

Security Awareness: Intro



Compliance vs. Security

- **Compliance does NOT equal Security**
 - Compliance is the act of conforming to documented standards or requirements and providing validation of that conformance.
- **Compliance focuses on validation, security focuses on protection!**
- **Compliance standards are static in nature and are slow to be updated**
- **Security is a dynamic, ever-changing beast**

<http://www.nttcom.tv/2012/05/29/report-shows-compliance-does-not-equal-security/>

The latest [Strategic Security Survey](#) from InformationWeek shows security professionals are having a tough time keeping up with the complexities of IT security. Unfortunately, they may also be missing some of the most relevant threats to their information security because they tend to focus too closely on making sure they meet compliance requirements. Sadly, the yardstick for a good security program during the past 10 years has been whether you are compliant or not.

http://blogs.computerworld.com/19631/is_compliance_equal_to_security

Compliance focuses on validation, security focuses on protection. Your security policies should explicitly dictate how IT should be protected. Firewall configurations, antivirus plans, server security, user password requirements and more all fall into the realm of security.

Compliance standards are static in nature and are slow to be updated. However, security is a dynamic, ever-changing beast that will devour you the first time that you take your eyes off of it -- ok, maybe that's a little melodramatic but there are a lot of actors in my family.

Security Awareness: Intro



Why!

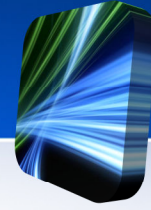
- **Why do we need Awareness? We have a firewall and we are compliant!**
- **Fundamentally, security is about people**
-Dr. Greg Newby
- **The primary cause of security breaches – **human error** – is not being adequately addressed. The person behind the PC continues to be the primary area where weaknesses are exposed.**
-Brian McCarthy, CompTIA COO

http://www.noticebored.com/html/why_awareness_.html

The true value of information security awareness – Source of good quotes

Information is the lifeblood of organizations, criminals want access to the data and steal money. They go after the weakest link – end users who are click happy!

Security Awareness: Intro



Weakest Link

- What is the weakest security link?
- **People are the Weakest Link!**
- What you don't know, can hurt you!
 - Phishing, Spear phishing, Social Engineering
 - What happens when you click that link?
- 44.8 percent of malware attacks required Human Interaction
- **You must teach think before you CLICK!**

What you don't know, can hurt you

"Unfortunately, people are still not thinking before opening an (e-mail) attachment. Every time a new virus comes out, people go out and do the same thing they shouldn't be doing," said Mike Breth, IT audit manager for the Westfield Group, an insurance and financial services company.

Security Awareness



Be aware! Be Secure!

- They Need to Know, how to identify suspicious emails!
- Teach them to Call IT Security, immediately if they click!
- Teach them about cyber-threats and the consequences!
- Conduct a Social Engineering Drill by Hiring IT Security firm & show them how easy it is to fail (2 years in a row)
- Awareness is about opening their eyes to the threats!
- Now you know, and *knowing is half the battle – GI Joe*

Security Awareness



Teaching Them

- Training is on going, never ending!
- It is a learning process for them
- It takes time and effort
- If they clicked it, don't yell at them work with them!



Security Awareness:

Do Not be the Weakest Link

Peter Garancis GSEC, CCNA, MSCA
AVP, Information Technology, Commerce State Bank, Inc.

We are a Cybercriminal Target



Did You Know!

- Targeted attacks are no longer limited to large organizations
- In 2011, nearly 20% of all cybercriminal targeted attacks are now directed at companies with fewer than 250 employees
- 58 percent of attacks target non-execs, employees in roles such as HR or sales

Targeted attacks are no longer limited to large organizations. More than 50 percent of such attacks target organizations with fewer than 2,500 employees, and almost 18 percent target companies with fewer than 250 employees. These organizations may be targeted because they are in the supply chain or partner ecosystem of a larger company and because they are less well-defended. Furthermore, 58 percent of attacks target non-execs, employees in roles such as human resources,, public relations, and sales. Individuals in these jobs may not have direct access to information, but they can serve as a direct link into the company. They are also easy for attackers to identify online and are used to getting proactive inquiries and attachments from unknown sources.

<http://www.darkreading.com/vulnerability-management/167901026/security/news/232901174/symantec-releases-internet-security-threat-report-volume-17.html>

I'm Invincible, NOT!



Warning! Warning!

