%2eod0ao445rz%2e1ris

Questions
Contact FIPCO’s Rob Foxx at 800-722-3498 ext. 249 or email FIPCO IT Services for more information.

"Make Security Part of You and Your Institution's DNA!"

Threat Intelligence Newsletter: June 24, 2022

Upcoming Threat Intelligence Peer Group Discussions
None available at the current time

****

Alerts & Warnings

Ransomware groups shift tactics and objectives
Malware can play a major or nonexistent role in ransomware attacks. Threat actors are often only in it for the money. Ransomware attacks are shifting from malware-centric threats to more nuanced and sophisticated tactics. The more savvy and technically adept groups behind these attacks are trying to extract as much ransom as possible by using data extortion and leak sites to increase the pressure on organizations.
https://www.cybersecuritydive.com/news/ransomware-shifting-tactics-objectives/625595/?utm_source=Sailthru&utm_medium=email&utm_campaign=Issue:%202022-06-17%20Cybersecurity%20Dive%20%5Bissue:42524%5D&utm_term=Cybersecurity%20Dive

Cyberattackers Abuse QuickBooks Cloud Service in 'Double-Spear' Campaign
Malicious invoices coming from the accounting software's legitimate domain are used to harvest phone numbers and carry out fraudulent credit-card transactions. Cyberattackers are hiding behind the QuickBooks brand to disguise their malicious activity, researchers are warning.
https://www.darkreading.com/remote-workforce/cyberattackers-abuse-quickbooks-cloud-service-ouble-spear-campaign?_mc=NL_DR_EDT_DR_daily_20220624&cid=NL_DR_EDT_DR_daily_20220624&sp_aid=111358&elq_cid=36315893&sp_eh=72a861290e89658b5ada8de6a8a9c12b185e8e45329503691618392cbd15751b&utm_source=eloqua&utm_medium=email&utm_campaign=DR_NL_Dark%20Reading%20Daily_06.24.22&sp_cid=45313&utm_content=DR_NL_Dark%20Reading%20Daily_06.24.22

Microsoft 365 Users in US Face Raging Spate of Attacks
A voicemail-themed phishing campaign is hitting specific industry verticals across the country, bent on scavenging credentials that can be used for a range of nefarious purposes. Microsoft 365 and Outlook customers in the US are in the crosshairs of a successful credential-stealing campaign that uses voicemail-themed emails as phishing lures. The flood of malicious emails anchoring the threat is emblematic of the larger problem of securing Microsoft 365 environments, researchers say.
https://www.darkreading.com/remote-workforce/microsoft-office-365-users-raging-spate-attacks?_mc=NL_DR_EDT_DR_daily_20220623&cid=NL_DR_EDT_DR_daily_20220623&sp_aid=111337&elq_cid=36315893&sp_eh=72a861290e89658b5ada8de6a8a9c12b185e8e45329503691618392cbd15751b&utm_source=eloqua&utm_medium=email&utm_campaign=DR_NL_Dark%20Reading%20Daily_06.23.22&sp_cid=45296&utm_content=DR_NL_Dark%20Reading%20Daily_06.23.22

56 Vulnerabilities Discovered in OT Products From 10 Different Vendors
Deep-dive study unearthed security flaws that could allow remote code execution, file manipulation, and malicious firmware uploads, among other badness. A new analysis of data from multiple sources has uncovered a total of 56 vulnerabilities in OT products from 10 vendors, including notable ones such as Honeywell, Siemens, and Emerson.
https://www.darkreading.com/vulnerabilities-threats/study-finds-56-vulnerabilities-in-ot-products-from-10-vendors?_mc=NL_DR_EDT_DR_daily_20220622&cid=NL_DR_EDT_DR_daily_20220622&sp_aid=111309&elq_cid=36315893&sp_eh=72a861290e89658b5ada8de6a8a9c12b185e8e45329503691618392cbd15751b&utm_source=eloqua&utm_medium=email&utm_campaign=DR_NL_Dark%20Reading%20Daily_06.22.22&sp_cid=45285&utm_content=DR_NL_Dark%20Reading%20Daily_06.22.22

24+ Billion Credentials Circulating on the Dark Web in 2022 — So Far
Username and password combinations offered for sale on the Dark Web by criminals has increased 65% since 2020. Passwordless technology may be one of the most hyped categories in cybersecurity at the moment, but the reality on the ground is that passwords are still widely entrenched — and wildly insecure. Some 24.6 billion complete sets of usernames and passwords are currently in circulation in cybercriminal marketplaces as of this year, a report has found.
https://www.darkreading.com/vulnerabilities-threats/24-billion-credentials-circulate-dark-web-2022?_mc=NL_DR_EDT_DR_daily_20220621&cid=NL_DR_EDT_DR_daily_20220621&sp_aid=111299&elq_cid=36315893&sp_eh=72a861290e89658b5ada8de6a8a9c12b185e8e45329503691618392cbd15751b&utm_source=eloqua&utm_medium=email&utm_campaign=DR_NL_Dark%20Reading%20Daily_06.21.22&sp_cid=45278&utm_content=DR_NL_Dark%20Reading%20Daily_06.21.22

Internet Explorer Now Retired but Still an Attacker Target
Though the once-popular browser is officially now history as far as Microsoft support goes, adversaries won't stop attacking it, security experts say. Microsoft's official end-of-support for the Internet Explorer 11 desktop application on June 15 relegated to history a browser that's been around for almost 27 years. Even so, IE still likely will provide a juicy target for attackers.
https://www.darkreading.com/vulnerabilities-threats/internet-explorer-will-likely-remain-an-attacker-target-for-some-time?_mc=NL_DR_EDT_DR_daily_20220617&cid=NL_DR_EDT_DR_daily_20220617&sp_aid=111247&elq_cid=36315893&sp_eh=72a861290e89658b5ada8de6a8a9c12b185e8e45329503691618392cbd15751b&utm_source=eloqua&utm_medium=email&utm_campaign=DR_NL_Dark%20Reading%20Daily_06.17.22&sp_cid=45251&utm_content=DR_NL_Dark%20Reading%20Daily_06.17.22

Google details commercial spyware that targets both Android and iOS devices
Google has warned of an enterprise-grade spyware strain targeting Android and iOS mobile device users. According to Google Threat Analysis Group (TAG) researchers Benoit Sevens and Clement Lecigne, as well as Project Zero, a distinct government and enterprise-grade iOS and Android spyware variant is now in active circulation.
https://www.zdnet.com/article/google-details-commercial-spyware-that-targets-both-android-and-ios-devices/

****

Hints & Tips plus Security Awareness

7 Ways to Avoid Worst-Case Cyber Scenarios
In the wake of devastating attacks, here are some of the best techniques and policies a company can implement to protect its data. While technology has changed the world for the better, this rising dependence has also increased cyber risks. From an exponential increase in online scams to a growing number of human-error problems, there's a greater need to prepare for worst-case cybersecurity scenarios.
https://www.darkreading.com/risk/7-ways-to-avoid-worst-case-cyber-scenarios

Passwords: Do Actions Speak Louder Than Words?
For most of us, passwords are the most visible security control we deal with on a regular basis, but we are not very good at it. Whether we as a whole are doing better or worse in terms of password security is still unclear, but one thing is certain: We are clearly overconfident in our perceptions about our security activities.
https://www.darkreading.com/edge-threat-monitor/passwords-actions-speak-louder-than-words?_mc=NL_DR_EDT_DR_daily_20220618&cid=NL_DR_EDT_DR_daily_20220618&sp_aid=111263&elq_cid=36315893&sp_eh=72a861290e89658b5ada8de6a8a9c12b185e8e45329503691618392cbd15751b&utm_source=eloqua&utm_medium=email&utm_campaign=DR_NL_Dark%20Reading%20Daily_06.18.22&sp_cid=45257&utm_content=DR_NL_Dark%20Reading%20Daily_06.18.22

Beat the Vacation Rental Scammers!
Hundreds of vacationers, maybe thousands, are going to be disappointed in the coming weeks when they discover their vacation rental doesn't exist or that someone is already living there.
https://scambusters.org/vacationrental.html

****

News & Views

Testing fingerprint cards
Biometric payment cards use fingerprints, which are securely verified on-card by using an integrated fingerprint sensor, meaning all payments can be carried out without physically touching the payment terminal. The fingerprint is linked with the card by the consumer at home, and the fingerprint template is only stored on the card.
https://www.finextra.com/newsarticle/40446/fidor-bank-to-test-fingerprint-cards

Tech skill proficiency dropped 'significantly' in 2021: report
High demand and a lack of skills have contributed to talent shortages, particularly in the tech space.
https://www.ciodive.com/news/tech-skill-proficiency-2021-report/625796/?utm_source=Sailthru&utm_medium=email&utm_campaign=Issue:%202022-06-23%20CIO%20Dive%20%5Bissue:42614%5D&utm_term=CIO%20Dive

Why Paper Receipts are Money at the Drive-Thru
Check out this handmade sign posted to the front door of a shuttered Jimmy John's sandwich chain shop in Missouri last week. See if you can tell from the store owner's message what happened.
https://krebsonsecurity.com/2022/06/why-paper-receipts-are-money-at-the-drive-thru/

****

"Ctrl -F" for The Board

Security disconnect: Why the CISO role is evolving
CISOs are too focused on security operations, writing policies or vendor management. Their time is better spent shaping business strategy. Non-security business leaders perceive cybersecurity as a technical issue that does not drive business outcomes.
https://www.cybersecuritydive.com/news/gartner-ciso-role-evolution-security-leader/610330/?utm_source=Sailthru&utm_medium=email&utm_campaign=Issue:%202022-06-22%20Cybersecurity%20Dive%20%5Bissue:42594%5D&utm_term=Cybersecurity%20Dive

Digital transformations – Why technology alone will not transform your bank
Everything positive and sustainable that a banking organization will achieve begins with defining the culture it wants to have and then putting into place the changes and values it needs to get there. Yet, even with this road map, many banks fail at culture transformation because they stumble on some avoidable pitfalls.
https://www.bankingdive.com/spons/digital-transformations-why-technology-alone-will-not-transform-your-bank/624901/

Questions
Contact FIPCO's Rob Foxx at 800-722-3498 ext. 249 or email FIPCO IT Services for more information.

"Make Security Part of You and Your Institution's DNA!"

Threat Intelligence Newsletter: July 1, 2022

FIPCO®
IT Audit
Round Table
Discussions

Upcoming Threat Intelligence Peer Group Discussions
None available at the current time

****

Alerts & Warnings

Popular child-tracking Android apps contain gaping security holes
Android apps with over 85 million installations spy on the parents that use them to track their children, and some even contain links to malicious sites. Experts think it's not entirely safe to expose kids' data to third-party vendors.
https://cybernews.com/security/popular-child-tracking-android-apps-contain-gaping-security-holes/?utm_source=newsletter&utm_medium=email&utm_campaign=CyberNewsLetter_73

FBI says fraud on LinkedIn a 'significant threat' to platform and consumers
SAN FRANCISCO — Fraudsters who exploit LinkedIn to lure users into cryptocurrency investment schemes pose a "significant threat" to the platform and consumers, according to Sean Ragan, the FBI's special agent in charge of the San Francisco and Sacramento, California, field offices.
https://www.cnbc.com/2022/06/17/fbi-says-fraud-on-linkedin-a-significant-threat-to-platform-and-consumers.html

Microsoft prepares to forget about Windows 8.1 with end of support notifications
Microsoft is preparing to send reminders to Windows 8.1 users that support will end on January 10th 2023. The software giant will start sending notifications to existing Windows 8.1 devices next month, as a first reminder leading up to the January 2023 support cutoff.
https://www.theverge.com/2022/6/24/23181347/microsoft-windows-8-1-end-of-support-notifications-pop-ups

Is your remote IT job candidate legit?
Instances of stolen identity and applicants using deepfakes are plots at home in a spy novel. Aside from reports of stolen PII used to apply for remote positions, the voice spoofing, or even voice deepfakes mean fraudsters are going extra lengths to secure jobs.
https://www.cybersecuritydive.com/news/deepfakes-IT-remote-work/626246/?utm_source=Sailthru&utm_medium=email&utm_campaign=Issue:%202022-06-29%20Cybersecurity%20Dive%20%5Bissue:42762%5D&utm_term=Cybersecurity%20Dive

Organizations Battling Phishing Malware, Viruses the Most
Organizations may not frequently encounter malware targeting cloud systems or networking equipment, but the array of malware they do encounter just occasionally is no less disruptive or damaging. That is where the focus needs to be.
https://www.darkreading.com/edge-threat-monitor/organizations-battling-phishing-malware-viruses-the-most?_mc=NL_DR_EDT_DR_daily_20220625&cid=NL_DR_EDT_DR_daily_20220625&sp_aid=111374&elq_cid=36315893&sp_eh=72a861290e89658b5ada8de6a8a9c12b185e8e45329503691618392cbd15751b&utm_source=eloqua&utm_medium=email&utm_campaign=DR_NL_Dark%20Reading%20Daily_06.25.22&sp_cid=45322&utm_content=DR_NL_Dark%20Reading%20Daily_06.25.22

FREE Windows OS 11 Download Includes FREE Vidar Info-Stealer Malware
It's well-known that downloading apps and other software from unofficial sites, including social media outlets, is risky at best. Yet those who know better still do it for their own reasons, like getting a free download of Windows OS 11 they would otherwise have to pay for. Cybersecurity experts warn "free software" often has many strings attached, and none of them good. An infection from Vidar info-stealing malware is an example of just how wrong a free software download can go.
https://www.sosdailynews.com/news.jspx?&articleid=99272D25819006D76AFB7BAD4ECCB176&sx=26446

****

Hints & Tips plus Security Awareness

Bank Trends in Safeguarding Seniors' Financial Lives
Scam artists are ever on the move to exploit America's seniors. Banks are taking this threat seriously, and have increased their efforts to combat financial fraud and abuse.
https://www.aba.com/training-events/online-training/bank-trends-in-safeguarding-seniors-financial-lives

Evolving Beyond the Password: It's Time to Up the Ante
While there's an immediate need to improve MFA adoption, it's also critical to move to more advanced and secure passwordless frameworks, including biometrics. The fact that we continue to rely on passwords this deep into the digital age is more than a bit jarring. These alphanumeric scraps, the equivalent of digital skeleton keys, once served as a valuable tool.
https://www.darkreading.com/edge-articles/evolving-beyond-the-password-it-s-time-to-up-the-ante?_mc=NL_DR_EDT_DR_daily_20220625&cid=NL_DR_EDT_DR_daily_20220625&sp_aid=111374&elq_cid=36315893&sp_eh=72a861290e89658b5ada8de6a8a9c12b185e8e45329503691618392cbd15751b&utm_source=eloqua&utm_medium=email&utm_campaign=DR_NL_Dark%20Reading%20Daily_06.25.22&sp_cid=45322&utm_content=DR_NL_Dark%20Reading%20Daily_06.25.22

Evolving Beyond the Password: Vanquishing the Password
Using WebAuthn, physical keys, and biometrics, organizations can adopt more advanced passwordless MFA and true passwordless systems. Getting to passwordless won't be easy, but the concept is finally

gaining momentum. Although several vendors have offered passwordless MFA and true passwordless technology for a few years — mostly relegated to enterprise use — a more comprehensive framework is now taking shape. Apple, Google, and Microsoft have jointly agreed to adopt passwordless in earnest.
https://www.darkreading.com/dr-tech/evolving-beyond-the-password-vanquishing-the-password

7 Steps to Stronger SaaS Security
Continuous monitoring is key to keeping up with software-as-a-service changes, but that's not all you'll need to get better visibility into your SaaS security. When the White House warned all businesses to be on high alert for cyberattacks earlier this year, it was a wake-up call for many. While these kinds of warnings are often directed at government agencies or even critical infrastructure companies, a blanket warning is unusual.
https://www.darkreading.com/cloud/7-steps-to-stronger-saas-security?_mc=NL_DR_EDT_DR_daily_20220627&cid=NL_DR_EDT_DR_daily_20220627&sp_aid=111376&elq_cid=36315893&sp_eh=72a861290e89658b5ada8de6a8a9c12b185e8e45329503691618392cbd15751b&utm_source=eloqua&utm_medium=email&utm_campaign=DR_NL_Dark%20Reading%20Daily_06.27.22&sp_cid=45324&utm_content=DR_NL_Dark%20Reading%20Daily_06.27.22

****

News & Views

Remote work availability for white-collar jobs is down, data shows
Research on on-site, remote and hybrid work models varies. The pandemic provided many employees with their first extended remote-work experience — and many have said they'll never go back. Others have welcomed a return to the office, and still more prefer a hybrid approach, according to March survey results.
https://www.ciodive.com/news/remote-work-white-collar-jobs/626064/?utm_source=Sailthru&utm_medium=email&utm_campaign=Newsletter%20Weekly%20Roundup:%20CIO%20Dive:%20Daily%20Dive%2006-25-2022&utm_term=CIO%20Dive%20Weekender

Ransomware Volume Nearly Doubles 2021 Totals in a Single Quarter
After a 2021 beleaguered by ransomware, attack volumes continue to balloon in 2022. In fact, a report issued Tuesday indicates that in just the first three months of this year, the volume of ransomware detections almost doubled the total volume reported for all of last year.
https://www.darkreading.com/attacks-breaches/ransomware-volume-doubles-2021-totals-single-quarter?_mc=NL_DR_EDT_DR_daily_20220629&cid=NL_DR_EDT_DR_daily_20220629&sp_aid=111421&elq_cid=36315893&sp_eh=72a861290e89658b5ada8de6a8a9c12b185e8e45329503691618392cbd15751b&utm_source=eloqua&utm_medium=email&utm_campaign=DR_NL_Dark%20Reading%20Daily_06.29.22&sp_cid=45352&utm_content=DR_NL_Dark%20Reading%20Daily_06.29.22

BEC: Replacing Ransomware As Preferred Cybercrime
Business email compromise (BEC) is yet another effort by scammers to illegally use the identity of a company in order to gain something. This could be financial gain, but could also be to gather information. Often those who are doing BEC crime issue fake invoices or contracts to customers to try to get them to part with cash, believing erroneously that the requests are legitimate. And the targets of this type of crime are not the entry-level employees, but those who have something those scammers really want.
https://www.sosdailynews.com/news.jspx?&articleid=615D9862E3169B1551FCFCD664A47746&sx=26446

****

"Ctrl -F" for The Board

Stakes for Boards in Succession Planning
Boards of directors know how vital CEO succession planning is, but sometimes a stark reminder arrives to drive the point home, writes Debra Cope in the latest issue of the ABA Banking Journal Directors Briefing. While a profound loss can hit like an earthquake, a bank that's ready to pull its succession plan off the shelf and put it into action is in the best position to handle the shockwaves.
https://bankingjournal.aba.com/2022/06/when-its-time-to-invoke-the-succession-plan/?utm_source=eloqua&utm_medium=email&utm_campaign=newsbytes&utm_content=NEWSBYTES-20220629

Security disconnect: Why the CISO role is evolving
CISOs are too focused on security operations, writing policies or vendor management. Their time is better spent shaping business strategy. Non-security business leaders perceive cybersecurity as a technical issue that does not drive business outcomes.
https://www.cybersecuritydive.com/news/gartner-ciso-role-evolution-security-leader/610330/?utm_source=Sailthru&utm_medium=email&utm_campaign=Issue:%202022-06-28%20Cybersecurity%20Dive%20%5Bissue:42733%5D&utm_term=Cybersecurity%20Dive

Questions
Contact FIPCO's Rob Foxx at 800-722-3498 ext. 249 or email FIPCO IT Services for more information.

"Make Security Part of You and Your Institution's DNA!"

Threat Intelligence Newsletter: July 12, 2022

Upcoming Threat Intelligence Peer Group Discussions
None available at the current time

****

Alerts & Warnings

Ransomware Strain Uses RDP Flaws to Hack Into Your Network
MedusaLocker ransomware actors most often gain access to victim devices through vulnerable Remote Desktop Protocol (RDP) configurations [T1133]. Actors also frequently use email phishing and spam email campaigns—directly attaching the ransomware to the email—as initial intrusion vectors [T1566].
https://www.cisa.gov/uscert/ncas/alerts/aa22-181a

Google Chrome WebRTC Zero-Day Faces Active Exploitation
The heap buffer-overflow issue in Chrome for Android could be used for DoS, code execution, and more. A zero-day security vulnerability in Google Chrome for Android is being actively exploited in the wild, the Internet giant says.
https://www.darkreading.com/vulnerabilities-threats/google-chrome-webrtc-zero-day-active-exploitation?_mc=NL_DR_EDT_DR_daily_20220706&cid=NL_DR_EDT_DR_daily_20220706&sp_aid=111496&elq_cid=36315893&sp_eh=72a861290e89658b5ada8de6a8a9c12b185e8e45329503691618392cbd15751b&utm_source=eloqua&utm_medium=email&utm_campaign=DR_NL_Dark%20Reading%20Daily_07.06.22&sp_cid=45405&utm_content=DR_NL_Dark%20Reading%20Daily_07.06.22

Preparing for Retaliatory Attacks From Russia
FBI's Elvis Chan Warns Businesses Against Complacency. "I'm concerned that at some point the Russians are going to launch cyber retaliatory attacks against the United States at election infrastructure and the transportation, financial and energy sectors," says Elvis Chan, supervisory special agent at the San Francisco Division of the FBI.
https://www.govinfosecurity.com/preparing-for-retaliatory-attacks-from-russia-a-19442?rf=2022-07-02__ACQ_DBT__Slot8_ART19442&mkt_tok=MDUxLVpYSS0yMzcAAAGFXnQ2WPgVMAHmhCwKCYEFRKjPmopbi-apWj6fmuH--9yMvVax6i18myZD9__aM-gPhy3bX5cNm0e5NcywDTgj6D-wbPTgnmqpKwXBR-fqKCZn7yUT9w

Software Supply Chain Attack Hits Thousands of Apps
Security researchers at ReversingLabs have reportedly uncovered a new supply chain attack impacting software manufacturing that affects thousands of applications and websites. According to the researchers, the software is impacted due to the use of malicious npm packages and modules dating back at least six months.
https://www.infosecurity-magazine.com/news/software-supply-chain-attack/

On Guard! LinkedIn Scams Are Soaring
Scams on LinkedIn, the social media site for professionals, with more than 800 million members, have unexpectedly rocketed by more than 200 percent during the first half of this year. Researchers can't pinpoint the cause beyond noting that the surge is due to cunning phishing attempts offering fake job opportunities in order to steal login credentials. But it's enough to set alarm bells ringing among the network and Internet security firms.
https://scambusters.org/linkedin3.html

Shimming Right Along To Skim Your Payment Card Number
By now, most of us have at least one or two EMV (Europay, MasterCard, Visa) cards. These are the payment cards that were touted as far more secure than the ones with the magnetic strips on the backs. And indeed, if you ask Visa these cards have resulted in a 75% decrease in fraud in the three years since they were introduced. Cybercriminals are of course finding ways to take advantage of the EMV cards too. Now, there are reports of a new method called “shimming,” which is the new “skimming.”
https://www.sosdailynews.com/news.jspx?&articleid=7FFA0E98AA9EFF1C8CDF3C4DC27ADFFC&sx=26446

****

Hints & Tips plus Security Awareness

How tech leaders can earn C-suite trust
Do corporate boards of directors see the CIO as a trusted advisor? More often than not, the answer is no. The clout of senior technology executives is growing in the C-suite as more companies act on aspirations to become technology companies. But without trust in their actions and counsel, a company can fail to innovate at the pace it wants to in an age of increasing technology dependency.
https://www.ciodive.com/news/C-suite-trust-CIO-executives/626476/?utm_source=Sailthru&utm_medium=email&utm_campaign=Issue:%202022-07-06%20CIO%20Dive%20%5Bissue:42885%5D&utm_term=CIO%20Dive

18 Zero-Days Exploited So Far in 2022
It didn't have to be this way: So far 2022's tranche of zero-days shows too many variants of previously patched security bugs, according Google Project Zero. So far this year, a total of 18 security vulnerabilities have been exploited as unpatched zero-days in the wild, according to an analysis – and half of those were preventable flaws.
https://www.darkreading.com/vulnerabilities-threats/18-zero-days-exploited-2022?_mc=NL_DR_EDT_DR_daily_20220701&cid=NL_DR_EDT_DR_daily_20220701&sp_aid=111454&elq_cid=36315893&sp_eh=72a861290e89658b5ada8de6a8a9c12b185e8e453295036916l8392cbd15751b&utm_source=eloqua&utm_medium=email&utm_campaign=DR_NL_Dark%20Reading%20Daily_06.30.22&sp_cid=45377&utm_content=DR_NL_Dark%20Reading%20Daily_06.30.22

Zero-Days Aren't Going Away Anytime Soon & What Leaders Need to Know
There were a record number of zero-day attacks last year, but some basic cyber-hygiene strategies can help keep your organization more safe. Few security exploits are the source of more sleepless nights for security professionals than zero-day attacks.
https://www.darkreading.com/attacks-breaches/zero-days-aren-t-going-away-anytime-soon-and-what-leaders-need-to-know?_mc=NL_DR_EDT_DR_daily_20220701&cid=NL_DR_EDT_DR_daily_20220701&sp_aid=111454&elq_cid=36315893&sp_eh=72a861290e89658b5ada8de6a8a9c12b185e8e45329503691618392cbd15751b&utm_source=eloqua&utm_medium=email&utm_campaign=DR_NL_Dark%20Reading%20Daily_06.30.22&sp_cid=45377&utm_content=DR_NL_Dark%20Reading%20Daily_06.30.22

****

News & Views

3 Cyber Threats Resulting From Today's Technology Choices to Hit Businesses by 2024
Companies need to consider the cost to disengage from the cloud along with proactive risk management that looks at governance issues resulting from heavy use of low- and no-code tools.
https://www.darkreading.com/vulnerabilities-threats/3-cyber-threats-resulting-from-today-s-technology-choices-to-hit-businesses-by-2024?_mc=NL_DR_EDT_DR_daily_20220706&cid=NL_DR_EDT_DR_daily_20220706&sp_aid=111496&elq_cid=36315893&sp_eh=72a861290e89658b5ada8de6a8a9c12b185e8e45329503691618392cbd15751b&utm_source=eloqua&utm_medium=email&utm_campaign=DR_NL_Dark%20Reading%20Daily_07.06.22&sp_cid=45405&utm_content=DR_NL_Dark%20Reading%20Daily_07.06.22

5 Surprising Cyberattacks AI Stopped This Year
See how these novel, sophisticated, or creative threats used techniques such as living off the land to evade detection from traditional defensive measures — but were busted by AI. We're now halfway through 2022, and already we have seen a range of cyberattacks, familiar and unfamiliar, disrupting organizations. However, we have also seen uplifting stories of successful threat detection efforts, as well.
https://www.darkreading.com/dr-tech/5-surprising-cyberattacks-ai-stopped-this-year?_mc=NL_DR_EDT_DR_daily_20220702&cid=NL_DR_EDT_DR_daily_20220702&sp_aid=111467&elq_cid=36315893&sp_eh=72a861290e89658b5ada8de6a8a9c12b185e8e45329503691618392cbd15751b&utm_source=eloqua&utm_medium=email&utm_campaign=DR_NL_Dark%20Reading%20Daily_07.02.22&sp_cid=45385&utm_content=DR_NL_Dark%20Reading%20Daily_07.02.22

US, Israel Initiate Cybersecurity Collaboration Program
Plan Aims to Enhance Cyber Resilience of the 2 Nations' Critical Infrastructure. The U.S. and Israel have agreed to a new joint cybersecurity program called BIRD Cyber to enhance the cyber resilience of both countries' critical infrastructures. Grants of up to $1.5 million will be given to entities who jointly develop advanced cybersecurity applications under this program.
https://www.databreachtoday.com/us-israel-initiate-cybersecurity-collaboration-program-a-19500?rf=2022-07-05_ENEWS_ACQ_DBT__Slot6_ART19500&mkt_tok=MDUxLVpYSS0yMzcAAAGFbgi_UVI3sPDJsrhnmw-g7MJw6ZvLjiucUB4Itp5_B-vWMHAuNga_QS-VOvBlXGTIEVxdLp9CLh0jhidedJd_yDLY-RpesEDzljONfEQhu4eTOz7yYA

Horizon Offers $1M Bounty to Hackers Who Stole $100M
Attackers Appear to Have Compromised a Multi-Signature Contract. Blockchain company Harmony has offered a $1 million bounty to hackers who stole $100 million worth of Ethereum tokens. It also says it won't push for criminal charges if the funds are returned.
https://www.databreachtoday.com/horizon-offers-1m-bounty-to-hackers-who-stole-100m-a-19457?rf=2022-07-02__ACQ_DBT__Slot1_ART19457&mkt_tok=MDUxLVpYSS0yMzcAAAGFXnQ2V4ci7mpEJ3ajV-6Q8pN04RWPxyLoUjujoj_RQSB5fmUczj1et6efMrTJpHQdObW9Xsi2FSs0rgT10BYrJNFrYXrwOg9Li6D9oGR-bW6fHf_4kA

****

"Ctrl -F" for The Board

The Value of Competitor Social Media Analysis
Social media for banks is a necessity. That's a given. You meet customers where they are, and today, that's online. But customers (and potential customers) are not just engaging and interacting with one bank's website, apps and social accounts. They are seeing competitors' accounts, too. Bank marketers must leverage social media analytics to understand what works for their competitors—and figure out how to do it better
https://bankingjournal.aba.com/2022/07/the-value-of-competitor-social-media-analysis/?utm_source=eloqua&utm_medium=email&utm_campaign=newsbytes&utm_content=NEWSBYTES-20220706

CISO priorities for the second half of 2022
Sometimes sticking to the basics is the best approach. That's what CISOs say they will focus on as their priorities in the second half of 2022.
https://www.cybersecuritydive.com/news/ciso-priorities-for-the-second-half-of-2022/626490/?utm_source=Sailthru&utm_medium=email&utm_campaign=Issue:%202022-07-06%20Cybersecurity%20Dive%20%5Bissue:42913%5D&utm_term=Cybersecurity%20Dive

Questions
Contact FIPCO's Rob Foxx at 800-722-3498 ext. 249 or email FIPCO IT Services for more information.

"Make Security Part of You and Your Institution's DNA!"

Threat Intelligence Newsletter: July 15, 2022

FIPCO®
IT Audit
Round Table
Discussions

Upcoming Threat Intelligence Peer Group Discussions
None available at the current time

****

Alerts & Warnings

Why Browser Vulnerabilities Are a Serious Threat — and How to Minimize Your Risk
Everyone uses browsers to access a wide range of networked systems, from shopping sites to enterprise management. As a result, browsers collect tons of sensitive information — from passwords to credit card data — that hackers are eager to get their hands on.
https://www.darkreading.com/attacks-breaches/why-browser-vulnerabilities-are-a-serious-threat-and-how-to-minimize-your-risk?_mc=NL_DR_EDT_DR_daily_20220707&cid=NL_DR_EDT_DR_daily_20220707&sp_aid=111517&elq_cid=36315893&sp_eh=72a861290e89658b5ada8de6a8a9c12b185e8e45329503691618392cbd15751b&utm_source=eloqua&utm_medium=email&utm_campaign=DR_NL_Dark%20Reading%20Daily_07.07.22&sp_cid=45413&utm_content=DR_NL_Dark%20Reading%20Daily_07.07.22

Fake Google Software Updates Spread New Ransomware
"HavanaCrypt" is also using a command-and-control server that is hosted on a Microsoft Hosting Service IP address, researchers say. Threat actors are increasingly using fake Microsoft and Google software updates to try to sneak malware on target systems. The latest example is "HavanaCrypt," a new ransomware tool that researchers from Trend Micro recently discovered in the wild disguised as a Google Software Update application.
https://www.darkreading.com/attacks-breaches/attacker-using-fake-google-software-update-to-distribute-new-ransomware?_mc=NL_DR_EDT_DR_daily_20220712&cid=NL_DR_EDT_DR_daily_20220712&sp_aid=111583&elq_cid=36315893&sp_eh=72a861290e89658b5ada8de6a8a9c12b185e8e45329503691618392cbd15751b&utm_source=eloqua&utm_medium=email&utm_campaign=DR_NL_Dark%20Reading%20Daily_07.12.22&sp_cid=45457&utm_content=DR_NL_Dark%20Reading%20Daily_07.12.22

New Phishing Attacks Shame, Scare Victims into Surrendering Twitter, Discord Credentials
Scams pressure victims to "resolve an issue that could impact their status, business." A recent wave of social media phishing schemes doubles down on aggressive scare tactics with phony account-abuse accusations to coerce victims into handing over their login details. Last week alone, Malwarebytes Labs uncovered two phishing scams, targeting Twitter and Discord (a voice, video, and text chat app).
https://www.darkreading.com/remote-workforce/new-wave-phishing-attacks-shame-scare-victims-into-surrendering-twitter-discord-credentials?_mc=NL_DR_EDT_DR_daily_20220712&cid=NL_DR_EDT_DR_daily_20220712&sp_aid=111583&elq_cid=36315893&sp_eh=72a861290e89658b5ada8de6a8a9c12b185e8e45329503691618392cbd15751b&utm_source=eloqua&utm_medium=email&utm_campaign=DR_NL_Dark%20Reading%20Daily_07.12.22&sp_cid=45457&utm_content=DR_NL_Dark%20Reading%20Daily_07.12.22

RedAlert: A Ransomware that Targets Multiple OS Platforms
RedAlert (aka N13V), a new ransomware threat, has been found, that encrypts both Windows and Linux VMWare ESXi servers.
https://cyware.com/news/redalert-a-ransomware-that-targets-multiple-os-platforms-47b4d715?_hsmi=78978938&_hsenc=p2ANqtz-90o9cVF-3hvQYG-Yc56QknHtiV8-zopuo3ee1iGLLT5MtxLmeGs1jMmfazvyqdDMS8iR8aBnrAmmYix40FMDmGovZpvg

****

Hints & Tips plus Security Awareness

NIST releases encryption tools to combat quantum computing threats
The Commerce Department’s National Institute of Standards and Technology this week selected the first group of encryption tools designed to withstand the assault of a future quantum computer, which could potentially crack the security used to protect privacy in digital systems such as online banking and email software.
https://bankingjournal.aba.com/2022/07/nist-releases-encryption-tools-to-combat-quantum-computing-threats/?utm_source=eloqua&utm_medium=email&utm_campaign=newsbytes&utm_content=NEWSBYTES-20220711

Threat actors favor brute force attacks to hit cloud services
Google Cloud warned that organizations face their greatest threat due to weak passwords and vulnerable software.
https://www.cybersecuritydive.com/news/brute-force-attacks-cloud-services/627100/?utm_source=Sailthru&utm_medium=email&utm_campaign=Issue:%202022-07-13%20Cybersecurity%20Dive%20%5Bissue:43059%5D&utm_term=Cybersecurity%20Dive

What Do All of Those Cloud Cybersecurity Acronyms Mean?
Acronyms serve as a gatekeeper — if you don't sling the lingo, you don't belong. So here's a quick guide to the letter salad of cloud cybersecurity.
https://www.darkreading.com/edge-ask-the-experts/what-do-all-those-cloud-cybersecurity-acronyms-mean-?_mc=NL_DR_EDT_DR_daily_20220709&cid=NL_DR_EDT_DR_daily_20220709&sp_aid=111567&elq_cid=36315893&sp_eh=72a861290e89658b5ada8de6a8a9c12b185e8e45329503691618392cbd15751b&utm_source=eloqua&utm_medium=email&utm_campaign=DR_NL_Dark%20Reading%20Daily_07.09.22&sp_cid=45441&utm_content=DR_NL_Dark%20Reading%20Daily_07.09.22

Apple Lockdown Mode Aims to Prevent State-Sponsored Spyware

Smartphone giant Apple wants to thwart spyware wielded by governments against criminals and dissidents alike through an "extreme, optional protection" feature that lets users limit the functionality of their device. In a preview of its next mobile and desktop operating systems set for debut this fall, the California company unveiled "Lockdown Mode," a set of restrictions that renders many message attachments inaccessible, webpages slower to load and FaceTime calls harder to make. The idea is to sharply reduce the attack surface available to makers of spyware such as Israel's NSO Group or Italy's RCS Labs.
https://www.databreachtoday.com/apple-lockdown-mode-aims-to-prevent-state-sponsored-spyware-a-19531?rf=2022-07-08_ENEWS_ACQ_DBT__Slot6_ART19531&mkt_tok=MDUxLVpYSS0yMzcAAAGFfXmVgquDzwdezzYhOgW3ctf7mBgAZ2aeCsu9W8pPkQOArdXfPyNYpQE57RSKXbQebfZ_9pPA0qw-1ubGysMhqA3rHFVrencvstiSeuGfpY5koMEoCA

A Simple Formula for Getting Your IT Security Budget Approved

Although there is a greater awareness of cybersecurity threats than ever before, it is becoming increasingly difficult for IT departments to get their security budgets approved. Security budgets seem to shrink each year and IT pros are constantly being asked to do more with less. Even so, the situation may not be hopeless. There are some things that IT pros can do to improve the chances of getting their security budgets approved.
https://thehackernews.com/2022/07/a-simple-formula-for-getting-your-it.html?_m=3n%2e009a%2e2785%2eod0ao445rz%2e1s3y

****

News & Views

Why Small And Medium-Sized Companies Face More Cyber Challenges Than Large Ones: Survey

The recent warning from the Cybersecurity and Infrastructure Security Agency (CISA) about the impact of Russia’s invasion of Ukraine was a wake-up call for all companies and organizations about the increased threats of cyberattacks, The failure to pay attention to and act on those threats could create crises for business leaders.
https://www.forbes.com/sites/edwardsegal/2022/07/13/why-small-and-medium-companies-face-more-cyber-challenges-than-large-ones-survey/amp/

Companies cannot see — or protect — nearly half of all device endpoints

Managing corporate devices was hard pre-pandemic. But as digital sprawl bloomed, visibility fell further behind. The growth of remote work since early 2020 created a massive distribution point sprawl within organizations.
https://www.cybersecuritydive.com/news/corporate-endpoint-detection/627143/?utm_source=Sailthru&utm_medium=email&utm_campaign=Issue:%202022-07-13%20Cybersecurity%20Dive%20%5Bissue:43059%5D&utm_term=Cybersecurity%20Dive

Why so many CIOs are ineffective — and what to do about it

Why? It’s not because of the reasons often linked to CIO turnover, like security breaches or failed projects, though those can sometimes be secondary factors. It’s primarily because we haven’t done enough to establish ourselves as strategic business leaders first and technology leaders second.
https://www.ciodive.com/news/cio-strategic-leader-pwc/626759/?utm_source=Sailthru&utm_medium=email&utm_campaign=Newsletter%20Weekly%20Roundup:%20CIO%20Dive:%20Daily%20Dive%2007-09-2022&utm_term=CIO%20Dive%20Weekender

Online Payment Fraud Expected to Cost $343B Over Next 5 Years
Fraudster innovation will continue to drive successful phishing, business email compromise, and socially engineered attacks, researchers say. Despite ratcheted-up efforts to prevent account takeover, fraudsters are cashing in on a range of online payment fraud schemes, which researchers predict will cost retail organizations more than $343 billion over the next five years
https://www.darkreading.com/application-security/online-payment-fraud-expected-to-cost-343b-over-5-years?_mc=NL_DR_EDT_DR_daily_20220712&cid=NL_DR_EDT_DR_daily_20220712&sp_aid=111583&elq_cid=36315893&sp_eh=72a861290e89658b5ada8de6a8a9c12b185e8e45329503691618392cbd15751b&utm_source=eloqua&utm_medium=email&utm_campaign=DR_NL_Dark%20Reading%20Daily_07.12.22&sp_cid=45457&utm_content=DR_NL_Dark%20Reading%20Daily_07.12.22

QuickBooks Vishing Scam Targets Small Businesses
Businesses receive an invoice via email with a credit card charge and are asked to call a fake number and hand over personal information to receive a refund. Cybercriminals are posing as Intuit's popular accounting software package QuickBooks to target Google Workspace and Microsoft 365 small business users in a voice-phishing scam.
https://www.darkreading.com/application-security/quickbooks-vishing-scam-targets-small-businesses?_mc=NL_DR_EDT_DR_daily_20220713&cid=NL_DR_EDT_DR_daily_20220713&sp_aid=111604&elq_cid=36315893&sp_eh=72a861290e89658b5ada8de6a8a9c12b185e8e45329503691618392cbd15751b&utm_source=eloqua&utm_medium=email&utm_campaign=DR_NL_Dark%20Reading%20Daily_07.13.22&sp_cid=45464&utm_content=DR_NL_Dark%20Reading%20Daily_07.13.22

****

"Ctrl -F" for The Board

As cyber talent demand heats up, hiring managers should shift expectations
Companies trying to fill cybersecurity roles need to stop looking for unicorns and expand their search to qualified, but often overlooked, job candidates. A recent data analysis from CyberSeek confirmed what many in cybersecurity know all too well: The job market is on fire. U.S. employers posted roughly 715,000 cybersecurity roles in the 12-month period ending in April 2022. Demand for cybersecurity jobs increased 43% over that 12-month period, compared to 18% for the rest of the job market.
https://www.cybersecuritydive.com/news/cybersecurity-talent-ISACA-ISC2-Cyberseek/626976/?utm_source=Sailthru&utm_medium=email&utm_campaign=Issue:%202022-07-13%20Cybersecurity%20Dive%20%5Bissue:43059%5D&utm_term=Cybersecurity%20Dive

Cybersecurity Has a Talent Shortage & Non-Technical People Offer a Way Out
There's no one-size-fits-all handbook to guide the battle against cybercriminals. Most often, it requires cybersecurity defenders to fit together different pieces of a human puzzle that will vary depending on a myriad of geographical, political, and cultural influences.
https://www.darkreading.com/careers-and-people/cybersecurity-has-a-talent-shortage-non-technical-people-offer-a-way-out?_mc=NL_DR_EDT_DR_daily_20220711&cid=NL_DR_EDT_DR_daily_20220711&sp_aid=111569&elq_cid=36315893&sp_eh=72a861290e89658b5ada8de6a8a9c12b185e8e45329503691618392cbd15751b&utm_source=eloqua&utm_medium=email&utm_campaign=DR_NL_Dark%20Reading%20Daily_07.11.22&sp_cid=45443&utm_content=DR_NL_Dark%20Reading%20Daily_07.11.22

Ransomware Scourge Drives Price Hikes in Cyber Insurance
Cybersecurity insurance costs are rising, and insurers are likely to demand more direct access to organizational metrics and measures to make more accurate risk assessments. The rising cost of ransomware attacks is helping push significant premium increases in cyber-insurance policies in the UK and US, new data shows.
https://www.darkreading.com/attacks-breaches/ransomware-scourge-drives-price-hikes-in-cyber-insurance?_mc=NL_DR_EDT_DR_daily_20220712&cid=NL_DR_EDT_DR_daily_20220712&sp_aid=111583&elq_cid=36315893&sp_eh=72a861290e89658b5ada8de6a8a9c12b185e8e45329503691618392cbd15751b&utm_source=eloqua&utm_medium=email&utm_campaign=DR_NL_Dark%20Reading%20Daily_07.12.22&sp_cid=45457&utm_content=DR_NL_Dark%20Reading%20Daily_07.12.22

Questions
Contact FIPCO’s Rob Foxx at 800-722-3498 ext. 249 or email FIPCO IT Services for more information.

"Make Security Part of You and Your Institution's DNA!"

Threat Intelligence Newsletter: July 22, 2022

FIPCO®
IT Audit
Round Table
Discussions

Upcoming Threat Intelligence Peer Group Discussions
None available at the current time

****

Alerts & Warnings

Travelers Wants Out of Contract With Insured That Allegedly Misrepresented MFA Use
In what may be one of the first court filings of its kind, insurer Travelers is asking a district court for a ruling to rescind a policy because the insured allegedly misrepresented its use of multifactor authentication (MFA) – a condition to get cyber coverage.
https://www.insurancejournal.com/news/national/2022/07/12/675516.htm

Large-Scale Phishing Campaign Bypasses Multifactor Authentication
Researchers from Microsoft last week discovered multiple iterations of an adversary-in-the-middle phishing campaign that has targeted more than 10,000 organizations since September 2021. Per the blog, the attempts target Office 365 users by spoofing the Office online authentication page, which serves as the AiTM agent by intercepting the whole authentication process and extracting data such as passwords and session cookies.
https://www.microsoft.com/security/blog/2022/07/12/from-cookie-theft-to-bec-attackers-use-aitm-phishing-sites-as-entry-point-to-further-financial-fraud/?utm_source=eloqua&utm_medium=email&utm_campaign=riskcyberbulletin&utm_content=RiskCyber-20220718

PayPal-themed phishing kit allows complete identity theft
Sometimes phishers are just after your username and password, but other times they are after every scrap of sensitive information they can extract from you. To do that, they use tools like the phishing kit recently analyzed by Akamai researchers.
https://www.helpnetsecurity.com/2022/07/14/paypal-themed-phishing-kit/

LockBit ransomware hitting network servers
The implications of threat actors gaining access to network servers and spreading ransomware is worrisome because once the malware gains admin controls it can create a group policy to stop services,

end processes and reproduce quicker at greater scale. Affiliates of the LockBit ransomware group are infiltrating on-premises servers to spread malware on targeted networks.
https://www.cybersecuritydive.com/news/lockbit-ransomware-network-servers/627709/?utm_source=Sailthru&utm_medium=email&utm_campaign=Issue:%202022-07-21%20Cybersecurity%20Dive%20%5Bissue:43257%5D&utm_term=Cybersecurity%20Dive

How Hackers Create Fake Personas for Social Engineering
On April 18, 2022, a handful of US citizens scrambled to get their taxes filed. While tax season is usually a stressor, consider that these filers got some unsolicited help. Imagine that somehow, strangers that might resemble angels just appeared in their lives, offering guidance and help to work with them through this process … all through the computer screen.
https://www.darkreading.com/attacks-breaches/how-hackers-create-fake-personas-for-social-engineering?_mc=NL_DR_EDT_DR_daily_20220721&cid=NL_DR_EDT_DR_daily_20220721&sp_aid=111710&elq_cid=36315893&sp_eh=72a861290e89658b5ada8de6a8a9c12b185e8e45329503691618392cbd15751b&sp_eh=72a861290e89658b5ada8de6a8a9c12b185e8e45329503691618392cbd15751b&utm_source=eloqua&utm_medium=email&utm_campaign=DR_NL_Dark%20Reading%20Daily_07.21.22&sp_cid=45535&utm_content=DR_NL_Dark%20Reading%20Daily_07.21.22

Hackers steal 50,000 credit cards from 300 U.S. restaurants
Payment card details from customers of more than 300 restaurants have been stolen in two web-skimming campaigns targeting three online ordering platforms. Web-skimmers, or Magecart malware, are typically JavaScript code that collects credit card data when online shoppers type it on the checkout page.
https://www.bleepingcomputer.com/news/security/hackers-steal-50-000-credit-cards-from-300-us-restaurants/?_hsmi=210059059&_hsenc=p2ANqtz-9wfOhGccUBN0N2TWPWZRUwfmC6C2Uvhn_Bc0nhi3NqsXscOfIBTn6gibIxBfC9ifXNCsN2V7WO5_ne___IctHfVK3ag9Q

****

Hints & Tips plus Security Awareness

3 Golden Rules of Modern Third-Party Risk Management
It's time to expand the approach of TPRM solutions so risk management is more effective in the digital world. SaaS-to-SaaS integrations are an inherent part of modern software-as-a-service use in business, and the adoption of third-party services is scaling rapidly to adapt. Malicious actors aren't lagging behind. They realize the lucrative benefits of leveraging these integrations to steal, leak, or abuse organizational assets.
https://www.darkreading.com/risk/3-golden-rules-of-modern-third-party-risk-management?_mc=NL_DR_EDT_DR_daily_20220714&cid=NL_DR_EDT_DR_daily_20220714&sp_aid=111625&elq_cid=36315893&sp_eh=72a861290e89658b5ada8de6a8a9c12b185e8e45329503691618392cbd15751b&utm_source=eloqua&utm_medium=email&utm_campaign=DR_NL_Dark%20Reading%20Daily_07.14.22&sp_cid=45475&utm_content=DR_NL_Dark%20Reading%20Daily_07.14.22

10 Ways to Check Website Safety
Is that website safe? That should be the first question you ask when visiting a new Internet page for the first time. But too often it's not -- you're in a hurry, perhaps it looks okay, or maybe someone you know sent you the link. The result: You end up giving away confidential information or downloading malicious computer code that can result in data and identity theft and, most commonly these days, ransomware.
https://scambusters.org/websitesafe.html

A Simple Formula for Getting Your IT Security Budget Approved
Although there is a greater awareness of cybersecurity threats than ever before, it is becoming increasingly difficult for IT departments to get their security budgets approved. Security budgets seem to shrink each year and IT pros are constantly being asked to do more with less. Even so, the situation may not be hopeless. There are some things that IT pros can do to improve the chances of getting their security budgets approved.
https://thehackernews.com/2022/07/a-simple-formula-for-getting-your-it.html?_m=3n%2e009a%2e2786%2eod0ao445rz%2e1s5c

****

News & Views

How CISOs can prepare for new and unpredictable cyberthreats
CISOs often ask, “How do I avoid being hit by the next major cyberattack?” The problem is, that’s the wrong question. If there’s one thing every CISO knows to be true, it’s that cybersecurity is unpredictable.
https://www.cybersecuritydive.com/news/CISO-cyber-threat-strategy/626947/?utm_source=Sailthru&utm_medium=email&utm_campaign=Newsletter%20Weekly%20Roundup:%20Cybersecurity%20Dive:%20Daily%20Dive%2007-16-2022&utm_term=Cybersecurity%20Dive%20Weekender

Too Much Remains Unknown About Data Breaches
Ransomware attacks and data breaches: One thing both have in common, besides the former often causing the latter, is the challenge of attempting to accurately understand their true scale and impact. A principle problem is that while some organizations report certain types of breaches, oftentimes their breach notifications lack useful detail. How they were hacked, exactly what attackers stole or the identity theft risk facing individuals whose details were exposed all remain secret.
https://www.databreachtoday.com/blogs/too-much-remains-unknown-about-data-breaches-p-3253?rf=2022-07-18_ENEWS_ACQ_DBT__Slot1_BLOG3253&mkt_tok=MDUxLVpYSS0yMzcAAAGFsSeE3jamkUWGqDwrAjW-un2ebqDlE3GNoolboWeSen1M-q5CCVh7vUDsM5-iPk7p9ZErUgWcYGPKZcHUkTbojMtcXk7awkTz-XeWpC0KIshd7IxqvQ

****

"Ctrl -F" for The Board

5 Key Things We Learned from CISOs of Smaller Enterprises Survey
New survey reveals lack of staff, skills, and resources driving smaller teams to outsource security. As business begins its return to normalcy (however "normal" may look), CISOs at small and medium-size enterprises (500 – 10,000 employees) were asked to share their cybersecurity challenges and priorities, and their responses were compared the results with those of a similar survey from 2021.
https://thehackernews.com/2022/07/5-key-things-we-learned-from-cisos-of.html?_m=3n%2e009a%2e2787%2eod0ao445rz%2e1s62

Questions
Contact FIPCO’s Rob Foxx at 800-722-3498 ext. 249 or email FIPCO IT Services for more information.

"Make Security Part of You and Your Institution's DNA!"