- There is no such thing as perfect security
- Bad guys are compromising companies that have made expensive, responsible, and sustained efforts to defend their infrastructure
- **A Security breaches are inevitable!**
- **When a breach occurs, we want to be ready & prepared. So we can react fast & stop it!**

Malware: The Cyber Threat



Definitions

- **Malware** : Short for **malicious software** is any software that does bad things to your computer [Virus, Trojan, Worm]
- **Crimeware**: This malicious software is written by cyber criminals with the purpose of making money illegally. [Zeus, Spyeye]
- **Scareware**: Scam software of no benefit that is sold to consumers via certain unethical marketing practices. [Fake Anti-Virus]
- **Spyware**: A type of malware used to collect information without your knowledge. [Keylogger]

Websites and Malware



Did You Know!

- 30,000+ websites are infected every day and 80% of those infected sites are legitimate (SophosLab)
- 82 percent of malicious websites are hosted on compromised hosts.
- Advanced threats can be described in six stages: lures, redirects, exploit kits, dropper files, call-home communications, and data theft.

In the second half of the year we saw an average of approximately 30,000 new malicious URLs every day, an increase of more than 50% since our mid-year 2011 report.

The web will undoubtedly continue to be the most prominent vector of attack. Cybercriminals tend to focus where the weak spots are and use a technique until it becomes far less effective. We saw this with spam email, which is still present but less popular with cybercriminals as people deploy highly effective gateways. The web remains the dominant source of distribution for malware—in particular malware using social engineering, or targeting the browser and associated applications with exploits. Social media platforms and similar web applications have become hugely popular with the bad guys, a trend that is only set to continue.

<http://www.sophos.com/medialibrary/PDFs/other/SophosSecurityThreatReport2012.pdf>

Be Happy, Be Click Happy- NOT!



Did You Know!

- Cybercriminals prey on our curiosity, luring one to click a link or open an attachment.
- Nearly all data-stealing attacks today involve the web and/or e-mail.
- **44.8** percent of malware attacks required Human Interaction
- The use social engineering to take advantage of the human element as the weakest link is on the increase.

By preying on our curiosity, cybercriminals are able to use psychological traps to profit from unsuspecting users of technology.

"Nearly all data-stealing attacks today involve the web and/or e-mail. And many increasingly use social engineering to take advantage of the human element as the weakest link. Since the current generation of attackers use multiple data points and threat vectors to target their victims, only a solution that understands the entire threat lifecycle and combines data from each phase can protect against them."

Malware Evolution



Threats

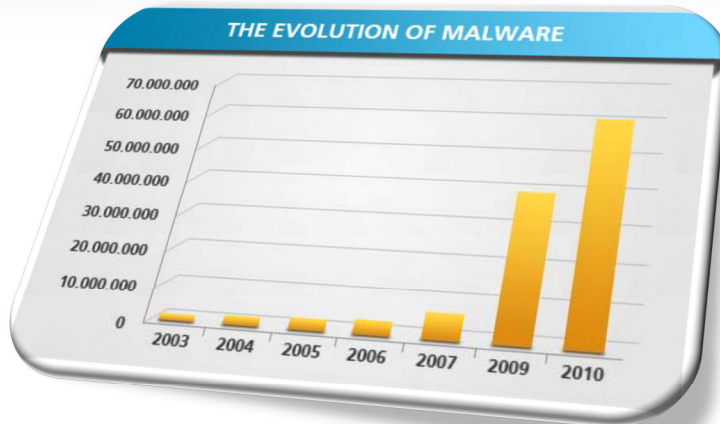
- Only a few years ago there were some 500 new threats every month
- Malware has been evolving and growing very quickly in the recent years.
- Can you guess how much malware is detected daily in 2011?

Exponential Growth of Malware



Threats

- In 2011 Panda Security detected 73,000 new variants a day, up 10K from 2010



PandaLabs, our anti-malware laboratory, receives on average 63,000 new threats every day. And this doesn't account for everything that is created, just what reaches us. It is not just a question of exponential growth, but an increasing trend. By 2009, our Collective Intelligence database contained almost 40,000,000 classified threats, and in 2010 we added some 20,000,000 more. That means we now have more than 60,000,000...

Five years ago, there were only 92,000 strains of malware cataloged throughout the company's 15-year history. This figure rose to 14 million by 2008 and 60 million by 2010, which gives a good indication of the rate of growth.