Threat Intelligence Newsletter: August 1, 2022

FIPCO®
IT Audit
Round Table
Discussions

Upcoming Threat Intelligence Peer Group Discussions
None available at the current time

****

Alerts & Warnings

What chip price hikes will mean for enterprise tech buyers
As semiconductor costs rise, executives lie at a crossroads: defer projects or ask for more resources? Inflation is carving a path across sectors — and computer chip prices show it. Intel recently began informing customers of upcoming price hikes, the company confirmed in an email to CIO Dive.
https://www.ciodive.com/news/semiconductor-chip-price-hikes-IT/627953/?utm_source=Sailthru&utm_medium=email&utm_campaign=Issue:%202022-07-25%20CIO%20Dive%20%5Bissue:43318%5D&utm_term=CIO%20Dive

Snowballing Ransomware Variants Highlight Growing Threat to VMware ESXi Environments
Luna, Black Basta add to rapidly growing list of malware tools targeted at virtual machines deployed on VMware's bare-metal hypervisor technology. The latest confirmations of the growing attacker interest in VMware ESXi environments are two ransomware variants that surfaced in recent weeks and have begun hitting targets worldwide.
https://www.darkreading.com/attacks-breaches/snowballing-ransomware-variants-highlight-growing-threat-to-vmware-esxi-environments?_mc=NL_DR_EDT_DR_daily_20220725&cid=NL_DR_EDT_DR_daily_20220725&sp_aid=111740&elq_cid=36315893&sp_eh=72a861290e89658b5ada8de6a8a9c12b185e8e45329503691618392cbd15751b&sp_eh=72a861290e89658b5ada8de6a8a9c12b185e8e45329503691618392cbd15751b&utm_source=eloqua&utm_medium=email&utm_campaign=DR_NL_Dark%20Reading%20Daily_07.25.22&sp_cid=45566&utm_content=DR_NL_Dark%20Reading%20Daily_07.25.22

Magecart Supply Chain Attacks Hit Hundreds of Restaurants
Security researchers have identified two seperate Magecart campaigns that target online ordering platforms. The campaigns are designed by the attackers for financial gain and the Magecart e-skimming

software possesses the ability to exfiltrate card details. So far, the campaign has affected at least 311 US restaurants by injecting the software into three platforms.
https://www.infosecurity-magazine.com/news/magecart-supply-chain-attacks/

Sending Phishing Emails From PayPal
In June, we wrote about how hackers were sending phishing emails directly from QuickBooks. It worked like this: A hacker would create a free account in QuickBooks. They would create a spoofed invoice, either for Norton or Microsoft, and then send it to the user. Since it's created in QuickBooks, the email comes across as legitimate.
https://www.avanan.com/blog/sending-phishing-emails-from-paypal

****

Hints & Tips plus Security Awareness

3 ways going "passwordless" benefits your IT team
Companies that shift to passwordless systems find their IT teams spend less time on password issues, are less stressed about dealing with passwords, and can focus on more strategic issues. Webinar Aug 2, 2022 11:00AM CST
https://resources.industrydive.com/a-passwordless-world?utm_source=CIO&utm_medium=InlineJuly25&utm_campaign=LastPass

What the POTS shutdown will mean for faxing in the banking industry
After a remarkable 100-year run, the FCC is officially closing the door on traditional analog copper POTS (Plain Old Telephone Service), the standard telephone infrastructure we've all used forever. For businesses in virtually every industry, the old-fashioned copper wires have been the default communication protocol not only for phone usage but for other services such as analog fax lines and—for banks and other financial services institutions in particular—onsite alarm systems.
https://www.bankingdive.com/spons/what-the-pots-shutdown-will-mean-for-faxing-in-the-banking-industry/627696/

Where 5 programs are investing to close cyber skills gap
In line with a White House push to close the cyber skills gap, technology firms, nonprofits and other organizations have launched a range of programs to develop a new generation of workers. The National Cyber Workforce and Education Summit highlighted an ongoing push to help meet an urgent demand for qualified cybersecurity professionals.
https://www.cybersecuritydive.com/news/cyber-skills-gap/627835/?utm_source=Sailthru&utm_medium=email&utm_campaign=Issue:%202022-07-26%20Cybersecurity%20Dive%20%5Bissue:43366%5D&utm_term=Cybersecurity%20Dive

Where colocation fits in the modernization roadmap
Despite cloud benefits, many companies struggle to contain costs and reap the upsides of migration, creating opportunities for colocation data centers. On-premises data center use is in slow but steady decline as companies shift workloads to the cloud. But businesses are realizing the cloud is far from a one-stop shop, creating opportunities for colocation data centers.
https://www.ciodive.com/news/colocation-data-center-migration-hybrid-cloud/628051/?utm_source=Sailthru&utm_medium=email&utm_campaign=Issue:%202022-07-26%20CIO%20Dive%20%5Bissue:43348%5D&utm_term=CIO%20Dive

How to retain tech talent

Leaders must rely on multiple strategies — from compensation to project assignment — to show employees a long-term career arc within their ranks. While recession fears ripple through the market, the last two years of business technology resilience has illustrated why the IT function will become more, not less, important to organization navigating financial challenges.

https://www.ciodive.com/news/tech-talent-retention-salaries-culture-upskilling/627395/?utm_source=Sailthru&utm_medium=email&utm_campaign=Issue:%202022-07-25%20CIO%20Dive%20%5Bissue:43318%5D&utm_term=CIO%20Dive

****

News & Views

Relentless vulnerabilities and patches induce cybersecurity burnout

Cybersecurity professionals are confronting a chronic vulnerability-patch cycle and the situation is getting worse. A relentless pace of vulnerability discoveries and disclosures imposes a cyclical patching process on cybersecurity professionals that has proven unsustainable for most organizations.

https://www.cybersecuritydive.com/news/vulnerabilities-patches-burnout/628123/?utm_source=Sailthru&utm_medium=email&utm_campaign=Issue:%202022-07-26%20Cybersecurity%20Dive%20%5Bissue:43366%5D&utm_term=Cybersecurity%20Dive

No More Ransom helps millions of ransomware victims in 6 years

The No More Ransom project celebrates its sixth anniversary today after helping millions of ransomware victims recover their files for free. Launched in July 2016, No More Ransom is an online portal and a public-private partnership created by law enforcement (Europol and the Dutch National Police) and IT security companies (Kaspersky and McAffee).

https://www.bleepingcomputer.com/news/security/no-more-ransom-helps-millions-of-ransomware-victims-in-6-years/?utm_source=Sailthru&utm_medium=email&utm_campaign=Issue:%202022-07-26%20Cybersecurity%20Dive%20%5Bissue:43366%5D&utm_term=Cybersecurity%20Dive

How Risk-Based Vulnerability Management Has Made Security Easier

Trying to remediate everything was never a winning strategy. RBVM is an approach that gets organizations better results with less effort. For the past five years, the National Vulnerability Database (NVD) has broken its own record of reported vulnerabilities and is on pace to do the same in 2022. With a threat landscape growing that quickly, it's no surprise to see security teams can't keep pace.

https://www.darkreading.com/risk/how-risk-based-vulnerability-management-has-made-security-easier?_mc=NL_DR_EDT_DR_daily_20220727&cid=NL_DR_EDT_DR_daily_20220727&sp_aid=111771&elq_cid=36315893&sp_eh=72a861290e89658b5ada8de6a8a9c12b185e8e45329503691618392cbd15751b&sp_eh=72a861290e89658b5ada8de6a8a9c12b185e8e45329503691618392cbd15751b&utm_source=eloqua&utm_medium=email&utm_campaign=DR_NL_Dark%20Reading%20Daily_07.27.22&sp_cid=45588&utm_content=DR_NL_Dark%20Reading%20Daily_07.27.22

****

"Ctrl -F" for The Board

Big Banks Face Big Fines Over Messaging Apps
Five of America’s biggest investment banks are preparing to pay a combined $1 billion in fines for letting their workers use unauthorized messaging apps. As Bloomberg News reported Friday (July 15), Morgan Stanley is preparing to pay a $200 million fine, the same amount JPMorgan Chase has already paid. Meanwhile, Citigroup, Goldman Sachs and Bank of America are also in discussions to pay a similar fine to regulators, sources told Bloomberg.
https://www.pymnts.com/bank-regulation/2022/big-banks-face-big-fines-over-messaging-apps/

How ‘Invisible’ Tech Is Revolutionizing the U.S. Banking System
There are upward of 10,000 depository institutions, spanning banks, credit unions and other providers. All of them, Vermeersch said, are grappling with a continuing shift in the way banking is being done and a shift in how consumers and commercial enterprises want to bank. An increasing slice of daily financial life is being conducted on mobile devices and tablets — and apps, too, of course.
https://www.pymnts.com/digital-first-banking/2022/how-invisible-tech-is-revolutionizing-the-u-s-banking-system/

Cryptocurrency regulation is changing. Here’s what you need to know
The emergence of crypto assets, such as cryptocurrencies, is seen by many as part of a broader trend toward more diverse financial market infrastructures that both enhance choice and offer new ways to meet current and future payment needs.
https://www.weforum.org/agenda/2022/07/cryptocurrency-regulation-global-standard/

Questions
Contact FIPCO’s Rob Foxx at 800-722-3498 ext. 249 or email FIPCO IT Services for more information.

"Make Security Part of You and Your Institution's DNA!"

Threat Intelligence Newsletter: August 5, 2022

FIPCO®
IT Audit
Round Table
Discussions

Upcoming Threat Intelligence Peer Group Discussions
None available at the current time

****

Alerts & Warnings

Data breaches grow costlier for financial institutions
Data breaches cost financial intuitions an average of $5.97 million in 2021 and 2022, with health care being the only sector with a higher cost per breach, according to a report released yesterday by IBM Security. IBM commissioned a 12-month study of 550 organizations across multiple sectors as part of an annual report on data breaches. The cost of dealing with a data breach for financial institutions rose by $250,000 compared to a similar study conducted in 2020-2021. IBM defined financial services as banks, insurance and investment companies.
https://bankingjournal.aba.com/2022/07/data-breaches-grow-costlier-for-financial-institutions/?utm_source=eloqua&utm_medium=email&utm_campaign=newsbytes&utm_content=NEWSBYTES-20220729

VirusTotal: Threat Actors Mimic Legitimate Apps, Use Stolen Certs to Spread Malware
A study of malware submitted to VirusTotal shows cybercriminals and other threat actors are deploying a variety of abuse-of-trust approaches to spread malware and to dodge traditional defenses, often exploiting the implicit trust between a reputable software supplier and the user.
https://www.darkreading.com/vulnerabilities-threats/virustotal-threat-actors-mimic-legitimate-apps-use-stolen-certs-to-spread-malware?_mc=NL_DR_EDT_DR_daily_20220803&cid=NL_DR_EDT_DR_daily_20220803&sp_aid=111893&elq_cid=36315893&sp_eh=72a861290e89658b5ada8de6a8a9c12b185e8e45329503691618392cbd15751b&sp_eh=72a861290e89658b5ada8de6a8a9c12b185e8e45329503691618392cbd15751b&utm_source=eloqua&utm_medium=email&utm_campaign=DR_NL_Dark%20Reading%20Daily_08.03.22&sp_cid=45655&utm_content=DR_NL_Dark%20Reading%20Daily_08.03.22

Massive New Phishing Campaign Targets Microsoft Email Service Users

The campaign uses adversary-in-the-middle techniques to bypass multifactor authentication, evade detection. Researchers are warning about a new, large-scale phishing campaign aimed at Microsoft Outlook email services users. The team at ThreatLabz discovered the new phishing kit and said it uses an adversary-in-the-middle (AiTM) model, which can be effective for evading detection by email and network security protections, as well as bypassing multifactor authentication protections.
https://www.darkreading.com/attacks-breaches/massive-new-phishing-campaign-targeting-microsoft-email-users?_mc=NL_DR_EDT_DR_daily_20220803&cid=NL_DR_EDT_DR_daily_20220803&sp_aid=111893&elq_cid=36315893&sp_eh=72a861290e89658b5ada8de6a8a9c12b185e8e45329503691618392cbd15751b&sp_eh=72a861290e89658b5ada8de6a8a9c12b185e8e45329503691618392cbd15751b&utm_source=eloqua&utm_medium=email&utm_campaign=DR_NL_Dark%20Reading%20Daily_08.03.22&sp_cid=45655&utm_content=DR_NL_Dark%20Reading%20Daily_08.03.22

Scammers Sent Uber to Take Elderly Lady to the Bank

Email scammers sent an Uber to the home of an 80-year-old woman who responded to a well-timed email scam, in a bid to make sure she went to the bank and wired money to the fraudsters. In this case, the woman figured out she was being scammed before embarking for the bank, but her story is a chilling reminder of how far crooks will go these days to rip people off.
https://krebsonsecurity.com/2022/08/scammers-sent-uber-to-take-elderly-lady-to-the-bank/

Be careful what you download: 17 password-stealing Android apps removed from Google Play

Cybersecurity researchers say DawDropper campaign delivered four kinds of trojan malware to victims after bypassing Play Store protections. Seventeen malicious apps designed to infect Google Android users with banking malware have been removed from the Play Store. The malware campaign has been detailed by cybersecurity researchers at Trend Micro who've dubbed it DawDropper and say it delivers four types of banking trojan – TeaBot, Octo, Hydra and Ermac – in what's described as a dropper-as-a-service (DaaS) attack because the payload is only dropped after the app has been downloaded.
https://www.zdnet.com/article/be-careful-what-you-download-17-password-stealing-android-apps-removed-from-google-play/

Microsoft warns of stealthy backdoors used to target Exchange Servers

There's been an uptick in malware native to Microsoft's Internet Information Services (IIS) web server that is being used to install backdoors or steal credentials and is hard to detect, warns Microsoft. Microsoft has offered insights into how to spot and remove malicious IIS extensions, which aren't as popular as web shells as a payload for Exchange servers but are useful to an attacker as they "mostly reside in the same directories as legitimate modules used by target applications, and they follow the same code structure as clean modules," Microsoft notes.
https://www.zdnet.com/article/microsoft-warns-of-stealthy-backdoors-used-to-target-exchange-servers-email/

Watch Out For These 7 Costly Inflation Scams

Scammers are piling misery on top of the 40-year high level of inflation by cashing in on the cost-of-living crunch that's sweeping the nation. They know consumers, especially those who live from one paycheck to the next, are worrying about making ends meet. According to the Better Business Bureau, consumers are starting to panic about rising costs and the possibility of further increases in the coming months. That makes them extra-vulnerable to scams pretending to ease their financial burden.
https://scambusters.org/inflation.html

QR Code Dangers And The Risks Behind Using Them
There's danger now lurking behind those busy black-and-white boxes that are QR codes and that now seem to be found everywhere for everything, including viewing restaurant menus. Always a quick way scan for information, more businesses are using them now more than ever. A study by Ivanti takes a look at what's really going on behind QR's and their findings should make anyone think twice before they reach to scan a QR code with their mobile device.
https://www.sosdailynews.com/news.jspx?&articleid=5E431EC65F76C0C75A318F49863AF72D&sx=26446

Can Hackers Take A Bite Out Of Your Mobile Pay Solution?
With the many digital payment options available today, finding the most secure providers can be a challenge. The popularity of digital wallets has grown over time and writing checks and even using plastic cards for payments are quickly becoming the dinosaurs of our non-digital past. Mobile payment apps like Venmo (owned by PayPal) and PayPal itself are popular payment apps, but each have suffered their share of hacking problems. Many users now own mobile wallets and pay for goods and services with a quick tap of their phone. Using a mobile pay solution like Apple Pay, Google Pay, or Samsung Pay for those transactions may offer peace of mind knowing your payment data is safe and out of the reach of hackers.
https://www.sosdailynews.com/news.jspx?&articleid=98AFD2BFEC907438BCDB397136B75172&sx=26446

Cisco Business Routers Found Vulnerable to Critical Remote Hacking Flaws
Cisco on Wednesday rolled out patches to address eight security vulnerabilities, three of which could be weaponized by an unauthenticated attacker to gain remote code execution (RCE) or cause a denial-of-service (DoS) condition on affected devices.
https://thehackernews.com/2022/08/cisco-business-routers-found-vulnerable.html?_m=3n%2e009a%2e2803%2eod0ao445rz%2e1skg

****

Hints & Tips plus Security Awareness

Survey finds young people most likely to fall for phone scams
More than half of mobile subscribers reported losing money to phone scam calls in a recent survey on the prevalence of the problem, with young people the most likely to fall for scams. Branded communications provider First Orion surveyed 2,100 mobile subscribers about their experiences with scam calls and found that 53% of respondents said they had received more scam calls in 2022 than in 2021. Based on measured proprietary scam call data, the company estimates that U.S. mobile subscribers received more than 100 billion scam calls during the first six months of 2022.
https://bankingjournal.aba.com/2022/08/survey-finds-young-people-most-likely-to-fall-for-phone-scams/?utm_source=eloqua&utm_medium=email&utm_campaign=newsbytes&utm_content=NEWSBYTES-20220803

These ransomware hackers gave up when they hit multi-factor authentication
More evidence that multi-factor authentication works. Police explain how they have seen ransomware gangs abandon attacks when they hit MFA security. A ransomware attack was prevented just because the intended victim was using multi-factor authentication (MFA) and the attackers decided it wasn't worth the effort to attempt to bypass it.
https://www.zdnet.com/article/why-you-really-need-multi-factor-authentication-these-ransomware-hackers-gave-up-when-they-saw-it/?utm_source=eloqua&utm_medium=email&utm_campaign=riskcyberbulletin&utm_content=RiskCyber-20220801

Massive New Security Update For 3.2 Billion Chrome Users Confirmed

Google Chrome security has experienced a busy past few weeks and there is no sign of slowing down. Just days after two emergency fixes for vulnerabilities being exploited in the wild and a record number of Chromium zero-days across 2021 was announced, Google has released another massive security update that applies to billions of Chrome users. The new update that will take Google Chrome to version 101.0.4951.41 fixes more than 30 security vulnerabilities across Windows, Mac, and Linux devices.
https://www.oodaloop.com/briefs/2022/05/02/massive-new-security-update-for-3-2-billion-chrome-users-confirmed/

Getting Ahead of Supply Chain Attacks

Attackers are willing to replicate entire networks, purchase domains, and persist for months, not to mention spend significantly to make these campaigns successful. The one-year anniversary of the Kaseya attack this month marks an appropriate time to look back at supply chain threats and what has — and has not — changed. Let's start with what has changed: more checklists. Oversight across code that's loaded across customer sites now involves far more paperwork, especially for managed service providers (MSPs).
https://www.darkreading.com/attacks-breaches/getting-ahead-of-supply-chain-attacks?_mc=NL_DR_EDT_DR_daily_20220802&cid=NL_DR_EDT_DR_daily_20220802&sp_aid=111868&elq_cid=36315893&sp_eh=72a861290e89658b5ada8de6a8a9c12b185e8e45329503691618392cbd15751b&sp_eh=72a861290e89658b5ada8de6a8a9c12b185e8e45329503691618392cbd15751b&utm_source=eloqua&utm_medium=email&utm_campaign=DR_NL_Dark%20Reading%20Daily_08.02.22&sp_cid=45643&utm_content=DR_NL_Dark%20Reading%20Daily_08.02.22

****

News & Views

Most cyberattacks come from ransomware, email compromise

Attackers are scanning for vulnerabilities in unpatched systems within 15 minutes, stressing the pace and scale of the threat. Attackers gained access to targeted networks through three primary initial vectors: phishing, known software vulnerabilities and brute-force credential attacks.
https://www.cybersecuritydive.com/news/ransomware-email-cyberattacks-unit42/628551/?utm_source=Sailthru&utm_medium=email&utm_campaign=Issue:%202022-08-01%20Cybersecurity%20Dive%20%5Bissue:43507%5D&utm_term=Cybersecurity%20Dive

Staffing woes and inefficient tool use spread IT departments thin

For teams with skilled talent, using inefficient tools leads to less job satisfaction and more retention problems, an IDC analyst said. In many instances, a myriad of obstacles hinder the ability of IT teams to contribute to business goals successfully.
https://www.ciodive.com/news/digital-infrastructure-staffing-shortages/628136/?utm_source=Sailthru&utm_medium=email&utm_campaign=Newsletter%20Weekly%20Roundup:%20CIO%20Dive:%20Daily%20Dive%2007-30-2022&utm_term=CIO%20Dive%20Weekender

****

"Ctrl -F" for The Board

3 Tips for Creating a Security Culture
Trying to get the whole organization on board with better cybersecurity is much tougher than it may sound. With cyberattacks becoming more frequent and costly, not to mention the additional challenges inherent in securing a remote workforce, it is more important than ever that organizations build a culture of security. This of course, isn't a new thing to say and yet it keeps needing to be said. So, why haven't we solved this yet?
https://www.darkreading.com/careers-and-people/3-tips-for-overcoming-challenges-to-creating-a-security-culture?_mc=NL_DR_EDT_DR_daily_20220801&cid=NL_DR_EDT_DR_daily_20220801&sp_aid=111851&elq_cid=36315893&sp_eh=72a861290e89658b5ada8de6a8a9c12b185e8e45329503691618392cbd15751b&sp_eh=72a861290e89658b5ada8de6a8a9c12b185e8e45329503691618392cbd15751b&utm_source=eloqua&utm_medium=email&utm_campaign=DR_NL_Dark%20Reading%20Daily_08.01.22&sp_cid=45629&utm_content=DR_NL_Dark%20Reading%20Daily_08.01.22

Advisory to FDIC-Insured Institutions Regarding Deposit Insurance and Dealings with Crypto Companies
To address certain misrepresentations about FDIC deposit insurance by some crypto companies, the FDIC is issuing an Advisory to FDIC-insured institutions Regarding Deposit Insurance and Dealings with Crypto Companies (FDIC Crypto Advisory). Additionally, a Fact Sheet on What the Public Needs to Know About FDIC Deposit Insurance and Crypto Companies (Deposit Insurance Fact Sheet) has been posted to the FDIC’s website to provide additional information about deposit insurance coverage.
https://www.fdic.gov/news/financial-institution-letters/2022/fil22035.html?source=govdelivery&utm_medium=email&utm_source=govdelivery

Questions
Contact FIPCO’s Rob Foxx at 800-722-3498 ext. 249 or email FIPCO IT Services for more information.

"Make Security Part of You and Your Institution's DNA!"

Threat Intelligence Newsletter: August 12, 2022

FIPCO®
IT Audit
Round Table
Discussions

Upcoming Threat Intelligence Peer Group Discussions
None available at the current time

****

Alerts & Warnings

Twilio Customer Data Breached via SMS Phishing of Employees
What begins with "the security of our customers' data is of paramount importance" and ends with a pledge "to help impacted customers in every way possible"? Enter a data breach notification issued Sunday by Twilio. The San Francisco-based customer engagement platform provider counts hundreds of thousands of businesses as customers. Information collected by the company includes contact details for customers, as well as their customers, plus the contents of messages they send back and forth.
https://www.databreachtoday.com/twilio-customer-data-breached-via-sms-phishing-employees-a-19734?rf=2022-08-09_ENEWS_ACQ_DBT__Slot1_ART19734&mkt_tok=MDUxLVpYSS0yMzcAAAGGIkGbv-FVrFvF3jjqMtoFlzOHSQWKunAKx-IOqHT1AQJDBBD4gp6WLyn_8P_zQoPKW1hgpqSpnomB2dMOF9rhEWJadlKqev0aucYMoZ5UDxCi1ndWhQ

Stolen Data Gives Attackers Advantage Against Text-Based 2FA
With names, email addresses, and mobile numbers from underground databases, one person in five is at risk of account compromise even with SMS two-factor authentication in place. Companies that rely on texts for a second factor of authentication are putting about 20% of their customers at risk because the information necessary to attack the system is available in compromised databases for sale on the Dark Web.
https://www.darkreading.com/cloud/stolen-data-attackers-advantage-text-based-2fa?_mc=NL_DR_EDT_DR_daily_20220808&cid=NL_DR_EDT_DR_daily_20220808&sp_aid=111971&elq_cid=36315893&sp_eh=72a861290e89658b5ada8de6a8a9c12b185e8e45329503691618392cbd15751b&sp_eh=72a861290e89658b5ada8de6a8a9c12b185e8e45329503691618392cbd15751b&utm_source=eloqua&utm_medium=email&utm_campaign=DR_NL_Dark%20Reading%20Daily_08.08.22&sp_cid=45696&utm_content=DR_NL_Dark%20Reading%20Daily_08.08.22

It Might Be Our Data, But It's Not Our Breach
A cybersecurity firm says it has intercepted a large, unique stolen data set containing the names, addresses, email addresses, phone numbers, Social Security Numbers, and dates of birth on nearly 23 million Americans. The firm's analysis of the data suggests it corresponds to current and former customers of AT&T. The telecommunications giant stopped short of saying the data wasn't theirs, but it maintains the records do not appear to have come from its systems and may be tied to a previous data incident at another company.
https://krebsonsecurity.com/2022/08/it-might-be-our-data-but-its-not-our-breach/

Zero-Day Bug Responsible for Massive Twitter Breach
A zero-day vulnerability in Twitter's code base was responsible for a major data breach that is thought to have affected 5.4 million users, the social media firm has revealed. The threat actor was hoping to sell the profile data for $30,000 on a cybercrime site. Some information was scraped from public Twitter profiles, including location and image URL. However, they were crucially able to link account emails and phone numbers with account IDs by leveraging the vulnerability.
https://www.infosecurity-magazine.com/news/zeroday-bug-responsible-massive/

QR Code Dangers and The Risks Behind Using Them
There's danger now lurking behind those busy black-and-white boxes that are QR codes and that now seem to be found everywhere for everything, including viewing restaurant menus. Always a quick way scan for information, more businesses are using them now more than ever. A study by Ivanti takes a look at what's really going on behind QR's and their findings should make anyone think twice before they reach to scan a QR code with their mobile device.
https://www.sosdailynews.com/news.jspx?&articleid=5E431EC65F76C0C75A318F49863AF72D&sx=26446

Tips to Avoid Social Media Cybercrime
We love social media these days. Facebook, Snapchat, Twitter, LinkedIn, and many others can lead to lots of sharing and fun, but also carry significant risks. This is particularly true now that cybercriminals are collating data and using it against us for targeting phishing attacks.
Online social networks may seem all in fun and harmless, but they are anything but that.
https://www.sosdailynews.com/news.jspx?&articleid=26B1E34A7BC4C9B1D084570A5C15777B&sx=26446

Cybercrooks Doing Cybersecurity? When NOT To Return An Urgent Voicemail Call
Surprise! Hackers are up to no good, again. This time they're relying on their acting skills to convince employees there's been a cyberattack at their place of work. They leave a phishing voicemail with urgent instructions to return the call. It's a sneaky way to get the information they need to pull-off a system-wide malware infection. In whatever way a hacker can best monetize this crime is likely the route they'll take, including lucrative ransomware attacks.
https://www.sosdailynews.com/news.jspx?&articleid=48EF0C79C4482DBA17A500B1778150BC&sx=26446

****

Hints & Tips plus Security Awareness

Employees love flexibility in the tech workplace — and tech leaders should, too
For tech employees, flex time and slack time provide the flexibility they crave. For tech leaders, flexible work initiatives keep employees happy and productivity high. In the battle to retain tech talent, businesses are rethinking what employees want and need.
https://www.ciodive.com/news/flexible-work-hybrid-slack-flex/628925/?utm_source=Sailthru&utm_medium=email&utm_campaign=Issue:%202022-08-05%20CIO%20Dive%20%5Bissue:43623%5D&utm_term=CIO%20Dive

Companies remain bullish on IT spend, unfazed by financial headwinds
Talk of recession has companies cutting back on discretionary spending while planning larger modernization efforts, a strategy born from recent recession history.
https://www.ciodive.com/news/recession-tech-spend-investment/628924/?utm_source=Sailthru&utm_medium=email&utm_campaign=Issue:%202022-08-05%20CIO%20Dive%20%5Bissue:43623%5D&utm_term=CIO%20Dive

****

News & Views

The 11 most-prevalent malware strains of 2021 fuel cybercrime
Cybercriminals remain the most prolific users of malware, wielding these top strains to deliver ransomware and steal data. Malware strains are like a bad habit — the type that can evolve into something far worse. The typical lifespan of the most-prevalent malware strains found in 2021 was at least five years, according to a joint advisory from the Cybersecurity and Infrastructure Security Agency and the Australian Cyber Security Centre.
https://www.cybersecuritydive.com/news/top-malware-strains-CISA/628993/?utm_source=Sailthru&utm_medium=email&utm_campaign=Issue:%202022-08-05%20Cybersecurity%20Dive%20%5Bissue:43644%5D&utm_term=Cybersecurity%20Dive

White House to incorporate performance metrics into national cybersecurity strategy
The ONCD, led by Chris Inglis, has been working on the national cybersecurity strategy in order to gain a more comprehensive understanding of the nation's ability to deter malicious cyberattacks in the future and more effectively respond and recover from those attacks.
https://www.cybersecuritydive.com/news/white-house-cybersecurity-strategy/628998/?utm_source=Sailthru&utm_medium=email&utm_campaign=Issue:%202022-08-05%20Cybersecurity%20Dive%20%5Bissue:43644%5D&utm_term=Cybersecurity%20Dive

Human Threat Hunters Are Essential to Thwarting Zero-Day Attacks
Machine-learning algorithms alone may miss signs of a successful attack on your organization. Zero-day attacks that exploit unpatched software vulnerabilities saw exponential growth last year. According to cybersecurity researchers like the Zero-Day Tracking Project, 2021 saw more than 80 zero-day exploits recorded, versus 36 in 2000. There are already 22 such exploits on record for the first half of 2022.
https://www.darkreading.com/attacks-breaches/human-threat-hunters-are-essential-to-thwarting-zero-day-attacks?_mc=NL_DR_EDT_DR_daily_20220810&cid=NL_DR_EDT_DR_daily_20220810&sp_aid=112025&elq_cid=36315893&sp_eh=72a861290e89658b5ada8de6a8a9c12b185e8e45329503691618392cbd15751b&sp_eh=72a861290e89658b5ada8de6a8a9c12b185e8e45329503691618392cbd15751b&utm_source=eloqua&utm_medium=email&utm_campaign=DR_NL_Dark%20Reading%20Daily_08.10.22&sp_cid=45716&utm_content=DR_NL_Dark%20Reading%20Daily_08.10.22

Don't Have a COW: Containers on Windows and Other Container-Escape Research
Several pieces of Black Hat USA research will explore container design weaknesses and escalation of privilege attacks that can lead to container escapes. In what's shaping up to be a summer of container escapes, a pair of talks slated for Black Hat USA next month will explore the kinds of architectural weaknesses in operating systems and in container platforms that can make it easy for attackers break down the barriers of container isolation and run roughshod over cloud infrastructure.
https://www.darkreading.com/application-security/dont-have-a-cow-containers-on-windows-and-other-container-escape-

research?sp_aid=111991&elq_cid=36315893&sp_eh=72a861290e89658b5ada8de6a8a9c12b185e8e45329503691618392cbd15751b&sp_eh=72a861290e89658b5ada8de6a8a9c12b185e8e45329503691618392cbd15751b&utm_source=eloqua&utm_medium=email&utm_campaign=DR_NL_Dark%20Reading%20Daily_08.09.22&sp_cid=45708&utm_content=DR_NL_Dark%20Reading%20Daily_08.09.22

What will cryptocurrency market look like in 2027? Here are 5 predictions
One year isn't enough time to witness many fundamental changes, but five years is just enough for everything to change. The year is 2027. It's a time of great innovation and technological advancement, but also a time of chaos. What will the crypto market look like in 2027?
https://cointelegraph.com/news/what-will-cryptocurrency-look-like-in-2027-here-are-5-predictions

****

"Ctrl -F" for The Board

Senate bill would couch Bitcoin, Ether under CFTC purview
Stakes in the turf war over crypto oversight have heightened in recent months as the value of tokens has plummeted, prompting bankruptcies of high-profile platforms such as Celsius and Voyager.
https://www.bankingdive.com/news/stabenow-boozman-cftc-crypto-digital-commodity-bill/628780/?utm_source=Sailthru&utm_medium=email&utm_campaign=Issue:%202022-08-05%20Banking%20Dive%20%5Bissue:43618%5D&utm_term=Banking%20Dive

Questions
Contact FIPCO's Rob Foxx at 800-722-3498 ext. 249 or email FIPCO IT Services for more information.

"Make Security Part of You and Your Institution's DNA!"

Threat Intelligence Newsletter: August 19, 2022

FIPCO® IT Audit Round Table Discussions

Upcoming Threat Intelligence Peer Group Discussions
None available at the current time

****

Alerts & Warnings

Zeppelin Ransomware Advisory
The Cybersecurity and Infrastructure Security Agency and the FBI last week released a joint cybersecurity advisory with technical details on Zeppelin ransomware along with recommended actions, mitigations, and resources for organizations to use to respond to this cyber threat.
https://www.cisa.gov/uscert/sites/default/files/publications/AA22-223A_Zeppelin_CSA.pdf?utm_source=eloqua&utm_medium=email&utm_campaign=riskcyberbulletin&utm_content=RiskCyber-20220815

Mailchimp breach shines new light on digital identity, supply chain risk
Sophisticated threat actors are targeting weak links in the email marketing space to go after vulnerable financial targets. A malicious round of social engineering attacks against Mailchimp and at least one of its customers, DigitalOcean, highlights a persistent trend in the information security space of threat actors targeting vulnerable organizations by abusing the digital identity supply chain.
https://www.cybersecuritydive.com/news/mailchimp-breach-digital-identity-supply-chain/629993/?utm_source=Sailthru&utm_medium=email&utm_campaign=Issue:%202022-08-18%20Cybersecurity%20Dive%20%5Bissue:43940%5D&utm_term=Cybersecurity%20Dive

Cloudflare thwarts 'sophisticated' phishing attack strategy that bruised Twilio
Dissimilar responses from Cloudflare and Twilio bear important lessons in transparency, resiliency, and access. Twilio employees aren't the only individuals recently targeted by a sophisticated phishing attack. Cloudflare on Tuesday said three employees fell for a phishing attack with very similar characteristics but, unlike Twilio, the content delivery network was able to thwart intrusion.
https://www.cybersecuritydive.com/news/cloudflare-twilio-phishing/629293/?utm_source=Sailthru&utm_medium=email&utm_campaign=Newsletter%20Weekly%20Roundup:%20Cybersecurity%20Dive:%20Daily%20Dive%2008-13-

2022&utm_term=Cybersecurity%20Dive%20Weekender

PayPal Phishing Scam Uses Invoices Sent Via PayPal
Scammers are using invoices sent through PayPal.com to trick recipients into calling a number to dispute a pending charge. The missives — which come from Paypal.com and include a link at Paypal.com that displays an invoice for the supposed transaction — state that the user's account is about to be charged hundreds of dollars. Recipients who call the supplied toll-free number to contest the transaction are soon asked to download software that lets the scammers assume remote control over their computer.
https://krebsonsecurity.com/2022/08/paypal-phishing-scam-uses-invoices-sent-via-paypal/

When Efforts to Contain a Data Breach Backfire
Earlier this month, the administrator of the cybercrime forum Breached received a cease-and-desist letter from a cybersecurity firm. The missive alleged that an auction on the site for data stolen from 10 million customers of Mexico's second-largest bank was fake news and harming the bank's reputation. The administrator responded to this empty threat by purchasing the stolen banking data and leaking it on the forum for everyone to download.
https://krebsonsecurity.com/2022/08/when-efforts-to-contain-a-data-breach-backfire/

How You Sign Into Your Facebook Account May Get Your Account Compromised
When you go to your Facebook login page, you're likely to see a pop-up window asking if you'd rather sign-in using your Google account credentials. It's hard to resist…it's easy, convenient, and you don't have those pesky password problems. But is that little window there simply for convenience or is there more to it? A security researcher found there's a lot more to it. That is, using Gmail to sign into your Facebook account can get your account and credentials stolen.
https://www.sosdailynews.com/news.jspx?&articleid=E2D4CE63DB475AAC11C27463328FAF9F&sx=26446

****

Hints & Tips plus Security Awareness

US falters while 'cybercriminals have been eating our lunch,' ex-CISA chief Krebs says
The U.S. government holds tremendous power and potential to better defend against and prevent cyberthreats, but bureaucratic morass and myopic thinking are getting in the way, Chris Krebs, a founding partner at Krebs Stamos Group, said Wednesday at the Black Hat USA conference in Las Vegas.
https://www.cybersecuritydive.com/news/government-overhaul-cisa-krebs/629585/?utm_source=Sailthru&utm_medium=email&utm_campaign=Issue:%202022-08-12%20Cybersecurity%20Dive%20%5Bissue:43801%5D&utm_term=Cybersecurity%20Dive

Don't count on government, tech vendors to fix security woes, former CISA chief Krebs says
The state of cybersecurity is bad and it's going to get worse, Chris Krebs said at Black Hat. But somehow things might eventually get better. Chris Krebs has been "wandering in the wilderness" the last 18 months, asking questions of individuals in technology and all levels of government. The general sentiment he's gathered: "Things are going to get worse before they get better."
https://www.ciodive.com/news/krebs-blackhat-cybersecurity-woes/629472/?utm_source=Sailthru&utm_medium=email&utm_campaign=Issue:%202022-08-12%20CIO%20Dive%20%5Bissue:43785%5D&utm_term=CIO%20Dive

Lessons From the Cybersecurity Trenches

Threat hunting not only serves the greater good by helping keep users safe, it rewards practitioners with the thrill of the hunt and solving of complex problems. Tap into your background and learn to follow your instincts.

https://www.darkreading.com/threat-intelligence/lessons-from-the-cybersecurity-trenches?_mc=NL_DR_EDT_DR_daily_20220818&cid=NL_DR_EDT_DR_daily_20220818&sp_aid=112155&elq_cid=36315893&sp_eh=72a861290e89658b5ada8de6a8a9c12b185e8e45329503691618392cbd15751b&sp_eh=72a861290e89658b5ada8de6a8a9c12b185e8e45329503691618392cbd15751b&utm_source=eloqua&utm_medium=email&utm_campaign=DR_NL_Dark%20Reading%20Daily_08.18.22&sp_cid=45798&utm_content=DR_NL_Dark%20Reading%20Daily_08.18.22

****

News & Views

Does a recession lead to more financial fraud?

Fraud follows the money. It is useful to think of recession as a factor within the “Fraud Triangle” framework devised by service firm MNP to help us understand what leads people to commit fraud.

https://www.fintechfutures.com/2022/08/does-a-recession-lead-to-more-financial-fraud/

Fed puts onus on banks to check legality of crypto ventures

Like the FDIC, the central bank urges banks to notify the regulator before starting crypto activity. But unlike the OCC, the Fed doesn’t detail what is permissible under law. Before engaging in crypto-related activity, banking organizations supervised by the Federal Reserve should notify their lead point of contact at the central bank to ensure the activity is legal.

https://www.bankingdive.com/news/federal-reserve-crypto-activity-guidance-fdic-occ-legal/629899/?utm_source=Sailthru&utm_medium=email&utm_campaign=Issue:%202022-08-17%20Banking%20Dive%20%5Bissue:43877%5D&utm_term=Banking%20Dive

****

"Ctrl -F" for The Board

Banks meet challenges with hybrid work

Hybrid work has proved a challenge for banks, which traditionally rely on in-house employees. However, banks can open up a new world of opportunities by taking advantage of hybrid work.

https://www.atmmarketplace.com/articles/banks-meet-challengesopportunities-with-hybrid-work/

CISO salaries balloon, likely spurred by demand

Tenure matters, but not as you might suspect. Median total cash compensation fell for CISOs who have been in their roles at least five years, Heidrick & Struggles found. More attention to enterprise cybersecurity has raised the visibility of cybersecurity chiefs. Cybersecurity fallouts are heavily documented in financial documents and regulators are raising the bar for security standards and disclosure.

https://www.ciodive.com/news/ciso-salaries-2022/629938/?utm_source=Sailthru&utm_medium=email&utm_campaign=Issue:%202022-08-18%20CIO%20Dive%20%5Bissue:43916%5D&utm_term=CIO%20Dive

Moving up: CTOs scale the corporate ladder, join CIOs in the C-suite
CTOs are confronting new challenges in defining their role: establishing their value to the business. Companies have turned to technology — and technologists — to provide leadership in areas core to the business. CTOs, CIOs and other chief officers of data, digital and IT operations are redefining their roles, taking on new managerial responsibilities. In some cases, they are setting themselves up to advance into corporate leadership positions.
https://www.ciodive.com/news/CTOs-Join-CIOs-Tech-Leadership/629607/?utm_source=Sailthru&utm_medium=email&utm_campaign=Issue:%202022-08-15%20CIO%20Dive%20%5Bissue:43804%5D&utm_term=CIO%20Dive

Questions
Contact FIPCO’s Rob Foxx at 800-722-3498 ext. 249 or email FIPCO IT Services for more information.

"Make Security Part of You and Your Institution's DNA!"

Threat Intelligence Newsletter: August 26, 2022

Upcoming Threat Intelligence Peer Group Discussions
None available at the current time

****

Alerts & Warnings

Risk of cyberattack emerges as top concern of US executives
PwC research shows cyber risk is a top concern among entire C-suite and corporate boards as companies spend more to boost resilience.
https://www.ciodive.com/news/risk-cyberattack-top-concern-executives/630234/

Apple Warns 1.5 Billion iPhone and Mac Users to Update Their Software Immediately
his week, Apple released a series of critical software updates for users of iPhones, iPads, and Macs. Apple doesn't typically release security fixes outside of regular updates, which tells you how seriously the company is taking this vulnerability.
https://www.inc.com/jason-aten/apple-warns-1-a-half-billion-iphone-mac-users-to-update-their-software-immediately.html

CISA: Just-Disclosed Palo Alto Networks Firewall Bug Under Active Exploit
The bug tracked as CVE-2022-0028 allows attackers to hijack firewalls without authentication, in order to mount DDoS hits on their targets of choice.
https://www.darkreading.com/vulnerabilities-threats/cisa-palo-alto-firewall-bug-active-exploit

VMware LPE Bug Allows Cyberattackers to Feast on Virtual Machine Data
An insider threat or remote attacker with initial access could exploit CVE-2022-31676 to steal sensitive data and scoop up user credentials for follow-on attacks.
https://www.darkreading.com/cloud/vmware-lpe-bug-cyberattackers-virtual-machine-data

Windows Vulnerability Could Crack DC Server Credentials Open
The security flaw tracked as CVE-2022-30216 could allow attackers to perform server spoofing or trigger authentication coercion on the victim.

https://www.darkreading.com/remote-workforce/windows-vulnerability-could-crack-dc-server-credentials-open

Mac Attack: North Korea's Lazarus APT Targets Apple's M1 Chip
Lazarus continues to expand an aggressive, ongoing spy campaign, using fake Coinbase job openings to lure in victims.
https://www.darkreading.com/endpoint/mac-attack-north-korea-lazarus-apt-apple-m1-chip

Hospitals in US, France Dealing With Cyber Extortionists
Texas Hospital Still Being Pressured, While French Hospital Responds to Ransomware
https://www.databreachtoday.com/hospitals-in-us-france-dealing-cyber-extortionists-a-19874

PayPal Phishing Scam Uses Invoices Sent Via PayPal
Scammers are using invoices sent through PayPal.com to trick recipients into calling a number to dispute a pending charge. The missives -- which come from Paypal.com and include a link at Paypal.com that displays an invoice for the supposed transaction -- state that the user's account is about to be charged hundreds of dollars. Recipients who call the supplied toll-free number to contest the transaction are soon asked to download software that lets the scammers assume remote control over their computer.
https://krebsonsecurity.com/2022/08/paypal-phishing-scam-uses-invoices-sent-via-paypal/

Ring Camera Recordings Exposed Due to Vulnerability in Android App
Security researchers at Checkmarx discovered a security vulnerability in Ring surveillance cameras earlier this year. According to the security firm, Amazon has recently published a vulnerability affecting the Android app for the surveillance cameras. The flaw exposed user data as well as video recordings.
https://www.oodaloop.com/briefs/2022/08/23/ring-camera-recordings-exposed-due-to-vulnerability-in-android-app/

Are Online Teaching Apps Spying On Your Kids?
Online teaching via education technology apps - EdTech for short - has become a big thing in recent years. But it's not just students who benefit. Providers are learning stuff too - by harvesting data about your kids and using it for who knows what purposes.
https://scambusters.org/onlineteaching.html

****

Hints & Tips plus Security Awareness

How attackers are breaking into organizations
Threat actors lean heavily on phishing attacks, vulnerabilities in software and containers, and stolen credentials, according to top cyber vendor research.
https://www.cybersecuritydive.com/news/how-attackers-break-organizations/629686/

Apathy Is Your Company's Biggest Cybersecurity Vulnerability — Here's How to Combat It
Make security training more engaging to build a strong cybersecurity culture. Here are four steps security and IT leaders can take to avoid the security disconnect.
https://www.darkreading.com/attacks-breaches/apathy-is-your-company-s-biggest-cybersecurity-vulnerability-here-s-how-to-combat-it

Facing the New Security Challenges That Come With Cloud
Organizations relying on multicloud or hybrid-cloud environments without a true understanding of their security vulnerabilities do so at their peril.
https://www.darkreading.com/cloud/facing-the-new-security-challenges-that-come-with-cloud

****

News & Views

Historic highs in tech job postings persist through first half of year
Despite a June dip, demand for IT talent remains at an all-time high and has remained strong over the first six months of 2022. Tech job postings rose 45% in the first half of 2022, according to Tuesday's Dice Tech Job Report, an increase of 52% from the same period last year.
https://www.ciodive.com/news/tech-talent-demand-surge-2022/630338/

3 ways to ensure technology becomes a business imperative
Technology organizations often have a transactional relationship with the rest of the business. But there are ways to build a new culture around IT, the CTO of Advance Auto Parts says.
https://www.ciodive.com/news/advance-auto-parts-technology-business-imperative/629838/

Risk of cyberattack emerges as top concern of US executives
A PwC study shows cyber risk is a top concern among entire C-suite and corporate boards as companies are spending additional funds to boost resilience.
https://www.cybersecuritydive.com/news/risk-cyberattack-top-concern-executives/630096

Cyber Resiliency Isn't Just About Technology, It's About People
To lessen burnout and prioritize staff resiliency, put people in a position to succeed with staffwide cybersecurity training to help ease the burden on IT and security personnel.
https://www.darkreading.com/vulnerabilities-threats/cyber-resiliency-isn-t-just-about-technology-it-s-about-people

****

"Ctrl -F" for The Board

Like a marathon, modernization needs pacing, planning, and persistence
A strategic approach to cloud spending is crucial as companies eye the finish line in race to modernize.
https://www.ciodive.com/news/Cloud-Modernization-Spend-Strategy/630224/

Telework has improved team performance for government workers, research finds
The government's success with team performance offers a guidepost for HR pros trying to balance executive uncertainty about remote and hybrid work, employee desire to continue doing so and managers' role in bridging the issues.
https://www.smartcitiesdive.com/news/telework-improved-team-performance-government-workers/630018/

CISO salaries balloon, likely spurred by demand
Tenure matters, but not as you might suspect. Median total cash compensation fell for CISOs who have been in their roles at least five years, Heidrick & Struggles found.
https://www.ciodive.com/news/ciso-salaries-2022/629938/

Think Your Business Is Too Small For Hackers? It's Time To Think Again
"Cyberattacks only happen to big companies with lots of valuable data and assets to steal," thought most small business owners at one time or another. But there's a false sense of security when SMB (small-to-medium-sized business) owners believe hackers aren't interested in a small company. After all, bad actors will just move on to bigger and better targets with much more to steal, right? Wrong.
https://www.sosdailynews.com/news.jspx?&articleid=4BF19C33A6CBC279A5A3FF92B5CBE19B&sx=26446

Questions
Contact FIPCO's Rob Foxx at 800-722-3498 ext. 249 or email FIPCO IT Services for more information.

"Make Security Part of You and Your Institution's DNA!"

Threat Intelligence Newsletter: September 6, 2022

FIPCO®
IT Audit
Round Table
Discussions

Upcoming Threat Intelligence Peer Group Discussions
None available at the current time

****

Alerts & Warnings

Free COVID test scam targets people on Medicare
Scammers have been targeting Medicare recipients with a fake offer to get “free COVID tests.” They’re calling and running websites, online and television ads to try to convince people to give their Medicare information. But if you give them your information, they’ll bill fraudulent charges to Medicare.
https://consumer.ftc.gov/consumer-alerts/2022/08/free-covid-test-scam-targets-people-medicare?utm_source=govdelivery

Microsoft Reports Russian Hackers Gain Powerful Authentication Bypass
Microsoft warned last week that Nobelium, the hacking group behind the 2020 SolarWinds supply chain attack, is using a post-compromise capability to maintain persistent access to compromised environments. Named MagicWeb by Microsoft researchers, the threat actors gain admin privileges to an Active Directory Federated Services server and replace a legitimate dynamic-link library with the malicious MagicWeb DLL that allows manipulation of the claims and user authentication certificates.
https://www.microsoft.com/security/blog/2022/08/24/magicweb-nobeliums-post-compromise-trick-to-authenticate-as-anyone/?/

LastPass breached, portions of source code stolen, CEO says
The unauthorized actor did not access data or encrypted vaults from its more than 33 million registered users, however the company deployed containment and mitigation measures.
https://www.cybersecuritydive.com/news/lastpass-breach-password-manager/630624/

Student Loan Breach Exposes 2.5M Records
2.5 million people were affected, in a breach that could spell more trouble down the line. EdFinancial and the Oklahoma Student Loan Authority (OSLA) are notifying over 2.5 million loanees that their personal data was exposed in a data breach.
https://threatpost.com/student-loan-breach-exposes-2-5m-records/180492/

Cybercriminals Weaponizing Ransomware Data for BEC Attacks
Attacked once, victimized multiple times: Data marketplaces are making it easier for threat actors to find and use data exfiltrated during ransomware attacks in follow-up attacks.
https://www.darkreading.com/edge-threat-monitor/cybercriminals-weaponizing-ransomware-data-for-bec-attacks

TikTok for Android Bug Allows Single-Click Account Hijack
A security vulnerability (CVE-2022-28799) in one of TikTok for Android's deeplinks could affect billions of users, Microsoft warns.
https://www.darkreading.com/vulnerabilities-threats/tiktok-android-bug-allows-single-click-account-hijack

How 1-Time Passcodes Became a Corporate Liability
Phishers are enjoying remarkable success using text messages to steal remote access credentials and one-time passcodes from employees at some of the world's largest technology companies and customer support firms. A recent spate of SMS phishing attacks from one cybercriminal group has spawned a flurry of breach disclosures from affected companies, which are all struggling to combat the same lingering security threat: The ability of scammers to interact directly with employees through their mobile devices.
https://krebsonsecurity.com/2022/08/how-1-time-passcodes-became-a-corporate-liability/

Is Someone Stealing Your Words for Voice Cloning?
High-tech scammers have started using voice cloning to make their imposter calls sound more realistic than ever. They're using the technology to imitate the voices of friends and relatives for distress calls like those used for grandparent scams or fake kidnap messages.
https://scambusters.org/voicecloning.html

Smartphone Malware Alert – Androids And iPhones Infected With Hermit Spyware
No one likes the idea of their smartphone spying on them, so this latest spyware find is sure to go over like a lead balloon. Named "Hermit" by Lookout Research, the company announced this spyware is infecting both Android and iPhone users. Aside from the damage Hermit can do, Lookout Research suspects a telecom company, Tykelab Srl, may be hiding and using the spyware for their own gain.
https://www.sosdailynews.com/news.jspx?&articleid=F78A2CBA03599A68F3CAD26F13AB788F&sx=26446

Over 1,800 Android and iOS Apps Found Leaking Hard-Coded AWS Credentials
Researchers have identified 1,859 apps across Android and iOS containing hard-coded Amazon Web Services (AWS) credentials, posing a major security risk.
"Over three-quarters (77%) of the apps contained valid AWS access tokens allowing access to private AWS cloud services," Symantec's Threat Hunter team, a part of Broadcom Software, said in a report shared with The Hacker News.
https://thehackernews.com/2022/09/over-1800-android-and-ios-apps-found.html

****

Hints & Tips plus Security Awareness

What You Need to Know About the Psychology Behind Cyber Resilience

Understanding how and why people respond to cyber threats is key to building cyber-workforce resilience. The complexity, ceaselessness, and increasingly destructive nature of today's cyber threats creates a high cognitive workload.
https://www.darkreading.com/vulnerabilities-threats/what-you-need-to-know-about-the-psychology-behind-cyber-resilience

****

News & Views

Changing cyber insurance guidance from Lloyd's reflects a market in turmoil
Rising ransomware attacks and higher payout demands have battered the insurance industry, leaving many organizations exposed and vulnerable. A critical, but long-anticipated decision by Lloyd's last week to phase out coverage for state-sponsored cyberattacks illustrates an insurance market that has been under increasing financial pressure for years.
https://www.ciodive.com/news/lloyds-cyber-insurance-exclusions/630864/?utm_source=Sailthru&utm_medium=email&utm_campaign=Issue:%202022-08-31%20CIO%20Dive%20%5Bissue:44206%5D&utm_term=CIO%20Dive

Who Pays for an Act of Cyberwar?
Cyberinsurance doesn't cover acts of war. But even as cyberattacks mount, the definition of "warlike" actions remains blurry.
https://www.wired.com/story/russia-ukraine-cyberwar-cyberinsurance/?utm_source=Sailthru&utm_medium=email&utm_campaign=Issue:%202022-08-31%20Cybersecurity%20Dive%20%5Bissue:44227%5D&utm_term=Cybersecurity%20Dive

****

"Ctrl -F" for The Board

California Fines Sephora $1.2 Million for Privacy Violations
Retailer Accused of Selling Customer Data While Failing to Honor Opt-Out Requests
https://www.databreachtoday.com/california-fines-sephora-12-million-for-privacy-violations-a-19911

Questions
Contact FIPCO's Rob Foxx at 800-722-3498 ext. 249 or email FIPCO IT Services for more information.

"Make Security Part of You and Your Institution's DNA!"

Threat Intelligence Newsletter: September 9, 2022

Upcoming Threat Intelligence Peer Group Discussions
None available at the current time

****

Alerts & Warnings

Next-Gen Linux Malware Takes Over Devices With Unique Tool Set
The Shikitega malware takes over IoT and endpoint devices, exploits vulnerabilities, uses advanced encoding, abuses cloud services for C2, installs a cryptominer, and allows full remote control.
https://www.darkreading.com/vulnerabilities-threats/next-gen-linux-malware-takes-over-devices-unique-toolset

Code-Injection Bugs Bite Google, Apache Open Source GitHub Projects
The insecurities exist in CI/CD pipelines and can be used by attackers to subvert modern development and roll out malicious code at deployment. A pair of security vulnerabilities discovered in the GitHub environments of two very popular open source projects from Apache and Google could be used to stealthily modify project source code, steal secrets, and move laterally inside an organization.
https://www.darkreading.com/vulnerabilities-threats/code-injection-bugs-google-apache-open-source-github-projects

TikTok Denies Breach After Hacker Claims ‘2 Billion Data Records’ Stolen
The first reports of an alleged hack appeared on the Breach Forums message board September 3. A user with the handle of AgainstTheWest posted what was claimed to be screenshots from a TikTok and WeChat breach. In that posting, the user said, referring to the alleged stolen data, that they had "yet to decide if we want to sell it or release it to the public."
https://www.forbes.com/sites/daveywinder/2022/09/06/has-tiktok-us-been-hacked-and-2-billion-database-records-stolen/?sh=30325f31105d

North Korea’s Lazarus hackers are exploiting Log4j flaw to hack US energy companies
Security researchers have linked a new cyber espionage campaign targeting U.S., Canadian and Japanese energy providers to the North Korean state-sponsored Lazarus hacking group. Threat intelligence company Cisco Talos said Thursday that it has observed Lazarus — also known as APT38 — targeting unnamed energy providers in the United States, Canada and Japan between February and July this year.

https://www.oodaloop.com/technology/2022/09/08/north-koreas-lazarus-hackers-are-exploiting-log4j-flaw-to-hack-us-energy-companies/

IRS Leaks 120,000 Taxpayers' Personal Details
The US Internal Revenue Service (IRS) accidentally posted sensitive taxpayer data to its site, potentially putting those affected at risk of follow-on fraud. The problem stemmed from the machine-readable (XML) Form 990-T. "Form 990-T is the business tax return used by tax-exempt entities, including tax-exempt organizations, government entities and retirement accounts, to report and pay income tax on income that is generated from certain investments or income unrelated to their exempt purpose," the IRS explained in a brief statement.
https://www.infosecurity-magazine.com/news/irs-leaks-120000-taxpayers/

Apple Quietly Releases Another Patch for Zero-Day RCE Bug
Apple continues a staged update process to address a WebKit vulnerability that allows attackers to craft malicious Web content to load malware on affected devices. Apple has quietly rolled out more updates to iOS to fix an actively exploited zero-day security vulnerability that it patched earlier this month in newer devices. The vulnerability, found in WebKit, can allow attackers to create malicious Web content that allows remote code execution (RCE) on a user's device.
https://www.darkreading.com/vulnerabilities-threats/apple-patch-zero-day-rce-bug

Sob Story and Sympathy Won't Get You A Free PS5
Scammers know if they can spin a sob story that brings victims near to tears, the cash just rolls in. And there's no shortage of people lining up for their latest con - offering the much sought-after PS5 games console for free. Their latest trick is currently sweeping Facebook, popping up in all sorts of unlikely places - mostly public groups on the social media network whose topics have nothing to do with the alleged tragedy -- as well as on neighborhood trading sites. The tale of woe starts with a post statement that's meant to disarm readers and goes something like "I hope it's okay to post this on this page...." This basically gives the scammer free rein to go off-topic.
https://scambusters.org/ps5.html

New Student Debt Relief Program Sparks Surge In Scams
Scammers have already jumped aboard last week's announcement of a student debt relief program and extension of the loan repayment pause. They're using it to boost their bag of con tricks that are stealing millions of dollars from students, graduates, and their families every year. Confusion over who's entitled to the debt forgiveness program, and for how much, plays straight into the crooks' hands. The Department of Education is still working on the final details and the application process, so it can be a frustrating time for student borrowers.
https://scambusters.org/studentdebt.html

****

Hints & Tips plus Security Awareness

3 Critical Steps for Reducing Cloud Risk
Having a better understanding of how clouds are built, connected, and managed helps organizations mitigate risks and reduce attack surfaces.
https://www.darkreading.com/cloud/3-critical-steps-for-reducing-cloud-risk

Fraudsters say the Darndest Things | How to Avoid BEC
Business email compromise (BEC) is when threat actors use email fraud to attack organizations, deceiving people into doing something they believe is helping the company. To request funds from victims, BEC

threat actors conduct a variety of scams impersonating coworkers, vendors, or customers.
Webinar Wednesday, Sep. 14, 2022 1:00 PM Central
https://www.databreachtoday.com/webinars/fraudsters-say-darndest-things-how-to-avoid-bec-w-4298?

Transacting in Person with Strangers from the Internet
Communities like Craigslist, OfferUp, Facebook Marketplace and others are great for finding low- or no-cost stuff that one can pick up directly from a nearby seller, and for getting rid of useful things that don't deserve to end up in a landfill. But when dealing with strangers from the Internet, there is always a risk that the person you've agreed to meet has other intentions. Nearly all U.S. states now have designated safe trading stations — mostly at local police departments — which ensure that all transactions are handled in plain view of both the authorities and security cameras.
https://krebsonsecurity.com/2022/09/transacting-in-person-with-strangers-from-the-internet/

****

News & Views

4 Scenarios for the Digital World of 2040
Our digital future depends on the choices we make today. We need to invest in cybersecurity technologies and skills so that humanity can control its future. As we observe the evolution of the war in Ukraine, particularly the use of cyberwarfare, we are presented with many questions about the long-term evolution of the cybersecurity landscape. Likewise, we've seen the pandemic bring about the rapid acceleration of digitalization — its place in our lives is no longer in question. But before plunging headfirst into this technological race, should we not ask ourselves where this evolution might be taking us of in terms of cybersecurity?
https://www.darkreading.com/the-cyber-future/4-scenarios-for-the-digital-world-of-2040

Terror groups may turn to NFTs to raise funds and spread messages: WSJ
National security experts have raised the alarm bells over the IS-NEWS #01 NFT, which is being seen as the first case of an NFT created and shared by a "terrorist sympathizer." The first known case of a nonfungible token (NFT) created and shared by a "terrorist sympathizer" has come to light, raising concerns that the immutable nature of blockchain tech could help the spread of terrorist messages and propaganda.
https://cointelegraph.com/news/terror-groups-may-turn-to-nfts-to-raise-funds-and-spread-messages-wsj

****

"Ctrl -F" for The Board

Gen Z in IT: Tech leaders focus on values to support changing work styles, priorities
While HR is in charge of attracting talent through mission statements and initiatives, CIOs and managers must demonstrate their commitment to the goals that attracted the talent in the first place.
https://www.ciodive.com/news/Gen-Z-IT-workplace-tech/630971/?utm_source=Sailthru&utm_medium=email&utm_campaign=Newsletter%20Weekly%20Roundup:%20CIO%20Dive:%20Daily%20Dive%2009-03-2022&utm_term=CIO%20Dive%20Weekender

Questions
Contact FIPCO's Rob Foxx at 800-722-3498 ext. 249 or email FIPCO IT Services for more information.

"Make Security Part of You and Your Institution's DNA!"

Threat Intelligence Newsletter: September 19, 2022

FIPCO®
IT Audit
Round Table
Discussions

Upcoming Threat Intelligence Peer Group Discussions
None available at the current time

****

Alerts & Warnings

Microsoft, Cloud Providers Move to Ban Basic Authentication
Microsoft moves ahead with a plan to sunset basic authentication, and other providers are moving — or have moved — to requiring more secure authentication as well. Is your company ready?
https://www.darkreading.com/cloud/microsoft-cloud-providers-ban-basic-authentication

Say Hello to Crazy Thin 'Deep Insert' ATM Skimmers
A number of financial institutions in and around New York City are dealing with a rash of super-thin "deep insert" skimming devices designed to fit inside the mouth of an ATM's card acceptance slot. The card skimmers are paired with tiny pinhole cameras that are cleverly disguised as part of the cash machine.
https://krebsonsecurity.com/2022/09/say-hello-to-crazy-thin-deep-insert-atm-skimmers/

Samsung was hacked… again
Samsung, a South Korean multinational manufacturing conglomerate, joined the ever-growing list of high-profile companies with cyber security problems. Earlier this week, the consumer electronics giant confirmed a second data breach for this year after systems located in the USA were hacked.
https://www.pandasecurity.com/en/mediacenter/security/samsung-hacked-again

High-risk ConnectWise Automate vulnerability fixed, admins urged to patch ASAP
ConnectWise has fixed a vulnerability in ConnectWise Automate, a popular remote monitoring and management tool, which could allow attackers to compromise confidential data or other processing resources.
https://www.helpnetsecurity.com/2022/09/09/connectwise-automate-vulnerability

Apple Releases iOS and macOS Updates to Patch Actively Exploited Zero-Day Flaw
Apple has released another round of security updates to address multiple vulnerabilities in iOS and macOS, including a new zero-day flaw that has been used in attacks in the wild. The issue, assigned the identifier CVE-2022-32917, is rooted in the Kernel component and could enable a malicious app to execute arbitrary code with kernel privileges.
https://thehackernews.com/2022/09/apple-releases-ios-and-macos-updates-to.html

High-Severity Firmware Security Flaws Left Unpatched in HP Enterprise Devices
A number of firmware security flaws uncovered in HP's business-oriented high-end notebooks continue to be left unpatched in some devices even months after public disclosure. Binarly, which first revealed details of the issues at the Black Hat USA conference in mid-August 2022, said the vulnerabilities "can't be detected by firmware integrity monitoring systems due to limitations of the Trusted Platform Module (TPM) measurement."
https://thehackernews.com/2022/09/high-severity-firmware-security-flaws.html

****

Hints & Tips plus Security Awareness

The modern CISO: Today's top cybersecurity concerns and what comes next
CISOs are up against talent shortages and retention concerns amid an increasingly sophisticated threat landscape.
https://www.cybersecuritydive.com/news/top-ciso-concerns-cybersecurity-strategy/631172

5 Ways to Mitigate Your New Insider Threats in the Great Resignation
Companies are in the midst of an employee "turnover tsunami" with no signs of a slowdown. According to Fortune Magazine, 40% of the U.S. is considering quitting their jobs. This trend – coined the great resignation - creates instability in organizations. High employee turnover increases security risks, and companies are more vulnerable to attacks from human factors worldwide.
https://thehackernews.com/2022/09/5-ways-to-mitigate-your-new-insider.html?_m=3n%2e009a%2e2838%2eod0ao445rz%2e1tf2

****

News & Views

IT certifications ease tech job access as employers lower degree requirements
The tech talent crunch has companies looking beyond academic credentials to meet workforce demand. For burgeoning IT pros, there's a chance to level up.
https://www.ciodive.com/news/IT-certifications-degree-requirements/631858/

US is shoring up gaps in cyber policy, but critical goals remain unfulfilled
Legislators say the Cyberspace Solarium Commission led to significant national security enhancements, but analysts are calling for urgent momentum on a federal law on data privacy and security.
https://www.cybersecuritydive.com/news/cyberspace-solarium-commission-bipartisan-success/631515

Companies Are Hacking Their Way Around the Chip Shortage
The supply chain issues have no end in sight, so manufacturers are being forced to improvise. As the global chip shortage stretches toward the two-year mark, manufacturers are pulling some unusual tricks to keep production lines moving.
https://www.wired.com/story/chip-shortage-hacks/

****

"Ctrl -F" for The Board

Because That's Where The Money Is. Top Cybersecurity Threats To Financial Institutions
Since they're not secured like Fort Knox, online banks, credit unions, investment firms, and other financial establishments continue to be prime targets for cybercrime. Cybersecurity Ventures finds in 2025, the global price tag for cybercrime will reach $10.5 trillion. The following attacks are used most often against finance firms.
https://www.sosdailynews.com/news.jspx?&articleid=63FE70B5BC26F3E088713B560607ECD1&sx=26446

Questions
Contact FIPCO's Rob Foxx at 800-722-3498 ext. 249 or email FIPCO IT Services for more information.

"Make Security Part of You and Your Institution's DNA!"

Threat Intelligence Newsletter: September 23, 2022

FIPCO®
IT Audit
Round Table
Discussions

Upcoming Threat Intelligence Peer Group Discussions
None available at the current time

****

Alerts & Warnings

Stolen single sign-on credentials for major firms available for sale on dark web
Stolen SSO credentials are available for half of the top 20 public companies, and 25% of the entire S&P 500, BitSight found.
https://www.cybersecuritydive.com/news/stolen-single-sign-on-credentials-for-sale/632241/

Multifactor authentication has its limits, but don’t blame the technology
Despite phishing attacks that evaded authentication and engulfed many technology companies of late, organizations shouldn’t hesitate to use MFA.
https://www.cybersecuritydive.com/news/multifactor-authentication-limits/631046

****

Hints & Tips plus Security Awareness

Tips to succeed as an incoming tech leader
Before executives can set strategy, they must first build trust within the team — and understand how the company operates.
https://www.ciodive.com/news/onboarding-tech-leaders-tips/631765

How do I monitor privileged accounts?
Monitoring and auditing privileged accounts are critical for businesses in several ways. It’s a fundamental security tenet. It’s a must-have to comply with security and regulatory compliance requirements. It’s also a critical tool in the Security and Incident Response teams’ arsenal during a breach investigation.
https://www.cybersecuritydive.com/spons/how-do-i-monitor-privileged-accounts/631347/

How to Dodge New Ransomware Tactics
The evolving tactics increase the threat of ransomware operators, but there are steps organizations can take to protect themselves.
https://www.darkreading.com/attacks-breaches/how-to-dodge-new-ransomware-tactics

Business Application Compromise & the Evolving Art of Social Engineering
Be wary of being pestered into making a bad decision. As digital applications proliferate, educating users against social engineering attempts is a key part of a strong defense.
https://www.darkreading.com/vulnerabilities-threats/business-application-compromise-the-evolving-art-of-social-engineering

Best Practices to Measure and Conquer Vendor Cybersecurity Risk
IT vendors are essential to businesses across the globe - now more than ever. Vendors help organizations deliver new capabilities, serve their customers, stay competitive, and keep the lights on (literally and figuratively). But they also bring new risk to the table, both directly and through their own vendor relationships. Without a smart process of developing and scaling the program, organizations struggle to keep up with the ever-evolving cyber risk brought by the vendors. OnDemand Webinar
https://www.databreachtoday.com/webinars/live-webinar-today-best-practices-to-measure-conquer-vendor-w-4287

10 Ways To Protect Yourself From Robotext Spam
Remember when your email inbox was flooded with spam? Well, it probably still is but you're so used to it, you barely notice. But now spammers and scammers have stepped up their game, bombarding us with spam SMS text messages, or "robotexts" as they're being called.
https://scambusters.org/robotext.html

****

News & Views

Updates can spell trouble for IT. What to consider with Windows 11 — and beyond
For tech departments, an update is more than just a push-to-start procedure. IT professionals must ensure updates are not a hindrance to the business.
https://www.ciodive.com/news/microsoft-windows-11-version-22h2-update/632396/

IT’s fiercest foe: user expectations from consumer-facing technology
The digital user experience lets people easily navigate new tech, leading employees to wonder why workplace tech isn’t as simple to use.
https://www.ciodive.com/news/workplace-tech-SaaS-collaboration-tool/632281/

US government rejects ransom payment ban to spur disclosure
Federal authorities strongly discourage organizations from paying ransoms, but Anne Neuberger of the National Security Council explains why it decided against a ban.
https://www.cybersecuritydive.com/news/government-ransomware-guidance/632136/

Survey Shows CISOs Losing Confidence in Ability to Stop Ransomware Attacks
Despite an 86% surge in budget resources to defend against ransomware, 90% of orgs were impacted by attacks last year, a survey reveals.
https://www.darkreading.com/application-security/survey-cisos-losing-confidence-stop-ransomware-attacks

5 Best Practices for Building Your Data Loss Prevention Strategy
Several recent high-profile instances of data loss serve as cautionary tales for organizations handling sensitive data — including a recent case where the personal data of nearly half a million Japanese citizens was put in a compromising position when the USB drive on which it was stored was mislaid.
https://www.darkreading.com/attacks-breaches/5-best-practices-for-building-your-data-loss-prevention-strategy

****

"Ctrl -F" for The Board

How much do IT pros like their jobs? It depends on where they work
Despite companies touting salary increases, improved culture and flexibility, it appears not all organizations are taking the same precautions to retain their IT staff.
https://www.ciodive.com/news/IT-pros-tech-workers-pay-staffing-stability/632070/

Questions
Contact FIPCO's Rob Foxx at 800-722-3498 ext. 249 or email FIPCO IT Services for more information.

"Make Security Part of You and Your Institution's DNA!"

Threat Intelligence Newsletter: September 30, 2022

FIPCO®
IT Audit
Round Table
Discussions

Upcoming Threat Intelligence Peer Group Discussions
None available at the current time

****

Alerts & Warnings

Most Attackers Need Less Than 10 Hours to Find Weaknesses
Vulnerable configurations, software flaws, and exposed Web services allow hackers to find exploitable weaknesses in companies' perimeters in just hours, not days.
https://www.darkreading.com/attacks-breaches/attackers-less-than-ten-hours-find-weaknesses

Malicious Apps With Millions of Downloads Found in Apple App Store, Google Play
The threat actors behind a newly discovered malicious advertising app operation have been active since at least 2019, but researchers tracking their evolution report the group has become more sophisticated, expanding beyond its previous Android-specific attacks into the iOS ecosystem.
https://www.darkreading.com/attacks-breaches/malicious-apps-millions-downloads-apple-google-app-stores

Cyberattackers Compromise Microsoft Exchange Servers via Malicious OAuth Apps
Cybercriminals took control of enterprise Exchange Servers to spread large amounts of spam aimed at signing people up for bogus subscriptions. Attackers are deploying malicious OAuth applications on compromised cloud tenants, with the goal of taking over Microsoft Exchange Servers to spread spam.
https://www.darkreading.com/application-security/cyberattackers-compromise-microsoft-exchange-servers-malicious-oauth-apps

IRS Warns of "Industrial Scale" Smishing Surge
The Internal Revenue Service (IRS) has warned US taxpayers of an "exponential" increase in text-based phishing attempts and urged users to report campaigns to help the government disrupt them.
https://www.infosecurity-magazine.com/news/irs-warns-of-industrial-scale/

The Number One Way To Prevent Elder Fraud
A sharp rise in elder fraud - scams and theft targeting older folk - is causing alarm across the US. In its latest annual report, the Internet Crime Complaint Center (IC3) declares: "The number of elderly victims has risen at an alarming rate, while the loss amounts are even more staggering." If you're in this population group or have older family members, would you be able to spot a scam and know what action to take?
https://scambusters.org/elderfraud.html

Do You Have A Ticket To Nowhere? Know The Latest AirlineRebooking Scams
By now we've seen news clips showing the chaos at airports all over the country. Over-booked flights and airline staff shortages are leading to massive flight cancellations and hours long wait times to board a plane. This may well be a sign of the times, but that won't help you feel any better when you learn your flight was cancelled. Airline travelers need to be aware scammers are exploiting this bizarre time to enrich themselves with your money.
https://www.sosdailynews.com/news.jspx?&articleid=B22AF31485BCC52953E0F4F515AB2C51&sx=26446

3-2-1…Account Deleted. Phishing Scheme Uses Ransomware Tactic To Force Action
The huge countdown clock on your screen started with 60 minutes, but now only two minutes remain. The hacker warns that if you don't enter your login credentials, your account and those of others at work around you will be deleted. It's a pressure-packed dilemma, so what do you do? It's a question those caught on the hook of this unusual email phishing campaign can answer, for sure.
https://www.sosdailynews.com/news.jspx?&articleid=1BD2905C993D31BA63461520DECC83DE&sx=26446

****

Hints & Tips plus Security Awareness

Ransomware: Best Practices for Prevention, Mitigation, and Recovery
Ransomware is the threat that keeps on giving. Years after it progressed to being the top security concern that most organizations have, ransomware remains a growing problem.
Available on demand
https://www.brighttalk.com/webcast/19410/552652

4 Data Security Best Practices You Should Know
There are numerous strategies to lessen the possibility and effects of a cyberattack but doing so takes careful planning and targeted action.
https://www.darkreading.com/attacks-breaches/4-data-security-best-practices-you-should-know

Tips for Securing Your Mobile Devices
Nearly all of us these days have some type of mobile device that is essentially a part of us. It is filled with all kinds of personal information, such as our contacts, our email conversations, and perhaps even our health information. Losing it, having it accessed without permission, or finding out it's infested with malware can be a really scary moment. Fortunately, there are some things you can do to protect those devices and the information on them.
https://www.sosdailynews.com/news.jspx?&articleid=E52F81ACD0E1CA2BE4BFF71F1DDBAE08&sx=26446

****

News & Views

ABA Statement for the Record: "Stopping Senior Scams: Empowering Communities to Fight Fraud."
Given the circumstances seniors are facing, ABA, its non-profit foundation, and the banking industry are expanding their commitment to protecting America's elders and are taking specific steps to combat elder financial exploitation. Download the statement to read the full text.
https://www.aba.com/-/media/documents/testimonies-and-speeches/aba-statement-for-the-record-senior-scams-09272022.pdf

Today's top cybersecurity concerns — and what comes next
Cybersecurity executives are up against talent shortages and retention concerns amid increasingly sophisticated threats.
https://www.ciodive.com/news/top-security-concerns-strategy/632633/

Preventing Cryptocurrency Cyber Extortion
To solve crime, the old saying still holds: "Follow the money." But how do you do that for cybercrimes when the money itself is decentralized and anonymous—as is the case with cryptocurrency? In today's threat environment, it's becoming increasingly crucial for enterprises to boost their cybersecurity maturity.
https://www.trendmicro.com/en_us/ciso/22/i/prevent-cyber-extortion.html

Twitter Password Reset Bug Exposed User Accounts
Twitter has remediated an issue that allowed accounts to stay logged in across multiple devices even after a voluntary password reset. In an update yesterday, the social media company explained that the bug meant users who proactively changed their passwords on one device may have still been able to access open sessions on other screens.
https://www.infosecurity-magazine.com/news/twitter-password-reset-bug-exposed/

****

"Ctrl -F" for The Board

Why IT needs HR and HR needs IT
HR and IT teams rely on each other to streamline operations, widen visibility, and boost employee experience. It's a symbiotic relationship that benefits all parts of the business.
https://www.ciodive.com/news/Fleetcor-CHRO-HR-IT-CIO/632807

Questions
Contact FIPCO's Rob Foxx at 800-722-3498 ext. 249 or email FIPCO IT Services for more information.

"Make Security Part of You and Your Institution's DNA!"

Threat Intelligence Newsletter: October 7, 2022

FIPCO®
IT Audit
Round Table
Discussions

Upcoming Threat Intelligence Peer Group Discussions
None available at the current time

****

Alerts & Warnings

Reshaping the Threat Landscape: Deepfake Cyberattacks Are Here
It's time to dispel notions of deepfakes as an emergent threat. All the pieces for widespread attacks are in place and readily available to cybercriminals, even unsophisticated ones.
https://www.darkreading.com/threat-intelligence/threat-landscape-deepfake-cyberattacks-are-here

CyOps Threat Alert: Microsoft Exchange Zero Days
On September 30, 2022, two new zero-day vulnerabilities were found in the Microsoft Exchange Server. The two new vulnerabilities can create a remote code execution with elevated privileges to collect information, inject malicious DLLs, drop malicious files, and execute through WMIC.
https://www.cynet.com/blog/cyops-threat-alert-microsoft-exchange-zero-days/

Vice Society Publishes LA Public School Student Data, Psych Evals
After a flat refusal to pay the ransom, Los Angeles Unified School District's stolen data has been dumped on the Dark Web by a ransomware gang.
https://www.darkreading.com/attacks-breaches/vice-society-publishes-la-public-school-student-data-psych-evals

Dangerous New Attack Technique Compromising VMware ESXi Hypervisors
China-based threat actor used poisoned vSphere Installation Bundles to deliver multiple backdoors on systems, security vendor says. VMware issued urgent new mitigation measures and guidance on Sept. 29 for customers of its vSphere virtualization technology after Mandiant reported detecting a China-based threat actor using a troubling new technique to install multiple persistent backdoors on ESXi hypervisors.
https://www.darkreading.com/attacks-breaches/attackers-develop-dangerous-new-technique-for-compromising-esxi-hypervisors

Capital One Phish Showcases Growing Bank-Brand Targeting Trend
Capital One lures leveraged the bank's new partnership with Authentify, showing that phishers watch the headlines, and take advantage.
https://www.darkreading.com/attacks-breaches/capital-one-phish-trend-targeting-bank-brands

Malware Shifting to Virtual Environments, Warns Mandiant
Threat Intel Shows Possible Chinese Cyberspying Campaign Targets VMware Hypervisors. State-sponsored hackers may be shifting their targets from workstations to virtual environments where endpoint detection and response isn't supported, says Mandiant in a report detailing novel malware that attacks VMware hypervisors.
https://www.databreachtoday.com/malware-shifting-to-virtual-environments-warns-mandiant-a-20174

Glut of Fake LinkedIn Profiles Pits HR Against the Bots
A recent proliferation of phony executive profiles on LinkedIn is creating something of an identity crisis for the business networking site, and for companies that rely on it to hire and screen prospective employees. The fabricated LinkedIn identities — which pair AI-generated profile photos with text lifted from legitimate accounts — are creating major headaches for corporate HR departments and for those managing invite-only LinkedIn groups.
https://krebsonsecurity.com/2022/10/glut-of-fake-linkedin-profiles-pits-hr-against-the-bots/

Scam complaints rise by 63 percent in 2021 - banking ombudsman
Scam complaints are on the rise, increasing by 63 percent on the previous year, according to the Banking Ombudsman Scheme's latest report.
https://www.rnz.co.nz/news/national/475914/scam-complaints-rise-by-63-percent-in-2021-banking-ombudsman

****

Hints & Tips plus Security Awareness

Ransomware-Specific Resources Now Available in Cybersecurity Guide
The Federal Financial Institutions Examination Council yesterday announced that it had updated its "Cybersecurity Resource Guide for Financial Institutions" to include ransomware-specific resources to address the ongoing threat of ransomware incidents.
https://www.ffiec.gov/press/pdf/FFIECCybersecurityResourceGuide2022ApprovedRev.pdf

Time to Change Our Flawed Approach to Security Awareness
Defend against phishing attacks with more than user training. Measure users' suspicion levels along with cognitive and behavioral factors, then build a risk index and use the information to better protect those who are most vulnerable.
https://www.darkreading.com/vulnerabilities-threats/time-to-change-our-flawed-approach-to-security-awareness

Passwords Are Unfit - So Why Do We Still Have Them?
Andrew Shikiar knows more about the password economy than anybody else in the industry. The executive director of the FIDO Alliance says passwords are still around "because they work," albeit "in a very crude form." Half Hour Audio Interview
https://www.databreachtoday.com/interviews/passwords-are-unfit-so-do-we-still-have-them-i-5152

How To Prevent Social Media Account Hacks
"My account has been hacked. Please ignore a friend request." It may be of little comfort but if you've ever sent or received a message like that on, say Facebook or Instagram, you're actually among millions of users hit every year by social media account hackers. It's one of the fastest growing and most alarming Internet crimes, with security experts estimating that somewhere between 20 and 40 percent of all social network accounts have been compromised at some point.
https://scambusters.org/accounthack.html

Data breaches in the financial sector
The financial sector continues to suffer from a high rate of data breaches. The latest figures from the ICO's Data Security Incident Trends report reveal the sector has the third highest rates in the country, with over 2,874 incidents reported during Q4 2021/22.
https://www.globalbankingandfinance.com/data-breaches-in-the-financial-sector/

Protect Yourself From Phishing Scams: 8 Steps To Better Security
Since the mid 1990's, email phishing scams have been on the rise. Like most cybercrimes, hackers have improved and refined their phishing methods over time. Now, there's been a massive increase in targets due to the continuing coronavirus epidemic. Email phishing continues to be the method of choice for many cybercriminals to enter your device, steal your data, identity, finances, and more. A study by Tessian finds that 96% of phishing attacks arrive via email, showing the threat is very real.
https://www.sosdailynews.com/news.jspx?&articleid=02DAD576E847060E0BECE104D9A05826&sx=26446

****

News & Views

Why Don't CISOs Trust Their Employees?
Executives fear "malicious insiders" as top cyber threat to companies, research shows. Reasonable steps to secure and monitor systems may prevent reputational damage but are not enough. The changing hybrid or fully remote work model has brought numerous cybersecurity vulnerabilities as companies have less insight into the way employees are working remotely in a post-pandemic world.
https://www.darkreading.com/vulnerabilities-threats/why-don-t-cisos-trust-their-employees-

First 72 Hours of Incident Response Critical to Taming Cyberattack Chaos
Cybersecurity professionals tasked with responding to attacks experience stress, burnout, and mental health issues that are exacerbated by a lack of breach preparedness and sufficient incident response practice in their organizations
https://www.darkreading.com/attacks-breaches/incident-response-s-first-72-hours-critical-to-taming-chaos

3 Reasons Why BEC Scams Work in Real Estate
Identity verification could be the key to fighting back and building trust in an industry beset with high-stakes fraud.
https://www.darkreading.com/edge-articles/3-reasons-why-bec-scams-work-in-real-estate-and-how-to-fight-back

The Country Where You Live Impacts Password Choices
Literacy, levels of personal freedom, and other macro-social factors help determine how strong average passwords are in a given locale, researchers have found.
https://www.darkreading.com/operations/country-where-you-live-impacts-password-choices

****

"Ctrl -F" for The Board

Security to take an outsized role in IT spending in 2023
Most companies are reacting to a potential recession by cutting back on discretionary spending and other areas of the business while increasing tech budgets, according to the survey
https://www.cybersecuritydive.com/news/cybersecurity-productivity-software-tech-budgets/633253

Cyber Insurers Clamp Down on Clients' Self-Attestation of Security Controls
After one company suffered a breach that could have been headed off by the MFA it claimed to have, insurers are looking to confirm claimed cybersecurity measures.
https://www.darkreading.com/edge/cyber-insurers-clamp-down-on-clients-self-attestation-of-security-controls

Questions
Contact FIPCO’s Rob Foxx at 800-722-3498 ext. 249 or email FIPCO IT Services for more information.

"Make Security Part of You and Your Institution's DNA!"

Threat Intelligence Newsletter: October 14, 2022

Upcoming Threat Intelligence Peer Group Discussions
None available at the current time

****

Alerts & Warnings

Scammers exploit victims' pro-Russian sentiment
Fraudsters impersonate Putin’s close allies and ask for your help to move millions around – a mission impossible for Russian businesses since the invasion of Ukraine. The email comes out of the blue, yet it's tied with current events to make it more convincing. This time, scammers impersonate a close ally of Vladimir Putin, Viktor Zubkov. Zubkov, who served as the 36th Prime Minister of Russia in 2007-2008, and Putin's First Deputy Prime Minister during the presidency of Dmitry Medvedev, is also a board member of Gazprom, a state-owned energy giant.
https://cybernews.com/news/scammers-exploit-pro-russian-sentiment/

A New Wave of PayPal Invoice Scams Using Crypto Disguise
A new wave of PayPal invoice scams have been found using blockchain/cryptocurrency-related businesses as their disguise, security researchers from Japanese cybersecurity vendor Trend Micro found on found on October 09, 2022. While the scammers use a very common method, impersonating PayPal sellers to send random target invoices via PayPal systems saying users have been charged an amount of money and pushing them to click on malicious links, they use the names of famous companies/tokens on different blockchains to do so.
https://www.infosecurity-magazine.com/news/paypal-invoice-scams-using-crypto/

How Your Instagram and Facebook “Friends” Can Steal Your Social Media Account
It’s time to resurrect the old adage “With friends like these, who needs enemies?” Thanks to the nonprofit Identity Theft Resource Center (ITRC), their work has uncovered a social media hack victimizing users of Facebook and Instagram using friendship as a lure. Although attacks targeting social media users are nothing new, this latest scam tugs on the heartstrings of helping a friend in need. But the only thing this friend really needs is overtaking your social media account with your help, of course.
https://www.sosdailynews.com/news.jspx?&articleid=4D9C369714AE9F32D90C803DB4CCB857&sx=26446

****

Hints & Tips plus Security Awareness

Multifactor authentication is not all it's cracked up to be
Text message and email-based authentication aren't just the weakest variants of MFA. Cybersecurity professionals say they are broken. The recent spate of phishing attacks against identity-based authentication shows the extent to which MFA defenses can crumble, even under unsophisticated tactics.
https://www.cybersecuritydive.com/news/multifactor-authentication-weaknesses/633399

7 Practical Considerations for Effective Threat Intelligence
If your security team is considering, planning, building, or operating a threat intelligence capability, this advice can help. The rising value of information, the increased connectivity of systems, and the rapid uptake of cloud computing technology are significantly expanding the threat from cybercriminals and hostile groups, both in magnitude and severity.
https://www.darkreading.com/edge-articles/7-practical-considerations-for-effective-threat-intelligence

School Is in Session: 5 Lessons for Future Cybersecurity Pros
Opportunities in the field continue to grow — and show no signs of slowing down. The number of top universities and colleges across the US offering degrees in cybersecurity is now in the hundreds, and well-known college ranking services track the top programs. Note from Rob: For those of you who mentor this is great advice. For those who don't consider mentoring someone, the next wave of professionals needs guidance and we have the knowledge and experience to provide it going forward we will need all the help we can get to keep ourselves and organizations safe.
https://www.darkreading.com/careers-and-people/school-is-in-session-5-lessons-for-future-cybersecurity-pros

6 Things Every CISO Should Do the First 90 Days on the Job
A CISO's responsibilities have evolved immensely in recent years, so their first three months on the job should look a different today than they might have several years ago.
https://www.darkreading.com/careers-and-people/6-things-every-ciso-should-do-the-first-90-days-on-the-job

How To Identify, Remove, and Protect Against Mobile Spyware
Cell phones and other mobile devices are increasingly under attack from spyware and other malicious software. As more consumers switch from using desktop PCs to mobiles for their day-to-day online browsing, hackers and scammers are doing the same. Furthermore, they've gotten their hands on highly sophisticated surveillance apps previously only used by big organizations and governments.
https://scambusters.org/mobilespyware.html

How To Protect Yourself After A Data Breach
Data breaches seem to happen like clockwork. None of them are your fault, but the responsibility to protect yourself and your personal information rests square on your shoulders. It can seem like a daunting task, but there are some fundamental actions that can be taken right now that can make you a significantly safer from falling victim to a cyberattack. In this video, Jim Stickley will cover a wide range of types of data that can be exposed and how you can protect yourself. Credit Card, SSN, personal information, and other types of data are in the wild, so you need to be prepared.
https://www.sosdailynews.com/news.jspx?&articleid=618BB9CF8B15E1C4E06B82CDC8E5660D&sx

Children As Online Targets--What Every Parent Needs To Know
Adults should be well-aware of hacking and the risks involved when traversing online. But what many don't know is the sad truth that children are also targets of online abuse. Sadly, this includes infants. The good news is that parents aren't helpless when it comes to protecting their child's online activities and real-world identities. Knowing the signs of child identity theft, other harmful vulnerabilities and how you can help prevent them is a great way to start.
https://www.sosdailynews.com/news.jspx?&articleid=9A3F3A756BBD22C461CB7A120B5ED73D

****

News & Views

The hyperscalers are coming for your IT budget
AWS, Microsoft Azure and Google Cloud, the cloud megavendors, are set to command an ever-growing share of enterprise IT spend, according to Forrester. The dominance of the big three cloud services providers in the U.S. market is a standard part of the cloud storyline, but there are a few new wrinkles in the plot.
https://www.ciodive.com/news/AWS-Microsoft-Google-hyperscalers-cloud-budget/633979/

What is phishing-resistant multifactor authentication? It's complicated.
Higher levels of assurance can be achieved via physical keys with cryptographic protocols, but organizations shouldn't conflate resistance with infallibility. Multifactor authentication can bear weaknesses that render its efficacy moot. A common response and answer to the most problematic forms of MFA, though the details are limited at best, is phishing-resistant MFA.
https://www.cybersecuritydive.com/news/phishing-resistant-mfa/633703

We Can Save Security Teams From Crushing Workloads. Will We?
Today, the processing of mountain-high stacks of alarms is considered "security." That system is failing customers and the cybersecurity workforce. In one of my first jobs, I worked as a file clerk. I would arrive early in the morning to be greeted by a mountain-high stack of manila folders to process. I would spend the day knocking down the pile, only to be greeted by a new one the next day. It was clear that I was never going get ahead in that job.
https://www.darkreading.com/vulnerabilities-threats/we-can-save-security-teams-from-crushing-workloads-will-we-

****

"Ctrl -F" for The Board

CISOs, corporate boards in wide disagreement on cyber resilience
A study backed by researchers from MIT shows corporate boards are more focused on cyber risk but are out of alignment with CISOs on key issues. A wide gulf exists between perceptions of corporate board members and CISOs over the abilities of their companies to handle a cyberattack, according to a study by Proofpoint and Cybersecurity at MIT Sloan.
https://www.cybersecuritydive.com/news/cisos-boards-cyber-disagreement/633692

Report: Big U.S. Banks Are Stiffing Account Takeover Victims
When U.S. consumers have their online bank accounts hijacked and plundered by hackers, U.S. financial institutions are legally obligated to reverse any unauthorized transactions as long as the victim reports the fraud in a timely manner. But new data released this week suggests that for some of the nation's largest banks, reimbursing account takeover victims has become more the exception than the rule.
https://krebsonsecurity.com/2022/10/report-big-u-s-banks-are-stiffing-account-takeover-victims/

Questions
Contact FIPCO's Rob Foxx at 800-722-3498 ext. 249 or email FIPCO IT Services for more information.

"Make Security Part of You and Your Institution's DNA!"

Threat Intelligence Newsletter: October 21, 2022

FIPCO®
IT Audit
Round Table
Discussions

Upcoming Threat Intelligence Peer Group Discussions
None available at the current time

****

Alerts & Warnings

Attackers switch to self-extracting password-protected archives to distribute email malware
This variation on an old technique does not require the victim to provide a password to execute the malware. Distributing malware inside password-protected archives has long been one of the main techniques used by attackers to bypass email security filters. More recently, researchers have spotted a variation that uses nested self-extracting archives that no longer require victims to input the password.
https://www.csoonline.com/article/3677448/attackers-switch-to-self-extracting-password-protected-archives-to-distribute-email-malware.html

Feature-Rich 'Alchimist' Cyberattack Framework Targets Windows, Mac, Linux Environments
The comprehensive, multiplatform framework comes loaded with weapons, and it is likely another effort by a China-based threat group to develop an alternative to Cobalt Strike and Sliver. Researchers have uncovered a potentially dangerous cyberattack framework targeting Windows, Linux, and Mac systems that they assess is likely already being used in the wild.
https://www.darkreading.com/attacks-breaches/new-alchimist-attack-framework-targets-windows-mac-linux-environments

Scammers Targeting Those Seeking Student Loan Forgiveness
The FBI warned earlier this week that fraudsters are targeting individuals seeking student loan forgiveness via email, text, phone, and online. The attackers are masquerading as administrators from the Federal Student Loan Forgiveness Program. The campaign’s primary goal is to steal personally identifiable information from targets, the FBI says.
https://www.oodaloop.com/briefs/2022/10/20/scammers-targeting-those-seeking-student-loan-forgiveness/

Credit Piggybacking: What It Is And Why It's Dangerous
If you're desperate to build up your credit score - as many are during these tough financial times - you may have come across ads from companies offering to do just this for you, using a tactic known as piggybacking. But if you use this approach, you could end up in worse money troubles or even breaking the law... if you get snared by one of the scam firms operating in this gray area of financial support.
https://scambusters.org/piggyback.html

WordPress Security Update 6.0.3 Patches 16 Vulnerabilities
WordPress 6.0.3 fixes nine stored and reflected cross-site scripting (XSS) vulnerabilities, as well as open redirect, data exposure, cross-site request forgery (CSRF), and SQL injection flaws. WordPress security company Defiant has shared a description of each vulnerability. Four of them have a 'high severity' rating, and the rest have 'medium' or 'low' severity.
https://www.securityweek.com/wordpress-security-update-603-patches-16-vulnerabilities

Banks face their 'darkest hour' as malware steps up, maker of antivirus says
When I saw it, I had to reverse engineer it, Kaspersky's lead security researcher tells us. INTERVIEW Crimeware targeting banks and other financial-services organizations today features sophisticated capabilities and evasion tools, according to Kaspersky's lead security researcher Sergey Lozhkin. "The darkest hour is now for the financial industry, especially for big and medium-sized corporations," Lozhkin said, during a panel discussion on threats to financial services organizations.
https://www.theregister.com/2022/10/13/blacklotus_malware_kaspersky

****

Hints & Tips plus Security Awareness

Fakers Gonna Fake: How to Detect and Prevent Synthetic Identity Fraud
Confirming the identity of an existing account holder or for a new account opening is an expensive responsibility looming over the financial sector. Without proper oversight and controls, it results in massive losses, regulatory fines, and the threat of reputational damage.
https://www.about-fraud.com/2022/10/06/fakers-gonna-fake-how-to-detect-and-prevent-synthetic-identity-fraud/

Combating Elder Financial Exploitation
Every year older adults lose billions due to elder financial exploitation, which is the illegal or improper use of a senior's funds, property, or assets. Between 2019 and 2020, suspicious activity reports involving elder financial exploitation increased from $2.6 billion to $3.4 billion — the largest increase since 2013. Join the ABA Foundation and the Department of Justice for a free webinar that will help you recognize signs of elder financial exploitation and offer strategies to protect your older customers against this growing problem. Webinar: October 27, 2022, 1:00PM - 2:00PM
https://www.aba.com/training-events/online-training/combating-elder-financial-exploitation

4 tips to protect IT employees from phishing attacks
No one is perfect, and that includes your IT professionals. Here's what security experts say could help mitigate human error. Everybody makes mistakes, but the missteps of some can prove more costly than others.
https://www.cybersecuritydive.com/news/cybersecurity-spear-phishing-tech/634147

Understanding Cyber Attackers & Their Methods
Every day, your enterprise is at risk of being hacked. But just who are the cyber attackers, and what are their motivations? What methods might they use to crack enterprise data, and how do they stage their attacks? Insight on today's cyber adversaries, their methods and exploits, and how to stop them. Virtual Event: November 17, 2022, !0:00AM – 4:00 PM
https://vts.informaengage.com/dark-reading-understanding-cyber-attackers-and-their-methods/

What Fast-Talkers Can Teach Us About Vetting Vendors
Here's how to differentiate vendors that can back up their words with solutions and those that cannot. These people spout long sentences with big words that have very little meaning. They also seem to have a response for everything (words) yet almost never follow up on or complete anything (action).
https://www.darkreading.com/edge-articles/what-fast-talkers-can-teach-us-about-vetting-vendors

****

News & Views

As cybersecurity threats rage, colleges invest in risk prevention and pay higher insurance premiums
Cyber insurance policy renewal price increases are typically between 40% and 60%, with some increases hitting the triple digits, S&P said.
https://www.cybersecuritydive.com/news/college-cyber-threats-insurance-premiums/633570

US CISA Official: 'Forcefully Nudge' Users to Adopt MFA
MFA Is the Internet Equivalent of Seat Belts in Cars, Jen Easterly Tells Conference. The time for customer coddling over multifactor authentication must end, top U.S. government cybersecurity officials told an industry audience.
https://www.databreachtoday.com/us-cisa-official-forcefully-nudge-users-to-adopt-mfa-a-20286

How Card Skimming Disproportionally Affects Those Most In Need
When people banking in the United States lose money because their payment card got skimmed at an ATM, gas pump or grocery store checkout terminal, they may face hassles or delays in recovering any lost funds, but they are almost always made whole by their financial institution. Yet, one class of Americans — those receiving food assistance benefits via state-issued prepaid debit cards — are particularly exposed to losses from skimming scams, and usually have little recourse to do anything about it.
https://krebsonsecurity.com/2022/10/how-card-skimming-disproportionally-affects-those-most-in-need/

Anti-Money Laundering Service AMLBot Cleans House
AMLBot, a service that helps businesses avoid transacting with cryptocurrency wallets that have been sanctioned for cybercrime activity, said an investigation published by KrebsOnSecurity last year helped it shut down three dark web services that secretly resold its technology to help cybercrooks avoid detection by anti-money laundering systems.
https://krebsonsecurity.com/2022/10/anti-money-laundering-service-amlbot-cleans-house/

****

"Ctrl -F" for The Board

Boards looking to CEOs, not CIOs, to lead digital initiatives
The change in digital leadership will be most pronounced in technology-heavy industries, including banking, retail, telecom and healthcare, Gartner says. Nearly two-thirds of board directors are planning to increase their risk appetite through 2024, according to a Gartner survey released Wednesday. Last year, 57% of boards were planning to increase their risk appetite.
https://www.ciodive.com/news/CEO-board-of-directors-tech-leaders/634283

Cyber defense is not IT's job alone, CISA CTO says
While tech executives must provide critical tools and procedures to lower cyber risk, the whole organization is responsible for fending off attackers. Gattoni, who joined the Department of Homeland Security in 2010, said organizations are up against a threat landscape in flux. What's needed is a stronger focus on personalizing defense strategies, he said.
https://www.ciodive.com/news/brian-gattoni-cto-cisa/634398

Gen Z, Millennial Workers Are Bigger Cybersecurity Risks Than Older Employees
Younger workers surveyed are less likely to follow established business cybersecurity protocols than their Gen X and baby boomer counterparts, a new survey finds. A new survey shows Generation Z and millennials, younger workers who have grown up as digital natives, are surprisingly more careless about their employer's cybersecurity than their senior Gen X and baby boomer colleagues.
https://www.darkreading.com/threat-intelligence/gen-z-millennial-workers-are-bigger-cybersecurity-risks-than-older-employees

Questions
Contact FIPCO's Rob Foxx at 800-722-3498 ext. 249 or email FIPCO IT Services for more information.

"Make Security Part of You and Your Institution's DNA!"

Threat Intelligence Newsletter: October 28, 2022

Upcoming Threat Intelligence Peer Group Discussions
None available at the current time

****

Alerts & Warnings

Cybersecurity Risks & Stats This Spooky Season
From ransomware to remote workers to cyber-extortion gangs to Fred in shipping who clicks on the wrong link, cybersecurity concerns can keep you awake this season and all seasons. Autumn is here and with it, pumpkins, Halloween, and scary movies. And despite the horrors that accompany the season, for many people, nothing is more terrifying than … cybersecurity risks.
https://www.darkreading.com/vulnerabilities-threats/cybersecurity-risks-and-stats-this-spooky-season

Hackers Threaten to Sell Stolen Medibank Data, Seek Ransom
Australian Insurance Firm 'Working Urgently' to Verify Theft Claim. A ransomware group claiming to have stolen personal data from Australian insurer Medibank is demanding payment, the company announced just days after assuring customers that it had seen no evidence of data theft stemming from a cybersecurity incident it detected on Oct. 12.
https://www.databreachtoday.com/hackers-threaten-to-sell-stolen-medibank-data-seek-ransom-a-20291

Scammers Targeting Those Seeking Student Loan Forgiveness
FBI warns that cybercriminals are stealing personal information by posing as administrators of the Student Loan Debt Relief Plan.
https://www.darkreading.com/attacks-breaches/scammers-targeting-those-seeking-student-loan-forgiveness

Holograms and Deepfake Videos Used In Job and Investment Scams
Scammers have developed a new weapon in the digital fraud war that could create major problems for consumers and businesses - holograms. Holograms are digital 3D images created by light beams, which make it appear as if an object or person is really there.
https://scambusters.org/hologram.html

Downloading Some Apps May Get Your Device All Mixed Up

Over the past few years, we have all been discouraged from mixing with others, for fear of catching a nasty virus. As we know, time has passed and we are mingling amongst ourselves a bit more. But there is something else out there doing a fair bit of stirring up things and also passing on some nasty infections. NullMixer is a new malware dropper that has infected over 47,000 windows PCs, according to Kaspersky. Users looking for cracked and pirated software are at greater risk of downloading the malware; in some cases, merely by clicking a link to get some pirated software will infect your device. If you click on a malicious link, you end up downloading the malware and upon launching the program, NullMixer is deployed. It infects the PC, releasing over 20 trojans which will run unnoticed on your computer.
https://www.sosdailynews.com/news.jspx?&articleid=FE97472077B9EA680F9DD5577FF6FE7F&

IRS Warns Of An Exponential Increase In Tax Related Scams

Tax scams are starting a bit earlier this year. The IRS is already issuing warnings to taxpayers to be on the lookout for tax scams. The specific ones they are a concerned with are SMS/text messaging (smishing) scams. The agency says these have increased "exponentially" in recent months and particularly within the past few weeks.
https://www.sosdailynews.com/news.jspx?&articleid=545486BFA27002E59F812AB3740DAF62&

The Most Hacked Apps To Get To Your Details

We share a lot these days. Some might even say we spout personal details like a water from a fire hydrant, especially when it comes to social media. For hackers, that means they have us all right where they want us. Researchers at TechShielder put in some work and found that there are a number of apps available to us that actually have been repeatedly compromised and share our personal information with plenty of others that we may not want to have our information.
https://www.sosdailynews.com/news.jspx?&articleid=6BA34F26817C8EFDD3789EB2E0F743CA&

Hackers Started Exploiting Critical "Text4Shell" Apache Commons Text Vulnerability

WordPress security company Wordfence on Thursday said it started detecting exploitation attempts targeting the newly disclosed flaw in Apache Commons Text on October 18, 2022. The vulnerability, tracked as CVE-2022-42889 aka Text4Shell, has been assigned a severity ranking of 9.8 out of a possible 10.0 on the CVSS scale and affects versions 1.5 through 1.9 of the library.
https://thehackernews.com/2022/10/hackers-started-exploiting-critical.html

22-Year-Old Vulnerability Reported in Widely Used SQLite Database Library

A high-severity vulnerability has been disclosed in the SQLite database library, which was introduced as part of a code change dating all the way back to October 2000 and could enable attackers to crash or control programs.
https://thehackernews.com/2022/10/22-year-old-vulnerability-reported-in.htm

****

Hints & Tips plus Security Awareness

4 ways Target tracks cyberthreats to defend its systems

While threats and vulnerabilities swell — Target has more than 27,000 YARA rules to help it identify malware, for example — the most pressing and realistic threats get the greatest focus. "We are not only striving to be intelligence driven, but striving to be intelligence driven in the right way," said Derek Thomas, principal engineer on Target's cyber threat intelligence team. "It's not enough for us to focus on

the bottom of the pyramid of pain. We also want to focus on the parts that matter, what we call behavioral indicators."
https://www.ciodive.com/news/target-threat-intelligence/634648/

4 strategies for 'winning' IT vendor negotiations
"If you don't ask, you don't get": When vendor fees spike, customers can walk away with a better deal. Vendor contract negotiations are built into IT procurement cycles. Companies renew deals for ERPs and CRMs, cloud and add "as a Service" data, security and BI features as a regular part of business operations, mostly without incident.
https://www.ciodive.com/news/software-vendor-negotiation-strategies/634729/

The Battle Against Phishing Attacks and Similar Scams
Many entities fight an uphill battle against increasingly clever phishing and related scams that lead to serious data compromises, say former CIA analyst Eric Cole and former Department of Justice Assistant Attorney General David Kris, who are both advisers at security firm Theon Technology. 15 Minute Interview
https://www.databreachtoday.com/interviews/battle-against-phishing-attacks-similar-scams-i-5164

Measuring Your Security Posture: Explaining The ROI of Cyber Hygiene to the Board
Successful defense requires understanding the security posture of every device in your enterprise, it requires the ability to make decisions fast, and it requires the ability to execute on those decisions at enterprise scale but if bottlenecks exist within your organization, answering key questions such as "how secure is our company" can be a challenge. Webinar November 9, 2022, 1PM CST
https://www.databreachtoday.com/webinars/measuring-your-security-posture-explaining-roi-cyber-hygiene-to-board-w-4432

****

News & Views

How an Ohio district is cracking the code on cybersecurity training
Digital citizenship courses and lessons, where students learn how to navigate the online world, are typically found throughout the K-12 curriculum. These classes teach students how to create and consume digital content and can be woven into other toolsets, including social-emotional learning skills or digital etiquette. Cybersecurity is a step beyond digital citizenship, a toolset students can use to navigate digital spaces more safely. Miller said while it's important that students learn to be mindful of their digital footprint, his district's program gives them the skills to strengthen the safety of that online world.
https://www.cybersecuritydive.com/news/ohio-cybersecurity-training/634566/

Iron Man Started His Journey From Scratch & Your Security Awareness Program Can Too
Iron Man wasn't built in a day. Nor was his suit — or ego, for that matter. The creation of the superhero and his suit of high-tech armor came out of necessity — to keep shrapnel shards from puncturing his heart. The solution was the creation of Iron Man's first-ever electromagnetic reactor — and, well, the rest is Marvel Cinematic Universe history.
https://www.darkreading.com/attacks-breaches/iron-man-started-his-journey-from-scratch-your-security-awareness-program-can-too

****

"Ctrl -F" for The Board

3 areas for IT leaders to prioritize in 2023
Leaders are concerned about a financial downturn, Gartner research shows. But the right IT strategies can help put sustainable growth on overdrive. IT leaders need to take quick action to update how their businesses work, invest sustainably, and reduce cyber risk as financial uncertainty looms, according to analysts at the Gartner IT Symposium/Xpo 2022, in Orlando, Florida.
https://www.ciodive.com/news/gartner-conference-keynote-IT/634288/

3 reasons why every board needs a tech subcommittee
Today nearly every organization wants to call itself a tech company, most likely because the current perception is that the digital experience — above all else — ensures success and profitability. Given this landscape, tech is predictably a top priority for corporate decision makers. The paradox is that many corporate boards still don't give tech the weight and space it deserves in their deliberations.
https://www.ciodive.com/news/board-directors-technology-subcommittee/634803/

Questions
Contact FIPCO's Rob Foxx at 800-722-3498 ext. 249 or email FIPCO IT Services for more information.