Type of Attacks



Threats

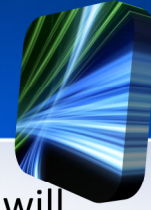
TABLE 1: FOUR MAJOR TYPES OF ATTACKS

THREAT ACTOR	EXAMPLE	TARGETS	OBJECTIVE
Criminal	Credit Card Theft	Enterprises that process credit cards or handle money such as retailers, banks, credit card processors.	Financial Gain
Hacktivists	Anonymous LulzSec	Anyone	Defamation, Press, Public Policy
Economic Espionage	Advanced Persistent Threat (APT)	Virtually any industry with an emphasis on blue chip companies and defense companies.	Economic Advantage
Nuisance	Botnets, Spam	Anyone, including individuals, small companies and large enterprises.	Launch points, nuisance, often consumer-based threats.

Drive By Downloads



The “Malware” Internet



Surf at own Risk


- *Drive-by download* is malware that will automatically downloaded to your computer, often without your consent or even your knowledge
- Drive-by downloads are particularly dangerous because they're so stealthy
- Unless you are protected, surfing the web can be dangerous since malware can automatically installs on the PC just visiting a web site!

One major cause is the growing number of drive-by download attacks. Drive-by downloads are an especially pernicious method cybercriminals use to install viruses and spyware, and otherwise take control of unsuspecting end users' computers.

Drive-by downloads are particularly dangerous because they're so stealthy: As their name suggests, they automatically install software on end users' computers without them knowing.

"Anytime someone else gets to decide what software, what code is running on your computer, then your computer—all the information on it and everything on the network that is connected to it—is at risk," says Daniel Peck, a research scientist with Barracuda Networks' Barracuda Labs.







Various Forms Malware






The Process

Today's landscape for web threats

Here are just a few of the techniques cybercriminals commonly use to distribute malware on the web:

-  **Blackhat search engine optimization (SEO)** ranks malware pages highly in search results.
-  **Social engineered click-jacking** tricks users into clicking on innocent-looking webpages.
-  **Spearphishing sites** mimic legitimate institutions, such as banks, in an attempt to steal account login credentials.
-  **Malvertising** embeds malware in ad networks that display across hundreds of legitimate, high-traffic sites.
-  **Compromised legitimate websites** host embedded malware that spreads to unsuspecting visitors.
-  **Drive-by downloads** exploit flaws in browser software to install malware just by visiting a webpage.

Malicious code typically installs spyware or malware by exploiting known vulnerabilities in your browser or associated plugins. These malware threats include:

-  **Fake antivirus** to extort money from the victim.
-  **Keyloggers** to capture personal information and account passwords for identity or financial theft.
-  **Botnet software** to subvert the system into silently joining a network that distributes spam, hosts illegal content or serves malware.

Cyber-crime organizations have a hierarchical structure whereby every action is performed by specialists. If you think about the different countries they are present in, you will get a clear idea of the number of people involved in these criminal activities, and who benefit from the anonymity provided by the Internet.