"Make Security Part of You and Your Institution's DNA!"

Threat Intelligence Newsletter: November 4, 2022

FIPCO® IT Audit Round Table Discussions

Upcoming Threat Intelligence Peer Group Discussions
None available at the current time

****

Alerts & Warnings

U.S. Bank data breach impacts 11K customers
U.S. Bank notified some customers on Friday that their personal information was accidentally shared by a third-party vendor, according to letters posted to the California Attorney General's website. Whether they use it to amplify the brand, recruit new employees, advertise new products, or even sell directly to consumers, corporate brands love social media.
https://www.cybersecuritydive.com/news/us-bank-data-breach/635365/

7 Hidden Social Media Cyber-Risks for Enterprises
Leaning on social media to amplify your company's brand? Here's a look at the emerging cybersecurity risks that can arise from TikTok, LinkedIn, Twitter, and other platforms.
https://www.darkreading.com/application-security/7-hidden-social-media-cyber-risks-enterprises

China-Backed APT10 Supercharges Spy Game With Custom Fileless Backdoor
The sophisticated and ever-evolving threat known as LodeInfo is being deployed against media, diplomatic, government, public sector, and think-tank targets. Chinese-speaking threat actor APT10 has been using a sophisticated and sometimes fileless backdoor to target media, diplomatic, governmental, public sector, and think-tank targets, since at least March, researchers have found. Note: Traditional Antivirus is unable to combat this.
https://www.darkreading.com/threat-intelligence/china-backed-apt10-spy-game-custom-fileless-backdoor

Watch Out For These 3 Energy Saving Scams
Who doesn't want to score energy savings these days? Not only are utility bills climbing, but we're also increasingly aware of the environmental cost of using our precious natural resources. Cue a bunch of scammers and their misleading sales spiels, tricking people into handing over their cash for dubious products and services they claim will deliver those savings and make us more eco-friendly.
https://scambusters.org/energysaving.html

WhatsApp Scammers Take Advantage Of Your Loved Ones
If you receive a WhatsApp message from a loved one asking for financial help, it's a very good idea to become a bit of a private investigator before turning over any funds. The popular chatting/phoning/video calling app has been taking a beating lately and once again it's the tool cybercriminals are using to get to your money. And they are pulling out the best of their social engineering and manipulation tactics to do it. This time, it's by masquerading as loved ones on WhatsApp.
https://www.sosdailynews.com/news.jspx?&articleid=DC457E9582EB41BED0F66D6CF6F20827

No, your CEO is not texting you
Everyone wants to stay on good terms with their employer. Threat actors know this too, and they exploit this weakness accordingly. Don't fall for it.
https://www.cybersecuritydive.com/news/ceo-phishing-campaigns/635568

****

Hints & Tips plus Security Awareness

How to stop ATM attacks
ATM attacks are becoming increasingly common and the criminals that perpetrate them are becoming bolder, with incidents ranging from explosive attacks to software attacks. As a result, banks are investing more money intro protecting ATMs.
https://www.atmmarketplace.com/articles/how-to-stop-atm-attacks/

'Point solutions just need to die': The end of the one-trick security tool
The deconstruction of security products makes companies grapple with avoidable IT challenges. There is a glut of cybersecurity tools that do one thing. Many organizations pay for dozens of these products or services, some of which go forgotten or otherwise unused.
https://www.ciodive.com/news/security-tool-strategy/635469

3 Steps Small Businesses Can Take to Prevent Cyberattacks
Setting priorities for internal security measures and outsourcing complex practices help protect small and midsize businesses. Due to their limited security budgets and high dependence on unmanaged IT systems, small businesses are often left vulnerable and frequently targeted by cybercriminals.
https://www.darkreading.com/edge-articles/3-steps-small-businesses-can-take-to-prevent-cyberattacks

Microsoft Authenticator gains feature to thwart spam attacks on MFA
Microsoft has rolled out 'number matching' in push notifications for its multi-factor authentication (MFA) app Microsoft Authenticator. The new advanced feature is generally available in Microsoft Authenticator and should help counter attacks on MFA that rely on push notification spam
https://www.zdnet.com/article/microsoft-authenticator-gains-feature-to-thwart-spam-attacks-on-mfa/

Common Signs Of Phishing To Keep In Mind When Your Inbox Overflows
With email phishing, deciphering what's real from what's fake can be a challenge. Our inboxes are stuffed with emails fighting to get our attention and get us to take some action. But how to ferret-out what's legitimate takes some cyber-smarts. Research shows email is the primary method of spreading 92% of all malware, and the U.S. is the target of 86% of all email phishing attacks. Whether at home or at work, email phishing is relentless, but being aware of characteristics they have in common can be a powerful tool. The ability to spot those familiar traits before it's too late can be the difference between a good day and a bad nightmare.
https://www.sosdailynews.com/news.jspx?&articleid=C08D6B4174C8551EE08B498BA0646D08

****

News & Views

FinCEN reports ransomware reporting has increased

On Tuesday, FinCEN released its most recent Financial Trend Analysis of ransomware-related BSA filings for 2021, and reported that ransomware continued to pose a significant threat to U.S. critical infrastructure sectors, businesses, and the public. The report focuses on ransomware trends in BSA filings from July-December 2021, and addresses the extent to which a substantial number of ransomware attacks appear to be connected to actors in Russia. This latest report builds on FinCEN's October 2021 report on the same topic.
https://www.fincen.gov/sites/default/files/2021-10/Financial%20Trend%20Analysis_Ransomware%20508%20FINAL.pdf

Small business owners want more advice from banks, study finds

A J.D. Power study found that small businesses trust banks and are seeking practical advice to pull through tough economic conditions. Small business owners navigating rising inflation, supply chain issues, and labor market tightness are keen to receive advice from their bank partners, according to the J.D. Power 2022 U.S. Small Business Banking Satisfaction Study.
https://www.bankingdive.com/news/small-business-owners-want-more-advice-from-banks-study-finds/635467/

****

"Ctrl -F" for The Board

Cybersecurity is an Infinite Game

Game theory, the study of competition and conflict, tells us there are two types of games: Finite Games and Infinite Games. Knowing which one you are playing is key to making optimal decisions. Finite games are those that have a beginning and an end. The objective of a finite game is to win. The game ends when all sides know who the winner is. Examples of finite games include most battles in a traditional war; they end when there is a decisive victory. Sporting events are examples of more peaceable finite games
https://www.oodaloop.com/archive/2022/10/28/cybersecurity-is-an-infinite-game/

Questions
Contact FIPCO’s Rob Foxx at 800-722-3498 ext. 249 or email FIPCO IT Services for more information.

"Make Security Part of You and Your Institution's DNA!"

Threat Intelligence Newsletter: November 11, 2022

FIPCO®
IT Audit
Round Table
Discussions

Upcoming Threat Intelligence Peer Group Discussions
None available at the current time

****

Alerts & Warnings

Mondelēz settlement in NotPetya case renews concerns about cyber insurance coverage
The legal dispute between the snack giant and insurer Zurich American, which lasted four years, raises further questions about how insurers cover acts of cyber war.
https://www.cybersecuritydive.com/news/mondelez-zurich-notpetya-cyber-insurance-settlement/636029

Don't Fall For These 7 Big Zelle Scams
Do you have Zelle? It's not just us asking. Those or similar are the words a scammer uses when they try to trick you while using this bank-owned cash transfer service. And although Zelle claims that 99.9 percent of its transactions are scam-free, the service is so popular that it still leaves room for hundreds of thousands of scams, which have doubled in some cases during the past few years.
https://scambusters.org/zelle.html

Online Shopping Season Brings Out The Holiday Fraud
As 2022 flies by, believe it or not, the holiday online shopping season is upon us. This is your annual reminder to be on the lookout for all kinds of cyber creeps who are out there waiting to take advantage of all of us just wanting some cheer with our shopping excitement in an otherwise uncertain time. As that time slowly ticks away, or rushes by, depending on your point of view, the hackers continue to improve upon their various cyber scams. Online scams are becoming harder to detect, but it’s important to remain vigilant.
https://www.sosdailynews.com/news.jspx?&articleid=2461C45A023BF475A3985E5A6ADE83E7

****

Hints & Tips plus Security Awareness

Always on call: How to avoid an IT meltdown

Communication, automation and preparation can turn an after-hours IT outage into a minor hiccup instead of a full meltdown.
https://www.ciodive.com/news/on-call-IT-system/635979

How to implement an effective system to address third-party risk
Current processes for assessing and managing third-party cybersecurity risks are cumbersome and ineffective. CISOs must adopt new principles to address business exposure.
https://www.cybersecuritydive.com/news/third-party-risk-cyber-security-strategies/635906

Build Security Around Users: A Human-First Approach to Cyber Resilience
Security is more like a seat belt than a technical challenge. It's time for developers to shift away from a product-first mentality and craft defenses that are built around user behaviors.
https://www.darkreading.com/risk/build-security-around-users-a-human-first-approach-to-cyber-resilience

****

News & Views

CISA’s K-12 cyber education program goes nationwide
Cyber.org Range will introduce students to cybersecurity concepts and prepare them for intermediate-level jobs in a severely understaffed industry. The Cybersecurity and Infrastructure Security Agency’s K-12 education initiative is going national. Cyber.org Range, a virtual cybersecurity education program that began in Louisiana, will expand to all 50 states, CISA Director Jen Easterly announced Monday.
https://www.cybersecuritydive.com/news/cisa-cyber-education-nationwide/636154

Retail Sector Prepares for Annual Holiday Cybercrime Onslaught
Retailers and hospitality companies expect to battle credential harvesting, phishing, bots, and various malware variants.
https://www.darkreading.com/risk/retail-sector-prepares-for-annual-holiday-cybercrime-onslaught

Economic Uncertainty Isn't Stopping Cybercrime Recruitment — It's Fueling It
Confused economies and rising unemployment rates foster a rich opportunity for cybercrime recruitment.
https://www.darkreading.com/attacks-breaches/economic-uncertainty-isn-t-stopping-cybercrime-recruitment-it-s-fueling-it

****

"Ctrl -F" for The Board

It's Time to See Cybersecurity Regulation as a Friend, Not a Foe
There's real value in having a better perspective around future regulation and compliance requirements.
https://www.darkreading.com/risk/it-s-time-to-see-cybersecurity-regulation-as-a-friend-not-a-foe

The Art of Calculating the Cost of Risk
Insurance and legislation affect how enterprises balance between protecting against breaches and recovering from them.
https://www.darkreading.com/edge-articles/the-art-of-calculating-the-cost-of-risk

Questions
Contact FIPCO’s Rob Foxx at 800-722-3498 ext. 249 or email FIPCO IT Services for more information.

"Make Security Part of You and Your Institution's DNA!"

Threat Intelligence Newsletter: November 18, 2022

Upcoming Threat Intelligence Peer Group Discussions
None available at the current time

****

Alerts & Warnings

Instant and Automated Payments Make Tempting Targets for Fraud
Faster B2B payments, back-office automation and alternative payments are all advancing rapidly, but these advances are creating new opportunities for fraudsters, so expect the innovation war between legitimate businesses and bad actors to heat up, not cool off.
https://www.pymnts.com/news/security-and-risk/2022/instant-automated-payments-make-tempting-targets-fraud/

BBB Scam Alert: These veterans' programs seem real. But watch out for impostors
As a veteran, navigating government programs and benefits is complicated. Scammers know this – and take full advantage of it. BBB Scam Tracker has received numerous reports of con artists who pretend to represent the government and target veterans with promises of special grants and other programs. If you or a family member is a veteran, stay alert to this common scam.
https://www.bbb.org/article/scams/27830-bbb-scam-alert-these-veterans-benefit-programs-seem-real-but-watch-out-for-impostors?utm_source=newslette

Nokia warns 5G security 'breaches are the rule, not the exception'
A majority of 5G network operators experienced up to six cyber incidents in the past year. Defenses are especially lacking for ransomware and phishing attacks. 5G was supposed to make wireless networks more secure, but that's not panning out, according to research conducted by GlobalData and commissioned by Nokia.
https://www.cybersecuritydive.com/news/5g-security-breaches/636693

Patch ASAP: Critical Citrix, VMware Bugs Threaten Remote Workspaces With Takeover
Hole-y software alert, Batman: Cybercriminal faves Citrix Gateway and VMware Workspace ONE have authentication-bypass bugs that could offer up total access to attackers. Critical authentication-bypass vulnerabilities in Citrix and VMware offerings are threatening devices running remote workspaces with

complete takeover, the vendors warned this week.
https://www.darkreading.com/vulnerabilities-threats/patch-asap-critical-citrix-vmware-bugs-remote-workspaces-takeover

Disneyland Malware Team: It's a Puny World After All
A financial cybercrime group calling itself the Disneyland Team has been making liberal use of visually confusing phishing domains that spoof popular bank brands using Punycode, an Internet standard that allows web browsers to render domain names with non-Latin alphabets like Cyrillic.
https://krebsonsecurity.com/2022/11/disneyland-malware-team-its-a-puny-world-after-all/

Protect Yourself from Buy Now, Pay Later Scams
The growing popularity of "buy now, pay later" (BNPL) credit plans, where consumers make interest-free, staged repayments for their purchases, has been hijacked by fraudsters on an alarming scale. They're using stolen or invented identity credentials to trick online retailers into handing over products and services for just a 25 percent deposit. And, although it's the retailers who carry the can for the rest of the debt, consumers are becoming increasingly caught up in the scam.
https://scambusters.org/paylater.html

****

Hints & Tips plus Security Awareness

Why Cybersecurity Should Highlight Veteran-Hiring Programs
Military veterans tend to have the kind of skills that would make them effective cybersecurity professionals, but making the transition is not that easy. Organizations are struggling to fill cybersecurity positions. That may be because they aren't using security staff efficiently and so they need more people. It could also just be that the increase in threats means there is more work to do.
https://www.darkreading.com/edge-articles/cybersecurity-needs-to-highlight-veteran-hiring-programs

Ransomware Attackers Don't Take Holidays
Cybereason's Sam Curry on the Financial and Business Impact of After-Hours Strikes Cyberattackers love to strike on weekends and holidays - that's not news. What is news: These attacks cost more than weekday incidents, and they take a heavy toll on defenders. 12 Minute Video
https://www.databreachtoday.com/ransomware-attackers-dont-take-holidays-a-20479

By Hook And By Crook. Top Scams Targeting Seniors, And How To Help Protect Against Them
It's a sad reality that our older citizens, those most unfamiliar with online scams, can be easily victimized. The FBI's IC3 (Internet Crime Complaint Center) 2021 Elder Fraud Report puts a spotlight on some of the most common scams used against those aged 60 and above, and some of the disturbing statistics that result. Know that scammers can victimize the same individual with a number of crimes at the same time. They can lose their money, access to an online account and for some, their identity.
https://www.sosdailynews.com/news.jspx?&articleid=55C69076193D2FE069A50E10A7B50F8C

Unforgiving Scammers Seek Your Credentials When Applying For Student Loan Debt Forgiveness
We can all use a little financial help from time to time; especially those saddled with student loan debt. So, there's no surprise that after the Student Loan Debt Relief Plan was announced and neared reality, an immediate uptick in fraud schemes surrounding this program started to appear. The FBI states scammers are working over time looking to take advantage of those individuals seeking this student forgiveness.
https://www.sosdailynews.com/news.jspx?&articleid=6027B881B7D921337819B546F8BA4253

****

News & Views

ABA to FCC: Stop illegal texts, protect banks' lawful texts
The American Banker Association led a group of trade groups in expressing support for the Federal Communication Commission's proposal to require mobile wireless providers to block text messages that are that are from invalid, unallocated or unused numbers, or those on a "do-not-originate" list, in a recently submitted comment letter.
https://bankingjournal.aba.com/2022/11/aba-to-fcc-stop-illegal-texts-protect-banks-lawful-texts/?utm_source=eloqua

CISA wants to change how organizations prioritize vulnerabilities
Federal authorities want to take the guesswork and manual decision-making processes out of the messy world of vulnerabilities. Vulnerability management is a whac-a-mole pursuit for many organizations, but federal authorities are trying to change that. The Cybersecurity and Infrastructure Security Agency on Thursday released its guide for Stakeholder-Specific Vulnerability Categorization and outlined three areas of focus for continued improvement.
https://www.cybersecuritydive.com/news/cisa-prioritize-vulnerabilities/636485/

Basics Will Block Most Ransomware Hits, Says UK Cyber Chief
Ransomware Remains Biggest Online Threat, Warns NCSC CEO Lindy Cameron. The vast majority of ransomware attacks could be blocked outright if victims focused on cybersecurity basics, says Britain's cybersecurity chief. "We still think that 90% of incidents in the U.K. could have been prevented if people had followed the basics," Lindy Cameron, president of the U.K. National Cyber Security Center, told attendees at a recent cybersecurity summit in Scotland.
https://www.databreachtoday.com/basics-will-block-most-ransomware-hits-says-uk-cyber-chief-a-20426

Australia Considers Ban on Ransomware Payments After Medibank Breach
Over the weekend, the Australian government announced that it is considering banning ransomware payments due to the Medibank data breach that impacted thousands of Australians. According to the Australian Federal Police, the cyberattack against Medibank has been linked to Russian cyber-criminals who may have an affiliation with the REvil cyber gang.
https://www.oodaloop.com/briefs/2022/11/15/australia-considers-ban-on-ransomware-payments-after-medibank-breach/

****

"Ctrl -F" for The Board

How Routine Pen Testing Can Reveal the Unseen Flaws in Your Cybersecurity Posture
Testing is an ongoing mission, not a one-and-done fix. Cybersecurity must evolve beyond reactively handling breaches and pivoting to protect an organization's data after the fact. Without proper precautions, cybercriminals from all over the world can easily take advantage of vulnerabilities within a company's Web applications, mobile applications, APIs, and more.
https://www.darkreading.com/vulnerabilities-threats/how-routine-pen-testing-can-reveal-the-unseen-flaws-in-your-cybersecurity-posture

What We Really Mean When We Talk About 'Cybersecurity'
A lack of precision in our terminology leads to misunderstandings and confusion about the activities we engage in, the information we share, and the expectations we hold. The words safety and security are

often the same in many languages. That is also true in the world of cyber, where we frequently say cybersecurity when we really mean cyber safety.
https://www.darkreading.com/vulnerabilities-threats/what-we-really-mean-when-we-talk-about-cybersecurity-

Questions
Contact FIPCO's Rob Foxx at 800-722-3498 ext. 249 or email FIPCO IT Services for more information.

"Make Security Part of You and Your Institution's DNA!"

Threat Intelligence Newsletter: December 2, 2022

FIPCO®
IT Audit
Round Table
Discussions

Upcoming Threat Intelligence Peer Group Discussions
None available at the current time

****

Alerts & Warnings

BBB Scam Alert: Don't click on that text! 5 ways to avoid delivery scams
Some consumers have recently been getting text messages stating a major delivery carrier needs them to "update delivery preferences" on a package by clicking on a link. The problem? The text is a scam, and the link results in the theft of personal information.
https://www.bbb.org/article/scams/16460-scam-alert-fake-text-delivery-scam

DEV-0569 finds new ways to deliver Royal ransomware, various payloads
Recent activity from the threat actor that Microsoft tracks as DEV-0569, known to distribute various payloads, has led to the deployment of the Royal ransomware, which first emerged in September 2022 and is being distributed by multiple threat actors. Observed DEV-0569 attacks show a pattern of continuous innovation, with regular incorporation of new discovery techniques, defense evasion, and various post-compromise payloads, alongside increasing ransomware facilitation.
https://www.microsoft.com/en-us/security/blog/2022/11/17/dev-0569-finds-new-ways-to-deliver-royal-ransomware-various-payloads/

Cybercriminals strike understaffed organizations on weekends and holidays
More than one-third of respondents said it took their organization longer to assess the scope, stop and recover from a holiday or weekend attack compared to a weekday, according to a Cybereason survey published Wednesday. Larger organizations with more than 2,000 employees were even more likely to experience delays.
https://www.ciodive.com/news/cyberattacks-weekends-holidays/637119/

Instagram Impersonators Target Thousands, Slipping by Microsoft's Cybersecurity
Cyberattackers have targeted students at national educational institutions in the US with a sophisticated phishing campaign that impersonated Instagram. The unusual aspect of the gambit is that they used a valid domain in an effort to steal credentials, bypassing both Microsoft 365 and Exchange email protections in the process.
https://www.darkreading.com/application-security/instagram-impersonators-target-thousands-microsoft-cybersecurity

Thousands of Amazon RDS Snapshots Are Leaking Corporate PII
A service that allows organizations to back up data in the cloud can accidentally leak sensitive data to the public Internet, paving the way for abuse by threat actors.
Legions of databases are being inadvertently exposed monthly, through a feature of an Amazon cloud-based data-backup service. The situation gives threat actors access to personally identifiable information (PII) that they can use in extortion, ransomware, or other threat activity, researchers have found.
https://www.darkreading.com/cloud/thousands-amazon-rds-snapshots-leaking-corporate-pii

Self-Replicating Malware Used by Chinese Cyberspies Spreads via USB Drives
A China-linked cyberespionage group tracked as UNC4191 has been observed using self-replicating malware on USB drives to infect targets, and the technique could allow them to steal data from air-gapped systems, Google-owned Mandiant reports.
https://www.securityweek.com/self-replicating-malware-used-chinese-cyberspies-spreads-usb-drives

****

Hints & Tips plus Security Awareness

Why cyberattackers love IT professionals — and how organizations can keep risk at bay
Limiting admin access is one step toward strengthening defenses, but there are other ways to reduce vulnerabilities. Years ago, the infamous Nigerian prince exemplified the phishing attack – a spray-and-pray approach targeting the masses in the hopes one person would take the bait. Today's attackers are much more sophisticated, having essentially adopted the tactics of targeted marketing. Two-thirds of organizations have seen an increase in spearphishing attacks aimed at specific end users, according to Proofpoint data.
https://www.ciodive.com/news/IT-vulnerabilities-cybersecurity-strategy/637548/

How To Sell Safely Online - And Avoid Scams
You've been planning to declutter before the year is out. And the holiday season is a great time to sell your stuff online. But how can you sell safely and avoid getting scammed? These days, there are more ways than ever to offer your unwanted items on the web - eBay, Craigslist, Facebook, local neighborhood sites, and more. But there are also more crooks than ever planning to rip you off - by tricking you into giving them money, by failing to pay, or by stealing your identity.
https://scambusters.org/sellsafe.html

QR Code Dangers And The Risks Behind Using Them
There's danger now lurking behind those busy black-and-white boxes that are QR codes and that now seem to be found everywhere for everything, including viewing restaurant menus. Always a quick way scan for information, more businesses are using them now more than ever. A study by Ivanti takes a look at

what's really going on behind QR's and their findings should make anyone think twice before they reach to scan a QR code with their mobile device.
https://www.sosdailynews.com/news.jspx?&articleid=5E431EC65F76C0C75A318F49863AF72D

2023 Holiday Scams
Welcome to the 2022 holiday season. What should be a time of joy and celebration for all, can turn into a time of stress and panic for some. Scams come in many forms most seemingly innocent. That's what makes them so difficult to avoid. Some scams are more sophisticated than others. Knowing these scams and how they work, will help you defend yourself and your loved ones this holiday season. Written by Rob Foxx from FIPCO. This article is meant for general distribution please feel free to post in lobbies on websites or anywhere else to increase awareness this season.
https://www.fipco.com/news/holiday-scams

Online Banking Smishing Scam
Text message scams are on the rise and in this Today Show segment, Jim Stickley demonstrates how easy it is from criminals to perform these attacks. Most people receive legitimate text alerts from their financial institution so a malicious text can be very believable. DON'T CLICK EVER. Simply open your mobile app or open a browser and sign into your account. If there is a real fraud alert, you will be notified once you are logged in.
https://www.sosdailynews.com/news.jspx?&articleid=2CE07759E8769CD625937DEDD21B3FF6

****

News & Views

FBI director says he's 'extremely concerned' about China's ability to weaponize TikTok
FBI Director Christopher Wray told Congress on Tuesday he is "extremely concerned" that Beijing could weaponize data collected through TikTok, the wildly popular app owned by the Chinese company ByteDance.
https://www.cyberscoop.com/fbi-wray-tells-congress-extremely-concerned-tiktok/

Bitcoin 'rarely' used for legal transactions, on 'road to irrelevance', say European Central Bank officials
European Central Bank officials alleged on Wednesday that bitcoin is "rarely used for legal transactions," is fueled by speculation and the recent erosion in its value indicates that it is on the "road to irrelevance," in a series of stringent criticism (bereft of strong data points) of the cryptocurrency industry as they urged regulators to not lend legitimacy to digital tokens in the name of innovation.
https://techcrunch.com/2022/11/30/bitcoin-rarely-used-for-legal-transactions-on-road-to-irrelevance-say-european-central-bank-officials/

Security awareness training needs a revamp
Awareness training plays an important role in an organization's overall cybersecurity posture. But while security tools and platforms are regularly updated or replaced to meet the challenges of a constantly changing threat landscape, security awareness training has remained stagnant.
https://www.cybersecuritydive.com/news/new-security-awareness-training-cyber/637170/

****

"Ctrl -F" for The Board

As CIOs tighten tech spend, demand for cybersecurity services grows
Managed service providers can help fill talent needs and tame costs, but that strategy may require additional risk mitigation. Companies looking to fend off cybercriminals are turning to third-party firms to help thwart an expanding network of threat actors. Cybersecurity spending, which encompasses services and products, is expected to grow by 10% to 15% over the next 12 to 18 months, but product spending over the same period will decline 10% to 15%, said Doug Saylors, a partner at research and advisory firm ISG.
https://www.ciodive.com/news/MSP-cybersecurity-technology-spending/637253

Amid Legal Fallout, Cyber Insurers Redefine State-Sponsored Attacks as Act of War
As carriers rewrite their act-of-war exclusions following the NotPetya settlement between Mondelez and Zurich, organizations should read their cyber insurance policies carefully to see what is still covered. The consequences from NotPetya, which the US government said was caused by a Russian cyberattack on Ukraine in 2017, continue to be felt as cyber insurers modify coverage exclusions, expanding the definition of an "act of war." Indeed, the 5-year-old cyberattack appears to be turning the cyber insurance market on its head.
https://www.darkreading.com/edge-articles/amid-notpetya-fallout-cyber-insurers-define-state-sponsored-attacks-as-act-of-war

Questions
Contact FIPCO’s Rob Foxx at 800-722-3498 ext. 249 or email FIPCO IT Services for more information.

"Make Security Part of You and Your Institution's DNA!"

Threat Intelligence Newsletter: December 16, 2022

FIPCO®
IT Audit
Round Table
Discussions

Upcoming Threat Intelligence Peer Group Discussions
None available at the current time

****

Alerts & Warnings

BBB Scam Alert: Don't fall for this online seller trick when buying handmade gifts
How the scam works You're browsing online when you find a special gift or holiday decoration that you'd like to purchase. The photos seem professional, and everything looks normal… except for one thing. In the item description, you find a message from the seller advising you not to make the purchase through the online sales platform where you have discovered it. Instead, the seller encourages you to purchase the item directly from their independent website, promising you'll get a hefty discount if you do.
https://www.bbb.org/article/scams/27901-dont-fall-for-this-online-seller-trick-when-buying-handmade-gifts

BBB Tip: The naughty list - BBB's 12 scams of Christmas
With 2022 quickly winding down, Better Business Bureau has compiled our naughty list of the top 12 scams of Christmas. When shopping or donating this holiday season, watch out for schemes trying to swipe your cash or steal your personal information. You can avoid most of the scams on this list by taking a few simple precautions. Always exercise caution with social media ads promoting discounted items, holiday events, job opportunities, and donation requests, as well as direct messages from strangers. If you are asked to make a payment or donation by wire transfer, through a third party, or by prepaid debit or gift card, treat it as a red flag.
https://www.bbb.org/article/news-releases/23497-the-naughty-list-bbbs-12-scams-of-christmas

Cuba ransomware group hitting US organizations in 5 critical sectors
Cuba ransomware actors are still successfully targeting U.S. organizations in five critical infrastructure sectors, including financial services, government facilities, healthcare, critical manufacturing and IT, the FBI and Cybersecurity and Infrastructure Security Agency said Thursday in a joint advisory.
https://www.cybersecuritydive.com/news/cuba-ransomware-group-us-critical-sectors/637974

CommonSpirit Ransomware Breach Affects About 624,000 So Far
Leaked Data Includes Names, Addresses and Birthdates. The ransomware hacking incident at CommonSpirit affected the data of at least approximately 624,000 individuals, the hospital chain told federal regulators. The second-largest nonprofit hospital chain in the United States has slowly dribbled out information about the ransomware attack it first detected in early October.
https://www.healthcareinfosecurity.com/commonspirit-ransomware-breach-affects-about-624000-so-far-a-20689

APT37 Uses Internet Explorer Zero-Day to Spread Malware
IE is still a vector: South Koreans lured in with references to the deadly Halloween celebration crowd crush in Seoul last October. North Korean threat group APT37 was able to exploit an Internet Explorer zero-day vulnerability to deploy documents loaded with malware as part of its ongoing campaign targeting users in South Korea, including defectors, journalists, and human rights groups.
https://www.darkreading.com/remote-workforce/apt37-internet-explorer-zero-day-malware

Phishing in the Cloud: We're Gonna Need a Bigger Boat
SasS security is everyone's problem. Phishing has long been one of the best ways to gain access to a target organization. It didn't used to be this way. In the early days of computer security, the remote code exploit (RCE) was the preferred method of gaining access, as it required no user interaction. In fact, if something required user interaction, it wasn't considered a serious threat. Better security practices started to take hold, and the RCE method of access became much more challenging. And it turned out, getting users to interact was easier than ever imagined.
https://www.darkreading.com/endpoint/phishing-in-the-cloud-we-re-gonna-need-a-bigger-boat

Fraudsters Siphon $360M From Retailers Using 50M Fake Shoppers
Cyberattackers focused on ad fraud and clickjacking stole millions during Black Friday by hijacking shopper accounts and tying up transactions.
Online fraudsters posing as consumers likely siphoned off more than $360 million from the marketing budgets of online businesses by generating fake clicks during Black Friday, while 20% of visits to retail sites on Cyber Monday were bots posing as shoppers and not humans, Web security firms said this week.
https://www.darkreading.com/threat-intelligence/fraudsters-siphon-360m-fake-shoppers

4 Arrested for Filing Fake Tax Returns With Stolen Data
Three Nigerian nationals and one UK citizen are facing extradition to the US following their recent arrest for cybercrimes related to a tax refund scam. The Department of Justice unsealed indictments of Akinola Taylor, Olayemi Adafin, Olakunle Oyebanjo, and Kazeem Olanrewaju Runsewe, who are accused of breaching US company servers, stealing personal information, and using that data to file fraudulent Internal Revenue Service (IRS) tax documents and collect refunds.
https://www.darkreading.com/attacks-breaches/4-arrested-for-filing-fake-tax-returns-with-stolen-data

SiriusXM, MyHyundai Car Apps Showcase Next-Gen Car Hacking
A trio of security bugs allow remote attackers to unlock or start the car, operate climate controls, pop the trunk, and more — all via poorly coded mobile apps.
At least three mobile apps tailored to allow drivers to remotely start or unlock their vehicles were found to have security vulnerabilities that could allow unauthenticated malicious types to do the same from afar. Researchers say securing APIs for these types of powerful apps is the next phase in preventing connected car hacking.
https://www.darkreading.com/application-security/siriusxm-myhyundai-car-apps-showcase-next-gen-car-hacking

10 Warning Signs Of A Love Bomb Cheat
Are you under siege from a love bomber - someone who blasts you with so much fake affection that you fall under their total control? Psychologists have labelled love bombing among the cruelest tactics underpinning romance scams, which cost Americans more than half a billion dollars last year, much of it through online relationships where the pair never meet. So, it's important to recognize the symptoms before you fall victim.
https://scambusters.org/lovebomb.html

Schoolyard Bully Trojan Apps Stole Facebook Credentials from Over 300,000 Android Users
More than 300,000 users across 71 countries have been victimized by a new Android threat campaign called the Schoolyard Bully Trojan. Mainly designed to steal Facebook credentials, the malware is camouflaged as legitimate education-themed applications to lure unsuspecting users into downloading them. The apps, which were available for download from the official Google Play Store, have now been taken down. That said, they still continue to be available on third-party app stores.
https://medium.com/@spixnet.gmbh/schoolyard-bully-trojan-apps-stole-facebook-credentials-from-over-300-000-android-users-9f385fd6dd0a

****

Hints & Tips plus Security Awareness

Reduce Risk and Prove Security Efficacy with Next-Gen MDR/XDR
Security operations is hard. The threat landscape is constantly evolving. Business and IT initiatives create an ever-expanding attack surface. Myriad security products overwhelm operators and drive costs up. And as cybersecurity becomes a topic in board rooms, CISOs are not only under pressure to reduce risk, but also to prove the efficacy of their security postures.
https://www.brighttalk.com/webcast/19819/568906

What does it take to be good at cybersecurity?
Few large enterprises meet Deloitte’s standards for high cyber maturity. The 21% that do recognize benefits not typically associated with security. Cybersecurity prowess requires defense in depth, and few enterprises meet that need. The difference between high, medium and low cyber maturity levels comes down to three sets of practices — planning, activities and board engagement, according to Deloitte.
https://www.cybersecuritydive.com/news/cybersecurity-maturity-deloitte/638193

Phishing 101: How to Not Fall for a Phishing Attack
Join us for an informative webinar session as we dive into the hard truth of phishing attacks. Phishing has evolved to be more precise and deceptive than ever before, with the influx of mobile devices, screen sizes and many other sophisticated schemes tricking users into divulging information that can compromise credentials. Webinar January 10, 2023, 10:30 AM CST
https://www.databreachtoday.com/webinars/phishing-101-how-to-fall-for-phishing-attack-w-4553

When Tragedy Arises, Scammers Rise To The Occasion
Scams surrounding crisis situations or high-profile events never cease. Taking advantage of current events and crises are a lure many cyberthieves cannot wait to take advantage of for their own gain. Natural disasters, such as the earthquake in Papua New Guinea and the fundraising surrounding it opens a door for scammers to steal donations from those who give to provide relief for those in need. Others such as the recent death of Queen Elizabeth II are also fair game for cybercrime.
https://www.sosdailynews.com/news.jspx?&articleid=E05B984BBE0BE983E79F17BCE2A23EEB

Keeping Your Bank Account And Credit Cyber-Smart
Financial institutions and hacking go hand-in-hand these days and keeping your bank account and credit from being the next victim is more important than ever. The safest approach, although the least favorite, is assuming that if your data hasn't yet been hacked that at some point it will be. Hacking banks and their account holders is the most direct cash infusion a hacker can get…and they know it. According to Kaspersky Lab, attacks on ATMs alone hit an all-time high in 2017 with malware-as-a-service (MAAS) opportunities. With this service, even hacking "hacks" who have no cybercrime experience can watch an instructional "how to" video on how to target an ATM successfully. With all the relentless email phishing attacks and step-by-step advice on hacking, guarding our finances with common sense protection is something we all need to do. It all starts by being proactive with your accounts.
https://www.sosdailynews.com/news.jspx?&articleid=C291AA65F52DE424133B75CA6ECAA7C9

Top 4 SaaS Security Threats for 2023
With 2022 coming to a close, there is no better time to buckle down and prepare to face the security challenges in the year to come. This past year has seen its fair share of breaches, attacks, and leaks, forcing organizations to scramble to protect their SaaS stacks. March alone saw three different breaches from Microsoft, Hubspot, and Okta.
https://thehackernews.com/2022/12/top-4-saas-security-threats-for-2023.html

What Stricter Data Privacy Laws Mean for Your Cybersecurity Policies
For today's businesses data privacy is already a big headache, and with modern privacy laws expanding to more of the world's population, regulatory compliance is on track to become a more complicated, high-stakes process touching on every aspect of an organization. In fact, Gartner predicts that by 2024, 75% of the Global Population will have its personal data covered under privacy regulations.
https://thehackernews.com/2022/12/what-stricter-data-privacy-laws-mean.html

****

News & Views

Yes, It's Possible—Frictionless Account Fraud Protection
Over the past few years, bank account fraud has become one of the largest threats against financial institutions (FIs). Just last year, there's been over $52B in identity fraud losses affecting 42 million U.S. consumers. And this grew 79% y-o-y. Community banks and credit unions must find a way to balance methods of managing fraudulent activity with attracting new customers. Otherwise, they may be left behind. And the stakes are higher than ever. At the same time FIs are looking at high application abandonment rates.
https://www.finextra.com/blogposting/23293/yes-its-possiblefrictionless-account-fraud-protection

V**et software security as part of enterprise procurement, NIST says**
The guidance, an answer to last year's executive order, examines where and when potential supply chain vulnerabilities can surface. The National Institute of Standards and Technology (NIST) published updated guidance that encourages enterprises to assess supply chain risks throughout the procurement process and to continue monitoring for potential vulnerabilities in source code.
https://www.cybersecuritydive.com/news/nist-software-supply-chain-security/623412

New AI Bot Could Take Phishing, Malware to a Whole New Level
Experts Warn ChatGPT Could Usher in Phishing 3.0, Democratize Hacking Technology. Anything that can write a software code can also write malware. While most threat actors take several hours and sometimes even days to write malicious code, the latest AI technology can do it in seconds. Even worse, it could open the door to rapid innovation for hackers with little or no technical skills or help them overcome language barriers to writing the perfect phishing email.
https://www.databreachtoday.com/new-ai-bot-could-take-phishing-malware-to-whole-new-level-a-20709

Swiss Government Wants to Implement Mandatory Duty to Report Cyber-Attacks
The Swiss government has recently made efforts to deem it mandatory for critical infrastructure providers to report cyberattacks to the National Cyber Security Centre. The efforts have resulted in proposed amendments to the Information Security Act. The Swiss Parliament has been tasked with amending the act, which aims to provide more transparency into cyberattacks and sound the alarm on cyber threats in the country. The Swiss government published a press release last week stating that cyberattacks have large consequences to the security of the Swiss economy.
https://www.oodaloop.com/briefs/2022/12/08/swiss-government-wants-to-implement-mandatory-duty-to-report-cyber-attacks/

****

"Ctrl -F" for The Board

The Privacy War Is Coming
Privacy standards are only going to increase. It's time for organizations to get ahead of the coming reckoning. Since the dawn of digital marketing, people have been asked to provide their personal information in exchange for information online. This "information swap" is still a common digital tactic. However, it isn't just marketing forms that collect data. Contact forms, checkout carts, and digital healthcare forms are all examples of ways data is being captured.
https://www.darkreading.com/endpoint/the-privacy-war-is-coming

Questions
Contact FIPCO’s Rob Foxx at 800-722-3498 ext. 249 or email FIPCO IT Services for more information.

"Make Security Part of You and Your Institution's DNA!"

Threat Intelligence Newsletter: December 22, 2022

FIPCO®
IT Audit
Round Table
Discussions

Upcoming Threat Intelligence Peer Group Discussions
None available at the current time

****

Alerts & Warnings

BBB Scam Alert: How to spot an out-of-stock scam before it's too late
With the holiday shopping season in full swing, BBB Scam Tracker has gotten dozens of reports of a crafty new online shopping con. This time, scammers claim a product you purchased is out of stock, but they never process your promised refund.
https://www.bbb.org/article/scams/27957-bbb-scam-alert-how-to-spot-an-out-of-stock-scam-before-its-too-late

Little Rock School District approves $250K payment in ransomware settlement
While trying to retrieve stolen data from its network, the Little Rock School District's board voted 6-3 on Dec. 5 to approve a $250,000 settlement that would end a recent ransomware incident. An LRSD school board member accidentally shared the dollar amount of the settlement during the public board meeting.
https://www.cybersecuritydive.com/news/little-rock-school-ransomware-payment/639083

Holiday Spam, Phishing Campaigns Challenge Retailers
Revived levels of holiday spending have caught the eye of threat actors who exploit consumer behaviors and prey on the surge of online payments and digital activities during the holidays. As the holiday season barrels to a conclusion, malicious actors are attempting to take advantage of harried consumers by ramping up the volume of spam and phishing attacks in the form of unsolicited emails and email-based threats — and businesses stand to suffer.
https://www.darkreading.com/attacks-breaches/holiday-spam-phishing-campaigns-challenge-retailers

****

Hints & Tips plus Security Awareness

ABA Foundation, FBI Release Infographic on Avoiding Holiday Scams
The ABA Foundation and FBI on Friday released a new infographic offering consumers tips to avoid online shopping scams this holiday season. The graphic provides advice for recognizing warning signs, lists good cyber habits, urges consumers to do business with companies they trust and explains why payment methods matter when it comes to settling disputes. Good information to post in lobbies.

https://bankingjournal.aba.com/2022/12/aba-foundation-fbi-release-infographic-on-avoiding-holiday-scams/

Combating Ransomware Attacks: Which Strategies Hold Promise?
Governments and defenders have made great strides to better understand the scope of the ransomware problem and take steps to disrupt it, says cybersecurity veteran Jen Ellis. A top challenge remains calculating the extent of ransomware's harm to the economy and people's everyday lives. Obtaining accurate and complete information - including data on who's being affected and how, and by which cybercrime groups - is a challenge. "We know now that there's an iceberg, and we know what the tip of the iceberg looks like, but we don't know what percentage of that iceberg we can see," Ellis says.
https://www.databreachtoday.com/interviews/combating-ransomware-attacks-which-strategies-hold-promise-i-5195

Your Data For Sale On The Dark Web And What You Can Do About It
As much as we love the convenience of our digital world, we know a hefty price tag can come with it. The world is full of bad actors whose goal is to get their hands on our sensitive, personally identifiable information, or PII. Should you find your PII is for sale on the dark web, it helps to know there are options for doing something about it, even if you think it’s too late. Just some of that hijacked PII can include passwords, email and physical addresses, Social Security numbers, financial accounts, and much more.
https://www.sosdailynews.com/news.jspx?&articleid=CDAB8C96D8AB0C905C33B2AA55368ACB

****

News & Views

Banks might dump Zelle due to fraud refund scheme
Banks may choose to drop partnerships with instant payments apps, like Zelle, if they have to reimburse scam victims. The seven banks that own Zelle recently launched a plan to reimburse scam victims if the scammer is pretending to be a bank employee, according to a report by Washington Post.
https://www.atmmarketplace.com/news/banks-might-dump-zelle-due-to-fraud-refund-scheme/

Incident responders brace for end-of-year cyber scaries
Fears of the next SolarWinds or Log4j-style incident hitting over the holidays have some cybersecurity experts on edge. While many professionals might approach the end of a year as a time for pause and reflection, setting goals for the new year or at least some respite, cybersecurity professionals can’t shake the premonition that something bad is about to occur.
https://www.cybersecuritydive.com/news/cyber-security-incident-response-holiday-prep/639137

****

"Ctrl -F" for The Board

Cyber Security Is Not a Losing Game – If You Start Right Now
Reality has a way of asserting itself, irrespective of any personal or commercial choices we make, good or bad. For example, just recently, the city services of Antwerp in Belgium were the victim of a highly disruptive cyberattack. As usual, everyone cried "foul play" and suggested that proper cybersecurity measures should have been in place. And again, as usual, it all happens a bit too late. There was nothing special or unique about the attack, and it wasn't the last of its kind either.
https://thehackernews.com/2022/12/cyber-security-is-not-losing-game-if.html

Questions
Contact FIPCO’s Rob Foxx at 800-722-3498 ext. 249 or email FIPCO IT Services for more information.

"Make Security Part of You and Your Institution's DNA!"

Threat Intelligence Newsletter: January 3, 2023

FIPCO®
IT Audit
Round Table
Discussions

Upcoming Threat Intelligence Peer Group Discussions
None available at the current time

****

Alerts & Warnings

Email hijackers scam food out of businesses, not just money
IN BRIEF Business email compromise (BEC) continues to be a multibillion-dollar threat, but it's evolving, with the FBI and other federal agencies warning that cybercriminals have started using spoofed emails to steal shipments of physical goods – in this case, food.
https://www.theregister.com/2022/12/17/in_brief_security/

Adult Google Ad Fraud Campaign Garnered Millions of Impressions
Malwarebytes has released an advisory detailing a fraudulent online ad campaign using Google Ads. The campaign leverages adult websites and advertising to entice victims into clicking on malicious links that made the operators behind the campaign hundreds of thousands of dollars a month. Malwarebytes states that the scammers loaded a full blog as their popunder, which contains dozens of stolen articles from other sites.
https://www.oodaloop.com/briefs/2022/12/22/adult-google-ad-fraud-campaign-garnered-millions-of-impressions/

Cyber-Incident Causes System Failures at Canadian Children's Hospital
A major Canadian pediatric hospital has suffered from a cyberattack that caused outages and several networks to go down. The hospital is based in Toronto, Canada and is known as SickKids. The hospital informed the public of the cyber incident earlier this week via Twitter and confirmed that the situation .
https://www.oodaloop.com/briefs/2022/12/22/cyber-incident-causes-system-failures-at-canadian-childrens-hospital/

Industrial bank Files Notice of Data Breach, Leaking Consumers SSNs and Financial Account Information
On December 23, 2022, IBW Financial Corporation ("IBW"), the holding company for Industrial Bank, reported a data breach with the Attorney General of Montana after discovering that sensitive consumer information was compromised following what appears to have been a cyberattack committed against the company's computer network.

https://www.jdsupra.com/legalnews/industrial-bank-files-notice-of-data-4551926/

****

Hints & Tips plus Security Awareness

BBB Tip: Don't get scammed out of a gift card this season
Whether you're buying a gift card online or grabbing one off the shelf at a store, shop carefully to make sure you're not falling for a scam.
https://www.bbb.org/article/news-releases/14400-dont-get-scammed-out-of-a-gift-card-this-season

10 Gartner tech trends to watch in 2023
From new entrants to incumbents, one thing is true for each technology: customization is key. Business technology has two primary edicts: cut costs through efficiency and help businesses increase revenue. It’s part of the standard pitch for every vendor out there.
https://www.ciodive.com/news/gartner-tech-trends-symposium/634251/

Explore CISA’s 37 steps to minimum cybersecurity
The agency placed a premium on low cost, high impact security efforts, which account for more than 40% of the goals. The Cybersecurity and Infrastructure Security Agency released its long-awaited, cross sector cybersecurity performance goals Thursday, in a bid to raise the security baselines. Far from esoteric, the efforts listed are meant to serve as a broadly-digestible roadmap to minimum operational security.
https://www.cybersecuritydive.com/news/cisa-cpg-cybersecurity-performance-goals-critical-infrastructure/635224

Children As Online Targets--What Every Parent Needs To Know
Adults should be well-aware of hacking and the risks involved when traversing online. But what many don’t know is the sad truth that children are also targets of online abuse. Sadly, this includes infants. The good news is that parents aren’t helpless when it comes to protecting their child’s online activities and real-world identities. Knowing the signs of child identity theft, other harmful vulnerabilities and how you can help prevent them is a great way to start.
https://www.sosdailynews.com/news.jspx?&articleid=9A3F3A756BBD22C461CB7A120B5ED73D

The Perks Of Cleaning Out Your Friends List
Some friends are forever, and others are social media friends you no longer need, want, know, or trust. It’s a segment of social media that often gets overlooked, and revisiting that list of friends who have access to your posts can benefit you and your online security. Now is the perfect time to take stock of your list and do a friendship sweep. After all, do you really want total strangers seeing a video of that beginner ballet recital you starred in five years ago? You may not be the person you were then, and your circle of friends may not be the same either. So why are they still on your friends list?
https://www.sosdailynews.com/news.jspx?&articleid=BE7CF1348C0D96FD2B4E3B4FC93CFB62

Accelerate Your Incident Response
Tis the season for security and IT teams to send out that company-wide email: "No, our CEO does NOT want you to buy gift cards." As much of the workforce signs off for the holidays, hackers are stepping up their game. We will no doubt see an increase in activity as hackers continue to unleash e-commerce scams and holiday-themed phishing attacks. Hackers love to use these tactics to trick end users into compromising not only their personal data but also their organization's data. But that does not mean you should spend the next couple of weeks in a constant state of anxiety. Instead, use this moment as an opportunity to ensure that your incident response (IR) plan is rock solid.

https://thehackernews.com/2022/12/accelerate-your-incident-response.html

****

News & Views

How attackers are breaking into organizations
Threat actors lean heavily on phishing attacks, vulnerabilities in software and containers, and stolen credentials, according to top cyber vendor research. Threat actors are constantly on the lookout for new or more susceptible pathways to break in and gain access to an organization's data or network.
https://www.cybersecuritydive.com/news/how-attackers-break-organizations/629686/

Face it, password policies and managers are not protecting users
Passwords have not worked as a solid security strategy in a long time. The policies are there, so why are passwords security's weak spot? If you use a computer, you probably already know this: Passwords are failing at protecting users. "Passwords as a security strategy are dead," said David Maynor, senior director of threat intelligence with Cybrary.
https://www.cybersecuritydive.com/news/password-policies-cyber-strategy-mfa/635912

INSIDERS WORRY CISA IS TOO DISTRACTED FROM CRITICAL CYBER MISSION
Four years in, CISA appears to be struggling with internal divisions over the direction of the agency, morale problems and growing concerns about leadership priorities. CyberScoop spoke with 14 current and former CISA employees and 18 additional people familiar with CISA's internal operations. Most described an agency that lacks a clearly defined strategic direction and often seems more focused on its public image than working on the nation's thorniest cybersecurity problems.
https://www.cyberscoop.com/cisa-dhs-easterly-cyber-mission/

NSA PUBLISHES THE 2022 CYBERSECURITY YEAR IN REVIEW
Shares NSA Mission Focuses and Demonstrates How It Produces Cybersecurity Outcomes for the Nation. This year's report highlights NSA's ability to scale cybersecurity solutions through strong partnerships, resulting in speed and agility. "By protecting the U.S. Government's most sensitive networks, we cascade solutions that help secure critical infrastructure, U.S. allies, and businesses and consumers around the world," said Rob Joyce, NSA Cybersecurity Director. "Our efforts to protect those networks help protect yours."
https://www.nsa.gov/Press-Room/News-Highlights/Article/Article/3247606/nsa-publishes-2022-cybersecurity-year-in-review/

****

"Ctrl -F" for The Board

Financial Services Was Among Most-Breached Sectors in 2022
Industry Has Logged 566 Data Breaches Worldwide So Far, Public Notifications Reveal. Everyone knows why criminals have long loved to rob banks. But in this era of robbers operating remotely, which tactics are cybercriminals actually employing and how often are they successful?
https://www.databreachtoday.com/financial-services-was-among-most-breached-sectors-in-2022-a-20760

Questions
Contact FIPCO's Rob Foxx at 800-722-3498 ext. 249 or email FIPCO IT Services for more information.

"Make Security Part of You and Your Institution's DNA!"

Threat Intelligence Newsletter: January 6, 2023

FIPCO®
IT Audit
Round Table
Discussions

Upcoming Threat Intelligence Peer Group Discussions
None available at the current time

****

Alerts & Warnings

BBB Scam Alert: 'Tis the season to donate, and scammers are taking advantage
With so many purchases during the holiday season, it can be easy to miss a fraudulent credit card charge or two – especially if it appears to be from a charity. Keep a close eye on your credit card statement this time of year.
https://www.bbb.org/article/scams/27976-scam-alert-tis-the-season-to-donate-and-scammers-are-taking-advantage

LastPass: Notice of Recent Security Incident
To date, we have determined that once the cloud storage access key and dual storage container decryption keys were obtained, the threat actor copied information from backup that contained basic customer account information and related metadata including company names, end-user names, billing addresses, email addresses, telephone numbers, and the IP addresses from which customers were accessing the LastPass service.
https://blog.lastpass.com/2022/12/notice-of-recent-security-incident/

Driving Through Defenses | Targeted Attacks Leverage Signed Malicious Microsoft Drivers
SentinelOne has observed prominent threat actors abusing legitimately signed Microsoft drivers in active intrusions into telecommunication, BPO, MSSP, and financial services businesses. Investigations into these intrusions led to the discovery of POORTRY and STONESTOP malware, part of a small toolkit designed to terminate AV and EDR processes.
https://www.sentinelone.com/labs/driving-through-defenses-targeted-attacks-leverage-signed-malicious-microsoft-drivers/

How Doctored Photos Help Social Security Scammers

How much is your Social Security number worth? Actually, it only costs $4 to buy a stolen SSN on the dark web. Or it is free to them if they steal it. But the cost to the victim could be astronomical. Your number is actually one of the most valuable pieces of information for identity thieves. If they get ahold of it, they can use it to take out loans in your name, damaging your credit reputation, and potentially costing you a lot more.
https://scambusters.org/socialsecurity5.html

'Tis The Season Of Fake Shopping Sites

As we're all getting back into the holiday spirit after a somewhat glum 2020 season, it's important to remember that the holiday shopping season doesn't end on December 25. In fact, some retailers put their marketing effort into overdrive. There are after holidays sales, new year's sales, and even "getting rid of all this stuff we didn't sell at Christmas" sales advertised under some creative title. Retailers try to take advantage of the shopping spirit as far into the new year as they can and those who like to capitalize on this by creating phishing campaigns combined with fake shopping sites with lookalike domains (domain jacking) or taking advantage of typos (typo squatting) are also upping their game.
https://www.sosdailynews.com/news.jspx?&articleid=74053A80EC0F3B6FF0D08E1B09AF579A

Hackers Using Stolen Bank Information to Trick Victims into Downloading BitRAT Malware

A new malware campaign has been observed using sensitive information stolen from a bank as a lure in phishing emails to drop a remote access trojan called BitRAT. The unknown adversary is believed to have hijacked the IT infrastructure of a Colombian cooperative bank, using the information to craft convincing decoy messages to lure victims into opening suspicious Excel attachments. The discovery comes from cybersecurity firm Qualys, which found evidence of a database dump comprising 418,777 records that is said to have been obtained by exploiting SQL injection faults.
https://thehackernews.com/2023/01/hackers-using-stolen-bank-information.html

****

Hints & Tips plus Security Awareness

The FBI's Perspective on Ransomware

Ransomware: contemporary threats, how to prevent them and how the FBI can help. In April 2021, Dutch supermarkets faced a food shortage. The cause was not a drought or a sudden surge in the demand for avocados. Rather, the reason was a ransomware attack. In the past years, companies, universities, schools, medical facilities, and other organizations have been targeted by ransomware threat actors, turning ransomware into the internet's most severe security crisis.
https://thehackernews.com/2023/01/the-fbis-perspective-on-ransomware.html

Windows Server 2012 and 2012 R2 reaching end of support

Windows Server 2012 and Windows Server 2012 R2 will end on October 10, 2023. After this date, these products will no longer receive security updates, non-security updates, bug fixes, technical support, or online technical content updates. Microsoft has migration guidance for both cloud and on-premises solutions.
https://learn.microsoft.com/en-US/lifecycle/announcements/windows-server-2012-r2-end-of-support

****

News & Views

Federal Reserve Alert To 'Significant Threat' To Financial System
The US central bank has warned that cryptocurrencies pose a "significant" threat to the wider banking system, writes Mark Hooson. In a joint statement, the Federal Reserve and US regulators including the Office of the Comptroller of the Currency – a branch of the US Treasury – said that risks related to the crypto industry must not be allowed to migrate to the banking system.
https://www.forbes.com/uk/advisor/investing/2023/01/04/cryptocurrency-updates/

EarSpy: Spying on Phone Calls via Ear Speaker Vibrations Captured by Accelerometer
As smartphone manufacturers are improving the ear speakers in their devices, it can become easier for malicious actors to leverage a particular side-channel for eavesdropping on a targeted user's conversations, according to a team of researchers from several universities in the United States.
https://www.securityweek.com/earspy-spying-phone-calls-ear-speaker-vibrations-captured-accelerometer

Google to Pay $29.5 Million to Settle Lawsuits Over User Location Tracking
Google has agreed to pay a total of $29.5 million to settle two different lawsuits brought by Indiana and Washington, D.C., over its "deceptive" location tracking practices. The lawsuits came in response to revelations in 2018 that the internet company continued to track users' whereabouts on Android and iOS through a setting called Web & App Activity despite turning Location History options off.
https://thehackernews.com/2023/01/google-to-pay-295-million-to-settle.html

****

"Ctrl -F" for The Board

Financial Services Was Among Most-Breached Sectors in 2022
Industry Has Logged 566 Data Breaches Worldwide So Far, Public Notifications Reveal. Everyone knows why criminals have long loved to rob banks. But in this era of robbers operating remotely, which tactics are cybercriminals actually employing and how often are they successful?
https://www.databreachtoday.com/financial-services-was-among-most-breached-sectors-in-2022-a-20760

Ohio Supreme Court Says Ransomware Is Not Physical Damage
Justices Rule Against Software Developer in Bid to Use Insurance to Cover Attack. Ransomware hacking is not tantamount to a physical attack, the Ohio Supreme Court ruled, meaning a software developer cannot use its property insurance to cover losses.
https://www.govinfosecurity.com/ohio-supreme-court-says-ransomware-physical-damage-a-20808

Think Your Business Is Too Small For Hackers? It's Time To Think Again
"Cyberattacks only happen to big companies with lots of valuable data and assets to steal," thought most small business owners at one time or another. But there is a false sense of security when SMB (small-to-medium-sized business) owners believe hackers are not interested in a small company. After all, bad actors will just move on to bigger and better targets with much more to steal, right? Wrong.
https://www.sosdailynews.com/news.jspx?&articleid=4BF19C33A6CBC279A5A3FF92B5CBE19B

Questions
Contact FIPCO's Rob Foxx at 800-722-3498 ext. 249 or email FIPCO IT Services for more information.

"Make Security Part of You and Your Institution's DNA!"

Threat Intelligence Newsletter: January 12, 2023

FIPCO®
IT Audit
Round Table
Discussions

Upcoming Threat Intelligence Peer Group Discussions
None available at the current time

****

Alerts & Warnings

Identity Thieves Bypassed Experian Security to View Credit Reports
Identity thieves have been exploiting a glaring security weakness in the website of Experian, one of the big three consumer credit reporting bureaus. Normally, Experian requires that those seeking a copy of their credit report successfully answer several multiple-choice questions about their financial history. But until the end of 2022, Experian's website allowed anyone to bypass these questions and go straight to the consumer's report. All that was needed was the person's name, address, birthday, and Social Security number.
https://krebsonsecurity.com/2023/01/identity-thieves-bypassed-experian-security-to-view-credit-reports/

US Family Planning Non-Profit MFHS Confirms Ransomware Attack
US-based health and human services organization Maternal & Family Health Services (MFHS) has reported being hit by a ransomware attack. The non-profit made the announcement on Thursday, saying its systems were compromised between August 21, 2021, and April 4, 2022. An investigation launched in April last year revealed the attack may have exposed sensitive information to an unauthorized individual.
https://www.infosecurity-magazine.com/news/mfhs-confirms-ransomware-attack/

Five Guys Discloses Data Breach Affecting Employee PII
American fast food restaurant chain Five Guys has announced a data breach in a recent letter to customers from COO Sam Chamberlain. According to the letter, the security incident occurred in September 2022 and exposed sensitive customer data by an unauthorized party who accessed a file server. Stolen data would include employee personally identifiable information (PII) such as names, social security numbers and driver's license numbers.
https://www.infosecurity-magazine.com/news/five-guys-data-breach-affect/

Scammers Strive To Support You, Technically

Since at least October of 2022 the FBI has noticed an uptick in scams related to technical support. The scammers will pretend to be a company that is offering a technical support service that now wants to refund some money to you for a past service. There are other variations of the scam, but for the most part the goal is to get your information so they can do a wire transfer that steals money from you.
https://www.sosdailynews.com/news.jspx?&articleid=450D2AA4AC11B278C17ABC537EFDA875

Hackers Threaten Healthcare Co. With Pay Ransom Or Customer Medical Data Goes Public

A "pay up or else" threat was recently leveled against a healthcare company, something every business hopes won't ever happen to them. Hackers claim they have sensitive customer health data belonging to customers of Medibank, Australia's largest healthcare insurer. Healthcare providers worldwide should pay close attention to this ransomware threat since we know it's only a matter of time before we see similar attacks here in the U.S.
https://www.sosdailynews.com/news.jspx?&articleid=D07558DFF914CCD38C05B2C49F61B0A6

More Pop-Up Ads? Yes Please! Said No One. Ever!

Those intrusive pop-up ads that slow down our browsers and bounce the content we want to read are by most accounts, insufferable. Knowing that, developers have created ad blocker extensions to help with this annoying and potentially harmful web surfing issue. One self-proclaimed ad-blocking extension, AllBlock Chromium, however, is doing the exact opposite of what it says it does and those behind it are making profits off that broken promise
https://www.sosdailynews.com/news.jspx?&articleid=366D0673FEAB9A36D9199C14607D9E49

****

Hints & Tips plus Security Awareness

7 rules to communicate the business value of IT

Showing IT's value effectively can help improve approval rates for funding requests, especially in times of financial headwinds. Communicating the business value of IT is a critical CIO responsibility, yet many CIOs struggle to do so effectively. In conversations with business leadership, CIOs will often focus on metrics around work performed, tasks accomplished or resources deployed, but such stories are not compelling for a non-technical audience.
https://www.ciodive.com/news/rules-IT-enterprise-value-gartner/640204

Beat The Scams In '23!

Beat the scammers in '23! How about that for a New Year's resolution? Yes, you can do it. In a world of uncertainties, one of the few things we can be sure of is that scams targeting consumers in 2023 will likely hit a new record. One in ten of us will fall victim in the next 12 months. Some people's lives will be changed forever through lost life savings. And the greedy scammers won't care a jot. Many people think they'd never be scammed. But time and time again, they're proved wrong. Even security experts, and at least one member of the Scambusters team, admit they've been taken for a ride. Avoiding scams depends to a large extent on commonsense and keeping a cool head. But sometimes that's easier said than done. However, following three simple rules will protect you from nearly all con tricks
https://scambusters.org/beatthescam.html

Tips to Avoid Social Media Cybercrime

We love social media these days. Facebook, Snapchat, Twitter, LinkedIn, and many others can lead to lots of sharing and fun, but also carry significant risks. This is particularly true now that cybercriminals are collating data and using it against us for targeting phishing attacks. Online social networks may seem all in

fun and harmless, but they are anything but that. Anyone participating in a social network online assumes some risk of becoming a victim of a con artist or other criminal. But this does not mean you should opt out of getting involved. It's part of our society, and in some cases an important part of doing business. Just be aware of the risks and take action to avoid being a victim of identity theft or another cybercrime.
https://www.sosdailynews.com/news.jspx?&articleid=26B1E34A7BC4C9B1D084570A5C15777B

Resurfaced Facebook Scam Promises To Help You Lose Weight Without Exercise
Many of us have likely gained the COVID-19 pounds or some weight over the past year. Scammers on Facebook are taking advantage of those of us wanting to shed the extra bacon. A scam that has actually been around for many years is resurfacing. You may have seen it forwarded to a friend's Facebook wall, or perhaps you were tagged. It purports to help you shed those cookies faster than you can fry an egg…like 20 pounds in 25 days! Yep, that is fast. It's also a scam.
https://www.sosdailynews.com/news.jspx?&articleid=5ACED212CE066D3EE04DEB7941EB6ABC

****

News & Views

Why Do User Permissions Matter for SaaS Security?
Earlier this year, threat actors infiltrated Mailchimp, the popular SaaS email marketing platform. They viewed over 300 Mailchimp customer accounts and exported audience data from 102 of them. The breach was preceded by a successful phishing attempt and led to malicious attacks against Mailchimp's customers' end users.
https://thehackernews.com/2023/01/why-do-user-permissions-matter-for-saas.html

****

"Ctrl -F" for The Board

The ransomware problem isn't going away, and these grim figures prove it
Up to 1,981 schools, 290 hospitals, 105 local governments and 44 universities and colleges were hit with ransomware in the US alone during 2022, demonstrating how ransomware attacks remain a significant cyber threat to the public sector and civil society.
https://www.zdnet.com/article/these-grim-figures-show-that-the-ransomware-problem-isnt-going-away/

Questions
Contact FIPCO's Rob Foxx at 800-722-3498 ext. 249 or email FIPCO IT Services for more information.

"Make Security Part of You and Your Institution's DNA!"

Threat Intelligence Newsletter: January 19, 2023

FIPCO®
IT Audit
Round Table
Discussions

Upcoming Threat Intelligence Peer Group Discussions
None available at the current time

****

Alerts & Warnings

Ransomware attack exposes California transit giant's sensitive data
Vice Society, a prolific ransomware group, leaked data it claims to have stolen from San Francisco's Bay Area Rapid Transit. A ransomware attack against San Francisco's Bay Area Rapid Transit exposed highly sensitive and personal data after a threat group leaked the records Friday. The nation's fifth-largest transit system by ridership, and largest in California, remains operational.
https://www.cybersecuritydive.com/news/ransomware-attack-exposes-california-transit-giants-sensitive-data/640121/

Cybersecurity and the Myth of Quiet Quitting
People are working harder than ever, but they're not happy about it — and the insider threat is all too real. Quiet quitting, as the media reports it, is a myth.
https://www.darkreading.com/vulnerabilities-threats/cybersecurity-and-the-myth-of-quiet-quitting

Malware Comes Standard With This Android TV Box on Amazon
The bargain T95 Android TV device was delivered with preinstalled malware, adding to a trend of Droid devices coming out-of-the-box tainted. At $39.99 with a $3 coupon option for Amazon Prime members, the T95 Android 10.0 TV box might seem like a good value. But when an unsuspecting but cybersecurity-savvy customer ordered one up, he said it came "festooned" with malware — no extra charge.
https://www.darkreading.com/threat-intelligence/malware-standard-android-tv-box-amazon

Illegal Crypto Transaction Volumes Hit All-Time High
Over $20bn worth of illegal transactions were carried out using cryptocurrency last year, a record high that's likely to grow as more illicit activity is uncovered, according to Chainalysis. The blockchain analysis firm helps police, government agencies and other entities to trace cryptocurrency transactions for compliance, law enforcement and other goals.
https://www.infosecurity-magazine.com/news/illegal-crypto-transaction-volumes/

Fortinet says hackers exploited critical vulnerability to infect VPN customers
Remote code-execution bug was exploited to backdoor vulnerable servers. An unknown threat actor abused a critical vulnerability in Fortinet's FortiOS SSL-VPN to infect government and government-related organizations with advanced custom-made malware, the company said in an autopsy report on Wednesday.
https://arstechnica.com/information-technology/2023/01/fortinet-says-hackers-exploited-critical-vulnerability-to-infect-vpn-customers

Cisco Warns of Critical Vulnerability in EoL Small Business Routers
Cisco this week announced that no patches will be released for a critical-severity vulnerability impacting small business RV016, RV042, RV042G, and RV082 routers, which have reached end of life (EoL).
https://www.securityweek.com/cisco-warns-critical-vulnerability-eol-small-business-routers

Text Scams Impersonating Financial Institutions
Jim Stickley gives a quick warning about malicious text messages that appear to come from your financial institution. ~4 minutes
https://www.sosdailynews.com/news.jspx?&articleid=B00963CC8758A56BD65F9C07F7DFA7A5

TikTok Challenge Encourages Mischievous Behavior With Malicious Malware
To say that TikTok is a global phenomenon is to drastically understate the popularity of this social media platform. With over 1 billion users spread across 154 countries, it is highly unlikely that cybercriminals would ignore the potentially fertile ground of TikTok for long; and this has proven to be the case.
https://www.sosdailynews.com/news.jspx?&articleid=2D56E784B5362ABDB5C6F9234C8E3DC9

Facebook Is Spying On You
Facebook is monitoring you through third party mobile apps and on other organizations websites, even when you're not logged into Facebook. In this video I will show what they are up to and walk you through how to get your privacy back. If this helps you, be sure to share it.
https://www.sosdailynews.com/news.jspx?&articleid=62FD3D4064D38C09C49C49F2F3DA48C2

****

Hints & Tips plus Security Awareness

A ransomware negotiator shares 3 tips for victim organizations
This is no time for knee-jerk reactions. "Take a deep breath and slow things down," said Drew Schmitt, principal threat intelligence analyst at GuidePoint Security. Part of the role of a ransomware negotiator is to bring calm to a situation that can feel like a waking nightmare for the victim organization.
https://www.cybersecuritydive.com/news/ransomware-negotiator-three-tips/640609/

Tips to Avoid Social Media Cybercrime
We love social media these days. Facebook, Snapchat, Twitter, LinkedIn, and many others can lead to lots of sharing and fun, but also carry significant risks. This is particularly true now that cybercriminals are collating data and using it against us for targeting phishing attacks. Online social networks may seem all in fun and harmless, but they are anything but that. Anyone participating in a social network online assumes some risk of becoming a victim of a con artist or other criminal. But this does not mean you should opt out of getting involved. It's part of our society, and in some cases an important part of doing business. Just be aware of the risks and take action to avoid being a victim of identity theft or another cybercrime.
https://www.sosdailynews.com/news.jspx?&articleid=26B1E34A7BC4C9B1D084570A5C15777B

****

News & Views

5 Predictions For Banking And Fintech In 2023
It's the beginning of a new year, which means it's predictions/trends/forecast season for industry pundits.
https://www.forbes.com/sites/ronshevlin/2023/01/09/5-predictions-for-banking-and-fintech-in-2023

'Too-big-to-manage' banks could be broken up, OCC says
Banks whose size inhibits their abilities to address internal weaknesses and comply with regulations may need to be broken up, the acting head of the Office of the Comptroller of the Currency said Tuesday. The size and complexity of such "too-big-to-manage" banks can cause risk management breakdowns and negative surprises to occur too frequently, Acting Comptroller Michael Hsu said at a Brookings Institution event. "[E]ffective management is not infinitely scalable," he said.
https://www.bankingdive.com/news/occ-too-big-to-manage-banks-could-be-broken-up-CFPB-Michael-Hsu/640633/

Cyber, business interruption remain top global corporate risks
Potential cyber incidents and business interruption remained the two leading worldwide corporate risk concerns for the second year in a row, according to a report published Tuesday by Allianz Group's corporate insurance unit, Allianz Global Corporate & Specialty.
https://www.cybersecuritydive.com/news/cyber-business-interruption-top-business-risks/640616/

The cybersecurity talent shortage: The outlook for 2023
The available potential workforce isn't keeping pace with demand, and experts blame a lack of interest from young people entering the job market. The global cybersecurity workforce grew to encompass 4.7 million people, reaching its highest-ever levels, according to (ISC)2 2022 workforce study. That's the encouraging news.
https://www.ciodive.com/news/cybersecurity-talent-gap-worker-shortage/640396

Russia's Ukraine War Drives 62% Slump in Stolen Cards
The Russian invasion of Ukraine in early 2022 appears to have led to a double-digit decrease in stolen payment card records published to the dark web, according to Recorded Future.
The firm's Insikt Group division analyzed detailed threat intelligence gleaned from the cybercrime underground to compile its Annual Payment Fraud Report: 2022.
https://www.infosecurity-magazine.com/news/russias-ukraine-62-slump-stolen/

****

"Ctrl -F" for The Board

Tech priorities out of sync with security needs, CISA director says
As long as priorities and incentives are misaligned, security and safety needs will remain unmet. "We can't just let technology off the hook," Jen Easterly said. The consistent increase in annual cybercrime damages is not sustainable, Jen Easterly, director of the Cybersecurity and Infrastructure Security Agency said Thursday at CES in Las Vegas.
https://www.cybersecuritydive.com/news/tech-priorities-CISA-CES/639939

Questions
Contact FIPCO's Rob Foxx at 800-722-3498 ext. 249 or email FIPCO IT Services for more information.

"Make Security Part of You and Your Institution's DNA!"

Threat Intelligence Newsletter: January 27, 2023

FIPCO®
IT Audit
Round Table
Discussions

Upcoming Threat Intelligence Peer Group Discussions
None available at the current time

****

Alerts & Warnings

PayPal warns 35,000 customers of exposure following credential stuffing attack
Nearly 35,000 PayPal accounts were accessed via a credential stuffing attack, exposing personal information including names, addresses, social security numbers, tax identification numbers, and dates of birth, the company said Wednesday.
https://www.cybersecuritydive.com/news/paypal-credential-stuffing-attack/640804

T-Mobile breached again, 37M customer accounts exposed
This incident marks the latest in a series of data breaches, the worst of which occurred in August 2021 and exposed the personal data of at least 76.6 million people. T-Mobile on Thursday said a threat actor accessed personal data on about 37 million current customers in an intrusion that went undetected since late November.
https://www.cybersecuritydive.com/news/tmobile-breach-customer-compromise/640812

Threat actors lure phishing victims with phony salary bumps, bonuses
Multiple campaigns underscore threat actors' ability to shift tactics and target employees by exploiting current events and themes. Multiple threat research firms have uncovered a spate of phishing campaigns targeting professionals with details about salary increases, benefits changes and updated employee handbooks.
https://www.cybersecuritydive.com/news/phishing-lures-phony-hr-salary/640698

Experian Glitch Exposing Credit Files Lasted 47 Days
On Dec. 23, 2022, KrebsOnSecurity alerted big-three consumer credit reporting bureau Experian that identity thieves had worked out how to bypass its security and access any consumer's full credit report — armed with nothing more than a person's name, address, date of birth, and Social Security number. Experian fixed the glitch but remained silent about the incident for a month. This week, however, Experian

acknowledged that the security failure persisted for nearly seven weeks, between Nov. 9, 2022, and Dec. 26, 2022.
https://krebsonsecurity.com/2023/01/experian-glitch-exposing-credit-files-lasted-47-days/

Zendesk Hacked After Employees Fall for Phishing Attack
Customer service solutions provider Zendesk has suffered a data breach that resulted from employee account credentials getting phished by hackers. Cryptocurrency trading and portfolio management company Coinigy revealed last week that it had been informed by Zendesk about a cybersecurity incident.
https://www.securityweek.com/zendesk-hacked-after-employees-fall-for-phishing-attack/

WhatsApp Hit with €5.5 Million Fine for Violating Data Protection Laws
The Irish Data Protection Commission (DPC) on Thursday imposed fresh fines of €5.5 million against Meta's WhatsApp for violating data protection laws when processing users' personal information. At the heart of the ruling is an update to the messaging platform's Terms of Service that was imposed in the days leading to the enforcement of the General Data Protection Regulation (GDPR) in May 2018, requiring that users agree to the revised terms in order to continue using the service or risk losing access.
https://thehackernews.com/2023/01/whatsapp-hit-with-55-million-fine-for.html

Protecting Against Malicious Use of Remote Monitoring and Management Software
Today, the Cybersecurity and Infrastructure Security Agency (CISA), the National Security Agency (NSA), and the Multi-State Information Sharing and Analysis Center (MS-ISAC) released joint Cybersecurity Advisory (CSA) Protecting Against Malicious Use of Remote Monitoring and Management Software.
https://www.cisa.gov/uscert/ncas/alerts/aa23-025a

****

Hints & Tips plus Security Awareness

Ransomware Attacks: Strategies for Prevention and Recovery
As organizations remain susceptible to ransomware attacks, you can head into the new year with the latest research on strategies for defending against attacks as well as how to recover after an attack. True ransomware preparedness requires getting to know your security posture and then making it stronger, as well as creating a proactive action plan for the possibility that even these improved defenses could be breached. Webinar On Demand: 66min
https://www.brighttalk.com/webcast/5052/567236

3 Lessons Learned in Vulnerability Management
In 2022, multiple high-profile vulnerabilities like Log4j and OpenSSL provided important takeaways for future public reporting. As we pass the first anniversary of the Log4j vulnerability disclosure, it's a timely reminder that when a vulnerability is serious, it deserves our utmost attention. Organizations taking vulnerability disclosure more seriously is a net positive for the industry, especially because patching is so vital for basic cyber hygiene and accountability.
https://www.darkreading.com/edge-articles/3-lessons-learned-in-vulnerability-management

(UPDATE) CISA WARNS OF CRITICAL 'ManageEngine' RCE BUG EXPLOITED IN ATTACKS
Over 19,000 End-of-Life Cisco Routers Exposed to RCE Attacks The Cybersecurity and Infrastructure Security Agency (CISA) has added a remote code execution (RCE) affecting most Zoho ManageEngine products to its catalog of bugs known to be exploited in the wild. This security flaw is tracked as CVE-2022-47966 and was patched in several waves starting on October 27th, 2022. Unauthenticated threat actors can exploit it if the SAML-based single-sign-on (SSO) is or was enabled at least once before the attack to execute arbitrary code. https://nvd.nist.gov/vuln/detail/CVE-2022-47966

****

News & Views

Cyber Thieves Are Going After Retirement Accounts
Data security has been increased for tax returns, credit cards, and other traditional targets of cyber thieves. Now, the online thieves are making sophisticated attacks on employer retirement plans and the accounts in the plans. Data security at retirement plans varies, and the security can be breached several different ways. The cyber thieves probe to find the most vulnerable point of each plan.
https://www.forbes.com/sites/bobcarlson/2023/01/20/cyber-thieves-are-going-after-retirement-accounts

Why Analyzing Past Incidents Helps Teams More Than Usual Security Metrics
Traditional metrics don't reflect real-world severity. Instead, analyzing previously reported incidents can help teams decide how to react, a new report says. Accepted metrics for measuring the severity of security incidents, like mean time to repair (MTTR), may not be as reliable as previously thought and are not providing IT security teams with the correct information, according to Verica's latest "Open Incident Database Report" (VOID).
https://www.darkreading.com/edge-articles/why-analyzing-past-incidents-helps-teams-more-than-usual-security-metrics

How Deepfake Videos Could Land You In Trouble
One of the big challenges for us ordinary mortals in 2023 is to be able to tell deepfake videos from the real thing. Over the past year, the artificial intelligence behind deepfakes - digitally altered videos of a person usually saying something controversial - has come on by leaps and bounds. This is particularly bad news in a year running up to the 2024 presidential election. We can expect to see all manner of deep fakes pretending to be speeches delivered by political candidates.
https://scambusters.org/deepfake3.html

NIST - RELEASES POTENTIAL UPDATES TO ITS CYBERSECURITY FRAMEWORK
The National Institute of Standards and Technology wants to expand the cybersecurity guidance's scope and foster more international collaboration, among other proposed changes. The National Institute of Standards and Technology announced its intent to make new revisions to its Cybersecurity Framework document, with an emphasis on cyberdefense inclusivity across all economic sectors.
https://www.nist.gov/system/files/documents/2023/01/19/CSF_2.0_Concept_Paper_01-18-23.pdf

****

"Ctrl -F" for The Board

SaaS Security Posture Management (SSPM) as a Layer in Your Identity Fabric
The move to SaaS and other cloud tools has put an emphasis on Identity & Access Management (IAM). After all, user identity is one of the only barriers standing between sensitive corporate data and any unauthorized access. The tools used to define IAM make up its identity fabric. The stronger the fabric, the more resistant identities are to pressure from threat actors. However, those pressures are only increasing. Decentralized IT, evolving threats, and zero-trust tools are pushing many IAM tools to their limits. Note: If you are seeking an SSPM solution contact Rob rfoxx@fipco.com for more information.
https://thehackernews.com/2023/01/saas-security-posture-management-sspm.html

Questions
Contact FIPCO's Rob Foxx at 800-722-3498 ext. 249 or email FIPCO IT Services for more information.

"Make Security Part of You and Your Institution's DNA!"

Threat Intelligence Newsletter: February 3, 2023

FIPCO®
IT Audit
Round Table
Discussions

IfUpcoming Threat Intelligence Peer Group Discussions
None available at the current time

****

Alerts & Warnings

Social Security payments are going up. Watch for scammers taking advantage
Each year, the Social Security Administration (SSA) approves a cost-of-living adjustment (COLA) for recipients of Social Security benefits and Supplementary Security Income (SSI). Due to inflation, payments will increase by 8.7% this year. It's a significant increase – the highest COLA approved in more than 40 years – and scammers are taking advantage. If you or a loved one receive Social Security benefits, stay alert to the signs of a scam.
https://www.bbb.org/article/scams/28089-bbb-scam-alert-how-social-security-recipients-can-stay-alert-to-cost-of-living-adjustment-scams

Hackers Take Over Robinhood Twitter Account To Promote Scam
The scammers used the account to promote a fake token and NFT sale to over a million followers. Cybercriminals hacked the Twitter account of the Robinhood exchange on Wednesday. In a now-deleted tweet, the hacked account was used to promote a scam offering crypto tokens and NFTs on the Binance Smart Chain through the PancakeSwap decentralized exchange.
https://decrypt.co/119985/hackers-take-over-robinhood-twitter-account-to-promote-scam

Scammers Storm Into Extreme Weather Regions
Fierce storms, floods, and extreme cold across many parts of the US in recent weeks have prompted a new rash of weather scams. Several federal and local government agencies have issued warnings that con artists are on the prowl, trying to take advantage of people whose safety, homes, and power supplies were affected in the storms, which ran through much of December and January in various parts of the country. Even those not affected by storms can be caught out with freeze-related plumbing and heating issues as fraudsters pose as utility company officials and contractors, ready to take your money and run.
https://scambusters.org/weather.html

Google Ads Now Hijacked to Target Password Manager Users
A new malvertising campaign has surfaced that makes use of Google Ads to target users looking for password managers. Cybercriminals have increasingly been abusing the Google Ads platform to trick unsuspecting users into clicking on fake websites that spread malware. Earlier, the FBI had warned about the explosion of such attacks that impersonated websites involved in finances and duped users into sharing their login credentials and financial information.
https://cyware.com/news/google-ads-now-hijacked-to-target-password-manager-users-977b9ef2

SOVA Banking Trojan Infects Android Mobile Devices AND Can't Be Removed
There is a newly improved mobile banking trojan called SOVA that is leaving a path of destruction for those using Android mobile devices. Last year, SOVA trojan was found operating in the U.S. and several other countries and is actively expanding its geo-locations. This year, SOVA malware creators added new and improved tools and versions to its arsenal, making it able to target over 200 Android mobile apps, crypto exchanges, and e-wallets.
https://www.sosdailynews.com/news.jspx?&articleid=8011FBA03FC6DDE42F86640F87CA4ABE

Account Takeover Attacks Target 24 Million US Families. Is Yours Safe?
With cybercrime as pervasive as it is today, family members in the U.S. may find their social media, finance, and other accounts have been overtaken by cybercriminals. Research shows ATOs (account takeovers) are happening at an alarming rate, with data from SEON showing nearly 24 million families falling prey to these attacks last year alone.
https://www.sosdailynews.com/news.jspx?&articleid=EFBB57A7CAE539F9C4CE7F6672FEE3D2

Google Fi says hackers accessed customers' information
In an email sent to customers on Monday, obtained by TechCrunch, Google said that the primary network provider for Google Fi recently informed the company that there had been suspicious activity relating to a third-party support system containing a "limited amount" of Google Fi customer data.
https://techcrunch.com/2023/01/31/google-fi-customer-data-breach/

VMware vRealize Log Insight VMSA-2023-0001 IOCs
The recent VMware VMSA describes four new CVEs affecting VMware vRealize Log Insight. Three of these CVEs can be combined to give an attacker remote code execution as root. This vulnerability is exploitable in the default configuration for VMware vRealize Log Insight.
https://www.horizon3.ai/vmware-vrealize-cve-2022-31706-iocs/

****

Hints & Tips plus Security Awareness

Explore CISA's 37 steps to minimum cybersecurity
The agency placed a premium on low cost, high impact security efforts, which account for more than 40% of the goals. The Cybersecurity and Infrastructure Security Agency released its long-awaited, cross sector cybersecurity performance goals Thursday, in a bid to raise the security baselines. Far from esoteric, the efforts listed are meant to serve as a broadly digestible roadmap to minimum operational security.
https://www.cybersecuritydive.com/news/cisa-cpg-cybersecurity-performance-goals-critical-infrastructure/635224

Ransomware Attacks…Where's The Silver Bullet?
"This is a ransomware attack..." When these words pop-up on computer screens all over an organization, it stops victims in their tracks – but by then it's too late. Some common targets of these coldhearted ransomware crimes include hospitals, education, public transit, banking, government agencies, corporations, and yes indeed, individuals. To date, a silver bullet for preventing these devastating and dangerous ransomware attacks has yet to arrive.
https://www.sosdailynews.com/news.jspx?&articleid=AD5BEEA51C4B5E2836909ADE5EF3C921

Scheming Scam Alert! These Top Scams Are Heading Your Way
This year's top scams are bigger and better than ever. Phishing scams hit new heights during the pandemic and show no signs of slowing down. The FBI's Internet Crime Complaint Center (IC3) received over 2.1 million complaints from scam victims last year. The most common reports were about imposter scams, but that's just the tip of the iceberg. The FTC finds that last year, the financial cost of these fraudulent scams was more than $3.3 billion. Most scams are preventable, and awareness is the first step to stopping them. Below are some of the top scam attacks to look out for.
https://www.sosdailynews.com/news.jspx?&articleid=B6545CF9660AB8755DC9199E21A3AFB6

****

News & Views

Cybercrime To Cost The World 8 Trillion Annually In 2023
Cybercrime is predicted to cost the world $8 trillion USD in 2023, according to Cybersecurity Ventures. If it were measured as a country, then cybercrime would be the world's third largest economy after the U.S. and China. Press Release. We expect global cybercrime damage costs to grow by 15 percent per year over the next three years, reaching $10.5 trillion USD annually by 2025, up from $3 trillion USD in 2015.
https://cybersecurityventures.com/cybercrime-to-cost-the-world-8-trillion-annually-in-2023/

Cautious but confident, tech talent won't stop job hopping
Workforce reductions in big tech have tempered the Great Resignation, but IT workers are still testing the job market. In the first 24 days of 2023, more than 170 tech companies laid off more than 56,000 workers, data from Layoffs.fyi shows. The most high-profile of these, layoffs from tech giants Amazon, Google and Microsoft, impacted tens of thousands of workers.
https://www.ciodive.com/news/IT-talent-job-hopping-layoffs/641128

Cryptocurrency might be the greatest Ponzi scheme of all time
The seemingly limitless innovations that are springing out of information technology have created enormous opportunities for all kinds of predatory behavior uninhibited by social regulation. Cryptocurrencies are one of the leading contestants in this competition. Crypto is a Ponzi scheme. It's the IT version of what Bernie Madoff did in a mutual fund fraud in New York City in the 1980s and '90s, which was the greatest Ponzi scheme of all time − until now.
https://www.cincinnati.com/story/opinion/contributors/2023/01/29/opinion-cryptocurrency-might-be-the-greatest-ponzi-scheme-of-all-time/69836392007/

Why You Should Avoid Investing In Cryptocurrency In Retirement
Many people feel that investing in cryptocurrency is a way to increase their retirement savings, but it is not without risks. Cryptocurrency is a highly volatile asset class with prices that can fluctuate wildly in a short

amount of time. This makes it a risky choice for those who are retired or nearing retirement and need to protect their savings.
https://www.forbes.com/sites/andrewrosen/2023/01/26/why-you-should-avoid-investing-in-cryptocurrency-in-retirement

You Don't Know Where Your Secrets Are
Do you know where your secrets are? If not, I can tell you: you are not alone. Hundreds of CISOs, CSOs, and security leaders, whether from small or large companies, do not know either. No matter the organization's size, the certifications, tools, people, and processes: secrets are not visible in 99% of cases. It might sound ridiculous at first: keeping secrets is an obvious first thought when thinking about security in the development lifecycle. Whether in the cloud or on-premise, you know that your secrets are safely stored behind hard gates that few people can access. It is not just a matter of common sense since it's also an essential compliance requirement for security audits and certifications.
https://thehackernews.com/2023/01/you-dont-know-where-your-secrets-are.html

****

"Ctrl -F" for The Board

Top tech talent rewarded with remote work
Salary disparities between remote jobs and the industry average reflect the bargaining power of top tech talent. Web developer, software engineering and data science positions listed as remote also had the highest salaries.
https://www.ciodive.com/news/tech-workforce-remote-software-engineer-developer-data-science/641123

Questions
Contact FIPCO’s Rob Foxx at 800-722-3498 ext. 249 or email FIPCO IT Services for more information.

"Make Security Part of You and Your Institution's DNA!"

Threat Intelligence Newsletter: February 9, 2023

FIPCO®
IT Audit
Round Table
Discussions

Upcoming Threat Intelligence Peer Group Discussions
None available at the current time

****

Alerts & Warnings

New Facebook phishing scam scares page owners into sharing their password
The latest social media scam is yet another phishing scheme designed to scare Facebook users into sharing their login credentials. Here is how you can spot the scam and protect your account from hackers.
https://www.bbb.org/article/scams/28112-bbb-scam-alert-new-facebook-phishing-scam-scares-page-owners-into-sharing-their-password

No Blocking, No Issue: The Curious Ecosystem of Financial Advisor Impersonation Scams
An increasingly common and highly effective fraud technique known as "pig butchering" uses a complex web of social engineering techniques to defraud victims. These scams rely on slowly building trust with a target–often under the guise of a financial advisor or successful investor–in order to convince targets to invest in a scam, such as a cryptocurrency "investment," in which their funds are promptly stolen and rendered nearly impossible to recover.
https://www.domaintools.com/resources/blog/no-blocking-no-issue-the-curious-ecosystem-of-financial-advisor-impersonation-scams/

Hacker finds bug that allowed anyone to bypass Facebook 2FA
A bug in a new centralized system that Meta created for users to manage their logins for Facebook and Instagram could have allowed malicious hackers to switch off an account's two-factor protections just by knowing their phone number.
https://techcrunch.com/2023/01/30/facebook-two-factor-bypass-bug/

Ransomware attack spree hits thousands of VMware servers
Cyber authorities linked the attacks, dubbed ESXiArgs, to a two-year-old VMware vulnerability. At least 2,250 machines have been compromised. A global ransomware campaign hit thousands of organizations using specific versions of VMware ESXi starting Friday, according to cyber authorities and experts.
https://www.cybersecuritydive.com/news/ransomware-spree-vmware-servers/642121/

Ransomware Attack Forces Closure of Nantucket Schools

A ransomware attack targeting schools on the island of Nantucket, Massachusetts, forced the closure Tuesday of four establishments, counting a total of roughly 1700 students. The district's superintendent Elizabeth Hallett announced the decision in an email to parents and seen by Infosecurity.
https://www.infosecurity-magazine.com/news/ransomware-attack-nantucket/

City of London on High Alert After Ransomware Attack

A suspected ransomware attack on a key supplier of trading software to the City of London this week appears to have disrupted activity in the derivatives market. Ion Cleared Derivatives released a brief statement on Tuesday saying that it experienced a "cybersecurity event" that day which affected some of its services.
https://www.infosecurity-magazine.com/news/city-of-london-high-alert/

****

Hints & Tips plus Security Awareness

Creative Hacking Underscores The Need For MFA

Attackers are getting more creative by the day. It is more important than ever before with so many bad actors out there to make all your accounts ultra-secure. That means that using some method of multifactor authentication (MFA) is in order. Case in point: Recently, there was an elaborate scheme targeting unsuspecting users that would perhaps not have been victims, had MFA been enabled.
https://www.sosdailynews.com/news.jspx?&articleid=C291E7505E06C90F3145FB917159B279

SaaS in the Real World: Who's Responsible to Secure this Data?

When SaaS applications started growing in popularity, it was unclear who was responsible for securing the data. Today, most security and IT teams understand the shared responsibility model, in which the SaaS vendor is responsible for securing the application, while the organization is responsible for securing their data.
https://thehackernews.com/2023/02/saas-in-real-world-whos-responsible-to.html

NIST ISSUES PHISHING GUIDANCE

NIST has published a report encouraging the use of phishing-resistant authenticators. According to NIST Special Publication DRAFT 800-63-B4, a phishing-resistant authenticator offers "the ability of the authentication protocol to detect and prevent disclosure of authentication secrets and valid authenticator outputs to an impostor relying party without reliance on the vigilance of the subscriber."
https://www.nist.gov/blogs/cybersecurity-insights/phishing-resistance-protecting-keys-your-kingdom

****

News & Views

Cybercrime groups offer six-figure salaries, bonuses, paid time off to attract talent on dark web

Despite the obvious risks, tech jobs with hacking groups can be alluring for those who need the money or want to do the work. Cybercrime is a booming business. So, like any other thriving market, the masterminds behind ransomware syndicates or online scam operations need workers, too. And they are not just looking for other criminal hackers. Developers, administrators, and designers are in high demand.
https://cyberscoop.com/cybercrime-groups-jobs-talent-dark-web/

98% of organizations worldwide connected to breached third-party vendors
A total of 98% of organizations worldwide have integrations with at least one third-party vendor that has been breached in the last two years, according to a report released Wednesday from SecurityScorecard and the Cyentia Institute.
https://www.cybersecuritydive.com/news/connected-breached-third-party/641857

Why do hackers target cryptocurrencies?
Cryptocurrency investors continue to be a target for cyber-attacks, Cyber Security Hub investigates why. With more than 420 million cryptocurrency users, more than 12,000 cryptocurrencies worldwide and an estimated value of US$2.2bn by 2026, the digital currency marketplace is growing rapidly. This rapid growth, however, has made it a target for cyber attackers looking to defraud victims.
https://www.cshub.com/attacks/articles/why-do-hackers-target-cryptocurrencies

****

"Ctrl -F" for The Board

Corporate boards struggle to understand cybersecurity and digital transformation
Corporate board directors are struggling to oversee the rapidly evolving threat of cyberattacks, according to a report from Diligent Institute, which specializes in corporate governance issues. They consider cyber and data security as their most challenging issue.
https://www.cybersecuritydive.com/news/corporate-boards-cybersecurity-digital-transform/642062/

Tackling the New Cyber Insurance Requirements: Can Your Organization Comply?
With cyberattacks around the world escalating rapidly, insurance companies are ramping up the requirements to qualify for a cyber insurance policy. Ransomware attacks were up 80% last year, prompting underwriters to put in place a number of new provisions designed to prevent ransomware and stem the record number of claims. Among these are a mandate to enforce multi-factor authentication (MFA) across all admin access in a network environment as well as protect all privileged accounts, specifically machine-to-machine connections known as service accounts.
https://thehackernews.com/2023/02/tackling-new-cyber-insurance.html

Questions
Contact FIPCO's Rob Foxx at 800-722-3498 ext. 249 or email FIPCO IT Services for more information.

"Make Security Part of You and Your Institution's DNA!"

Threat Intelligence Newsletter: February 20, 2023

FIPCO®
IT Audit
Round Table
Discussions

Upcoming Threat Intelligence Peer Group Discussions
None available at the current time

****

Alerts & Warnings

What's known about the ESXiArgs ransomware hitting VMware servers
An initial strain affected thousands of devices before a new variant emerged. The latest burst of attacks hit Saturday.
https://www.cybersecuritydive.com/news/esxiargs-ransomware-vmware/642833/

US Warns Critical Sectors Against North Korean Ransomware Attacks
The US Cybersecurity and Infrastructure Security Agency has released an advisory directed towards the critical infrastructure sector. The Cybersecurity Advisory (CSA) warns the entities of ongoing ransomware activity likely perpetrated by North Korean state-sponsored actors.
https://www.infosecurity-magazine.com/news/us-warns-critical-sectors-north/

Snapchat Blackmailers Targeting Children
Young people, children even, have become a favorite target for scammers on the social media network Snapchat. The main aim of the crooks is to trick these youngsters into sending explicit photos of themselves and then to blackmail them - a crime known as "sextortion." The mobile app's developers claim they have 300 million users and nearly half of them are said to be in the 15-25 years age group.
https://scambusters.org/snapchat.html

Don't Fall For It! Phishing Email Attack Warns Your Facebook Page Will Be Suspended
If an email pops-up saying your Facebook account will be suspended, pay close attention. A new scam by cyber-crooks wants to steal your login information and other PII using their clever lure. With nearly 3 billion active Facebook (FB) users, this unique approach to data theft has more than enough prospective victims, so read on to make sure you will not be one of them.
https://www.sosdailynews.com/news.jspx?&articleid=8C8F2094FDDD4DB6F041717AB20BCBE6

Romance scammers' favorite lies exposed

Romance scammers tell all sorts of lies to steal your heart and money, and reports to the FTC show those lies are working. Last year's romance scam numbers looked a lot like 2021 all over again, and it's not a pretty picture. In 2022, nearly 70,000 people reported a romance scam, and reported losses hit a staggering $1.3 billion.[1] The median reported loss: $4,400.
https://www.ftc.gov/news-events/data-visualizations/data-spotlight/2023/02/romance-scammers-favorite-lies-exposed

****

Hints & Tips plus Security Awareness

Avoiding digital romance scams

As part of ongoing efforts to combat cyber-crimes and online financial fraud, Homeland Security Investigations (HSI) launched an awareness campaign on – Valentine's Day – to educate the public on dangers associated with online romance scams and how individuals can protect themselves and loved ones.
https://www.bankersonline.com/topstory/172799

LastPass Hack: Should You Switch Password Manager?

The online security world has been rocked by the recent disclosure that password manager LastPass has had its member database compromised. Here at Scambusters, we are big fans of password managers, and at least one member of our team uses LastPass.
https://scambusters.org/lastpasshack.html

A CISOs Practical Guide to Storage and Backup Ransomware Resiliency

One thing is clear. The "business value" of data continues to grow, making it an organization's primary piece of intellectual property. From a cyber risk perspective, attacks on data are the most prominent threat to organizations. Regulators, cyber insurance firms, and auditors are paying much closer attention to the integrity, resilience, and recoverability of organization data – as well as the IT infrastructure & systems that store the data.
https://thehackernews.com/2023/02/a-cisos-practical-guide-to-storage-and.html

****

News & Views

Waller warns banks of risks in crypto assets

In a presentation at the Global Interdependence Center Conference on "Digital Money, Decentralized Finance, and the Puzzle of Crypto on Friday, Federal Reserve Board Governor Christopher J. Waller cautioned that "crypto assets are risky and many of the firms dealing them are in their infancy .... [and] declines in crypto-asset values and associated business failures have led to many investors in the crypto industry getting hurt."
https://www.bankersonline.com/topstory/172768

Banks Are Breaking Up With Crypto During Regulatory Crackdown

Banks are backing away from crypto companies, spooked by a regulatory crackdown that threatens to sever digital currencies from the real-world financial system.
https://www.wsj.com/articles/banks-are-breaking-up-with-crypto-during-regulatory-crackdown-22de1832

Ranking Multi-Factor Authentication Types

In a world where technology can change in the blink of an eye, staying safe online can be a real challenge. Security steps that work today may be exploited tomorrow, so keeping up to date has never been more important. A report by the U.S. government's Cybersecurity & Infrastructure Security Agency (CISA) gives us a closer look at multi-factor authentication (MFA) identity verification tool. Below are highlights of their "Implementing Phishing-Resistant MFA" report that we can all learn from, especially those responsible for implementing an organization's MFA practices.
https://www.sosdailynews.com/news.jspx?&articleid=83D3776561C1321CDFB6F37D9738806C

****

"Ctrl -F" for The Board

IT security budgets triple as businesses confront more cyberattacks

The cost of combating cyberthreats has soared the past five years, as median IT security budgets more than tripled to $5.3 million in 2022, compared with $1.4 million in 2018
https://www.ciodive.com/news/it-security-budgets-triple-cyberattacks/642993/

Economic volatility to exacerbate cyber risk in 2023

A broad expectation for economic headwinds and continued market volatility exacerbates risks across the cybersecurity sector, the Bipartisan Policy Center
https://www.cybersecuritydive.com/news/economic-challenges-exacerbate-cyber-risk/642679

Questions
Contact FIPCO's Rob Foxx at 800-722-3498 ext. 249 or email FIPCO IT Services for more information.

"Make Security Part of You and Your Institution's DNA!"

Threat Intelligence Newsletter: February 24, 2023

FIPCO®
IT Audit
Round Table
Discussions

Upcoming Threat Intelligence Peer Group Discussions
None available at the current time

****

Alerts & Warnings

Make sure your free COVID-19 tests are not part of a scam
Since the beginning of the COVID-19 pandemic, scammers have been capitalizing on the crisis. Even now, BBB Scam Tracker regularly receives reports about pandemic-related scams. Be on the lookout for this still common con: phishing messages about at-home COVID-19 tests.
https://www.bbb.org/article/news-releases/22395-bbb-scam-alert-want-a-covid-test-theres-a-scam-for-that?utm_source=newsletter&utm_medium=email&utm_content=full%20article%20for%20examples%20of%20this%20scam&utm_campaign=scam-alert

DDoS Attacks Becoming More Potent, Shorter in Duration
US, India and East Asia Were Top Targets in 2022, Microsoft Report Says. Tech giant Microsoft says it observed distributed denial-of-services attacks become shorter in duration in 2022 while also becoming more potent and capable of larger impact.
https://www.databreachtoday.com/ddos-attacks-becoming-more-potent-shorter-in-duration-a-21283

FBI Warns: Ransomware Victims Threatened By Attacker Phone Calls
The FBI recently released a warning about ransomware victims being threatened by phone calls from their attackers. These attack groups want their ransom demand paid and are willing to escalate their threat tactics to do it. One of the best answers for victims of such an attack is having data backup systems that restore data and entirely avoid paying a ransom.
https://www.sosdailynews.com/news.jspx?&articleid=3A58DF3B96B2F0F83149B60CB767B7C4

****

Hints & Tips plus Security Awareness

It's That Time Again: These Are The Worst Passwords Of 2022
Every year, we look forward to the lists of the past years' most ridiculously lousy passwords used by, well, those who really do not seem to care about their account security. By this point, we do not really buy that these password users truly believe they are being clever or even that they are ignorant. The Internet and online accounts have been around far too long for that, and cybersecurity breaches are even discussed on mainstream media. So, there really are no excuses for using the words on these lists. Yet, some just cannot stop themselves. While the rankings seem to change year to year, sadly, the passwords do not vary by much.
https://www.sosdailynews.com/news.jspx?&articleid=F564F337C1A4101F7618A91BD46EAB4F&

Common Signs Of Phishing To Keep In Mind When Your Inbox Overflows
With email phishing, deciphering what is real from what's fake can be a challenge. Our inboxes are stuffed with emails fighting to get our attention and get us to take some action. But how to ferret-out what is legitimate takes some cyber-smarts. Research shows email is the primary method of spreading 92% of all malwares, and the U.S. is the target of 86% of all email phishing attacks. Whether at home or at work, email phishing is relentless, but being aware of characteristics they have in common can be a powerful tool. The ability to spot those familiar traits before it's too late can be the difference between a good day and a bad nightmare.
https://www.sosdailynews.com/news.jspx?&articleid=C08D6B4174C8551EE08B498BA0646D08

Evolving Malware And The Future Landscape Of Cyberattacks
Constantly in search of new, lucrative opportunities and quick to ditch what is less profitable, hackers are always looking for new vulnerabilities to exploit. The potential for new malware and new cybercrimes is always present and new hacking trends are a part of that. Comparitech, a pro-consumer website helping users navigate technology, helps shed light on these ever-evolving threats.
https://www.sosdailynews.com/news.jspx?&articleid=51E228E1DAD014B7D81033364905A9D9

The Secret Vulnerability Finance Execs are Missing
A few years ago, a Washington-based real estate developer received a document link from First American – a financial services company in the real estate industry – relating to a deal he was working on. Everything about the document was perfectly fine and normal. The odd part, he told a reporter, was that if he changed a single digit in the URL, suddenly, he could see somebody else's document.
https://thehackernews.com/2023/02/the-secret-vulnerability-finance-execs.html

****

News & Views

How attackers are breaking into organizations
Threat actors lean heavily on phishing attacks, vulnerabilities in software and containers, and stolen credentials, according to top cyber vendor research. Threat actors are constantly on the lookout for new or more susceptible pathways to break in and gain access to an organization's data or network.
https://www.cybersecuritydive.com/news/how-attackers-break-organizations/629686/

Stressed much? It is chronic in cybersecurity
Half of security leaders will change jobs by 2025, Gartner predicts, spurred by a sector wide cycle of burnout.
https://www.cybersecuritydive.com/news/CISO-stress-burnout-security/643406

PhishPal: How PayPal Became a Hackers' Haven
In July of last year, we wrote about a new campaign where hackers are sending phishing emails and malicious invoices directly from PayPal. This is different from the plenty of attacks we have seen that spoof PayPal. This is a malicious invoice that comes directly from PayPal. And since it comes directly from PayPal, it becomes incredibly difficult not only for email security services to stop but also for end-users to respond to it accordingly.
https://www.avanan.com/blog/phishpal-how-paypal-became-a-hackers-haven

****

"Ctrl -F" for The Board

Attackers reduce complexity to catch more potential victims
Palo Alto Networks warns attackers are building economies of scale by conducting more efficient operations and complementing their skills with commercially available tools.
https://www.cybersecuritydive.com/news/attackers-reduce-complexity/643399

Questions
Contact FIPCO's Rob Foxx at 800-722-3498 ext. 249 or email FIPCO IT Services for more information.