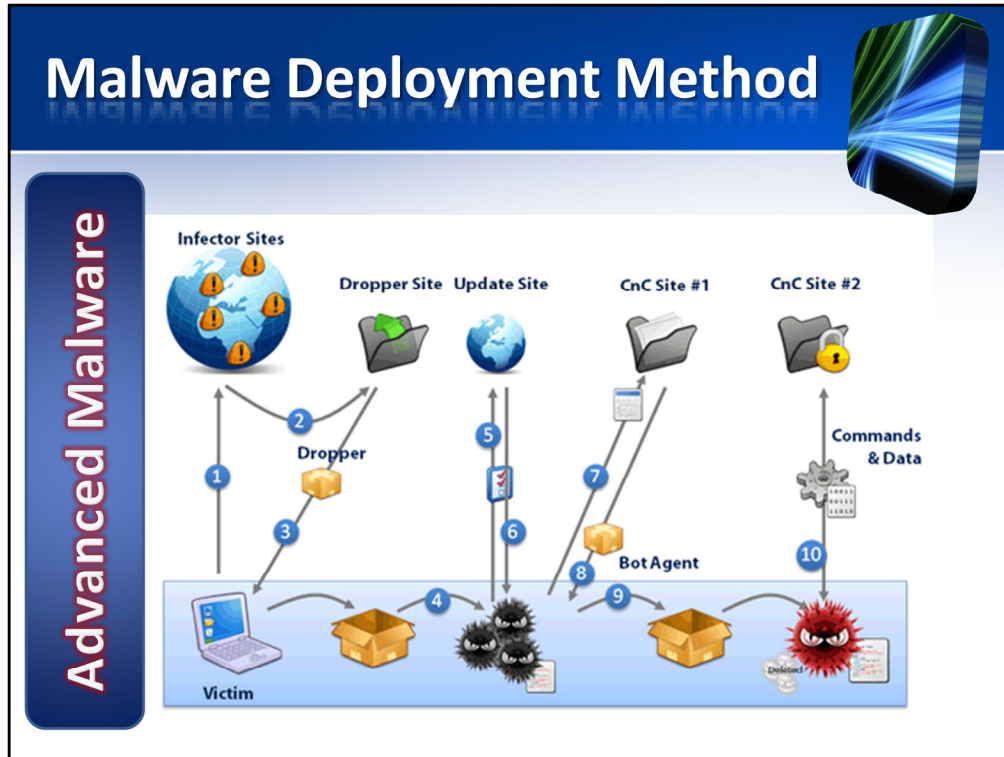
The heads of the criminal organizations start the ball rolling; they contract programmers and hackers, along with other technical experts, to launch indiscriminate attacks. Sometimes they will operate on their own and other times in coordination, often certain individuals will have several roles.

In general, hackers belonging to the criminal organization assign other hackers (or they take on the task themselves) the task of creating, phishing, bots, spam, fake Web pages to be indexed on search engines, etc.

New malware can be created and distributed in just a few minutes with Crimeware Toolkits or pre-prepared kits. This includes the online purchase of computer threats and the simplicity with which the message -with a little bit of social engineering- can be distributed across popular channels.

Social engineering is then used to trick victims through the most popular distribution vectors: email continues to be one of the most frequently used, although now social media (such as Facebook, YouTube, MySpace, Twitter, etc.) and fake Web pages positioned on well-known search engines (so called BlackHat SEO) are becoming increasingly popular.

Malware Deployment Method






1. Victim surfs to a website or clicks on email with link (e.g. phishing, drive-by download).
 2. Browser is redirected to a malicious dropper site.
 3. Victim is misled into downloading the dropper - or dropper is automatically downloaded through an exploit.
 4. Dropper unpacks on the Victim machine and runs.
 5. Dropper contacts a new site: UPDATE.
 6. UPDATE sends C&C instructions.
 7. Dropper contacts C&C Site #1 with Victim identity details.
 8. C&C Site #1 sends encrypted malware with new C&C instructions. Might even be 'locked' to Victim machine.
 9. Malware is decrypted by Dropper and installed. Dropper may stay behind as false evidence for investigators, or delete itself so that investigators believe that no infection has occurred.
 10. Malware contacts C&C Site #2. Sends passwords/data/etc. as encrypted payload.
- Steps 8, 9 and 10 can repeat indefinitely, with the malware 'evidence' and C&C connection instructions changing constantly. The malware can be repurposed or told to lay silent for prolonged periods of time.
 - Some security solutions attempt to detect and analyze the malware as it enters the organization in an effort to capture C&C details and forensics that could help with malware removal. Unfortunately, the lifecycle of the infection can happen so quickly, the malware that was analyzed no longer exists on the victim's machine.

A Compromised Network



Seek and Find

TABLE 2: EVIDENCE OF COMPROMISE BEYOND MALWARE

EVIDENCE OF COMPROMISE	DESCRIPTION
 Unauthorized Use of Valid Accounts	<p>In 100% of the cases Mandiant responded to this year the attacker used valid credentials.</p> <p>Evidence of such account activity can be found through the examination of Windows event logs, registry entries, file ownership, and network traffic captures.</p>
 Remote System/File Access	<p>Attackers use compromised systems to remotely access systems and files within the target environment.</p> <p>The Windows registry and web browser history often contains evidence of this activity.</p>
 Trace Evidence & Partial Files	<p>Attackers frequently remove tools, scripts, and files generated by their activities.</p> <p>Remnants of attacker activity can be found in restore points, scheduled task logs, and the Windows event logs.</p>

Malware In Action



Malware Detection



Hide and Seek

- Malware is not noisy (easy to find) it has evolved over the last 2-3 years to be extremely stealthy and hard to detect
- Malware will stay under the radar while it's doing its criminal activity
- The average time from infiltration to detection of security breaches is 173.5 days (Trustwave)