"Make Security Part of You and Your Institution's DNA!"

Threat Intelligence Newsletter: March 3, 2023

FIPCO®
IT Audit
Round Table
Discussions

Upcoming Threat Intelligence Peer Group Discussions
None available at the current time

****

Alerts & Warnings

Chinese State Hackers Level Up Their Abilities: CrowdStrike
A Chinese law requiring mandatory disclosure to the government of vulnerability reports appears to be paying dividends for state-connected hacking. Chinese hackers with a connection to Beijing ramped up their use of zero-day vulnerabilities when attacking North American targets during 2022, says threat intelligence firm CrowdStrike.
https://www.databreachtoday.com/chinese-state-hackers-level-up-their-abilities-crowdstrike-a-21326

Crime Blotter: Hackers Fail to Honor Promises to Delete Data
Police Say Gang Extorted Millions From Victims Not Just by Stealing, But Lying Too. Cybercrime experts have long urged victims to never pay a ransom in return for any promises attackers make to delete stolen data.
https://www.databreachtoday.com/blogs/crime-blotter-hackers-fail-to-honor-promises-to-delete-data-p-3399

New HardBit 2.0 Ransomware Tactics Target Insurance Coverage
Hackers Demand Info on Victim's Cyber Insurance Policy to Negotiate Ransom Demand. A newly uncovered ransomware group is employing previously unseen extortion tactics - demanding to know the victim's cyber insurance coverage - to extort millions of dollars in ransom.
https://www.databreachtoday.com/new-hardbit-20-ransomware-tactics-target-insurance-coverage-a-21286

Don't "Lose" Your Home To Title Theft Crooks
Imagine receiving a foreclosure notice on your home. Plus, maybe demands to pay off a second mortgage and other outstanding bills. And perhaps even an eviction notice. All of this when you don't even have a

mortgage and have always paid all your bills on time. If this happens to you, it's likely you're a victim of home title theft, or home deed fraud. Someone forged your signature on the deed transfer and other legal documents and, at least at first glance, has taken ownership of your house without you knowing.
https://scambusters.org/titletheft.html

BlackLotus is the first bootkit bypassing UEFI Secure Boot on Windows 11
ESET discovered a stealthy Unified Extensible Firmware Interface (UEFI) bootkit dubbed BlackLotus that is able to bypass the Secure Boot on Windows 11.
https://securityaffairs.com/142864/malware/blacklotus-bootkit-bypass-secure-boot-win11.html

Wanted! Nighttime Bandit Steals PII Using Google Ads
Users that are searching for popular software have recently become the targets of malvertising which leverages Google Ads to install Trojan versions of Raccoon Stealer and Vidar. These malware versions are sneakily hidden within Google advertising…you know; those advertisements you see on the side of your browser window or plastered all over social media. This bandit, if clicked, will then proceed to install malware on your device.
https://www.sosdailynews.com/news.jspx?&articleid=C230E7E3DD396DC6923B486F859DFD0A

Tips To Avoid Malicious QR Codes
Jim Stickley reviews several ways you can avoid falling for a malicious QR code scam. QR codes are part of everyday life and therefore are trusted which makes them perfect to impersonate. In this video Jim covers ways you can take a couple seconds to verify the validity of the QR code before scanning. He also covers signs that a clicked QR code is malicious. 4-minute video
https://www.sosdailynews.com/news.jspx?&articleid=B66CA29A5080978005BF924DD003E400

Experts Sound Alarm Over Growing Attacks Exploiting Zoho ManageEngine Products
Multiple threat actors have been observed opportunistically weaponizing a now-patched critical security vulnerability impacting several Zoho ManageEngine products since January 20, 2023. Tracked as CVE-2022-47966 (CVSS score: 9.8), the remote code execution flaw allows a complete takeover of the susceptible systems by unauthenticated attackers.
https://thehackernews.com/2023/02/experts-sound-alarm-over-growing.html

PSA: Houzez Theme Unauthenticated Privilege Escalation Vulnerability Exploited in The Wild.
(WORDPRESS VULNERABILITY)
The Houzez theme is a premium theme sold on ThemeForest and has over 35,000 sales. It’s described as a theme specifically designed for the real estate industry. It offers easy-to-use tools that will allow you to manage your agency’s content and listings, while providing the best possible experience for your clients.
https://patchstack.com/articles/psa-houzez-theme-unauthenticated-privilege-escalation-vulnerability-exploited-in-the-wild/

****

Hints & Tips plus Security Awareness

Third-Party Providers Create Identity and Access Control Challenges for Fintech Apps
As with every other sector that has embraced digital transformation, cybercrime has become a more prominent threat in finance. According to VMware's Modern Bank Heists study, since the COVID-19 pandemic, there have been 238% more cyberattacks on companies in the financial sector, a shocking rise.
https://www.darkreading.com/edge-articles/third-party-providers-create-identity-and-access-control-challenges-for-fintech-apps

3 ways CIOs can drive business success in 2023
The CIO plays a critical role in helping companies adapt to shifting environments, writes Momentive CIO Eric Johnson.
https://www.ciodive.com/news/3-CIO-business-priorities/643054/

6 Critical Capabilities for an Application GRC Solution
Saviynt's Keri Bowman on How to Ensure Your Program Stacks Up With the Best. With application GRC more critical than ever in today's dynamic, dispersed environment, what are the critical capabilities needed in a solution? Keri Bowman of Saviynt offers six recommendations, including risk reporting and out-of-the-box rule sets and compliance management. 17 Min Recording
https://www.databreachtoday.com/6-critical-capabilities-for-application-grc-solution-a-20796

****

News & Views

Cyberthreats, Regulations Mount for Financial Industry
Nation-state adversaries, new reporting regulations, and a fast-paced threat landscape mean that financial services and technology firms need to bolster their security posture.
The cybersecurity landscape for financial institutions and finance technology (fintech) has changed dramatically in the past few years, and 2023 will likely be no different.
https://www.darkreading.com/risk/cyberthreats-regulations-mount-for-financial-industry

3 CISA principles for secure by design
The Biden administration is expected to emphasize safer development practices when it rolls out the national security strategy for cyber. Federal authorities and leading industry experts have reached a conclusion: technology customers can no longer afford to hunt down every single security flaw embedded in the applications they use.
https://www.cybersecuritydive.com/news/cisa-principles-secure-by-design/643745/

CISA director urges tech industry to take responsibility for secure products
Industry can no longer blame and shame customers who are victims of sophisticated attacks, Jen Easterly said. Cybersecurity and Infrastructure Security Agency Director Jen Easterly called for a transformative shift to put the onus on the technology industry to infuse security into their products during the design phase.
https://www.cybersecuritydive.com/news/cisa-director-tech-industry-secure-products/643642

Stressed much? It’s chronic in cybersecurity
Half of security leaders will change jobs by 2025, Gartner predicts, spurred by a sectorwide cycle of burnout. Of those, one-quarter are expected to move into entirely different roles. “Some will move workplaces, while others will take on different roles — for example, taking up creative roles or becoming an evangelist,” Deepti Gopal, director analyst at Gartner, said in an email.
https://www.ciodive.com/news/CISO-stress-burnout-security/643657/

****

"Ctrl -F" for The Board

Without governance, more software spending can create more problems

Understanding how vendors update their products can help CIOs keep track of capability gaps and avoid overlaps. Enterprise spending on software will not slow anytime soon, but without proper governance, wasted budgets will plague businesses.
https://www.ciodive.com/news/SaaS-spending-governance-AI-software/643450/

Questions
Contact FIPCO's Rob Foxx at 800-722-3498 ext. 249 or email FIPCO IT Services for more information.

"Make Security Part of You and Your Institution's DNA!"

Threat Intelligence Newsletter: March 9, 2023

FIPCO® IT Audit Round Table Discussions

Upcoming Threat Intelligence Peer Group Discussions
None available at the current time

****

Alerts & Warnings

Almost Half of Industrial Sector Computers Affected By Malware in 2022
Two out of every five (40.6%) operational technology (OT) computers used in industrial settings have been affected by malware in 2022. The data comes from a report published earlier today by security researchers at Kaspersky. The figures represent a 6% increase compared with the previous half of the year and almost 1.5 times more than in the second half of 2021.
https://www.infosecurity-magazine.com/news/half-industrial-sector-computers/

BlackLotus UEFI bootkit Can Bypass Secure Boot on Windows
Security firm ESET's cybersecurity researchers have shared their analysis of the world's first UEFI bootkit being used in the wild, which can bypass Secure Boot on fully updated UEFI systems. It can even bypass it on fully updated Windows 10 and 11 versions. https://www.hackread.com/blacklotus-uefi-bootkit-windows-secure-boot

Phishing Attack Uses UAC Bypass to Drop Remcos RAT Malware
The phishing attack commences by sending malicious emails disguised as financial files, such as invoices. The cybersecurity researchers at SentinelOne have observed a new phishing campaign in which attackers are abusing the Windows User Account Control (UAC) bypass to distribute the DBatLoader and Remcos RAT malware. The primary targets of this campaign are organizations in Eastern Europe.
https://www.hackread.com/phishing-attack-uac-bypass-remcos-rat-malware

Does Your Help Desk Know Who's Calling?
Phishing, the theft of users' credentials or sensitive data using social engineering, has been a significant threat since the early days of the internet – and continues to plague organizations today, accounting for more than 30% of all known breaches. And with the mass migration to remote working during the pandemic, hackers have ramped up their efforts to steal login credentials as they take advantage of the chaos and lack of in-person user verification.
https://thehackernews.com/2023/03/does-your-help-desk-know-whos-calling.html

PlugX Malware Being Distributed via Vulnerability Exploitation
ASEC (AhnLab Security Emergency Response Center) has recently discovered the installation of the PlugX malware through the Chinese remote-control programs Sunlogin and Awesun's remote code execution vulnerability. https://asec.ahnlab.com/en/49097/

Popular fintech apps expose valuable, exploitable secrets
92% of the most popular banking and financial services apps contain easy-to-extract secrets and vulnerabilities that can let attackers steal consumer data and finances, according to Approov.
https://www.helpnetsecurity.com/2023/03/06/financial-services-apps-vulnerabilities/

****

Hints & Tips plus Security Awareness

Top 5 Cryptocurrency Scams (And How To Avoid Them)
Cryptocurrency has been making headlines in recent years as investors seek to capitalise on the potential rewards offered by digital currencies. However, with the rise in the popularity of cryptocurrencies, there has also been a significant increase in scams targeting unsuspecting Australian investors. Shockingly, data from Scamwatch has revealed that Australians lost over $205 million to scams between 1 January and 1 May 2022, representing a staggering 166% increase compared to the same period last year.
https://www.forbes.com/advisor/au/investing/cryptocurrency/crypto-scams-to-watch/

Are You Getting Smished? How To Tell And How To Avoid It
It doesn't take much to be a smishing victim when just a text message does the trick. A member of the email phishing and voice (vishing) family of criminal scams, replying to a smishing text can be all that is needed to begin a successful scam. Knowing how smishing works and the tell-tale signs of these scams can help keep you from being the next smishing victim.
https://www.sosdailynews.com/news.jspx?&articleid=DA7BE4551A24F298580BBDDB4794AA06

****

News & Views

The US cyber strategy is out. Now, officials just have to implement it
Industry stakeholders signal a willingness to discuss further steps, while congressional leaders hint additional action may be on the table. The Biden administration plans to forge ahead with the hard work of implementing the ambitious goals of the national cyber strategy, which aims to shift much of the responsibility for developing a more resilient national infrastructure onto the technology industry.
https://www.cybersecuritydive.com/news/national-cyber-strategy-implement/644101

US Official Reproaches Industry for Bad Cybersecurity
CISA Director Says Programming Language Swap Will End Memory Safety Vulnerabilities. A top U.S. government official urged industry to become more conscientious over cybersecurity by preventing vulnerabilities from accumulating before products ship.
https://www.govinfosecurity.com/us-official-reproaches-industry-for-bad-cybersecurity-a-21320

****

"Ctrl -F" for The Board

Questions : Contact FIPCO's Rob Foxx at 800-722-3498 ext. 249 or email FIPCO IT Services for more information.

"Make Security Part of You and Your Institution's DNA!"

Threat Intelligence Newsletter: March 17, 2023

FIPCO®
IT Audit
Round Table
Discussions

Upcoming Threat Intelligence Peer Group Discussions
None available at the current time

****

Alerts & Warnings

Outlook zero day linked to critical infrastructure attacks
Researchers are warning that state-linked and financially motivated threat actors may try to exploit a critical zero-day vulnerability in Microsoft Outlook to launch new attacks against unpatched systems.
https://www.cybersecuritydive.com/news/zero-day-vulnerability-outlook-critical-infrastructure/645196

Bank failure panic fuels moment of opportunity for threat actors
As regulators step in to operate Silicon Valley and Signature banks, threat hunters and security executives warned organizations to look out for malicious activity.
https://www.bankingdive.com/news/bank-failure-panic-cybersecurity-threats-silicon-valley-signature/644964

Threat actors lure phishing victims with phony salary bumps, bonuses
Multiple campaigns underscore threat actors' ability to shift tactics and target employees by exploiting current events and themes.
https://www.cybersecuritydive.com/news/phishing-lures-phony-hr-salary/640698

FBI Warns About Cryptocurrency Theft Scams Using Play-to-Earn Games
The FBI has issued a public service announcement (PSA) warning on the utilization of play-to-earn games as part of a scheme to defraud users of funds stored in the form of cryptocurrency. Criminals are introducing victims to this kind of game and then use malware to extract the funds from cryptocurrency wallets linked to the game, according to the bureau.
https://news.bitcoin.com/fbi-warns-about-cryptocurrency-theft-scams-using-play-to-earn-games/

Three Big Internet Service Scams That Could Cost You Dearly
Who wants a cheaper internet service? Everyone, right? And faster, yes? And safer? You get the picture. And now, with the launch of new services to access the web - like 5G cellular and satellite networks, with

more to come - maybe our wishes will come true. Increased competition among internet service providers (ISPs) should hopefully drive down prices. But not yet. Unless you listen to the scammers.
https://scambusters.org/internetservice.html

When Partial Protection is Zero Protection: The MFA Blind Spots No One Talks About
Multi-factor Authentication (MFA) has long ago become a standard security practice. With a wide consensus on its ability to fend off more than 99% percent of account takeover attacks, it is no wonder why security architects regard it as a must-have in their environments. However, what seems to be less known are the inherent coverage limitations of traditional MFA solutions. While compatible with RDP connection and local desktop logins, they offer no protection to remote command line access tools like PsExec, Remote PowerShell and their likes.
https://thehackernews.com/2023/03/when-partial-protection-is-zero.html

****

Hints & Tips plus Security Awareness

6 reasons why your anti-phishing strategy isn't working
Phishing is a successful scam that is likely here to stay — and only get more effective. From over-reliance on technology to confusing and counterproductive training, here are six reasons why your anti-phishing strategy might be failing.
https://www.csoonline.com/article/3690511/6-reasons-why-your-anti-phishing-strategy-isn-t-working.html

Know When It's Time To Hang-Up. Don't Fall Victim To These New Phone Scams
Just recently, it was discovered three new phone scams are making the rounds. These scams play on our fears (a scammer favorite), they are tough to spot, and they are after your money. It is always smart to know how they work and when it is time to hang up. Looking at these scams can help save you and those you know from falling victim to them. The following statistics help show the financial severity of phone scams, and who's more likely to fall for them.
https://www.sosdailynews.com/news.jspx?&articleid=8AC99819BE10E822597FED02CA5B6796

How to Apply NIST Principles to SaaS in 2023
The National Institute of Standards and Technology (NIST) is one of the standard-bearers in global cybersecurity. The U.S.-based institute's cybersecurity framework helps organizations of all sizes understand, manage, and reduce their cyber-risk levels and better protect their data. Its importance in the fight against cyberattacks cannot be overstated.
https://thehackernews.com/2023/03/how-to-apply-nist-principles-to-saas-in.html

****

News & Views

Ransomware hit critical infrastructure hard in 2022, FBI says
More than one-third of ransomware attacks reported to the FBI last year impacted organizations in a critical infrastructure sector, according to the FBI Internet Crime Complaint Center's annual report released Friday.
https://www.cybersecuritydive.com/news/ransomware-critical-infrastructure-2022/645068

CISA Creates New Ransomware Vulnerability Warning Program
The US Cybersecurity and Infrastructure Security Agency (CISA) announced on Monday the creation of a new Ransomware Vulnerability Warning Pilot (RVWP) program. Stemming from the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA) and coordinated by the Joint Ransomware Task Force (JRTF), the RVWP will see CISA assess flaws commonly associated with known ransomware exploitation.
https://www.infosecurity-magazine.com/news/cisa-creates-ransomware-warning/

FBI says $10 billion lost to online fraud in 2022 as crypto investment scams surged
More than $10 billion in losses from online scams were reported to the FBI in 2022, the highest annual loss in the last five years, according to a new report from the bureau. The more than $3 billion jump in reports of online fraud from 2021 to 2022 was driven by a near-tripling in reports of cryptocurrency investment fraud, the FBI said in its annual Internet Crime Report.
https://edition.cnn.com/2023/03/13/politics/fbi-online-fraud-report/index.html

****

"Ctrl -F" for The Board

OnDemand Now: You Don't Know Your Environment - and IT Doesn't Either
As companies have gone through a digital transformation, increased adoption of cloud and Internet of Things (IoT), a growing remote workforce, and a technology talent shortage have led to an exponential rise in organizations' attack surface. This expansion makes it harder for security teams to correlate externally visible and internally managed assets and govern compromises that occur because of undiscovered, unmanaged, or poorly managed IT assets. 45 Min Webinar On demand
https://www.databreachtoday.com/webinars/ondemand-now-you-dont-know-your-environment-doesnt-either-w-4627

High-Level Execs Prime Targets For Whaling Attacks
Why settle for minnows when whales make much bigger, better targets? That is a question hackers might ask themselves when determining their next victim. With no shortage of information available online about C-Suite and other high-level executives, they make lucrative email phishing targets. These execs are known as “whales” and bad actors love reeling them in because it pays big time.
https://www.sosdailynews.com/news.jspx?&articleid=198C395B7C5EC6F71442850323D462C3

Questions
Contact FIPCO’s Rob Foxx at 800-722-3498 ext. 249 or email FIPCO IT Services for more information.

"Make Security Part of You and Your Institution's DNA!"

Threat Intelligence Newsletter: March 24, 2023

FIPCO® IT Audit Round Table Discussions

Upcoming Threat Intelligence Peer Group Discussions
None available at the current time

****

Alerts & Warnings

IRS warns of scammers offering “help”
WASHINGTON — The Internal Revenue Service today warned taxpayers to watch out for scammers who try to sell or offer help setting up an Online Account on IRS.gov that puts their tax and financial information at risk of identity theft. The IRS Online Account provides valuable tax information for people. But this information in the wrong hands can provide important information to help an identity thief try to submit a fraudulent tax return in the person's name in hopes of getting a big refund. People should watch out for these scam artists offering to help set up these accounts because these are identity theft attempts to run off with the taxpayer's personal or financial information.
https://www.irs.gov/newsroom/dirty-dozen-irs-warns-of-scammers-offering-help-to-set-up-an-online-account-creates-identity-theft-risk-for-honest-taxpayers

Phishing Scams Exploit Pricey Auto-Subscription Fears
With email among the top productivity tools in our everyday lives, we know cybercriminals have adopted it for their benefit, too. And now, according to an alert by the National Security Agency (NSA) and Cybersecurity and Infrastructure Security Agency (CISA), there is a new and highly lucrative email phishing campaign making the rounds.
https://www.sosdailynews.com/news.jspx?&articleid=3DE673858DA8096C217AE3B808D3C8AB

MacKeeper Utility Infects 50% Of Macs With Malware
There is something a bit rotten about a popular Apple utility software suite called MacKeeper. Since its release in 2010, the all-in-one security and optimization utility has had a troubled past. But it is what MacKeeper allows that now has users concerned: It accounts for nearly 50% of all MacOS infections due to

hacker intervention using malware. Cybercriminals love using popular programs to install malware, and it's clear that MacKeeper is one of them.
https://www.sosdailynews.com/index2.jspx?/news/2023/02/mackeeperutilityinfects50-of-macs-with-malware

Google Uncovers 18 Severe Security Vulnerabilities in Samsung Exynos Chips
Google is calling attention to a set of severe security flaws in Samsung's Exynos chips, some of which could be exploited remotely to completely compromise a phone without requiring any user interaction.
https://thehackernews.com/2023/03/google-uncovers-18-severe-security.html

Exploit released for Veeam bug allowing cleartext credential theft
Cross-platform exploit code is now available for a high-severity Backup Service vulnerability impacting Veeam's Backup & Replication (VBR) software. The flaw (CVE-2023-27532) affects all VBR versions and can be exploited by unauthenticated attackers to breach backup infrastructure after stealing cleartext credentials and gaining remote code execution as SYSTEM.
https://www.bleepingcomputer.com/news/security/exploit-released-for-veeam-bug-allowing-cleartext-credential-theft/

Nexus: a new Android botnet?
Nexus provides all the main features to perform ATO attacks (Account Takeover) against banking portals and cryptocurrency services, such as credentials stealing and SMS interception. It also provides a built-in list of injections against 450 financial applications.
https://www.cleafy.com/cleafy-labs/nexus-a-new-android-botnet

****

Hints & Tips plus Security Awareness

Ransomware groups shift tactics and objectives
Malware can play a major or nonexistent role in ransomware attacks. Threat actors are often only in it for the money. Ransomware attacks are shifting from malware-centric threats to more nuanced and sophisticated tactics.
https://www.cybersecuritydive.com/news/ransomware-shifting-tactics-objectives/625595

How to Keep Incident Response Plans Current
Review and update plans to minimize recovery time. Practice and a well-thumbed playbook that considers different scenarios will ensure faster recovery of critical data. The threat landscape is complex, and the tactics used by threat actors are constantly evolving. In this never-ending game of cat and mouse, it seems no matter what cybersecurity advancements the good guys make, it is a perpetual state of catch-up. As tactics evolve, so should readiness plans.
https://www.darkreading.com/attacks-breaches/how-to-keep-incident-response-plans-current

There Is Plenty Of Phishing On Online Apps--Don't Get Hooked
A recent documentary aired on subscription streaming service, Netflix, that highlighted how difficult it is to detect when someone is trying to take advantage of human nature and kindness. You may have seen it. It has been discussed on various media and it may be difficult to watch. But it is yet another example of how

criminals use social engineering and trust to get what they want. One interviewee tells the story of how she met a guy that matched and swept her off her feet and swept her bank account clean.
https://www.sosdailynews.com/news.jspx?&articleid=DE19FB275298F935C60480F8954EC4B0&sx=26446

Preventing Insider Threats in Your Active Directory
Active Directory (AD) is a powerful authentication and directory service used by organizations worldwide. With this ubiquity and power comes the potential for abuse. Insider threats offer some of the most potentials for destruction. Many internal users have over-provisioned access and visibility into the internal network. https://thehackernews.com/2023/03/preventing-insider-threats-in-your.html

****

News & Views

Why You Should Opt Out of Sharing Data With Your Mobile Provider
A new breach involving data from nine million AT&T customers is a fresh reminder that your mobile provider likely collects and shares a great deal of information about where you go and what you do with your mobile device — unless and until you affirmatively opt out of this data collection. Here is a primer on why you might want to do that, and how.
https://krebsonsecurity.com/2023/03/why-you-should-opt-out-of-sharing-data-with-your-mobile-provider/

The Best Defense Against Cyber Threats for Lean Security Teams
H0lyGh0st, Magecart, and a slew of state-sponsored hacker groups are diversifying their tactics and shifting their focus to… You. That is, if you are in charge of cybersecurity for a small-to-midsize enterprise (SME). https://thehackernews.com/2023/03/the-best-defense-against-cyber-threats.html

****

"Ctrl -F" for The Board

The Sobering State of Cybercrime And The Finserv Industry In 2022
In the cybersecurity world, it is always good vs. evil and like in a movie, we are waiting to find out who will win the constant battle. The latest version of Akamai's “Financial Services State of the Internet (SOTI) report,” does not paint a happy picture for the “good guys.” Especially in terms of the attackers’ increasing exploitation of zero-day vulnerabilities, Botnet activity, and increasingly effective phishing attacks, particularly related to the financial services industry.
https://www.sosdailynews.com/news.jspx?&articleid=210C7B71B85743A55BA941F541E41D43

Questions
Contact FIPCO’s Rob Foxx at 800-722-3498 ext. 249 or email FIPCO IT Services for more information.

"Make Security Part of You and Your Institution's DNA!"

Threat Intelligence Newsletter: April 3, 2023

FIPCO®
IT Audit
Round Table
Discussions

Upcoming Threat Intelligence Peer Group Discussions
None available at the current time

****

Alerts & Warnings

Hey, Siri: Hackers Can Control Smart Devices Using Inaudible Sounds
A technique, dubbed the "Near-Ultrasound Inaudible Trojan" (NUIT), allows an attacker to exploit smartphones and smart speakers over the Internet, using sounds undetectable by humans.
https://www.darkreading.com/vulnerabilities-threats/siri-hackers-control-smart-devices-inaudible-sounds

Tax Fraud Danger For Last-Minute Filers
Nearly one-third of Americans have not filed their taxes yet - putting them at a higher risk of losing their refund to tax fraudsters who got to the IRS first. The tax authorities always urge us to submit returns as quickly as possible, but since many of us find the process stressful or daunting, we tend to leave it until the last minute. In fact, an estimated 20 million taxpayers wait until the final couple of days before sending in their forms. https://scambusters.org/taxfraud.html

Background Check Services Breached: Over 20 Million Users Affected
Background-checking companies do just that. These background reports are used to approve people for loans, housing, credit scores, and more. Employment agencies also run credit and background checks on some of their employees and they are often used to check the accuracy of what people are telling them regarding their personal information. Federal agencies, social media, court records, state records, and criminal records, can be gathered by these background check agencies.
https://www.sosdailynews.com/news.jspx?&articleid=26A0770EFC910C161FD76329BC94878B

****

Hints & Tips plus Security Awareness

7 guidelines for identifying and mitigating AI-enabled phishing campaigns
Phishing has always been a thorn in the side of enterprise cybersecurity, and recent AI developments such as ChatGPT are making things even worse. Here are some guidelines for dealing with the increasingly sophisticated phishing threat. https://www.csoonline.com/article/3690418/7-guidelines-for-identifying-and-mitigating-ai-enabled-phishing-campaigns.html

A ransomware negotiator shares 3 tips for victim organizations
This is no time for knee-jerk reactions. “Take a deep breath and slow things down,” said Drew Schmitt, principal threat intelligence analyst at GuidePoint Security.
https://www.cybersecuritydive.com/news/ransomware-negotiator-three-tips/640609/

Where SSO Falls Short in Protecting SaaS
Single sign-on (SSO) is an authentication method that allows users to authenticate their identity for multiple applications with just one set of credentials. From a security standpoint, SSO is the gold standard. It ensures access without forcing users to remember multiple passwords and can be further secured with MFA. Furthermore, an estimated 61% of attacks stem from stolen credentials.
https://thehackernews.com/2023/03/where-sso-falls-short-in-protecting-saas.html

****

News & Views

FTC Action Leads to Lifetime Industry Ban for Operators of ‘Extended Vehicle Warranty’ Scam
Proposed court orders prohibit defendants from all extended warranty sales and from all outbound telemarketing. As a result of a Federal Trade Commission lawsuit, the operators of a telemarketing scam that called hundreds of thousands of consumers nationwide to pitch them expensive “extended automobile warranties” will face a lifetime ban from the extended automobile warranty industry and from all outbound telemarketing.
https://www.ftc.gov/news-events/news/press-releases/2023/03/ftc-action-leads-lifetime-industry-ban-operators-extended-vehicle-warranty-scam

Threat intelligence isn’t for everyone, Google says
Threat intelligence is not universally valuable, particularly for organizations that do not have the wherewithal to translate threat insights into action. Analysts from various Google business units addressed this challenge Wednesday during a Google Cloud security virtual event.
https://www.cybersecuritydive.com/news/threat-intelligence-google/645830/

Millions of Pen Tests Show Companies' Security Postures Are Getting Worse
A lack of website protections, Sender Policy Framework (SPF) records, and DNSSEC configurations leave companies open to phishing and data exfiltration attacks. The risk score for the average company worsened in the past year as companies fail to adapt to data exfiltration techniques and adequately protect Web applications.
https://www.darkreading.com/cloud/millions-pen-tests-companies-security-posture-getting-worse

****

"Ctrl -F" for The Board

Call Me, Maybe? The Stealth Disappearance of Social Engineering and Fraudulent Instruction Coverage
Anyone who owns a cellphone or uses an email address has received a communication from a scammer seeking to extract confidential information or trick the recipient into sending money to foreign countries. These attempts come in a variety of forms that have evolved, and have become more sophisticated, over time. https://www.jdsupra.com/legalnews/call-me-maybe-the-stealth-disappearance-7177824/

Questions
Contact FIPCO’s Rob Foxx at 800-722-3498 ext. 249 or email FIPCO IT Services for more information.

"Make Security Part of You and Your Institution's DNA!"

Threat Intelligence Newsletter: April 7, 2023

FIPCO®
IT Audit
Round Table
Discussions

Upcoming Threat Intelligence Peer Group Discussions
None available at the current time

****

Alerts & Warnings

BBB Scam Alert: Small businesses spot an invoice scam posing as the Geek Squad or PayPal
You may have encountered a fake invoice if you are running a small business (or keeping books for one). Phony bills have long been a favorite and effective trick of scammers. Recently, BBB Scam Tracker has gotten multiple reports of a new version of this scam, where con artists pretend to be contacting you as part of the Geek Squad, which is owned by Best Buy (BBB Accredited Business) or through PayPal (BBB Accredited Business).
https://www.bbb.org/article/news-releases/28461-bbb-scam-alert-invoice-scams

AI chatbots making it harder to spot phishing emails, say experts
Poor spelling and grammar that can help identify fraudulent attacks being rectified by artificial intelligence. Chatbots are taking away a key line of defence against fraudulent phishing emails by removing glaring grammatical and spelling errors, according to experts. The warning comes as policing organisation Europol issues an international advisory about the potential criminal use of ChatGPT and other “large language models”.
https://www.theguardian.com/technology/2023/mar/29/ai-chatbots-making-it-harder-to-spot-phishing-emails-say-experts

Business Email Compromise Tactics Used to Facilitate the Acquisition of Commodities and Defrauding Vendors
The FBI warns the public of criminal actors using Business Email Compromise (BEC) schemes to facilitate the acquisition of a wide range of commodities. BEC is one of the most financially damaging online crimes. It exploits the fact that so many of us rely on email to conduct business—both personal and professional.
https://www.ic3.gov/Media/Y2023/PSA230324

BEC Fraudsters Expand to Snatch Real-World Goods in Commodities Twist
Business email compromise scams are moving beyond just stealing cash, with some threat actors fooling companies into sending goods and materials on credit, and then skipping out on payment. Some cybercriminals are flipping their playbook on business email compromise (BEC) scams and, rather than posing as vendors seeking payment, are now posing as buyers, taking their profits in easily sold commodities.
https://www.darkreading.com/threat-intelligence/bec-fraudsters-expand-snatch-real-world-goods-commodities-twist

'Tactical Octopus' hackers using tax-related phishing scams to spread malware
Researchers are warning about a group of hackers that are using tax-related email lures to spread dangerous malware. Cybersecurity experts at Securonix said they have been tracking the group known as TACTICAL#OCTOPUS for months in advance of the April 18 U.S. tax deadline, finding that they are using seemingly valid employee W-2 tax documents, I-9 forms, and real estate purchase contracts to get people to download malware that gives the hackers wide-ranging access to devices.
https://therecord.media/hackers-use-phishing-schemes-tax-scams

Rorschach ransomware has the fastest file-encrypting routine to date
A new ransomware strain named Rorschach ransomware supports the fastest file-encrypting routine observed to date.
Check Point Research (CPR) and Check Point Incident Response Team (CPIRT) researchers detected a previously unknown ransomware strain, dubbed Rorschach ransomware, that was employed in attack against a US-based company. The experts pointed out that the Rorschach ransomware appears to be unique. According to the report published by Check Point, Rorschach is one of the fastest ransomwares observed to date.
https://securityaffairs.com/144425/cyber-crime/rorschach-ransomware-fast-encryption.html

CISA: Immediate patching needed for zero-days exploited for spyware distribution
Federal agencies have been urged by the Cybersecurity and Infrastructure Security Agency to remediate five of 10 zero-day vulnerabilities leveraged in two spyware campaigns by April 20, reports BleepingComputer.
https://www.scmagazine.com/brief/vulnerability-management/cisa-immediate-patching-needed-for-zero-days-exploited-for-spyware-distribution

New Wi-Fi Protocol Security Flaw Affecting Linux, Android, and iOS Devices
A group of academics from Northeastern University and KU Leuven has disclosed a fundamental design flaw in the IEEE 802.11 Wi-Fi protocol standard, impacting a wide range of devices running Linux, FreeBSD, Android, and iOS. https://thehackernews.com/2023/03/new-wi-fi-protocol-security-flaw.html

****

Hints & Tips plus Security Awareness

Your Key Weapon Against Biometric Data Theft
Security pros keep telling us that the age of the cumbersome use of passwords is nearly over and we'll all be using fingerprints, facial, eye-iris, voice recognition, and other forms of biometrics, even DNA, in their place. But the bad news is that scammers and hackers have developed software and theft techniques so they can use biometrics and pretend they are you. https://scambusters.org/biometric.html

Chinese fraudsters: evading detection and monetizing stolen credit card information
Cyber attacks are common occurrences that often make headlines, but the leakage of personal information, particularly credit card data, can have severe consequences for individuals. It is essential to understand the techniques employed by cyber criminals to steal this sensitive information. Credit card fraud in the United States has been on the rise, with total losses reaching approximately $12.16 billion in 2021, according to Insider Intelligence. Card-Not-Present (CNP) fraud constituted 72% of these losses, with a substantial portion attributed to Chinese fraudsters.
https://cybersecurity.att.com/blogs/security-essentials/chinese-fraudsters-evading-detection-and-monetizing-stolen-credit-card-information

Year-Round Package Delivery Scams To Watch For, 24-7-365
Be it by text, phone call, or email, cyber thieves love trying to scam us out of something of value. It could be for our personally identifiable information (PII), bank account information, payment card data, or all three at once. If there is one thing, we can count on today it's this: Every day, and likely every minute of the day, the world over, someone is being scammed in some way. Many "everyday" scams involve package delivery services. Whether you are expecting a package or not, it doesn't matter because scammers will steal what they can from you. Being aware of the common tactics used to catch us off-guard can help keep us scam safe. Below are widely used package delivery scam messages, so pay attention if you do not want to be next.
https://www.sosdailynews.com/news.jspx?&articleid=E92A6731EB563068291AFAA5B02C5EAC

Deep Dive Into 6 Key Steps to Accelerate Your Incident Response
Organizations rely on Incident response to ensure they are immediately aware of security incidents, allowing for quick action to minimize damage. They also aim to avoid follow on attacks or future related incidents. https://thehackernews.com/2023/03/deep-dive-into-6-key-steps-to.html

****

News & Views

CISA summons outside tips to alert victims of early-stage ransomware
Federal cyber authorities shared early, promising results last week of a pre-ransomware notification initiative designed to quickly alert organizations of intrusions before ransomware actors encrypt or steal data. The Cybersecurity and Infrastructure Security Agency's Joint Cyber Defense Collaborative pulls in tips from cybersecurity researchers, infrastructure providers and threat intelligence firms to notify victim organizations of early-stage ransomware activity, JCDC Associate Director Clayton Romans said Thursday in a blog post. https://www.cybersecuritydive.com/news/cisa-pre-ransomware-notification/646041

Tesla Model 3 Hacked in Less Than 2 Minutes at Pwn2Own Contest
In two days, ethical researchers from 10 countries have unearthed more than 22 zero-day bugs in a wide range of technologies at the annual hacking contest.
Researchers from France-based pen-testing firm Synacktiv demonstrated two separate exploits against the Tesla Model 3 this week at the Pwn2Own hacking contest in Vancouver. The attacks gave them deep access into subsystems controlling the vehicle's safety and other components.
https://www.darkreading.com/vulnerabilities-threats/tesla-model-3-hacked-2-minutes-pwn2own-contest

Google will require Android apps to let you delete your account
Google has announced a new Google Play Store data deletion policy that will require Android developers to provide users with an online option to delete their accounts and in-app data. According to the new policy, starting in early 2024, Google Play users will have better control over their data since every store listing will display links in the "Data deletion" area, allowing them to ask for their accounts and/or data to be deleted. https://www.bleepingcomputer.com/news/google/google-will-require-android-apps-to-let-you-delete-your-account

****

"Ctrl -F" for The Board

Protect Your Company: Ransomware Prevention Made Easy
Every year hundreds of millions of malware attacks occur worldwide, and every year businesses deal with the impact of viruses, worms, keyloggers, and ransomware. Malware is a pernicious threat and the biggest driver for businesses to look for cybersecurity solutions.
https://thehackernews.com/2023/04/protect-your-company-ransomware.html

Questions
Contact FIPCO’s Rob Foxx at 800-722-3498 ext. 249 or email FIPCO IT Services for more information.

"Make Security Part of You and Your Institution's DNA!"

Threat Intelligence Newsletter: April 18, 2023

FIPCO®
IT Audit
Round Table
Discussions

Upcoming Threat Intelligence Peer Group Discussions
None available at the current time

****

Alerts & Warnings

Palo Alto security software stung by ransomware strain
The ransomware was deployed using a DLL-sideloading technique using Palo Alto Network's Cortex XDR, which is a signed commercial security product. This technique has not commonly been used for ransomware.
https://www.cybersecuritydive.com/news/palo-alto-security-abused-ransomware/646775/

'BEC 3.0' Is Here With Tax-Season QuickBooks Cyberattacks
In next-gen, credential-harvesting attacks, phishing emails use cloud services and are free from the typical bad grammar or typos they have traditionally used (and which users have learned to spot).
https://www.darkreading.com/attacks-breaches/bec-3-tax-season-quickbooks-cyberattacks

Scam Victim? Don't Fall For This Asset Recovery Lie
What could be worse than being scammed? Being conned again by the same people or for the same trick when you call in a recovery scammer. It works like this: You get scammed out of money or property. Then someone, maybe even the original scammer in disguise, says they can get recoup your losses for a fee. So, you pay up and never hear from them again. Or you pay, and the crooks then say they need more money to cover expenses or taxes. And so on, until you realize what is going on.
https://scambusters.org/recovery2.html

Linux Systems Targeted By Notorious Ransomware Hacking Group
A well-known ransomware group is focusing its efforts on Linux systems, a noticeable departure from their previous attacks on Windows operating systems. It is a sign the notorious Clop hacking group continues to grow its ransomware campaigns despite prior efforts to shut the group down.
https://www.sosdailynews.com/news.jspx?&articleid=F3E74F4A0950C8296B2E399BAEA467B0

CISA Warns of 5 Actively Exploited Security Flaws: Urgent Action Required
The U.S. Cybersecurity and Infrastructure Security Agency (CISA) on Friday added five security flaws to its Known Exploited Vulnerabilities (KEV) catalog, citing evidence of active exploitation in the wild. This includes three high-severity flaws in the Veritas Backup Exec Agent software (CVE-2021-27876, CVE-2021-27877, and CVE-2021-27878) that could lead to the execution of privileged commands on the underlying system. The flaws were fixed in a patch released by Veritas in March 2021.
https://thehackernews.com/2023/04/cisa-warns-of-5-actively-exploited.html

You might want to avoid using free public charging stations. Here's why.
The FBI recently warned against using free public charging stations, saying hackers can use the connection to transmit malware onto your device. The agency advised consumers have their own charger and USB cord and use an electrical outlet. Note from FIPCO Data Blocker USB devices can remediate this risk.
https://www.usatoday.com/story/tech/2023/04/10/fbi-warns-against-using-public-charging-stations/11636024002/

****

Hints & Tips plus Security Awareness

Leftover data lurks across the enterprise, creating a business risk
When an organization has little visibility into the data in its possession, it becomes even more vulnerable to data leaks, breaches, and both insider and external threats. There is a good chance that someone in your organization is hoarding data.
https://www.cybersecuritydive.com/news/data-retention-cyber-risk/647131

Top 10 Cybersecurity Trends for 2023: From Zero Trust to Cyber Insurance
As technology advances, cyberattacks are becoming more sophisticated. With the increasing use of technology in our daily lives, cybercrime is on the rise, as evidenced by the fact that cyberattacks caused 92% of all data breaches in the first quarter of 2022. Staying current with cybersecurity trends and laws is crucial to combat these threats, which can significantly impact business development.
https://thehackernews.com/2023/04/top-10-cybersecurity-trends-for-2023.html

****

News & Views

Cyberattacks hit almost all companies last year, Sophos says
A constant barrage of malicious activity has organizations reeling, negatively impacting their ability to strategize or accomplish IT projects. Cyberattacks are not a roll of the dice for organizations, but rather a near certainty. Almost all organizations, 94%, experienced a cyberattack of some form during the last year, according to research Sophos released Tuesday.
https://www.cybersecuritydive.com/news/cyberattacks-hit-most-companies-sophos/646583/

IT security leaders still told to keep data breaches quiet, study finds
More than 2 in 5 IT and security professionals in the U.S. and Western Europe have been told to keep a cyber breach confidential, despite knowing the incidents should be disclosed, according to a report released Wednesday from Bitdefender.
https://www.cybersecuritydive.com/news/it-security-data-breaches-disclosure/647010/

Shadow IT accounts for more than one-third of enterprise apps: report
More than half of SaaS purchases, on average, are not properly categorized as software within expense platforms and other financial systems, the report shows.
https://www.ciodive.com/news/SaaS-spend-shadow-IT-governance-software/646816/

****

"Ctrl -F" for The Board

The route to CIO: How companies are sourcing tech execs
With salaries rising and portfolios expanding, the stakes are higher than ever to find technology leaders. Most companies cannot afford a disruption in tech leadership. The IT function is too deeply woven into the fabric of the business to risk discontinuity in technology operations.
https://www.ciodive.com/news/CIO-technology-leadership/646582/

Banks face a growing list of cyber risks, but also growing cyber insurance premiums
The news: Banks and financial institutions face ever-evolving cyber risks but paying for cyber insurance might not be part of their mitigation plans, per American Banker.
https://www.insiderintelligence.com/content/banks-face-growing-list-of-cyber-risks-also-growing-cyber-insurance-premiums

Questions
Contact FIPCO’s Rob Foxx at 800-722-3498 ext. 249 or email FIPCO IT Services for more information.

"Make Security Part of You and Your Institution's DNA!"

Threat Intelligence Newsletter: April 24, 2023

FIPCO®
IT Audit
Round Table
Discussions

Upcoming Threat Intelligence Peer Group Discussions
None available at the current time

****

Alerts & Warnings

BBB Business Scam Alert: Stay alert to Employee Retention Credit (ERC) scams this tax season
Business owners, con artists want to trick you into claiming tax credits that you aren't eligible for. The Internal Revenue Service warns about scams revolving around the Employee Retention Credit, a tax credit for businesses that continued paying employees during the COVID-19 shutdowns or had a significant income decline during the eligibility period. While most eligible employers have already claimed this credit, unscrupulous companies are advertising ERC services to draw in businesses that are not eligible for the credit.
https://www.bbb.org/article/scams/28551-bbb-scam-alert-stay-alert-to-employee-retention-credit-erc-scams-this-tax-season

Why is 'Juice Jacking' Suddenly Back in the News?
KrebsOnSecurity received a nice bump in traffic this week thanks to tweets from the Federal Bureau of Investigation (FBI) and the Federal Communications Commission (FCC) about "juice jacking," a term first coined here in 2011 to describe a potential threat of data theft when one plugs their mobile device into a public charging kiosk. It remains unclear what may have prompted the alerts, but the good news is that there are some fairly basic things you can do to avoid having to worry about juice jacking. FIPCO: See Data Blocker by PortaPow or similar devices for solutions.
https://krebsonsecurity.com/2023/04/why-is-juice-jacking-suddenly-back-in-the-news/

How To Stop Car Hackers In Their Tracks
Mobile computing takes on a whole new meaning when you apply it to your car. Modern vehicles are stuffed with so much technology, it's like you're driving a computer! So, it should come as no surprise that crooks have discovered many ways to take control of autos through car hack attacks. In fact, a survey by the Ponemon Institute found that nearly two-thirds of "connected" car owners said they were concerned about security. And no wonder. In an experiment, it took experts at one cybersecurity firm just two minutes to hack into a car's electronic control unit (ECU).
https://scambusters.org/carhack.html

The Number One Rule To Avoid Malicious Screen Overlays
You may not always be aware of it, but whenever you switch on your computer or open your mobile device screen, trouble, sometimes big trouble, is only a single click or tap away. And crooks have many ways of tricking you into clicking that dangerous link. Sometimes it's by pretending to be something they're not and many times you can't even see what they're up to.
https://scambusters.org/overlay.html

****

Hints & Tips plus Security Awareness

How to protect ATMs from advanced threats
As the technical capabilities of ATMs have increased, criminals have also improved their physical and digital methods to steal cash and consumer data from the machines. To protect ATMs, businesses must fully understand all of the threats against them.
https://www.atmmarketplace.com/blogs/how-to-protect-atms-from-advanced-threats/

Ransomware's 4 Favorite Entry Options And How To Counter Them
The growing scourge of businesses worldwide, ransomware attacks are currently at historic levels. Always improving, always stealthier, ransomware is the number one malware threat that businesses need to protect themselves against. Ransomware is behind countless problems for businesses worldwide, including significant down-time, loss of reputation, and customers, and significant financial expense.
https://www.sosdailynews.com/news.jspx?&articleid=3A614B210E356C4A153686A005EEEB9B

BOLO for These Most Dangerous Email Attachments
Keeping a lookout for suspicious emails has become a daily consequence of our cyber lives. Phishing emails are notorious for having malicious attachments and opening them is a sure way to compromise your device and its data. These attachments are full of malware, ready and waiting to infect your system with a simple click. Make no mistake, any attachment in a questionable email can be dangerous. However, researchers at F-Secure found that some of this year's biggest email spam campaigns used particular types of malicious attachments more than others.
https://www.sosdailynews.com/news.jspx?&articleid=6F2B005E848AC7F866F3A1D42161E83C

****

News & Views

Taking a closer look at video banking
Video banking is a now a multi-billion dollar industry. Where's it headed? ATM Marketplace takes a closer look. It is no surprise that customers now expect service on their own terms and at their own convenience. This includes not only simple banking services such as checking account balances but also more complex tasks such as loan origination, account openings and even financial advice.
https://www.atmmarketplace.com/blogs/taking-a-closer-look-at-video-banking/

Online Scams The New Top Cybercrime With 73% Of All Attacks
Move over former top cybercrimes, there's a new winner according to Group-IB experts who specialize in high-tech cybercrimes. Group-IB recently announced that online scams are now the number one type of cybercrime in the world today, with some referring to this as a "scamdemic." Researchers found that in

total, fraud now makes up 73% of all online attacks. There's a definite need for users to be aware of these scams, how they can work and how prevalent they are.
https://www.sosdailynews.com/news.jspx?&articleid=26A05043E51FA1FB52EA32B712D0A2C8

Uncovering (and Understanding) the Hidden Risks of SaaS Apps
Recent data breaches across CircleCI, LastPass, and Okta underscore a common theme: The enterprise SaaS stacks connected to these industry-leading apps can be at serious risk for compromise. CircleCI, for example, plays an integral, SaaS-to-SaaS role for SaaS app development. Similarly, tens of thousands of organizations rely on Okta and LastPass security roles for SaaS identity and access management. Enterprise and niche SaaS apps alike have effectively introduced multitudes of unmonitored endpoints into organizations of all sizes.
https://thehackernews.com/2023/04/uncovering-and-understanding-hidden.html

****

"Ctrl -F" for The Board

Phone Scammers Use Big Tech As Lures
Ask a robocall recipient and they'll tell you that robocalls are annoying and a waste of time. But the victim of a phone scam (vishing) will tell you it could mean losing a lot more than just time. Like email phishing, falling for a vishing scam can put you in danger of losing your identity, your money, and any other private information a criminal can get. So, what to do when the caller claims to be from a trusted business and has a legitimate reason to call?
https://www.sosdailynews.com/news.jspx?&articleid=AC33D77581F375FE8809D09AB2D9CC89

Questions
Contact FIPCO's Rob Foxx at 800-722-3498 ext. 249 or email FIPCO IT Services for more information.

"Make Security Part of You and Your Institution's DNA!"

Threat Intelligence Newsletter: May 1, 2023

FIPCO® IT Audit Round Table Discussions

Upcoming Threat Intelligence Peer Group Discussions
None available at the current time

****

Alerts & Warnings

Job hunting? Stay alert to resume formatting scams
To find the job of your dreams, you need a well-crafted resume, right? According to recent Scam Tracker reports, con artists have devised yet another way to trick job seekers out of money and personal information. If you are asked to pay to reformat your resume for a company's applicant tracking system (ATS) during your job search, think twice before you agree. This scam is convincing because many companies use software to automate resume reviews.
https://www.bbb.org/article/scams/28588-bbb-scam-alert-job-hunting-stay-alert-to-resume-formatting-scams

Google 2FA Syncing Feature Could Put Your Privacy at Risk
Researchers find that the encryption of a user's 2FA secrets are stripped after transportation to the cloud. After a 13-year-long wait, Google Authenticator has added a 2FA account-sync feature that allows its users to back up their 2FA code sequences into the cloud, after which they can restore them back into a new device.
https://www.darkreading.com/application-security/google-2fa-syncing-feature-could-put-your-privacy-at-risk

Many Public Salesforce Sites are Leaking Private Data
A shocking number of organizations — including banks and healthcare providers — are leaking private and sensitive information from their public Salesforce Community websites, KrebsOnSecurity has learned. The data exposures all stem from a misconfiguration in Salesforce Community that allows an unauthenticated user to access records that should only be available after logging in.
https://krebsonsecurity.com/2023/04/many-public-salesforce-sites-are-leaking-private-data/

Chinese Cyberspies Delivered Malware via Legitimate Software Updates
Chinese APT Evasive Panda has been observed targeting local members of an international NGO with the MgBot backdoor, delivered via legitimate software updates. A Chinese APT actor tracked as Evasive Panda

has been observed targeting in-country members of an international non-governmental organization (NGO) with the MgBot backdoor, and the malware was likely delivered through the legitimate update channels of popular Chinese software, cybersecurity firm ESET reports.
https://www.securityweek.com/chinese-cyberspies-delivered-malware-via-legitimate-software-updates/

New Atomic macOS Malware Steals Keychain Passwords and Crypto Wallets
Threat actors are advertising a new information stealer for the Apple macOS operating system called Atomic macOS Stealer (or AMOS) on Telegram for $1,000 per month, joining the likes of MacStealer. "The Atomic macOS Stealer can steal various types of information from the victim's machine, including Keychain passwords, complete system information, files from the desktop and documents folder, and even the macOS password," Cyble researchers said in a technical report.
https://thehackernews.com/2023/04/new-atomic-macos-stealer-can-steal-your.html

****

Hints & Tips plus Security Awareness

SANS Reveals Top 5 Most Dangerous Cyberattacks for 2023
SEO-aided attacks, developer targeting, and malicious use of AI top the list for 2023. RSA CONFERENCE 2023 - San Francisco — Expert instructors from the SANS Institute here yesterday detailed what they cite as the most dangerous forms of cyberattacks for 2023.
https://www.darkreading.com/attacks-breaches/sans-lists-top-5-most-dangerous-cyberattacks-in-2023

CISO Survival Guide for Cyberattacks
CISOs who have survived major cyber incidents recommend letting company ethos guide incident response. RSA CONFERENCE 2023 – San Francisco – The difference between a cyber crisis and any other type of emergency response is the unknown and the speed of events.
https://www.darkreading.com/vulnerabilities-threats/ciso-survival-guide-for-cyberattacks

Malware-Free Cyberattacks Are on the Rise; Here's How to Detect Them
Last year, 71% of enterprise breaches were pulled off quietly, with legitimate tools, research shows. RSA CONFERENCE 2023 – San Francisco – With little more than smart reconnaissance and existing tools, adversaries are increasingly capable of compromising an enterprise network without making any noise or leaving a trace behind.
https://www.darkreading.com/endpoint/malware-free-cyberattacks-rise-how-to-detect

****

News & Views

AI is coming to enhance human employees — not replace them
Machines should be seen as partners and assistants, since human expectations and limitations will restrict their abilities. Technology’s dizzying progression often leads to the worry that machines will one day replace humans in several kinds of tasks — including many forms of knowledge work.
https://www.ciodive.com/news/AI-chatbots-human-augmented/647868/

Google Bans 173,000 Bad Developers in 2022
Google is making it harder for malicious developers to get their software published on its Play store, while removing large volumes of bad accounts, it claimed in an update yesterday. The tech giant said it removed

173,000 bad accounts in 2022 and raised the bar for new developers by adding phone, email and “other identity verification methods.”
https://www.infosecurity-magazine.com/news/google-bans-173000-bad-developers/

Americans view crypto investing as unreliable. They’re right.
State securities regulators cited digital asset fraud as the biggest threat to investors for 2023. Cryptocurrency investing is like going to a ritzy casino — the sights and sounds of winning don’t mean the vast majority of people are richer than when they started playing. It’s all part of the lure and illusion.
https://www.washingtonpost.com/business/2023/04/21/americans-view-cryptocurrency-unreliable/

Financial Services Robust Security Forces Cybercriminals To Target Customers
Cybercrime is a conflict between two players. The experts focused on finding ways to foil attempts by cyber criminals to access information related to client accounts and the cyber criminals themselves. They are continually in search of loopholes in security solutions to access sensitive personal information. And if research from Akamai is true in their annual “State of the Internet” report, then cybersecurity teams are fighting a desperate fight against professional malware groups intent on using a variety of tactics. Comparing losses due to cybercriminal activity in 2022 with the losses incurred in 2021 paints a sobering picture of a cybercriminal fraternity that is very successfully exploiting security weaknesses.
https://www.sosdailynews.com/news.jspx?&articleid=9E9B39D4B214B9B9B563DBA949EDBA7B

****

"Ctrl -F" for The Board

Questions
Contact FIPCO’s Rob Foxx at 800-722-3498 ext. 249 or email FIPCO IT Services for more information.

"Make Security Part of You and Your Institution's DNA!"

Threat Intelligence Newsletter: May 5, 2023

Upcoming Threat Intelligence Peer Group Discussions
None available at the current time

****

Alerts & Warnings

BBB Scam Alert: How to spot a scam when shopping for refurbished products
Buying refurbished items can save you money, but it's important to research before you take the plunge. While many reputable businesses offer quality pre-owned electronics, appliances, and other products for a fraction of their original price, BBB Scam Tracker has received reports of con artists ripping off consumers by promising a great deal on "like-new" devices that they don't plan on delivering.
https://www.bbb.org/article/scams/28616-scam-alert-how-to-spot-a-scam-when-shopping-for-refurbished-products

Promising Jobs at the U.S. Postal Service, 'US Job Services' Leaks Customer Data
A sprawling online company based in Georgia that has made tens of millions of dollars purporting to sell access to jobs at the United States Postal Service (USPS) has exposed its internal IT operations and database of nearly 900,000 customers. The leaked records indicate the network's chief technology officer in Pakistan has been hacked for the past year, and that the entire operation was created by the principals of a Tennessee-based telemarketing firm that has promoted USPS employment websites since 2016.
https://krebsonsecurity.com/2023/05/promising-jobs-at-the-u-s-postal-service-us-job-services-leaks-customer-data/

Texas bank breach exposed thousands of Social Security numbers
Social Security numbers (SSNs) of over 17,000 US residents have been exposed after a Happy State Bank (HSB) employee's email account was compromised in a suspected cyberattack. HSB, a Texas-based financial business, notified customers about a business email compromise (BEC) that jeopardized thousands of customers' personal data.
https://cybernews.com/news/happy-state-bank-breach

Bootleg Apple Software Hides Cryptomining Malware On Macs
For those keeping up with technology news, it's not often Macs make hacking headlines. And for those who are simply Mac lovers, it's not wise to think hacks happen only to Androids since both are vulnerable.

A recent finding linking bootleg Apple software, malware, and cryptomining is a lesson all users can learn from. After all, a successful attack on Macs can end up targeting Androids, too. Security researchers at Jamf Threat Labs found a bootleg version of Final Cut Pro Apple software hiding cryptomining malware. https://www.sosdailynews.com/news.jspx?&articleid=A4FD1A0323D2036CBA1FDC38BB4764E2

How Using Your Browser's Spell-Check Is "R-I-S-K-Y" For Your PII

No one wants to write an email or other document with spelling errors or bad grammar. That's why using spell-check and other typing assistants have become so popular for business and personal use. But thanks to researchers at Otto-JavaScript (Otto-JS), they found using these helpful browser options sends your PII (personally identifiable information) to big tech companies like Google and Microsoft. No one wants to do that either, so continue reading to learn more about this previously unknown threat to PII. https://www.sosdailynews.com/news.jspx?&articleid=A82BCFEE5A20AF0EEA6962E24440E8E4

****

Hints & Tips plus Security Awareness

Bad Actors Employ Next-Gen Hacking Methods for Innovation

Accenture's Valerie Abend on How Cybercriminals Are Able to Move Faster. The number of ransoms paid by organizations is on the decline, which is positive news. But we know that the criminals are always innovating. Valerie Abend, global cyber strategy lead at Accenture, said cybercriminals are constantly learning to accomplish their objectives and are increasingly adopting next-generation hacking techniques. https://www.databreachtoday.com/bad-actors-employ-next-gen-hacking-methods-for-innovation-a-21753

The 5 Most Dangerous New Attack Techniques

SANS Technology Institute President Ed Skoudis on Ever-Changing Attack Surface 10 Min Video. The COVID-19 pandemic brought about notable shifts in technology and cybersecurity. It also widened the attack surface, making it bigger than ever before. This change is driven by factors such as hybrid workplaces, cloud migration and SaaS dependencies.
https://www.databreachtoday.com/5-most-dangerous-new-attack-techniques-a-21838

****

News & Views

Mandiant CEO's 7 tips for cyber defense

Organizations' institutional knowledge is an advantage that no adversary can match, Kevin Mandia told RSA Conference attendees. The Google-owned incident response firm, which Mandia founded, investigated 1,163 intrusions in 2022 and is currently responding to more than 100 security breaches — fundamental mistakes, oversights and misaligned priorities keep showing up.
https://www.cybersecuritydive.com/news/mandiant-ceo-7-tips-cyber-defense/648917/

Teenagers, young adults pose prevalent cyberthreat to US, Mandiant says

The brains behind high-profile attacks last year, teenagers and young adults use sophisticated social engineering techniques for intrusions. SAN FRANCISCO — A group of teenagers and individuals in their 20s from the U.S. and United Kingdom are among the most prevalent threat actors today, Mandiant Consulting CTO Charles Carmakal said Monday at an off-site media briefing during the RSA Conference.
https://www.cybersecuritydive.com/news/teenagers-young-adults-cyberthreat-mandiant/648554

White House to share roadmap for national cyber strategy implementation this summer
Acting National Cyber Director Kemba Walden said the strategy is built to have a 10-year shelf life, allowing for flexibility as new technologies and threats emerge.
https://www.cybersecuritydive.com/news/national-cyber-strategy-timeline/648668/

Google Chrome Drops Browser Lock Icon
Chrome 117 will retire the lock icon and replace it with a "tune" icon, reflecting evolving cybersecurity standards. Dating all the way back to circa 1990s Netscape, the tiny lock icon on the left-hand side of the Google Chrome browser search bar indicated the site had loaded over HTTPS. HTTPS sites with a secured connection between Chrome, the website, and network used to be rare — but today it's the default.
https://www.darkreading.com/application-security/google-chrome-loses-the-lock-icon

****

"Ctrl -F" for The Board

Three-Quarters of Firms Predict Breach in Coming Year
Most global organizations anticipate suffering a data breach or cyber-attack in the next 12 months, despite cyber-risk levels falling overall, according to Trend Micro. The security vendor's six-monthly Cyber Risk Index (CRI) was compiled from interviews with 3729 global organizations. The index itself is based on a numerical scale of -10 to 10, with -10 representing the highest level of risk. It is calculated by subtracting the score for cyber-threats from the score for cyber-preparedness.
https://www.infosecurity-magazine.com/news/threequarters-firms-predict-breach/

Questions
Contact FIPCO's Rob Foxx at 800-722-3498 ext. 249 or email FIPCO IT Services for more information.

"Make Security Part of You and Your Institution's DNA!"

Threat Intelligence Newsletter: May 12, 2023

FIPCO®
IT Audit
Round Table
Discussions

Upcoming Threat Intelligence Peer Group Discussions
None available at the current time

****

Alerts & Warnings

BBB Scam Alert: How to spot a scam when shopping for refurbished products
Buying refurbished items can save you money, but it's important to research before you take the plunge. While many reputable businesses offer quality pre-owned electronics, appliances, and other products for a fraction of their original price, BBB Scam Tracker has received reports of con artists ripping off consumers by promising a great deal on "like-new" devices that they don't plan on delivering.
https://www.bbb.org/article/scams/28616-scam-alert-how-to-spot-a-scam-when-shopping-for-refurbished-products

Beware of Fake Google Chrome Update Error Messages
Google Chrome users who use the browser regularly should be wary of a new attack campaign that distributes malware by posing as a Google Chrome update error message. The attack campaign has been operational since February 2023 and has a large impact area.
https://news.trendmicro.com/2023/05/01/fake-google-chrome-update-error-message/

Phishing Alert As Foreign Elder Fraud Battle Is Stepped Up
Seniors are being caught up in a new wave of phishing scams from overseas gangs. In the latest onslaught of what the US Department of Justice (DOJ) calls transnational elder fraud, scammers use the tried and tested tactic of tricking victims into disclosing personal confidential information via emails, phone calls, and text messages. But because they're based abroad, the fraudsters are more difficult to track down. This has prompted the DOJ to beef up its Transnational Elder Fraud Strike Force - a collaboration between various government and law enforcement agencies trying to stem the tides of overseas scams.
https://scambusters.org/elderfraud2.html

Is Microsoft OneNote Emailing You Malware? What To Know, What To Do
Microsoft's OneNote is making news, but not in the way the software giant would hope. OneNote, the note-taking app that's part of Microsoft Office, is being weaponized by QBot threat actors. Fans of OneNote, whether for business or personal use, should know QBot's email phishing campaign leads to stolen passwords, hijacked financial and browser data, and just about anything else there is to steal.
https://www.sosdailynews.com/news.jspx?&articleid=2D76948E6CAA44A9CFF1FA2B37513414

Medicare Phone Scams Spike During Peak Periods, But Are Still Circulating Now
Senior citizens and others on Medicare are an ongoing target for scammers. However, some Medicare scams spike at various points during the year, like other types of scams such as tax-related ones. Phone scams abound during peak "attention" time, such as the Medicare open enrollment period (OEP) with the goal of stealing PII for financial and other identity crimes. Those on Medicare and the people who care for them need to know how these OEP scams happen and how to avoid them.
https://www.sosdailynews.com/news.jspx?&articleid=49423383D76CD8A1655B41FFA25AE74F

QR codes used in fake parking tickets, surveys to steal your money
As QR codes continue to be heavily used by legitimate organizations—from Super Bowl advertisements to enforcing parking fees and fines, scammers have crept in to abuse the very technology for their nefarious purposes. A woman in Singapore reportedly lost $20,000 after using a QR code to fill out a "survey" at a bubble tea shop, whereas cases of fake car parking citations with QR codes targeting drivers have been observed in the U.S. and the U.K.
https://www.bleepingcomputer.com/news/security/qr-codes-used-in-fake-parking-tickets-surveys-to-steal-your-money/

****

Hints & Tips plus Security Awareness

How 7 cybersecurity experts manage their passwords
Cybersecurity Dive asked CISOs and other cyber experts what they do with their passwords. Here's how they manage the mess that awaits us all. Passwords, a necessary mechanism individuals and businesses lean on for access to services they use every day, are mostly despised by cybersecurity professionals. At the very least, they are begrudgingly accepted as the best and most universally adopted security feature available today.
https://www.cybersecuritydive.com/news/how-experts-manage-passwords/649431/

Your Data For Sale On The Dark Web And What You Can Do About It
As much as we love the convenience of our digital world, we know a hefty price tag can come with it. The world is full of bad actors whose goal is to get their hands on our sensitive, personally identifiable information, or PII. Should you find your PII is for sale on the dark web, it helps to know there are options for doing something about it, even if you think it's too late. Just some of that hijacked PII can include passwords, email and physical addresses, Social Security numbers, financial accounts, and much more.
https://www.sosdailynews.com/news.jspx?&articleid=CDAB8C96D8AB0C905C33B2AA55368ACB

****

News & Views

CISA director wary of technology industry repeating its mistakes with AI
The multibillion-dollar cybersecurity industry is the result of misaligned incentives, where the technology industry prioritized speed to market over security, said Jen Easterly, director of the Cybersecurity and Infrastructure Security Agency, at a Hack the Capitol event Wednesday.
https://www.cybersecuritydive.com/news/ai-cybersecurity-cisa-director-easterly/650054

Walden says cybersecurity strategy mostly well-received
The acting national cyber director says common ground exists in certain areas, but a great deal of work remains. Acting National Cyber Director Kemba Walden said the national cybersecurity strategy has been well received, however acknowledged there were areas of disagreement.
https://www.cybersecuritydive.com/news/kemba-walden-cybersecurity-strategy-well-received/649925

****

"Ctrl -F" for The Board

White House considers ban on ransom payments, with caveats
Experts suggest the effort, a reversal from the administration's previous stance, is fraught with complications that could cause unintended consequences. The White House and international partners in the fight against ransomware are considering a ban on ransom payments, eyeing a new and complicated means to counter financially motivated threat actors.
https://www.ciodive.com/news/white-house-considers-ransom-payment-ban/649734/

Cyber Professionals Are Stressed Out, Overworked, Underpaid
Candy Alexander of ISSA International Board on State of Cyber Professionals. Cybersecurity professionals are stressed out, overworked, underpaid and working on short-staffed teams, said Candy Alexander, president of the ISSA International Board. She advised organizations to look for the right indicators of a good cybersecurity culture. 7 Min Interview.
https://www.govinfosecurity.com/cyber-professionals-are-stressed-out-overworked-underpaid-a-21756

Questions
Contact FIPCO's Rob Foxx at 800-722-3498 ext. 249 or email FIPCO IT Services for more information.

"Make Security Part of You and Your Institution's DNA!"

Threat Intelligence Newsletter: May 19, 2023

FIPCO®
IT Audit
Round Table
Discussions

Upcoming Threat Intelligence Peer Group Discussions
None available at the current time

****

Alerts & Warnings

BBB Scam Alert: This solicitation looks like a notice about your mortgage. Here's how to spot it.
You receive a letter that appears to come from your mortgage provider. It's allegedly from the company's "Home Warranty Dept," and claims that your home warranty must be renewed. Before worrying, look closely at the letter and see what's happening. One BBB Scam Tracker report noticed: "At the very bottom of the letter in small print is the comment, 'Not all consumers have previous coverage. We are not affiliated with your current mortgage.'" Another homeowner reported: "The mailing is made to look like a check: it has the tear-away sides and inside is a 'Renewal Fee Voucher' for $199.00. It's not a check: it's an attempt to get you sign up for a home warranty."
https://www.bbb.org/article/scams/28701-bbb-scam-alert-this-solicitation-looks-like-a-notice-about-your-mortgage-heres-how-to-spot-it

Microsoft Teams Features Amp Up Orgs' Cyberattack Exposure
It's as they say: Teams is only as strong as its weakest links. Microsoft's collaboration platform offers Tabs, Meetings, and Messages functions, and they all can be exploited. Researchers have identified several ways hackers can leverage Microsoft Teams functionalities to phish users, or deliver malware directly to their computers without their knowing it.
https://www.darkreading.com/remote-workforce/microsoft-teams-features-amp-up-orgs-cyberattack-exposure

New Phishing-as-a-Service Tool Used in the Wild to Target Organizations
Cisco Talos researchers recently discovered that threat actors are targeting Microsoft 365 via the Greatness Phishing-as-a-Service (PhaaS) platform. The Greatness platform surged operations between December 2022 and March 2023, targeting Microsoft 365 users in the U.S., U.K. Canada, Australia, and South Africa. The victims primarily came from the manufacturing, healthcare, technology, and education sectors in the United States.
https://www.oodaloop.com/cyber/2023/05/12/new-phishing-as-a-service-tool-used-in-the-wild-to-target-organizations/

Bank Failure Scams, Fake Stamps, and Love Lies
Scammers are trying to cash in on news about recent bank failures by trying to scare customers into handing over their account details or transferring their deposits to sham accounts. Many financial institutions have issued warnings to their customers. For example, online bank CapitalOne says: "Scammers are using this moment of change to take advantage of unsuspecting customers. By preying on common anxieties, fraudsters can trick you into sending money to a phony bank account or providing your personal banking information."
https://scambusters.org/bankfailure.html

Is Microsoft OneNote Emailing You Malware? What To Know, What To Do
Microsoft's OneNote is making news, but not in the way the software giant would hope. OneNote, the note-taking app that's part of Microsoft Office, is being weaponized by QBot threat actors. Fans of OneNote, whether for business or personal use, should know QBot's email phishing campaign leads to stolen passwords, hijacked financial and browser data, and just about anything else there is to steal.
https://www.sosdailynews.com/news.jspx?&articleid=2D76948E6CAA44A9CFF1FA2B37513414

****

Hints & Tips plus Security Awareness

Why and how to report a ransomware attack
The majority of ransomware attacks go unreported, creating a blind spot that hampers response, recovery efforts and the prevention of future attacks. Ransomware attacks are notoriously underreported and cyber authorities acknowledge this incomplete data on ransomware activity creates a blind spot that hampers recovery, response efforts and the prevention of future attacks.
https://www.cybersecuritydive.com/news/how-report-ransomware-attack/650631

How CIOs overcome internal resistance to digital transformation
Modernization requires realigning company culture to support innovation — and executive leadership can drive that change. Technology may be the prime mover of enterprise modernization. But even the most potent tools are only as good as the hands that wield them.
https://www.ciodive.com/news/MIT-Sloan-CIO-Symposium-tech-change-management-leadership/650517/

****

News & Views

Flood of ransom payments continues as officials mull ban
The revived debate over the viability of a ransom payment ban comes down to the cost ransomware is causing organizations globally. As the White House floats the possibility of a ban on ransom payments, the number of organizations hit by ransomware that ultimately pay a ransom remains high.
https://www.cybersecuritydive.com/news/officials-mull-ban-ransom-payments-flood/650067

Apple Boots a Half-Million Developers From Official App Store

The mobile phone and MacBook giant also rejected nearly 1.7 million app submissions last year in an effort to root out malware and fraud. The Apple App Store supports more than 36 million registered Apple developers, but not all of those coding partners are benign. In a report on App Store safety this week, the computing giant noted that last year it booted nearly a half-million (428,000) developer accounts from the platform for carrying out fraud and abuse.
https://www.darkreading.com/cloud/apple-boots-half-million-devs-official-app-store

Making Sure Lost Data Stays Lost

Retired hardware and forgotten cloud virtual machines are a trove of insecure confidential data. Here's how to ameliorate that weakness. The stories are both infamous and legendary. Surplus computing equipment purchased at auction contains thousands of files with private information, including employee health records, banking information, and other data covered by a multitude of state and local privacy and data laws.
https://www.darkreading.com/edge-articles/making-sure-lost-data-stays-lost

Questions
Contact FIPCO’s Rob Foxx at 800-722-3498 ext. 249 or email FIPCO IT Services for more information.

"Make Security Part of You and Your Institution's DNA!"

Threat Intelligence Newsletter: May 26, 2023

Upcoming Threat Intelligence Peer Group Discussions
None available at the current time

****

Alerts & Warnings

BBB Scam Alert: How to stay safe when paying medical bills
If you get an unexpected message saying you owe money for medical services, think twice before you make a payment. BBB Scam Tracker has received reports about phony medical bills and collections departments. You receive a letter or a call informing you that you owe money on a medical bill. If you follow up, the "billing department" will insist that you need to pay immediately. If you don't, you will allegedly face consequences, such as fines, damage to your credit score, or even jail time. Eager to settle your debts, you provide your credit or debit card number. But before you pay, the scammer will ask you to confirm your name, address, and other sensitive information, which may include your Social Security or bank account number.
https://www.bbb.org/article/scams/28739-bbb-scam-alert-how-to-stay-safe-when-paying-medical-bills

BEC attacks rise as criminal hackers employ new tactics to evade detection
Business email compromise attacks are on the rise and becoming more sophisticated as threat actors are shifting tactics to evade detection, Microsoft found.
https://www.cybersecuritydive.com/news/bec-attacks-hackers-tactics-detection/650993

12 Facebook Marketplace Scams And How To Beat Them
A car buyer on the lookout for a new truck allegedly got taken for a ride to the tune of $15,000 after she spotted an enticing ad on Facebook Marketplace. She drove for four hours with a stack of cash for a parking lot meet-up, handed it over to the supposed seller while in the cab of the new truck, and was then ordered out at gunpoint, allowing the alleged crook to drive away. This was at the extreme end of a dollar range of Marketplace scams that happen every day in the US.
https://scambusters.org/marketplace.html

MALWARE & THREATS Millions of Smartphones Distributed Worldwide With Preinstalled 'Guerrilla' Malware
A threat actor tracked as Lemon Group has control over millions of smartphones distributed worldwide thanks to preinstalled Guerrilla malware. A threat actor has control over millions of smartphones distributed worldwide thanks to a piece of malware that has been preinstalled on the devices, Trend Micro warned.
https://www.securityweek.com/millions-of-smartphones-distributed-worldwide-with-preinstalled-guerrilla-malware

Are You Hacker-Bait? Phishing Malware Lets Picky Attackers Decide
If you've ever wondered if you're a juicy target for a cyberattack, don't fret because there's a new malware allowing bad actors to decide that for you. It's a creepy thought, but there's a new email phishing campaign installing malware that takes screenshots of a device and its contents and sends them to the hacker. If the data is deemed hack-worthy, it's the beginning of a financial nightmare for the chosen victims.
https://www.sosdailynews.com/news.jspx?&articleid=4E016D591898A7BFF77636782ED33F9B

****

Hints & Tips plus Security Awareness

Why and how to report a ransomware attack
The majority of ransomware attacks go unreported, creating a blind spot that hampers response, recovery efforts and the prevention of future attacks. Ransomware attacks are notoriously underreported and cyber authorities acknowledge this incomplete data on ransomware activity creates a blind spot that hampers recovery, response efforts and the prevention of future attacks.
https://www.ciodive.com/news/how-report-ransomware-attack/650779

10 Types of AI Attacks CISOs Should Track
Risk from artificial intelligence vectors presents a growing concern among security professionals in 2023. As CISOs work to future proof their cybersecurity strategy and infrastructure for tomorrow's emerging threats, artificial intelligence (AI) attacks are looming large in their thoughts. Even without the hype that's billowed around ChatGPT and generative AI's skyrocketing popularity, AI risk has started to unfold as a growing concern among security researchers and pundits in 2023.
https://www.darkreading.com/threat-intelligence/10-types-of-ai-attacks-cisos-should-track

Android Fingerprint Biometrics Fall to 'BrutePrint' Attack
Dictionary Attack Plus Neural Network Fools Security Checks, Researchers Find. Security researchers have demonstrated a practical attack that can be used to defeat biometric fingerprint checks and log into a target's Android smartphone.
https://www.databreachtoday.com/android-fingerprint-biometrics-fall-to-bruteprint-attack-a-22130

Email Phishing Spikes 569% in 2022 – What You Need To Know Now
If it looks like your inbox has more email phishing than ever, there's a good reason for that. Cofense released its "2023 Annual State of Email Security Report" a study of last year's email phishing trends. Their report found a walloping 569% spike in these phishing threats to organizations globally, along with other eye-opening results.
https://www.sosdailynews.com/news.jspx?&articleid=CEE7EF8EDA667EF27E0F359D543078B3

QR Code Scanning Scams – How To Use QR's Safely And Securely
In our never-ending pursuit of info-quick technology, QR (quick response) codes have found a huge following. In return, these codes seem to be everywhere and on everything. From TV screens to product packaging, web pages, and more, QR codes are easy to find. But like most technology we've grown to love, cybercriminals love it too but for very different reasons.
https://www.sosdailynews.com/news.jspx?&articleid=C5C58E78436C261FB2F67F76A2DF057B

****

News & Views

Why cyber is also a CIO problem
When an incursion occurs, IT teams need a recovery plan and backup systems ready to deploy.
https://www.ciodive.com/news/Cybersecurity-CIO-resilience-MIT-Sloan-Symposium/650695

Global Threat Intelligence Report
Delivering Actionable and Contextualized Intelligence to Increase Cyber Resilience. To effectively manage risk, security leaders must continually analyze the global threat landscape and understand how business decisions can influence their organization's threat profile. Similarly, business leaders require awareness of how security posture, risk exposure, and cyber defense strategy can affect their business operations.
https://www.blackberry.com/us/en/solutions/threat-intelligence/2023/threat-intelligence-report-april

****

"Ctrl -F" for The Board

Salary ranges are growing in tech hub job postings, Indeed finds
Compensation ranges across job postings have widened over the past year in areas with a large tech industry footprint, according to an Indeed report published Thursday.
https://www.ciodive.com/news/salary-ranges-indeed-tech-hubs/650926/

Questions
Contact FIPCO's Rob Foxx at 800-722-3498 ext. 249 or email FIPCO IT Services for more information.

"Make Security Part of You and Your Institution's DNA!"

Threat Intelligence Newsletter: June 5, 2023

FIPCO®
IT Audit
Round Table
Discussions

Upcoming Threat Intelligence Peer Group Discussions
None available at the current time

****

Alerts & Warnings

BBB Scam Alert: How to avoid scams when booking a hotel online
If you are planning an upcoming trip, keep an eye out for hotel booking scams. BBB Scam Tracker has gotten multiple reports of travelers falling victim to lookalike websites. Always confirm you are on the right website before making hotel reservations. You search for hotels in the city you plan to visit. Among the top search results is what appears to be an official hotel website or a legitimate travel booking agency. When you click the link, you find a website with professional photos from the hotel and reasonable pricing.
https://www.bbb.org/article/scams/28768-bbb-scam-alert-how-to-avoid-scams-when-booking-a-hotel-online

Microsoft Catches Chinese .Gov Hackers Targeting US Critical Infrastructure
In a campaign called Volt Typhoon, Microsoft says Chinese government hackers were siphoning data from critical infrastructure organizations in Guam, a U.S. territory in the Pacific Ocean. Microsoft says it has caught Chinese state-backed hackers siphoning data from critical infrastructure organizations in Guam, a U.S. territory in the Pacific Ocean. The discovery of Chinese-made cyberespionage malware in Guam is raising eyebrows because the tiny island is considered an important part of a future China/Taiwan military conflict.
https://www.securityweek.com/microsoft-catches-chinese-gov-hackers-in-guam-critical-infrastructure-orgs/

Organizations Warned of Backdoor Feature in Hundreds of Gigabyte Motherboards
A backdoor feature found in hundreds of Gigabyte motherboard models can pose a significant supply chain risk to organizations. Researchers at firmware and hardware security company Eclypsium discovered that hundreds of motherboard models made by Taiwanese computer components giant Gigabyte include backdoor functionality that could pose a significant risk to organizations.
https://www.securityweek.com/organizations-warned-of-backdoor-feature-in-hundreds-of-gigabyte-motherboards/

Online Romancers Tricked Into Becoming Money Mules

Scammers are tricking lonely hearts, mostly older or vulnerable romance-seekers, to act as money mules, laundering their stolen money. Cops call them "fraud facilitators," people who, sometimes unwittingly, play a key role in handling the proceeds of crime on behalf of crooks.
https://scambusters.org/moneymule2.html

Don't Click That ZIP File! Phishers Weaponizing .ZIP Domains to Trick Victims

A new phishing technique called "file archiver in the browser" can be leveraged to "emulate" a file archiver software in a web browser when a victim visits a .ZIP domain. "With this phishing attack, you simulate a file archiver software (e.g., WinRAR) in the browser and use a .zip domain to make it appear more legitimate," security researcher mr.d0x disclosed last week.
https://thehackernews.com/2023/05/dont-click-that-zip-file-phishers.html

MOVEit Transfer Critical Vulnerability (May 2023)

Progress has discovered a vulnerability in MOVEit Transfer that could lead to escalated privileges and potential unauthorized access to the environment. If you are a MOVEit Transfer customer, it is extremely important that you take immediate action as noted below in order to help protect your MOVEit Transfer environment, while our team produces a patch.
https://community.progress.com/s/article/MOVEit-Transfer-Critical-Vulnerability-31May2023

****

Hints & Tips plus Security Awareness

Ahead of summer holiday weekends, IT security leaders brace for deliberate cyber mischief

Recent history shows holiday weekends and vacations provide an attack surface bonanza for threat actors. Memorial Day weekend marks the unofficial start to the summer travel season and with it the potential for vacation-aligned network intrusions. U.S. authorities and network defenders in the private sector are quietly paying attention to potential threats that may emerge during key holiday weekends over the next three months.
https://www.cybersecuritydive.com/news/summer-holiday-weekends-cyber/651434

6 Steps to Effectively Threat Hunting: Safeguard Critical Assets and Fight Cybercrime

Finding threat actors before they find you is key to beefing up your cyber defenses. How to do that efficiently and effectively is no small task – but with a small investment of time, you can master threat hunting and save your organization millions of dollars. Consider this staggering statistic. Cybersecurity Ventures estimates that cybercrime will take a $10.5 trillion toll on the global economy by 2025. Measuring this amount as a country, the cost of cybercrime equals the world's third-largest economy after the U.S. and China. But with effective threat hunting, you can keep bad actors from wreaking havoc on your organization.
https://thehackernews.com/2023/05/6-steps-to-effective-threat-hunting.html

****

News & Views

CISA updates ransomware guide 3 years after its debut
The Cybersecurity and Infrastructure Security Agency for the first time since 2020 released an updated version of #StopRansomware, in partnership with the FBI, National Security Agency and the Multi-State Information Sharing and Analysis Center.
https://www.cybersecuritydive.com/news/cisa-updates-ransomware-guide-3-years/651145

****

"Ctrl -F" for The Board

The talent race is still on: Managing high demand for IT professionals
CIOs must reinvent their employee value proposition to attract and retain critical workers and execute digital aspirations. Organizations across the world are racing to compress decades worth of digital transformation and technology adoption into only a few years. This changes the IT talent search significantly, escalating competition to secure top technology talent.
https://www.ciodive.com/news/tech-talent-IT-CIO-Gartner/651423/

IT security budgets are shifting as companies target risk reduction
Organizations are designing their security spending around keeping the business secure and operations running smoothly. Despite the impact that cyber incidents have on an organization's overall business operations, security spending remains within the purview of the IT budget, albeit a small part. In 2022, IT security made up just 5.2% of IT budgets, according to research from Gartner.
https://www.ciodive.com/news/it-security-spending-shifts/651316/

Will Credit Monitoring Keep Me Safe?
Will credit monitoring alone safeguard you against identity theft? In a nutshell, the answer is a resounding "no." Credit monitoring and identity theft protection services both have their pros and cons. But if you are offered these services as a result of a data breach or other cyber incident, it's important to know what they are and do…and what they are not and don't and whether a credit freeze is really what you need.
https://www.sosdailynews.com/news.jspx?&articleid=8296DA911B889962C494235EFBC70394

Questions
Contact FIPCO's Rob Foxx at 800-722-3498 ext. 249 or email FIPCO IT Services for more information.

"Make Security Part of You and Your Institution's DNA!"

Threat Intelligence Newsletter: June 12, 2023

FIPCO®
IT Audit
Round Table
Discussions

Upcoming Threat Intelligence Peer Group Discussions
None available at the current time

****

Alerts & Warnings

Clop claims hundreds of MOVEit vulnerability victims
The prolific threat actor is responsible for two of the three high-profile, actively exploited vulnerabilities in file-transfer services so far this year. Cyber authorities are warning organizations that use Progress Software's MOVEit file transfer service to gird for widespread exploitation of the zero-day vulnerability the vendor first disclosed last week.
https://www.cybersecuritydive.com/news/clop-claims-hundreds-victims-moveit-vulnerability/652443

FBI: Sextortionist Campaigns Use Deepfakes to Target Children, Adults
Threat actors are lifting public images and videos from the Internet, altering them, and posting them online in a new wave of sextortion campaigns. Threat actors are manipulating stolen images and videos using artificial intelligence (AI) to create deepfakes that show innocent people — including minor children and non-consenting adults — in fake but explicit sexual activity. It's part of a growing new wave of sextortionist scams, the FBI is warning.
https://www.darkreading.com/attacks-breaches/fbi-sextortionist-campaigns-deepfakes-children-adults

Barracuda Urges Replacing — Not Patching — Its Email Security Gateways
It's not often that a zero-day vulnerability causes a network security vendor to urge customers to physically remove and decommission an entire line of affected hardware — as opposed to just applying software updates. But experts say that is exactly what transpired this week with Barracuda Networks, as the company struggled to combat a sprawling malware threat which appears to have undermined its email security appliances in such a fundamental way that they can no longer be safely updated with software fixes.
https://krebsonsecurity.com/2023/06/barracuda-urges-replacing-not-patching-its-email-security-gateways/

New ChatGPT Attack Technique Spreads Malicious Packages
A new cyber-attack technique using the OpenAI language model ChatGPT has emerged, allowing attackers to spread malicious packages in developers' environments. Vulcan Cyber's Voyager18 research team described the discovery in an advisory published today.
https://www.infosecurity-magazine.com/news/chatgpt-spreads-malicious-packages/

Verizon Warns of Common Smishing Scams
According to Verizon, one of the leading telecommunications companies, smishing (SMS phishing) is an increasingly prevalent form of cyber-attack targeting mobile phone users. Smishing messages are deceptive text messages that aim to trick individuals into divulging sensitive information or performing harmful actions. Verizon has identified several common types of these types of messages that users should be aware of to protect themselves from falling victim to these scams.
https://www.sosdailynews.com/news.jspx?&articleid=114B7F06ABFE4EE61CBFDFB218B1CECD

****

Hints & Tips plus Security Awareness

A CISO's View: How to Handle an Insider Threat
How does an employee get blackmailed into breaching company systems? It can be as simple as someone threatening their family and then saying, "Just stick this thumb drive into computer X located in this building and you won't hear from us again."
https://www.databreachtoday.com/blogs/cisos-view-how-to-handle-insider-threat-p-3420

****

News & Views

Interagency Guidance on Risks Associated with Third-Party Relationships
The FDIC and the other federal bank regulatory agencies today issued final joint guidance designed to help banking organizations manage risks associated with third-party relationships, including relationships with financial technology companies. Below are the materials made available:
https://www.fdic.gov/news/financial-institution-letters/2023/fil23029a.pdf
IMPORTANT REGULATION CHANGE FOR ALL IT AND INFOSEC PROFESSIONALS WITHIN THE BANKING SPHERE

Threat actors can use ChatGPT to sharpen cyberthreats, but no need to panic yet
Startling dangers, such as autonomous attack mechanisms and sophisticated malware coding, have yet to materialize. For now, the threat is more specific. ChatGPT has taken the world by storm and as it makes waves for consumers and business alike, security experts are wary of threat actors turning to generative AI for nefarious purposes. It’s a cause for worry, but not full-on panic.
https://www.cybersecuritydive.com/news/chatgpt-sharpen-cyberthreats/648292/

Verizon: When Ransomware Attacks Cost, They're Costing More
Ransom Payment Amounts Drop as Cleanup Costs Rise, Finds Annual Data Breach Report. Criminals are continuing to wield stolen credentials, ransomware and social engineering attacks to earn an illicit payday, Verizon found in its latest annual analysis of data breaches and how they happened.
https://www.databreachtoday.com/verizon-when-ransomware-attacks-cost-theyre-costing-more-a-22233

****

"Ctrl -F" for The Board

FBI 2022 INTERNET CRIME REPORT Over 800,000 Cybercrime Complaints, Losses Over $10 Billion
The introduction of the most recent FBI Internet Crime Report says, “At the FBI, we know ‘cyber risk is business risk’ and ‘cybersecurity is national security.’” And the numbers in the report back up this statement. The FBI report details more than 800,000 cyber crime-related complaints filed in 2022. Meanwhile, total losses were over $10 billion, shattering 2021’s total of $6.9 billion, according to the bureau’s Internet Crime Complaint Center (IC3). In the past five years, the IC3 received a total of 3.26 million complaints for $27.6 billion in losses. During 2022, the top five cyber crime types were:
https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf

Questions
Contact FIPCO’s Rob Foxx at 800-722-3498 ext. 249 or email FIPCO IT Services for more information.

"Make Security Part of You and Your Institution's DNA!"

Threat Intelligence Newsletter: June 16, 2023

FIPCO®
IT Audit
Round Table
Discussions

Upcoming Threat Intelligence Peer Group Discussions
None available at the current time

****

Alerts & Warnings

BBB Scam Alert: How to spot a credit check scam when apartment shopping
Moving this summer? Watch out for a new twist on fake rental ads. According to multiple BBB Scam Tracker reports, scammers use fake tenant credit checks to trick potential renters into compromising sensitive personal information.
https://www.bbb.org/article/scams/28841-bbb-scam-alert-how-to-spot-a-credit-check-scam-when-apartment-shopping

Verizon DBIR: Social Engineering Breaches Double, Leading to Spiraling Ransomware Costs
Ransomware continues its runaway growth with median payments reaching $50,000 per incident. A full three-quarters of data breaches in the last year (74%) involved the human element, mainly caused by employees either falling for social engineering attacks or making errors, with some misusing their access maliciously.
https://www.darkreading.com/threat-intelligence/verizon-dbir-social-engineering-breaches-spiraling-ransomware-costs

Brand-New Security Bugs Affect All MOVEit Transfer Versions (Second Breach)
Progress has issued a second patch for additional SQL flaws that are distinct from the zero-day that the Cl0p ransomware gang is exploiting. Just days after Progress Software patched a widely exploited zero-day vulnerability in its MOVEit Transfer app, the company has issued a second patch to address additional SQL Injection vulnerabilities in it that a security vendor uncovered during a code review this week.
https://www.darkreading.com/vulnerabilities-threats/brand-new-security-bugs-affect-all-moveit-transfer-versions

CISA Order Highlights Persistent Risk at Network Edge
The U.S. government agency in charge of improving the nation's cybersecurity posture is ordering all federal agencies to take new measures to restrict access to Internet-exposed networking equipment. The directive comes amid a surge in attacks targeting previously unknown vulnerabilities in widely used security and networking appliances.
https://krebsonsecurity.com/2023/06/cisa-order-highlights-persistent-risk-at-network-edge/

Verizon Warns of Uptick In SIM Swapping To Swap Their Scam For Your PII
SIM swapping, also called SIM hijacking, is when sneaky hackers get control of your mobile phone account and simply transfer your service to their own device, including your phone number. Once they manage to do that, they can access all your phone data and important accounts. Essentially, consider that if you can access it from your phone, so can they.
https://www.sosdailynews.com/news.jspx?&articleid=2B943625344277409149398B9E3BBCA39

Hijacking S3 Buckets: New Attack Technique Exploited in the Wild by Supply Chain Attackers
Without altering a single line of code, attackers poisoned the NPM package "bignum" by hijacking the S3 bucket serving binaries necessary for its function and replacing them with malicious ones. While this specific risk was mitigated, a quick glance through the open-source ecosystem reveals that dozens of packages are vulnerable to this same attack.
https://checkmarx.com/blog/hijacking-s3-buckets-new-attack-technique-exploited-in-the-wild-by-supply-chain-attackers/

****

Hints & Tips plus Security Awareness

Securing Your Online Financial Accounts – Can You Afford Not To?
Most of us would agree technology makes online banking a breeze. No more trips to the brick-and-mortar, parking, or waiting in line. But with that ease comes the reality that our financial accounts are vulnerable and valuable cybercrime targets. The best answer to that risk is being proactive about your online banking security. This is the first of a two-part look at steps you can take to further secure your own accounts. After all, can you afford not to?
https://www.sosdailynews.com/news.jspx?&articleid=AE7F636D0370FEB2B211DD9802231F25

****

News & Views

Half of IT employers are upskilling workers to overcome staffing woes
Emerging technologies such as AI and virtual reality could help with hiring and training, according to an Experis report. More than three-quarters of IT organizations are reporting difficulty finding talent with the right skills, and half are now training and upskilling their current workforce to address their challenges, according to a June 8 report from Experis, an IT professional resourcing firm and part of ManpowerGroup.
https://www.ciodive.com/news/IT-employers-upskilling-workers-tech/652900/

Is Your Email Account Hacked? What You Need To Know
The reality is these days, stolen email addresses are a dime a dozen. Thanks to relentless data breaches, it's safe to assume your email address is already in the wrong hands. Although it may not sound like much, it's a goldmine for further crimes involving you.
https://www.sosdailynews.com/news.jspx?&articleid=27A9FE04A8C665E012FA3AFBEFB10497

****

"Ctrl -F" for The Board

Children As Online Targets--What Every Parent Needs To Know
Adults should be well-aware of hacking and the risks involved when traversing online. But what many don't know is the sad truth that children are also targets of online abuse. Sadly, this includes infants. The good news is that parents aren't helpless when it comes to protecting their child's online activities and real-world identities. Knowing the signs of child identity theft, other harmful vulnerabilities and how you can help prevent them is a great way to start.
https://www.sosdailynews.com/news.jspx?&articleid=9A3F3A756BBD22C461CB7A120B5ED73D

Questions
Contact FIPCO's Rob Foxx at 800-722-3498 ext. 249 or email FIPCO IT Services for more information.

"Make Security Part of You and Your Institution's DNA!"

Threat Intelligence Newsletter: June 23, 2023

Upcoming Threat Intelligence Peer Group Discussions
None available at the current time

****

Alerts & Warnings

Consumers in the US lost $330 million to text scams in 2022, FTC says
Consumers have lost a whopping $330 million to SMS scams in 2022, according to the Federal Trade Commission's latest report. The analysis shows that financial losses more than doubled from the previous year, with attackers focused on taking advantage of users' carelessness and increased usage of mobile phones to shop, bank or even work.
https://www.bitdefender.com/blog/hotforsecurity/consumers-in-the-us-lost-330-million-to-text-scams-in-2022-ftc-says/

Ransomware Misconceptions Abound, to the Benefit of Attackers
It's time to update what we think we understand about ransomware, including new defensive measures and how fast the attack response should be. INFOSEC23 – London – With a threat as persistently pervasive as ransomware, myths and misconceptions are bound to emerge in tandem. Richard de la Torre, technical marketing manager at Bitdefender, used his time at the podium during this week's Infosecurity Europe conference to enumerate — and dispel — some of the more common ones.
https://www.darkreading.com/vulnerabilities-threats/ransomware-misconceptions-abound-to-the-benefit-of-attackers

Third MOVEit Transfer Vulnerability Disclosed by Progress Software
MOVEit has created a patch to fix the issue and urges customers to take action to protect their environments, as Cl0p attacks continue to mount, including on government targets. Yet another MOVEit Transfer vulnerability, CVE-2023-35708, was discovered this week by Progress Software, the third that the company has disclosed, alongside CVE-2023-34362 and CVE-2023-35036.
https://www.darkreading.com/vulnerabilities-threats/third-moveit-transfer-vulnerability-progress-software

Candy Scammers Use Your Phone And Zelle To Steal Your $$$
A woman sitting at a New York City café was approached by two kids selling candy for a supposedly worthy cause. That's when the two candy scammers went to work pulling her into their scheme. The end result for the victim was having all the funds in her banking account stolen; not just $5 for a candy bar. That's how easily this scam started, and she learned the hard way about smartphone scam security and P2P (peer-to-peer) payment apps like Zelle.
https://www.sosdailynews.com/news.jspx?&articleid=C9E5F64CBE680AFF050D7E6A5101CE0B

Barracuda Warns of Breach in ESG Appliances: Urges Immediate Patching or Replacement
In late May, Barracuda Networks, the network security solutions provider, issued a warning to its customers about a recent breach affecting some of its Email Security Gateway (ESG) appliances. According to the company, this device is used in more than 200,000 organizations. It turns out that threat actors took advantage of a zero-day vulnerability that has since been patched.
https://www.sosdailynews.com/news.jspx?&articleid=DCAB37F1BC2960764BDE53A6CF79C846

Gift Cards Being Used For Payment In BEC Scams, And What You Need To Know
Over the years, gift cards have become an enormous "go to" way of giving. Mageplaza found the purchase of gift cards this year will reach nearly $450 billion globally. And like many things involving monetary value and being human, cyber-scammers are exploiting gift cards for profit. They're now combining gift card fraud with the world's most lucrative cybercrime, business email compromise (BEC) attacks.
https://www.sosdailynews.com/news.jspx?&articleid=86936C5F2E4B4DFD2064832295BC0B68

****

Hints & Tips plus Security Awareness

Cybercrime Doesn't Take a Vacation
Organizations need to prepare for security threats as summer holidays approach. Summer is just around the corner, and every cybersecurity professional I know is braced for cybercriminals to take action. The Cybersecurity ad Infrastructure Security Agency (CISA), part of the Department of Homeland Security, warns that holidays are a period of heightened threat. That can be extrapolated to any time cybercriminals think IT security teams might be lean or preoccupied, such as the summer season, when workers typically take more time off and stay out of the office for longer.
https://www.darkreading.com/vulnerabilities-threats/cybercrime-doesnt-take-a-vacation

10 Important Security Tasks You Shouldn't Skip
Time and money are valuable and finite, but some actions are well worth spending those resources on. Most of us have benefited from the mistakes of others. While this may sound like an odd statement, it makes a lot of sense when you think about it. For those of us who have been fortunate enough to have others share their missteps with us and are smart enough to internalize and apply those lessons to our lives, we learn not to repeat their mistakes.
https://www.darkreading.com/edge/10-important-security-tasks-you-shouldn-t-skip

Securing Your Online Banking Accounts – Phishing Red Flags
As we saw in Part One, creating secure passwords for your online financial accounts is the first step to protecting them. Here in Part Two, knowing how to spot the red flags of email phishing when you see them is another essential security step to take. After all, can you afford not to?
https://www.sosdailynews.com/news.jspx?&articleid=AE9EF0ECD236B3EE5B07E38E99967810

****

News & Views

Why It's Risky to Neglect Mobile App Security
With competing demands, dev teams are often unable to prioritize mobile app security. Learn more about properly securing mobile apps and the cost if you don't. In the past few years, the growth of mobile phone ownership and usage triggered an increase in attention from threat actors. Today, there are more than 6 billion smartphones, which can access over 5 million apps. Additionally, mobile apps account for 90% of mobile phone use as compared to a mobile browser.
https://www.informationweek.com/security-and-risk-strategy/why-it-s-risky-to-neglect-mobile-app-security#

LastPass CEO reflects on lessons learned, regrets and moving forward from a cyberattack
Karim Toubba is ready to talk nearly a year after LastPass suffered a cyberattack that became one of the biggest security blunders of 2022. Karim Toubba didn't have much of a honeymoon at LastPass. Less than four months after he joined the company as CEO, a cyberattack that would evolve into one of the most high-profile security blunders of 2022 was underway.
https://www.cybersecuritydive.com/news/lastpass-ceo-reflects-cyberattack/652818

****

"Ctrl -F" for The Board

Cool Off With Quick Social Engineering Refresher
Let's dive into the world of social engineering and its impact on our lives, shall we? Brace yourself for a friendly reminder about this sneaky psychological manipulation technique that can really mess with your day. Picture this: someone cleverly exploits your mind to get you to do their bidding or spill sensitive information. It could never happen to you, right?
https://www.sosdailynews.com/news.jspx?&articleid=6B8608385CE6F24530537A42315BC9A7

Questions
Contact FIPCO's Rob Foxx at 800-722-3498 ext. 249 or email FIPCO IT Services for more information.

"Make Security Part of You and Your Institution's DNA!"

Threat Intelligence Newsletter: June 30, 2023

Upcoming Threat Intelligence Peer Group Discussions
None available at the current time

****

Alerts & Warnings

Patch Now: Cisco AnyConnect Bug Exploit Released in the Wild
A ready-made, low-complexity path to pwning the popular enterprise VPN clients for remote workers is now circulating in the wild. A security researcher has dropped a proof-of-concept (POC) exploit for a just-patched, high-severity security vulnerability in Cisco's client software for remote workers looking to connect to VPNs.
https://www.darkreading.com/application-security/patch-now-cisco-anyconnect-bug-exploit-released

BBB Scam Alert: Spot the scam before paying big bucks for Taylor Swift tickets
Tickets to Taylor Swift's Eras Tour have been in high demand since they first went on sale. With most tour dates sold out, fans searching for tickets have turned to ticket resellers, where even the cheapest seats sell for hundreds of dollars. Unfortunately, scammers have noticed the high demand and target Swifties with ticket scams. So far in 2023, BBB Scam Tracker has gotten about 30 reports involving fake Taylor Swift tickets.
https://www.bbb.org/article/scams/28902-bbb-scam-alert-spot-the-scam-before-paying-big-bucks-for-taylor-swift-tickets

AI linked to new crop of business email scams
Generative artificial intelligence tools such as ChatGPT could be aiding the proliferation of more convincing email scams aimed at stealing money from businesses, according to cybersecurity firm Fortra.
https://www.ciodive.com/news/AI-business-email-compromised/654075/

Job Seekers, Look Out for Job Scams
Scammers are setting out lures for people looking for work. If a position sounds too good to be true, it probably is. The economic downturn is already a devastating blow to job seekers everywhere. Now scammers are taking advantage of the situation by ramping up their methods of swindling people.
https://www.darkreading.com/edge/job-seekers-look-out-for-job-scams

Microsoft Teams Attack Skips the Phish to Deliver Malware Directly
Exploiting a flaw in how the app handles communication with external tenants gives threat actors an easy way to send malicious files from a trusted source to an organization's employees, but no patch is imminent.
https://www.darkreading.com/vulnerabilities-threats/microsoft-teams-attack-phish-deliver-malware-directly

2 More Apple Zero-Days Exploited in Ongoing iOS Spy Campaign
The zero-day security bugs are being used to deploy the sophisticated but "odd" TriangleDB spying implant on targeted iOS devices. Apple has released emergency patches for two new zero-day vulnerabilities in its software that an advanced persistent threat (APT) actor has been using to deploy malware in an ongoing iOS spying campaign dubbed "Operation Triangulation."
https://www.darkreading.com/endpoint/more-apple-zero-days-exploited-ios-spying-campaign

****

Hints & Tips plus Security Awareness

6 strategies for optimizing the security of your SaaS stack
At some point in your tenure as a business leader, you've likely been asked, "What keeps you up at night?" My answer is the same as that of any IT leader I know — data breaches, cyber attacks and other incidents that endanger the privacy and security of customers and colleagues alike.
https://www.ciodive.com/spons/6-strategies-for-optimizing-the-security-of-your-saas-stack/653536/

OpenTable Advises Diners To Close The Door On Payment Card Scams
The hospitality industry is not immune to credit card scams. With the increasing reliance on digital payment methods, criminals have become more sophisticated in exploiting vulnerabilities and stealing sensitive financial information. Recently, the restaurant reservations platform, OpenTable, sent a letter to users warning of an uptick in scams targeting diners and advised all restaurant-goers to be aware of the risks and how to avoid choosing that menu item.
https://www.sosdailynews.com/news.jspx?&articleid=458DFD2C75EB38091ABD509C0FFB151B

****

News & Views

Why Legacy System Users Prioritize Uptime Over Security
For line-of-business execs, the fear of mission-critical systems grinding to a halt overrides their cybersecurity concerns. How can CISOs overcome this? Dirk Hodgson, the director of cybersecurity for NTT Australia, tells a story. He once worked with a company that did scientific measurements. The highly specialized firm used highly specialized equipment, and one large piece of equipment cost them $2 million when purchased years ago.
https://www.darkreading.com/edge/why-legacy-system-users-prioritize-uptime-over-security

Growing SaaS Usage Means Larger Attack Surface
Software-as-a-service has its benefits, but abandoned SaaS integrations and idle data sharing introduce risk to the enterprise. Macro trends such as the shift to cloud services, a growing remote (or hybrid) workforce, and heavy reliance on third-party partners and contractors mean organizations are working with more software-as-a-service (SaaS) applications than ever. It also means that attackers are taking advantage of the ubiquity of SaaS as they target insecure default configurations and weakly secured identities.
https://www.darkreading.com/dr-tech/growing-saas-usage-means-larger-attack-surface

A.I. has a discrimination problem. In banking, the consequences can be severe
Deloitte notes that AI systems are ultimately only as good as the data they're given: Incomplete or unrepresentative datasets could limit AI's objectivity, while biases in development teams that train such systems could perpetuate that cycle of bias.
https://www.cnbc.com/2023/06/23/ai-has-a-discrimination-problem-in-banking-that-can-be-devastating.html

****

"Ctrl -F" for The Board

3 Steps to Successfully & Ethically Navigate a Data Breach
In this day of "not if, but when" for breaches, transparency and full disclosure are important to salvage a company's reputation and keep public trust. According to the latest report from the Identity Theft Research Center, there were 1,802 data breaches affecting more than 422 million victims in 2022. In today's volatile threat landscape, it's no longer a question of if your organization gets breached, but when — and more importantly, how — you will respond.
https://www.darkreading.com/attacks-breaches/3-steps-successfully-ethically-navigate-data-breach

Questions
Contact FIPCO's Rob Foxx at 800-722-3498 ext. 249 or email FIPCO IT Services for more information.