In the last three or four years there has been a major transformation in the nature of threats in the wild and how they have mutated into an extremely stealthy and hard to detect direction. That's been the most fundamental change in the last few years. [Malware] is not noisy, it's not designed to be obvious. It stays under the radar while it's doing its criminal activity; trying to make money for the criminal or nation state. That's really where the malware and the threat landscape have evolved. Malware is the key part of what the threat landscape is all about today. We have major cybercriminal activity on the Internet today with theft of identities, theft of credit card data, theft of intellectual property and actual theft of money from banks from within their corporate networks. All of this is enabled by this new sophisticated evolved class of malicious software.

<http://searchsecurity.techtarget.com/news/1373367/Modern-malware-stealthy-botnets-adapt-quickly-expert-says>

These questions have ramifications, particularly when we put them in the context of what evidence we do have. For example, if we discover that the discovered breaches are not exactly, as Foghorn would note, the sharpest knives in the drawer, what does it say about the ability of organizations to detect breaches when the average time from infiltration to detection is 173.5 days as reported by the Trustwave report?

<http://blog.triumfant.com/tag/antivirus-detection-rates/>

A Ghosts in the Machine!



Malware

- Malware can evade security with Stealth techniques!
- Attacks can begin with
 - Clicking the link in a phishing attack or spam email
 - Open an malicious attachment in an email
 - Drive-by download from a hacked site
 - Clicking the friendly looking link Facebook
- Malware can be a foothold allowing them to eventually compromise everything
- Malware can contact a malicious site and download more malware

Cyber attacks generally refer to criminal activity conducted via the Internet

Cyber crimes **tools of the trade** are malicious code, denial of service, stolen devices and web-based attacks.

weakest link

the end user

Attack often begins by simply luring an individual into clicking on an infected link.

The resulting page remotely exploits the individual, gains root access on the user's computer, and downloads malware to the user's computer in the background. The malware then acts as a control point inside the network, allowing the attacker to further expand the attack by finding other assets in the internal network, escalating privileges on the infected machine, and/or creating unauthorized administrative accounts — just to name a few tactics.

Letter of Dread.....



Lost Reputation

Dear Mr. W. E. Lost-r-money,

Our systems have been breached and ALL of your money has been stolen by a CyberCriminals. So **SORRY** they transferred \$25,000 dollars out of you accounts!

The monetary loss was due to the fact that I was watching a funny but malware laden bunny video. It came via email by friend, who by the way also hacked.

The video brought tears to my eyes and so do your monetary losses also. Have a nice day!

CSB Representative

The Cyber Crime Underground



Cyber Criminals

- Who makes the malware and why!
- What is the Cyber Crime Underground?
- What do they do with the information?
- How do they steal your money?
- Can we be protected?

Data is Valuable



Data = Money

- Data is VERY *valuable* - credit card No, Soc. Sec. No., passwords & bank accounts
- Criminals will steal, sell and profit from compromised confidential data
- Underground credit card shops specializing in the sale of compromised credit cards
- Credit Card sells with complete information as little \$2 for basic cards, \$25 for standard cards & \$40 for Gold, Platinum and Business

Details from these cards issued in the US can cost as little as \$2 for basic information, and \$25 for standard cards (\$40 for Gold, Platinum and Business) with complete information. Prices for European cards rise to \$5 in the first instance, and \$50 for full information (\$90 for most exclusive cards). The prices vary of course among different vendors, but these are average prices calculated from the information we have obtained across these sites. As we will see later, there are also discounts for bulk buying.

CyberCriminals - Hackers



Changing Tactics

- Hackers, no **CyberCriminals** aren't just producing malware for notoriety
- **They're producing it for large financial gain**
- Financially motivated cyber attackers are shifting toward longer-term presence on victim networks
- **They write malware that is really, really hard to detect**

Dirty Rotten Criminals



Cyber Attacks

- Cyber attacks generally refer to criminal activity conducted via the Internet.
- Cyber crimes can do serious harm to an organization's bottom line and reputation
- Around **80% of financial malware** is by Zeus with estimated global losses to be over **\$1 billion** in the last five years

☐ Cyber crimes can do serious harm to an organization's bottom line. We found that the median annualized cost of cyber crime for 50 organizations in our study is \$5.9 million per year, with a range of \$1.5 million to \$36.5 million each year per company. This represents an increase in median cost of 56 percent from our first cyber cost study published last year.