"Make Security Part of You and Your Institution's DNA!"

Threat Intelligence Newsletter: July 7, 2023

FIPCO®
IT Audit
Round Table
Discussions

Upcoming Threat Intelligence Peer Group Discussions
None available at the current time

****

Alerts & Warnings

BBB Scam Alert: This phishing scam claims a process server is looking for you
Many scams start with an intimidating phone call. A "debt collector" needs you to pay immediately. Or a "police officer" claims to have a warrant for your arrest. The latest variation involves a phony process server and a non-existent court case against you. BBB Scam Tracker has gotten numerous reports of this new twist. Here's how to spot it.
https://www.bbb.org/article/scams/28919-bbb-scam-alert-this-phishing-scam-claims-a-process-server-is-looking-for-you

Microsoft Teams Exploit Tool Auto-Delivers Malware
The "TeamsPhisher" cyberattack tool gives pen testers — and adversaries — a way to deliver malicious files directly to a Teams user from an external account, or tenant.
A new tool is available on GitHub that gives attackers a way to leverage a recently disclosed vulnerability in Microsoft Teams and automatically deliver malicious files to targeted Teams users in an organization.
https://www.darkreading.com/perimeter/microsoft-teams-exploit-toll-autodeliver-malware

Mobile Cyberattacks Soar, Especially Against Android Users
The number of malware samples is up as attackers aim to compromise users where they work and play: Their smartphones. Attackers are increasingly targeting users through their mobile devices, attacking vulnerabilities in services that are built into applications and mounting increasing numbers of SMS phishing attacks.
https://www.darkreading.com/endpoint/mobile-cyberattacks-soar-andoird-users

AI-Enabled Voice Cloning Anchors Deepfaked Kidnapping
Virtual kidnapping is just one of many new artificial intelligence attack types that threat actors have begun deploying, as voice cloning emerges as a potent new imposter tool. An incident earlier this year in which a cybercriminal attempted to extort $1 million from an Arizona-based woman whose daughter he claimed to have kidnapped is an early example of what security experts say is the growing danger from voice cloning enabled by artificial intelligence.
https://www.darkreading.com/attacks-breaches/ai-enabled-voice-cloning-deepfaked-kidnapping

Aqua Security Study Finds 1,400% Increase in Memory Attacks
Aqua Security's 2023 Cloud Native Threat Report reveals a significant increase in memory attacks, with a 1,400% rise compared to the previous year. These attacks focus on defense evasion and utilize masquerading techniques to evade detection, such as executing files from temporary storage locations.
https://www.techrepublic.com/article/aqua-security-study-increase-memory-attacks/

****

Hints & Tips plus Security Awareness

Take the Offensive Against Ransomware: Harnessing Threat Intelligence for Proactive Protection
In today's ever-evolving threat landscape, ransomware attacks have become increasingly intricate. To effectively prevent these malicious incidents, it is imperative to grasp their origins, evolving tactics, and emerging trends. Join us for an enlightening session where we will delve into the depths of the ransomware market, explore what is changing, evaluate potential impacts, and provide proactive strategies for staying ahead of these attacks. Webinar 7/12/23 @ Noon CST
https://go.recordedfuture.com/operational-risk-ransomware-na

Protecting Small Businesses From Ransomware on a Budget
One ransomware attack can be devastating for a small or midsize business. Here are four solid survival tips to ensure it doesn't turn into a disaster. If your organization is hit with a ransomware attack, it's going to cost you. According to Verizon's "2023 Data Breach Investigations Report"(DBIR), released earlier this month, the median loss to a ransomware attack has risen to $26,000 and can go as high as $2.25 million.
https://www.darkreading.com/edge/protecting-a-small-business-from-ransomware-on-a-budget

****

News & Views

A Golden Age of AI … or Security Threats?
Are we in a golden age of artificial intelligence? It's tough to make predictions — and probably ill-advised. Who wants to predict the future of such a new technology? We can, however, say some things for certain. A great deal is being made of AI's application to creative works, from voice acting to first drafts of screenplays. But AI is likely to be most useful when dealing with drudgery. This is good news for developers, if the promise matches early experiments — first drafts of code can be easily created and ready for developers to tweak and iterate upon.
https://www.darkreading.com/vulnerabilities-threats/a-golden-age-of-ai-or-security-threats-

Social Engineering Adds Depth to Red Team Exercises

Because social engineering usually succeeds, companies need to test whether their defenses can block adversaries that gain employees' trust. When Alethe Denis conducts a social engineering attack as part of a red team exercise, the Bishop Fox security consultant often presents the targets with the exact email template that her team intends to use — such as a dress-code missive from human resources — and yet the attack almost always succeeds.
https://www.darkreading.com/dr-tech/social-engineering-adds-depth-to-red-team-exercises

Microsoft Can Fix Ransomware Tomorrow

You can't encrypt a file you can't open — Microsoft could dramatically impact ransomware by slowing it down. Ransomware works by going through files, one by one, and replacing their content with an encrypted version. (Sometimes it also sends copies elsewhere, but that turns out to be slow, and sometimes sets off alarms.) Software on Microsoft Windows uses an application programming interface (API) called "CreateFile" to access files. Somewhat confusingly, CreateFile not only creates files but is also the primary way to open them.
https://www.darkreading.com/vulnerabilities-threats/microsoft-can-fix-ransomware-tomorrow

****

"Ctrl -F" for The Board

Questions

Contact FIPCO's Rob Foxx at 800-722-3498 ext. 249 or email FIPCO IT Services for more information.

"Make Security Part of You and Your Institution's DNA!"

Threat Intelligence Newsletter: July 14, 2023

FIPCO®
IT Audit
Round Table
Discussions

Upcoming Threat Intelligence Peer Group Discussions
None available at the current time

****

Alerts & Warnings

BBB Scam Alert: New social media scam claims to be giving away a piano
BBB Scam Tracker has gotten numerous reports of a clever new con that appears to be a friendly neighbor trying to give away their piano. Here's what you should know to spot this scam and avoid losing money to con artists. When you reach out to the "owner," they explain that they are downsizing due to a move or other circumstances. They need to find a good home for the piano. It's free…but you will need to cover the shipping cost. If you are interested, the owner will put you in touch with movers who will deliver it.
https://www.bbb.org/article/scams/28855-bbb-scam-alert-new-social-media-scam-claims-to-be-giving-away-a-piano

MOVEit vulnerability snags almost 200 victims, more expected
The education sector has been hit particularly hard as many widely used vendors in the space confirm impacts linked to the mass exploited vulnerability. The widely exploited vulnerability in Progress Software's MOVEit file transfer service has impacted nearly 200 organizations, according to Brett Callow, threat analyst at Emsisoft.
https://www.cybersecuritydive.com/news/moveit-vulnerability-200-victims/684977

Chinese APT Cracks Microsoft Outlook Emails at 25 Government Agencies
Foreign state-sponsored actors likely had access to privileged state emails for weeks, thanks to a token validation vulnerability. This spring, a Chinese threat actor had access to email accounts across 25 government agencies in Western Europe and the US, including the State Department.
https://www.darkreading.com/endpoint/chinese-apt-cracks-microsoft-outlook-emails-government-agencies

Amazon Prime Day Draws Out Cyber Scammers
Cybercriminals lining up to score off Amazon Prime Day shoppers, who spent more than $22B in US online sales alone last year, according to estimates. Amazon Prime Day runs from July 11-12, but scammers have already started to capitalize on the worldwide shopping event, which promises exclusive deals for a short time only.
https://www.darkreading.com/endpoint/amazon-prime-day-cyber-scammers

Hackers Exploit Policy Loophole in Windows Kernel Drivers
Using open source tools, attackers target Chinese speakers with malicious drivers with expired certificates, potentially allowing for full system takeover. Hackers are using open source tools to exploit a Windows policy loophole for kernel mode drivers to load malicious and unverified drivers with expired certificates, researchers have found. The activity — primarily targeted at Chinese-speaking Windows users — potentially gives threat actors full access to victims' systems.
https://www.darkreading.com/endpoint/hackers-exploit-policy-loophole-windows-kernel-drivers

Google Searches for 'USPS Package Tracking' Lead to Banking Theft
Attackers are leveraging well-executed brand impersonation in a Google ads malvertising effort that collects both credit card and bank details from victims. Threat actors are impersonating the United States Post Office (USPS) in a legitimate-looking malvertising campaign that diverts victims to a phishing site to steal payment-card and banking credentials, researchers have found.
https://www.darkreading.com/endpoint/google-searches-usps-tracking-banking-theft

Scammers Cash In On Americans' $150m Collagen Spend
Who doesn't want to keep their youthful looks? Well, maybe not all of us. But, as we age, wrinkles, dry skin, and thinning hair prompt Americans to spend more than $150 million every year (per NielsonIQ) on one particular supposedly anti-aging product - collagen.
https://scambusters.org/collagen.html

TikTok Collects User Biometric Data, Risking Face And Voice Print Abuse
Security experts are concerned about TikTok's latest user data grab. The company recently announced they're collecting new data on users from their video and audio files. Face and voice prints, called biometric data, is now being collected from TikTok's 689 million active global active users, currently without permission.
https://www.sosdailynews.com/news.jspx?&articleid=78377A79BE6527B25F86A14CB23E1EDD

****

Hints & Tips plus Security Awareness

How CIOs select their inner circle
To assemble the right team, CIOs must start by knowing themselves: what they can do — and what they can't. CIOs have a lot on their plates. Not only do they need to make sure an organization keeps functioning, but they also need to stay on top of what's best next for an organization. It's not an easy job.
https://www.ciodive.com/news/CIO-inner-circle-leadership-direct/654097

What to do after a data breach
Long before a data breach, well-prepared companies set up incident response teams with workers from multiple departments. At some point, every organization will have to deal with some sort of cyber incident.
https://www.cybersecuritydive.com/news/post-data-breach-strategy/653805

Does That App Really Need Your Location?
In October of 2014 a flashlight app for smartphones made the news in a bit of a dramatic way. The story went that an app that you can download to your device is really spying on you; stealing your information and sending it off to servers in other lands for bad guys to use for their own purposes. What? Why would a flashlight app do such a thing? Well, sadly, that still happens…all the time. Recall a recent story about Temu, the shopping app? It asked for just about every permission imaginable. But, like the flashlight, it doesn't need them.
https://www.sosdailynews.com/news.jspx?&articleid=6C6F1DDA4BE9B80048A1A26DD8760F4B

****

News & Views

Cybersecurity Is Driving Banks to the Cloud
Digital banking quickly became standard for consumers nationwide as the pandemic cemented a shift to mobile that had been years in the making. Consumers expect targeted and personalized digital banking experiences rather than one-size-fits-all. Forty-six percent want personalized help from their financial institutions (FIs) in avoiding fees, for example. Another 46% expect their banks to provide customizable account balance alerts.
https://www.pymnts.com/news/digital-banking/2023/cybersecurity-is-driving-banks-to-the-cloud/

White House shares the 69 initiatives slated to shore up national cybersecurity
"If the strategy represents the president's vision for the future, then this implementation plan is the roadmap to get there," Acting National Cyber Director Kemba Walden said. The Biden administration released its implementation plan for the national cybersecurity strategy Thursday, delegating cyber initiatives to a smattering of government agencies.
https://www.cybersecuritydive.com/news/national-cybersecurity-strategy-implementation-plan/686887

Only 5% of CISOs report to CEOs, survey finds
CISOs are still most likely to report to the CIO, but Heidrick & Struggles expects that to change as cyber responsibilities evolve. CISOs predominantly report to CIOs and are less likely to report to CEOs now than previous years, according to a Heidrick & Struggles survey.
https://www.cybersecuritydive.com/news/ciso-reporting-structure/685571

Top Takeaways From Table Talks With Fortune 100 CISOs
As organizations struggle to keep up with new regulations and hiring challenges, chief information security officers share common challenges and experiences. Recently, I toured the East Coast and met with Fortune 100 chief information security officers (CISOs) in different industries to have frank discussions about cybersecurity and the changing regulatory compliance landscape.
https://www.darkreading.com/attacks-breaches/top-takeaways-from-table-talks-fortune-100-cisos

EMAIL CYBERATTACKS SPIKED NEARLY 500% IN FIRST HALF OF 2023
Malware only lasts a couple of days in the wild as cyberattackers use automation to create new and customized malicious code at “blazing speed,” and bypassing traditional signature-based detection, Acronis says in its newly released Mid-Year Cyberthreats Report 2023.
https://www.msspalert.com/cybersecurity-research/email-cyberattacks-spiked-nearly-500-in-first-half-of-2023-acronis-reports

****

"Ctrl -F" for The Board

Cyberattacks Are a War We'll Never Win, but We Can Defend Ourselves
Giving ourselves a chance in this fight means acknowledging that yesterday's successful defensive tactics may already be obsolete. Dish Network. Uber. The data networks of several major US airports. These are only three examples of organizations targeted by cyberattacks — a scourge seemingly as constant as it is inevitable.
https://www.darkreading.com/attacks-breaches/cyberattacks-are-a-war-we-ll-never-win-but-we-can-defend-ourselves

Questions
Contact FIPCO’s Rob Foxx at 800-722-3498 ext. 249 or email FIPCO IT Services for more information.

"Make Security Part of You and Your Institution's DNA!"

Threat Intelligence Newsletter: July 21, 2023

FIPCO® IT Audit Round Table Discussions

Upcoming Threat Intelligence Peer Group Discussions
None available at the current time

****

Alerts & Warnings

BBB Scam Alert: Student loan pause is ending. Here's how to avoid scams
After more than three years of relief, the payment pause on student loans is coming to an end. This impacts millions of Americans, creating an excellent opportunity for scammers. In fact, BBB has already received multiple reports of scams related to student loan repayment citing "new 2023 guidelines." Get to know the signs of a scam and always be sure to do your research before sharing any personal information.
https://www.bbb.org/article/news-releases/27471-bbb-scam-alert-student-loan-pause-is-ending-how-to-avoid-scams

Fresh Phish: Malicious QR Codes Are Quickly Retrieving Employee Credentials
QR Code usage has skyrocketed in recent years. In fact, 97% of consumers had no idea what a QR Code was in 2012. But by 1Q22, Americas led the world in QR code usage with 2,880,960 scans, making these quirky codes an appealing path for new and sophisticated phishing campaigns.
https://www.inky.com/en/blog/fresh-phish-malicious-qr-codes-are-quickly-retrieving-employee-credentials

Linux Ransomware Poses Significant Threat to Critical Infrastructure
Organizations running Linux distributions need to prepare to defend their systems against ransomware attacks. Steps to ensure resiliency and basics such as access control reduce major disruptions. Linux systems run many of the most critical operations behind the scenes, including a good deal of our nation's critical infrastructure, and now more ransomware groups are introducing Linux versions. If these systems are disrupted by a ransomware attack, it could cause a catastrophic event.
https://www.darkreading.com/vulnerabilities-threats/linux-ransomware-poses-significant-threat-to-critical-infrastructure

Hackers Exploit WebAPK to Deceive Android Users into Installing Malicious Apps
Threat actors are taking advantage of Android's WebAPK technology to trick unsuspecting users into installing malicious web apps on Android phones that are designed to capture sensitive personal information. "The attack began with victims receiving SMS messages suggesting the need to update a mobile banking application," researchers from CSIRT KNF said in an analysis released last week. "The link contained in the message led to a site that used WebAPK technology to install a malicious application on the victim's device."
https://thehackernews.com/2023/07/hackers-exploit-webapk-to-deceive.html

Is That Shark Tank Product Ad A Fake?
Popular TV show Shark Tank is being widely used by scammers falsely claiming their products have been featured or even recommended in the entrepreneurial reality series. So much so that the show's makers and some of its investors have been forced to issue a warning against the fraudsters.
https://scambusters.org/sharktank.html

Cloudflare reports 'alarming surge' in DDoS sophistication, escalation in recent months
Attacks used to make websites and web services inaccessible are evolving and becoming more concerning, the company said Tuesday. The second quarter of 2023 has seen "an alarming escalation in the sophistication" of distributed denial-of-service attacks, Cloudflare said Tuesday, pointing to a proliferation of more targeted digital assaults designed to take down websites and other connected services.
https://cyberscoop.com/cloudflare-ddos-escalation

Malvertising Campaign Tracks Down Our Payment Card Info Using USPS
The fewer items we receive via the U.S. Postal Service (USPS) these days, the more excited we get when we do get packages delivered by the service. Well, cybercriminals are always up to something and now they are trying to take away our excitement when we go get the mail. Researchers at Malwarebytes provided a detailed process of how a recently discovered malvertising campaign works and helps criminals track down our payment card information for their own use.
https://www.sosdailynews.com/news.jspx?&articleid=4ED48C01E2630071C59DBB24F3F31374

Amazon "Free Stuff" Brushing Scam Makes Victims Pay The Price
Open your front door and there they are, boxes from Amazon you weren't expecting. The thought of getting free stuff might give you a giggle, but the truth is, the last laugh could be at your expense. That's because you've just been pulled into a "brushing" scam using you and Amazon to work. Brushing scams are happening more often than ever before, and a closer look at them shows how free stuff could end up costing you.
https://www.sosdailynews.com/news.jspx?&articleid=DCD2146FBD6BC101C38B15D4F4E54CC0

****

Hints & Tips plus Security Awareness

What You See Is Not What You Get; Latest Phishing Attack Skips Email Security Measures
It's no surprise that phishing is still prevalent in the cyber world. In fact, it remains the top way malware gets onto devices, and it still excels at getting people to give up their personal information. Phishing scams, and they are aplenty, aim to deceive individuals into divulging sensitive information such as passwords, payment card details, or all other kinds of personal data; some that you don't even think is all that useful to someone trying to scam you.
https://www.sosdailynews.com/news.jspx?&articleid=150B19DACE0276DB3C07D235CB92C55A

A Few More Reasons Why RDP is Insecure (Surprise!)

If it seems like Remote Desktop Protocol (RDP) has been around forever, it's because it has (at least compared to the many technologies that rise and fall within just a few years.) The initial version, known as "Remote Desktop Protocol 4.0," was released in 1996 as part of the Windows NT 4.0 Terminal Server edition and allowed users to remotely access and control Windows-based computers over a network connection.
https://thehackernews.com/2023/07/a-few-more-reasons-why-rdp-is-insecure.html

How to Manage Your Attack Surface?

Attack surfaces are growing faster than security teams can keep up. To stay ahead, you need to know what's exposed and where attackers are most likely to strike. With cloud migration dramatically increasing the number of internal and external targets, prioritizing threats and managing your attack surface from an attacker's perspective has never been more important. Let's look at why it's growing, and how to monitor and manage it properly with tools like Intruder.
https://thehackernews.com/2023/07/how-to-manage-your-attack-surface.html

****

News & Views

The Biden administration is tackling smart devices with a new cybersecurity label

The US Cyber Trust Mark would require smart products to meet certain thresholds, including ongoing software security support, to qualify for the program.
https://www.theverge.com/2023/7/18/23798153/fcc-cyber-trust-mark-biden-security

EU Cyber Resilience Act a 'death knell' for open source software, critics warn

Critics of the act claim that requirements for open source software usage could severely impact the community. The EU's proposed Cyber Resilience Act could spell disaster for the open source community, with critics describing the legislation as a 'death knell' for the industry.
https://www.itpro.com/software/open-source/eu-cyber-resilience-act-a-death-knell-for-open-source-software-critics-warn

****

"Ctrl -F" for The Board

Close Security Gaps with Continuous Threat Exposure Management

CISOs, security leaders, and SOC teams often struggle with limited visibility into all connections made to their company-owned assets and networks. They are hindered by a lack of open-source intelligence and powerful technology required for proactive, continuous, and effective discovery and protection of their systems, data, and assets.
https://thehackernews.com/2023/07/close-security-gaps-with-continuous.html

Questions
Contact FIPCO's Rob Foxx at 800-722-3498 ext. 249 or email FIPCO IT Services for more information.

"Make Security Part of You and Your Institution's DNA!"

Threat Intelligence Newsletter: July 28, 2023

Upcoming Threat Intelligence Peer Group Discussions
None available at the current time

****

Alerts & Warnings

BBB Scam Alert: Spot a vehicle transport scam before you move your car, truck or motorcycle
Moving is stressful, expensive, and time-consuming! That makes it a perfect opportunity for scammers. If you are relocating and need help transporting your vehicle, watch out for this scam. You search the internet for a vehicle transport service, hoping to get a quote. After browsing a few companies, you find one offering a great deal. All you have to do is send them a deposit of a few hundred dollars, usually via a digital wallet service.
https://www.bbb.org/article/news-releases/28997-scam-alert-spot-a-vehicle-transport-scam-before-you-move-your-car-truck-or-motorcycle

Linux Ransomware Poses Significant Threat to Critical Infrastructure
Organizations running Linux distributions need to prepare to defend their systems against ransomware attacks. Steps to ensure resiliency and basics such as access control reduce major disruptions. Linux systems run many of the most critical operations behind the scenes, including a good deal of our nation's critical infrastructure, and now more ransomware groups are introducing Linux versions. If these systems are disrupted by a ransomware attack, it could cause a catastrophic event.
https://www.darkreading.com/vulnerabilities-threats/linux-ransomware-poses-significant-threat-to-critical-infrastructure

Banks in Attackers' Crosshairs, via Open Source Software Supply Chain
In separate targeted incidents, threat actors tried to upload malware into the Node Package Manager registry to gain access and steal credentials. In two separate incidents, threat actors recently tried to introduce malware into the software development environment at two different banks via poisoned packages on the Node Package Manager (npm) registry.
https://www.darkreading.com/attacks-breaches/banks-in-attackers-crosshairs-via-open-source-software-supply-chain

Your FB Trusted Contacts Should Not Be Trusted
As anyone who uses Facebook (or any social media) there is a seemingly endless supply of scams that go around all the time. Once we think we've seen them all, we are bombarded again with new ones or with new versions of them. Often, trickier to spot. This goes on ad nauseam. School may be out for the summer, but education continues on when it comes to cybersecurity threats. One, first reported in 2017, is circulating again that takes advantage of a feature of Facebook that no longer is supported. It's the "Trusted Contacts" capability. The following is based on a true story.
https://www.sosdailynews.com/news.jspx?&articleid=3A5AFFCECE80FCB661BC9C0B5D11A8E4

Malicious Apps Evade Official App Store Security – Tips To Avoid Them
Last year saw a bumper crop of malicious apps and Google Play and Apple App stores found millions of them. These two official app sources stopped a combined 3.13 million bad apps from going public in their stores. But despite their security measures, some malicious apps still get through. Since both stores are by far the safest sources for clean app downloads, it's important to know how to spot the bad ones before it's too late.
https://www.sosdailynews.com/news.jspx?&articleid=67AB746B190DAFB65505DE1936BB4455

****

Hints & Tips plus Security Awareness

How do you reduce your IT costs?
In this blog, we'll provide three tips on reducing your IT costs: how to identify the right devices to upgrade, the importance of IT budgeting and an IT cost reduction checklist. IT is the backbone of every business. Without a strong and robust IT team that can maintain a high level of performance and reliability, business can suffer due to a lack of employee productivity, decreases in customer satisfaction, and overall poor performance.
https://www.bankingdive.com/spons/how-do-you-reduce-your-it-costs/686257/

You've Got Malware, We've Got Help
The world of mobile viruses can be a bit confusing, right? Don't worry, we've got you. While your phone can fall victim to malware, it's highly unlikely that it's going to result in an unrecoverable situation. What you may encounter are things like adware, bloatware, or those pesky pop-ups that drive you nuts. There is no shortage of those these days. These all can hitch a ride from third-party websites, apps, or even those suspicious email and text messages you receive all the time. But here we are to help!
https://www.sosdailynews.com/news.jspx?&articleid=E0CFDD6FDAB340430CA154A7A76D971B

****

News & Views

Google Categorizes 6 Real-World AI Attacks to Prepare for Now
The models powering generative AI like ChatGPT are open to several common attack vectors that organizations need to understand and get ready for, according to Google's dedicated AI Red Team. Google researchers have identified six specific attacks that can occur against real-world AI systems, finding that these common attack vectors demonstrate a unique complexity, That will require a combination of adversarial simulations and the help of AI subject-matter expertise to construct a solid defense, they noted.
https://www.darkreading.com/attacks-breaches/google-red-team-provides-insight-on-real-world-ai-attacks

Critical Infrastructure Workers Better At Spotting Phishing
Critical-infrastructure employees are comparatively more engaged in organizational security — and compliance training — than those in other sectors. Phishing simulation training for employees appears to work better at critical infrastructure organizations than it does across other sectors, with 66% of those employees correctly reporting at least one real malicious email attack within a year of training, new research has found.
https://www.darkreading.com/ics-ot/critical-infrastructure-workers-spotting-phishes

Will Security Keys Spell The End Of Passwords?
Thousands of data breaches and millions of individually hacked accounts and computers remind us of something most of us probably already know - passwords are past their sell-by date. They're no longer enough to protect us from online scammers and hackers. So, over the past few years, security experts have been coming up with new ideas to protect us from the online baddies.
https://scambusters.org/securitykey.html

****

"Ctrl -F" for The Board

IBM Report: Half of Breached Organizations Unwilling to Increase Security Spend Despite Soaring Breach Costs
AI/Automation cut breach lifecycles by 108 days; $470,000 in extra costs for ransomware victims that avoid law enforcement; Only one third-of organizations detected the breach themselves According to the 2023 IBM report, businesses are divided in how they plan to handle the increasing cost and frequency of data breaches. The study found that while 95% of studied organizations have experienced more than one breach, breached organizations were more likely to pass incident costs onto consumers (57%) than to increase security investments (51%).
https://newsroom.ibm.com/2023-07-24-IBM-Report-Half-of-Breached-Organizations-Unwilling-to-Increase-Security-Spend-Despite-Soaring-Breach-Costs

Cohesity Research Shows Businesses Are Open to Paying Ransoms Due to Cyber Resilience and Data Recovery Gaps
Over 90% believe the threat of ransomware to their industry has increased in 2023, and close to 3 in 4 (74%) respondents say their company will pay a ransom to recover data and restore business processes.
https://www.businesswire.com/news/home/20230725702169/en/Cohesity-Research-Shows-Businesses-Are-Open-to-Paying-Ransoms-Due-to-Cyber-Resilience-and-Data-Recovery-Gaps

Questions
Contact FIPCO’s Rob Foxx at 800-722-3498 ext. 249 or email FIPCO IT Services for more information.

"Make Security Part of You and Your Institution's DNA!"

Threat Intelligence Newsletter: August 4, 2023

FIPCO®
IT Audit
Round Table
Discussions

Upcoming Threat Intelligence Peer Group Discussions
None available at the current time

****

Alerts & Warnings

BBB Scam Alert: Double check that QR code before you pay for parking
QR codes are everywhere: signs, ads, menus, and even scams. BBB Scam Tracker has seen an influx of reports about a scam that involves fraudulent QR codes at parking lots. This time, scammers use them to steal parking fees and collect credit card information. It's the flip side of this parking ticket scam. Learn how the scam works to avoid falling victim.
https://www.bbb.org/article/scams/28996-bbb-scam-alert-double-check-that-qr-code-before-you-pay-for-parking

Scammers Love Barbie: Fake Videos Promote Bogus Ticket Offers That Steal Personal Info
Turns out, scammers really love Barbie. As Barbie makes her debut on the big screen, scammers are aiming to cash in on the summer blockbuster. A rash of scams have cropped up online, including bogus downloads of the film that install malware, Barbie-related viruses, and fake videos that point people to free tickets—but lead to links that steal personal info with spyware instead.
https://www.mcafee.com/blogs/internet-security/scammers-love-barbie-fake-videos-promote-bogus-ticket-offers-that-steal-personal-info/

How Malicious Android Apps Slip Into Disguise
Researchers say mobile malware purveyors have been abusing a bug in the Google Android platform that lets them sneak malicious code into mobile apps and evade security scanning tools. Google says it has updated its app malware detection mechanisms in response to the new research.
https://krebsonsecurity.com/2023/08/how-malicious-android-apps-slip-into-disguise/

Don't Get Scammed By Digital E-Signature Crooks
If you've ever had to sign a document electronically by pasting your signature or a code into a digital file, you'll know how much time, cost, and hassle the process saves you. But the growing popularity of e-signatures, as they're called, has also made them a target for scammers, despite stringent security by companies providing the service. E-signing is widely used in business but it's also increasingly common for consumers - for example, when signing mortgage agreements, tax forms, and many other types of legal documents. But if you get caught out by the scammers, it could cost you a fortune.
https://scambusters.org/esign.html

****

Hints & Tips plus Security Awareness

Suspecting The Unexpected – When Verification Codes Spell Trouble
There’s a new security challenge to verification codes we use during account logins. These numerical security codes are an extra layer to our identity that helps keep hackers out. But not all verification codes are there to help, especially when they pop up on your device for seemingly no reason. Since hackers love finding sneaky ways of getting beyond our security efforts, they’re now exploiting verification codes – for nefarious and self-serving reasons, of course!
https://www.sosdailynews.com/news.jspx?&articleid=994DBCFC3D044AD3559754C9B4FFAE81

Top Ransomware Groups Wreak Havoc Since 2020; Tips To Keep Ransomware At Bay
There are many ransomware groups lurking in the shadows these days. They may come out from time to time, hold a few businesses for ransom and then slink back into the abyss. Later, they may reappear and do it again. Some disappear but under a different name and others morph into a new group. One thing that stays consistent is that they are always there. Lately, a few have made their marks. Here is information on them and what you can do.
https://www.sosdailynews.com/news.jspx?&articleid=F92671DE29A522214C9FB93A55831684

****

News & Views

How Being Human Makes Us Targets For Online Scams
Being human comes with certain attributes cybercriminals love to exploit. In the world of online scams, our willingness to trust others can easily translate to a scam’s success. And since we can’t help being human, we need to keep in mind that scammers exploit our humanity to their benefit. But as humans, we can also spot an attempted scam when we see one, so chalk one up for being human!
https://www.sosdailynews.com/news.jspx?&articleid=7BC40D1A395B923CA91401F97D85B5E8

Dark Web Profile: 8Base Ransomware
In today’s cyber world, while the ransomware scene remains dynamic and active, new actors are emerging with significant numbers of victims. In this article, we will focus on 8Base Ransomware, which ranked in the top 5 most active groups last month according to Daily Dark Web, with 37 victim announcements in June.
https://socradar.io/dark-web-profile-8base-ransomware/

Hackers can abuse Microsoft Office executables to download malware
The list of LOLBAS files - legitimate binaries and scripts present in Windows that can be abused for malicious purposes, will soon include the main executables for Microsoft's Outlook email client and Access database management system. The main executable for the Microsoft Publisher application has already been confirmed that it can download payloads from a remote server.
https://www.bleepingcomputer.com/news/security/hackers-can-abuse-microsoft-office-executables-to-download-malware/

****

"Ctrl -F" for The Board

Questions
Contact FIPCO's Rob Foxx at 800-722-3498 ext. 249 or email FIPCO IT Services for more information.

"Make Security Part of You and Your Institution's DNA!"

Threat Intelligence Newsletter: August 11, 2023

FIPCO®
IT Audit
Round Table
Discussions

Upcoming Threat Intelligence Peer Group Discussions
None available at the current time

****

Alerts & Warnings

BBB Scam Alert: Protect yourself from “check washing”
Check use may be declining, but check fraud is still a serious problem. Watch out for this scam, dubbed “check washing,” which involves stealing checks from mailboxes and then altering them. Fortunately, you can do a few things to protect yourself and your business.
https://www.bbb.org/article/scams/28998-bbb-scam-alert-protect-yourself-from-check-washing

APT Bahamut Targets Individuals with Android Malware Using Spear Messaging
The team at CYFIRMA recently obtained advanced Android malware targeting individuals in the South Asia region. The suspicious Android malware is a dummy chatting app. Our initial technical analyses revealed that APT Bahamut is behind the attack. As technical analyses proceeded further, we also found footprints of tactics used by DoNot APT in the suspicious app belonging to APT Bahamut.
https://www.cyfirma.com/outofband/apt-bahamut-targets-individuals-with-android-malware-using-spear-messaging/

Scammers Target Social Media Verification Programs
After a number of false starts, social media giants like Facebook, Instagram, and Twitter are getting serious about "blue badge" verification. So are scammers. Both Meta (which owns Facebook and Instagram) and Twitter have relaunched programs this year offering verification badges - for a substantial monthly fee. So, the aim is not only to make certain accounts secure but also to make a lot of money in the process. According to an estimate from Bank of America, Meta could earn more than $1.7 billion a year by charging people for a badge, which sits alongside their name on the site.
https://scambusters.org/verification.html

BlackCat Brings Bad Luck Using Google Ads
Trend Micro researchers recently identified that a notorious ransomware group is using various malvertising tricks within Google Ads to distribute fake WinSCP installers. They are using Targeted Attack Detection (TAD) service. What is that, you say? This means that if you click on an infected ad that you see on your webpage, your network could get a bad case of cat scratch fever. Let's break it down a bit more.
https://www.sosdailynews.com/news.jspx?&articleid=E084F70BD9978E3B5C9A07A39F37A337

Look Before You Buy! eBay Marketplace Scams; How To Spot And Avoid Them
Cyber-scams are everyday threats, especially in the world of online marketplace shopping. It happens often and to anyone, as we learned from the historic spike in online scams during coronavirus lockdowns and beyond. Now, eBay's popular e-commerce marketplace is increasingly a target for cyber-scams and scammers. The company has taken an active step protecting their users by publishing scam warnings on their website. It includes spotting the red flags and tips on avoiding their most frequent scams.
https://www.sosdailynews.com/news.jspx?&articleid=9FE2BC49C6749EC939E1D81E57666DE5

The Truth About Temu Shopping App Gives Reasons To Delete It
Temu, the insanely popular Chinese-owned discount marketplace app is creating a stir in the U.S. With help from 50 million+ Americans now onboard, Temu snuck into first place bypassing Amazon, Walmart, and Shein with its global number of app users. And like any app you consider downloading, Temu deserves a closer look first. Not long after Temu's U.S. launch during last year's Superbowl, the app came under scrutiny from disillusioned customers and cybersecurity professionals, but for very different reasons.
https://www.sosdailynews.com/news.jspx?&articleid=82E7F1930EAE72F66AA7CFDD97FBBBEF

China-Linked Hackers Strike Worldwide: 17 Nations Hit in 3-Year Cyber Campaign
Hackers associated with China's Ministry of State Security (MSS) have been linked to attacks in 17 different countries in Asia, Europe, and North America from 2021 to 2023. Cybersecurity firm Recorded Future attributed the intrusion set to a nation-state group it tracks under the name RedHotel (previously Threat Activity Group-22 or TAG-22), which overlaps with a cluster of activity broadly monitored as Aquatic Panda, Bronze University, Charcoal Typhoon, Earth Lusca, and Red Scylla (or Red Dev 10).
https://thehackernews.com/2023/08/china-linked-hackers-strike-worldwide.html

Invisible Adware: Unveiling Ad Fraud Targeting Android Users
We live in a world where advertisements are everywhere, and it's no surprise that users are becoming tired of them. By contrast, developers are driven by profit and seek to incorporate more advertisements into their apps. However, there exist certain apps that manage to generate profit without subjecting users to the annoyance of ads. Is this really good?
https://www.mcafee.com/blogs/other-blogs/mcafee-labs/invisible-adware-unveiling-ad-fraud-targeting-android-users/

****

Hints & Tips plus Security Awareness

The Steps Security Leaders Must Take For Cyber Resilience in Financial Services
The cyber-criminal community is a rising threat to financial services firms and their increasing professionalism and coordination across the globe has been highlighted by the increase in the number of attacks across the sector. Ransomware in particular has increased in prevalence as an attack vector, spawning ransomware as a service to become a new threat. Regulators across the globe are rightly focusing on the need to bolster resilience and reduce operational risk to combat this threat, with many new regulations and guidelines on the horizon for capital markets firms. 27 Min Video
https://www.brighttalk.com/webcast/12821/590479

10 Key Controls to Show Your Organization Is Worthy of Cyber Insurance
More-effective cyber-risk management controls can help bolster a company's policy worthiness. Start with these 10 tips to manage risk as underwriter requirements get more sophisticated. Increasing concerns about ransomware and other breaches, especially at the credentials level, are likely why organizations are investing in cyber insurance at greater rates than ever before: 48% have already invested in cyber insurance (registration required) for identity-related incidents, and another 32% plan to invest.
https://www.darkreading.com/risk/10-key-controls-to-show-your-organization-is-worthy-of-cyber-insurance

Why Do Cybersecurity Awareness Programs Often Fail?
Security Awareness Expert John Scott on Adapting Tech and Process. Many security awareness training programs fail because organizations don't understand the risks they face, said John Scott, lead cybersecurity researcher at Culture AI. He said a successful training program "will help people by making sure that it's targeting the behaviors that address the key risks for the organization." 25 Min Webinar
https://www.databreachtoday.com/do-cybersecurity-awareness-programs-often-fail-a-22762

****

News & Views

2 in 3 finance workers would quit if flex work were taken away: survey
About 18% of 700 respondents to the Deloitte study said they preferred to work from the office three or four days a week, yet 62% said they felt it would be bad for their careers if they came in less.
https://www.bankingdive.com/news/deloitte-office-return-survey-jpmorgan-citi-flexible-caregiver-women/690417

****

"Ctrl -F" for The Board

How to Talk So Your CISO Will Listen
Tailor your business project proposal to suit the language your company's CISO speaks, be it business, technical, or compliance. Do your research first and gather support from around the company.
https://www.darkreading.com/vulnerabilities-threats/how-to-talk-so-your-ciso-will-listen

Teach a Man to Phish and He's Set for Life
One frustrating aspect of email phishing is the frequency with which scammers fall back on tried-and-true methods that really have no business working these days. Like attaching a phishing email to a traditional, clean email message, or leveraging link redirects on LinkedIn, or abusing an encoding method that makes it easy to disguise booby-trapped Microsoft Windows files as relatively harmless documents.
https://krebsonsecurity.com/2023/08/teach-a-man-to-phish-and-hes-set-for-life/

Questions
Contact FIPCO's Rob Foxx at 800-722-3498 ext. 249 or email FIPCO IT Services for more information.

"Make Security Part of You and Your Institution's DNA!"

Threat Intelligence Newsletter: August 18, 2023

FIPCO®
IT Audit
Round Table
Discussions

Upcoming Threat Intelligence Peer Group Discussions
None available at the current time

****

Alerts & Warnings

Disposed-of Gadgets Can Lead to Wi-Fi Network Hacks, Kaspersky Says
Wi-Fi settings are easily stolen when old gadgets are gotten rid of, which puts end users in the crosshairs for network attacks. When disposing of old technology — such as old phones, computers, printers, and smartwatches — it's essential to remember to clear the stored Wi-Fi network information. That's because this data is often unprotected and easy to retrieve from discarded gadgets, according to a new article on the dangers of leaky Wi-Fi access from Kaspersky.
https://www.darkreading.com/vulnerabilities-threats/disposed-of-gadgets-can-lead-to-wi-fi-network-hacks-kaspersky-says

AI Steals Passwords by Listening to Keystrokes With Scary Accuracy
The AI model trained on typing recorded over a smartphone was able to steal passwords with 95% accuracy. Trained with keystrokes on a laptop transmitted over a smartphone, a new AI model was able to overhear typing and steal passwords with 95% accuracy.
https://www.darkreading.com/attacks-breaches/ai-model-can-replicate-password-listening-to-keystrokes

3 Major Email Security Standards Prove Too Porous for the Task
Nearly 90% of malicious emails manage to get past SPF, DKIM, or DMARC, since threat actors are apparently using the same filters as legitimate users.
Email security standards are proving porous where malicious email attacks are concerned, since attackers use a deceptive link or new domains that comply with the same email security standards regular users employ to blunt threats like phishing, according to a vendor report released this week.
https://www.darkreading.com/vulnerabilities-threats/3-major-email-security-standards-falling-down-on-the-job

How Artificial Intelligence Is Turbocharging Frauds and Scams
A huge rise in imposter scams using artificial intelligence (AI) during the first few months of this year has set alarm bells ringing across the globe. "Artificial imposters," as they're being called, need to grab just a few seconds of a person's voice online to clone it and make realistic calls to friends and family - ranging from fake kidnap demands to pleas for financial help. And, according to latest research, as many as half of all Americans share their voices on the Internet every week. Which gives scammers plenty of targets to go for.
https://scambusters.org/artificial.html

AI Becomes Criminals' New Ally with the Emergence of FraudGPT
The digital landscape is facing a fresh threat: FraudGPT. This nefarious AI tool, hanging around at the backdoor of WormGPT, first popped up on July 22, 2023. Numerous underground websites and private Telegram channels were the first to notice its presence. What sets FraudGPT apart from other cyber threats is its versatility—it's a multi-purpose tool designed for an array of illicit activities.
https://www.sosdailynews.com/news.jspx?&articleid=9DDC42B2F71DFEF34D332D57A79B4A4D

****

Hints & Tips plus Security Awareness

Improved Password Cracking – How Easily Are Yours Stolen?
New upgrades to technology have made password-cracking a breeze. As a result, creating fortified passwords is more important than ever. We know rock-solid passwords do wonders in keeping intruders out, yet few of us actually use them. New data shows just how quickly, or not, different passwords get cracked these days depending on how they're built.
https://www.sosdailynews.com/news.jspx?&articleid=7DECE64FF593E6BBF40511D2D87BA014

Why You Need Continuous Network Monitoring?
Changes in the way we work have had significant implications for cybersecurity, not least in network monitoring. Workers no longer sit safely side-by-side on a corporate network, dev teams constantly spin up and tear down systems, exposing services to the internet. Keeping track of these users, changes and services is difficult – internet-facing attack surfaces rarely stay the same for long.
https://thehackernews.com/2023/08/why-you-need-continuous-network.html

****

News & Views

NIST releases draft overhaul of its core cybersecurity framework
It marks the first major update to federal risk guidance since 2014 and incorporates new issues, including supply chain security and threats to small business. The National Institute of Standards and Technology released a long-anticipated draft version of the Cybersecurity Framework 2.0 Tuesday, the first major update of the agency's risk guidance since 2014.
https://www.cybersecuritydive.com/news/nist-draft-overhaul-cybersecurity-framework/690381

Following Pushback, Zoom Says It Won't Use Customer Data to Train AI Models
Company's experience highlights the tightrope tech organizations walk when integrating AI into their products and services. Zoom says it will walk back a recent change to its terms of service that allowed the company to use some customer content to train its machine learning and artificial intelligence models.
https://www.darkreading.com/analytics/following-pushback-zoom-says-it-won-t-use-customer-data-to-train-ai-models

****

"Ctrl -F" for The Board

The Future of Cybersecurity Depends on Public-Private Partnership – Will We Get it Right?
In 2020, the U.S. Cyber Command (CYBERCOM) established its private sector partnership program dubbed UNDER ADVISEMENT, the purpose of which is to engage industry organizations and share critical cyber threat information and intelligence that supports both CYBERCOM missions and the private sector's cybersecurity priorities. According to CYBERCOM's website, formal agreements are made with private sector stakeholders in an effort to establish trust, create dialogue, and perhaps most importantly, establish a two-way information exchange channel.
https://www.oodaloop.com/archive/2023/08/10/the-future-of-cybersecurity-depends-on-public-private-partnership-will-we-get-it-right/

Nearly 60% Of Employees Leave After Cyberattack
When a business experiences a cybersecurity event, the road to recovery is challenging. There's the financial cost of recovery for sure, but research also shows up to 60% of employees leave their job after an attack. How to help retain staff after a security event is something every business leader should know how to do.
https://www.sosdailynews.com/news.jspx?&articleid=483138A3F11DD47A504AC8FEE4D10DCD

Questions
Contact FIPCO's Rob Foxx at 800-722-3498 ext. 249 or email FIPCO IT Services for more information.

"Make Security Part of You and Your Institution's DNA!"

Threat Intelligence Newsletter: August 28, 2023

Upcoming Threat Intelligence Peer Group Discussions
None available at the current time

****

Alerts & Warnings

BBB Scam Alert: How to spot this common vacation rental scam
BBB Scam Tracker has gotten numerous reports of a clever travel scam this summer vacation season. Con artists pretend to own a vacation rental and insist on being paid directly rather than through the official rental platform. If you book with them, you'll be out of money and face a potentially ruined vacation.
https://www.bbb.org/article/scams/29117-bbb-scam-alert-how-to-spot-this-newly-common-vacation-rental-scam

LinkedIn accounts hacked in widespread hijacking campaign
LinkedIn is being targeted in a wave of account hacks resulting in many accounts being locked out for security reasons or ultimately hijacked by attackers. As reported today by Cyberint, many LinkedIn users have been complaining about the account takeovers or lockouts and an inability to resolve the problems through LinkedIn support.
https://www.bleepingcomputer.com/news/security/linkedin-accounts-hacked-in-widespread-hijacking-campaign/

Knight ransomware distributed in fake Tripadvisor complaint emails
The Knight ransomware is being distributed in an ongoing spam campaign that pretends to be TripAdvisor complaints. Knight ransomware is a recent rebrand of the Cyclop Ransomware-as-a-Service, which switched its name at the end of July 2023.
https://www.bleepingcomputer.com/news/security/knight-ransomware-distributed-in-fake-tripadvisor-complaint-emails/

CISA says hackers are exploiting a new file transfer bug in Citrix ShareFile
Hackers are exploiting a newly discovered vulnerability in yet another enterprise file transfer software, the U.S. government's cybersecurity agency has warned. CISA on Wednesday added a vulnerability in Citrix ShareFile, tracked as CVE-2023-24489, to its Known Exploited Vulnerabilities (KEV) catalog. The agency warned that the flaw poses "significant risks to the federal enterprise," and mandated that federal civilian executive branch agencies — CISA included — apply vendor patches by September 6.
https://techcrunch.com/2023/08/17/cisa-hackers-citrix-sharefile-exploit

More Than Half of Browser Extensions Pose Security Risks
Spin.AI's risk assessment of some 300,000 browser extensions found 51% had overly permissive access and could execute potentially malicious behaviors. Many browser extensions that organizations permit employees to use when working with software-as-a-service (SaaS) apps such as Google Workspace and Microsoft 365 have access to high levels of content and present risks such as data theft and compliance issues, a new study has found.
https://www.darkreading.com/cloud/study-more-than-half-of-browser-extensions-pose-security-risks

Attackers Dangle AI-Based Facebook Ad Lures to Hijack Business Accounts
The offending ads and pages leveraged interest in AI to spread a malicious credential-stealing browser extension. A threat actor has been abusing paid Facebook ads to lure victims with the promise of AI technology to spread a malicious Chrome browser extension that steals users' credentials with the ultimate aim to take over business accounts.
https://www.darkreading.com/attacks-breaches/attackers-dangle-ai-based-facebook-ad-lures-to-take-over-business-accounts

Don't Fall For It! Phishing Email Attack Warns Your Facebook Page Will Be Suspended
If an email pops-up saying your Facebook account will be suspended, pay close attention. A new scam by cyber-crooks wants to steal your login information and other PII using their clever lure. With nearly 3 billion active Facebook (FB) users, this unique approach to data theft has more than enough prospective victims, so read on to make sure you won't be one of them.
https://www.sosdailynews.com/news.jspx?&articleid=8C8F2094FDDD4DB6F041717AB20BCBE6

Unforgiving Scammers Seek Your Credentials When Applying For Student Loan Debt Forgiveness
We can all use a little financial help from time to time; especially those saddled with student loan debt. So, there's no surprise that after the Student Loan Debt Relief Plan was announced and neared reality, an immediate uptick in fraud schemes surrounding this program started to appear. The FBI states scammers are working over time looking to take advantage of those individuals seeking this student forgiveness.
https://www.sosdailynews.com/news.jspx?&articleid=6027B881B7D921337819B546F8BA4253

****

Hints & Tips plus Security Awareness

4 ways organizations can take back the advantage from attackers
By reorienting systems defense around resilience, “we become more like attackers, we become nimble, empirical, curious,” Kelly Shortridge said at Black Hat USA 2023.
https://www.cybersecuritydive.com/news/cyber-attack-defense-strategies-Black-Hat/690547/

7 Reasons People Don't Understand What You Tell Them
No matter how clearly security professionals express themselves, not everyone thinks the same way. Here's why communication can go wrong. I've been fascinated by the difference between what one person writes, says, or does and what another person reads, hears, or perceives. Consider a situation we have likely all encountered: We are on a work call where one person shares some information, such as, "Project XYZ is on track and expected to be completed on time by the end of the calendar year." It is quite common that at some point during the call after that statement is made, either someone will ask, "What is the status of Project XYZ?" or someone will incorrectly repeat what was said (e.g., "Project XYZ will not be completed on time by the end of the calendar year").
https://www.darkreading.com/edge/7-reasons-people-don-t-understand-what-you-tell-them

Tourists Give Themselves Away by Looking Up. So Do Most Network Intruders.
In large metropolitan areas, tourists are often easy to spot because they’re far more inclined than locals to gaze upward at the surrounding skyscrapers. Security experts say this same tourist dynamic is a dead giveaway in virtually all computer intrusions that lead to devastating attacks like data theft and ransomware, and that more organizations should set simple virtual tripwires that sound the alarm when authorized users and devices are spotted exhibiting this behavior.
https://krebsonsecurity.com/2023/08/tourists-give-themselves-away-by-looking-up-so-do-most-network-intruders/

Cybercriminals turn to AI to bypass modern email security measures
Cybercriminals employ artificial intelligence (AI) to create complex email threats like phishing and business email compromise (BEC) attacks, while modern email security systems use AI to counter these attacks, according to Perception Point and Osterman Research.
https://www.oodaloop.com/briefs/2023/08/23/cybercriminals-turn-to-ai-to-bypass-modern-email-security-measures/

Triple Extortion Ransomware and the Cybercrime Supply Chain
Ransomware attacks continue to grow both in sophistication and quantity. 2023 has already seen more ransomware attacks involving data exfiltration and extortion than all of 2022, an increasing trend we expect to continue. This article will explore the business model of ransomware groups and the complex cybercrime ecosystem that has sprung up around them.
https://www.bleepingcomputer.com/news/security/triple-extortion-ransomware-and-the-cybercrime-supply-chain/

****

News & Views

For security to benefit from AI, companies need to shore up their data
CISOs need to address the structure, management and curation of data as they pursue benefits from generative AI, according to an IDC report. Artificial intelligence is showing up in new ways across almost every security tool enterprises rely on, but the industry's lopsided focus on the technology, instead of the underlying data, is misguided, according to IDC analysts.
https://www.cybersecuritydive.com/news/data-ai-defense/691709

CISA Committee Tackles Remote Monitoring and Management Protections
CISA's public-private partnership produces RMM strategies to shore up critical infrastructure and to educate the MSPs that provide remote access to them. Just two years after Cybersecurity and Infrastructure Security Agency (CISA) Director Jen Easterly unveiled the Joint Cyber Defense Collective (JCDC) initiative, a cooperative effort between public and private cybersecurity sectors, the group has presented its first piece of guidance: a road map to shore up the remote monitoring and management (RMM) systems ecosystem behind the country's critical infrastructure.
https://www.darkreading.com/vulnerabilities-threats/cisa-committee-tackles-remote-monitoring-and-management-protections

Google released first quantum-resilient FIDO2 key implementation
Google has announced the first open-source quantum resilient FIDO2 security key implementation, which uses a unique ECC/Dilithium hybrid signature schema co-created with ETH Zurich. FIDO2 is the second major version of the Fast IDentity Online authentication standard, and FIDO2 keys are used for passwordless authentication and as a multi-factor authentication (MFA) element.
https://www.bleepingcomputer.com/news/security/google-released-first-quantum-resilient-fido2-key-implementation/

Alarming lack of cybersecurity practices on world's most popular websites
The world's most popular websites lack basic cybersecurity hygiene, an investigation by Cybernews shows. Do you happen to love exploring DIY ideas on Pinterest? Scrolling through IMDB to pick the next movie to watch? Or simply scrolling through Facebook to see what your friends and enemies have been up to?
https://securityaffairs.com/149607/security/alarming-lack-cybersecurity-popular-websites.html

****

"Ctrl -F" for The Board

Government investigation puts spotlight on password insecurity
A team working for the Department of Interior's inspector general successfully cracked 1 in 5 active user passwords, a ratio that highlights traps in cybersecurity standards, Mike Kosask from LastPass writes.
https://www.cybersecuritydive.com/news/password-policies-inspector-general-lastpass/691757/

Questions
Contact FIPCO's Rob Foxx at 800-722-3498 ext. 249 or email FIPCO IT Services for more information.