☐ Cyber attacks have become common occurrences. The companies in our study experienced 72 successful attacks per week and more than one successful attack per company per week. This represents an increase of 44 percent from last year's successful attack experience.

☐ The most costly cyber crimes are those caused by malicious code, denial of service, stolen devices and web-based attacks. Mitigation of such attacks requires enabling technologies such as SIEM and enterprise governance, risk management and compliance (GRC) solutions.

Cyber attacks generally refer to criminal activity conducted via the Internet. These attacks can include stealing an organization's intellectual property, confiscating online bank accounts, creating and distributing viruses on other computers, posting confidential business information on the Internet and disrupting a country's critical national infrastructure. Recent well-publicized cyber attacks – for instance, Wikileaks, Epsilon, Sony, Citibank, Boeing, Google, and RSA – have affected private and public sector organizations.

Cyber Crime is “Big” Business



Cyber Criminals

- Recognize the real problem is **crime**, not **hacking**!
- Cyber-Criminals are crime syndicates who rob and steal via the internet!
- Cyber-Criminals are evolving into companies that work much like real-world companies!
- Cyber-Criminals are organized, smart, and loaded with time and resources
- It's lucrative, low-cost and almost risk-free!

They are crime syndicates who are rob and **steal via the internet!** **MONEY**, need I say more! It's **lucrative, low-cost** and almost **risk-free!** Tons of **abundant** exploitable **targets** (No Locks). Many criminal hacking operations have been discovered, complete with all the standard appearance of a legitimate business with offices, receptionists, and cubicles full of dutiful hackers. These are criminal enterprises in the truest sense and their reach extends far beyond that of an individual hacker.

Not only do we face more sophisticated adversaries today, but the types of information of value to them are continually expanding as well. These groups can do interesting things with the most seemingly innocuous bits of information.

They are crime syndicates who are rob and **steal via the internet!**

Today's hacker fits the following profile:

- ✓ Has far more resources available to facilitate an attack
- ✓ Has greater technical depth and focus
- ✓ Is well funded
- ✓ Is better organized

MONEY, need I say more! It's **lucrative, low-cost** and almost **risk-free!** Tons of **abundant** exploitable **targets** (Bad locks easy access)

Cyber Criminals Brokers of Data



Data = Money

- Criminals do not restrict themselves just to the sale of credit card information:
- Sell stolen online bank account credentials
- Sale of online service accounts such as Paypal, eBay, webmail (Hotmail, Gmail) or social networks (Facebook, Twitter)

Bank accounts: Criminals do not restrict themselves just to the sale of credit card information, they also directly offer the details needed to access online bank accounts.

Once again, the prices vary depending on the bank in question. And similarly, there are different prices depending on whether the information corresponds to an account with a guaranteed balance or not.

The guaranteed bank balance can be as much as \$0.5 million and start at \$20,000. Depending on the type of bank (and its security measures) as well as the available balance, prices for information range from \$80 to \$700.

It is important to bear in mind that many of these vendors distinguish between personal accounts and business accounts (which have higher available balances).

Cyber-Crime Professionals



Cyber-Criminals

- 

1. Programmers. Who develop the exploits and malware used to commit cyber-crimes.
- 

2. Distributors. Who trade and sell stolen data and act as vouchers for the goods provided by other specialists.
- 

3. Tech experts. Who maintain the criminal enterprise's IT infrastructure, including servers, encryption technologies, databases, and the like.
- 

4. Hackers. Who search for and exploit applications, systems and network vulnerabilities.
- 

5. Fraudsters. Who create and deploy various social engineering schemes, such as phishing and spam.
- 

6. Hosted systems providers. Who offer safe hosting of illicit content servers and sites.
- 

7. Cashiers. Who control drop accounts and provide names and accounts to other criminals for a fee.
- 

8. Money mules. Who complete wire transfers between bank accounts. The money mules may use student and work visas to travel to the U.S. to open bank accounts.
- 

9. Tellers. Who are charged with transferring and laundering illicitly gained proceeds through digital currency services and different world currencies.
- 

10. Organization Leaders. Often "people persons" without technical skills. The leaders assemble the team and choose the targets.

Cyber-criminal Professional, just like any work you have a title, duty and responsibility. Cyber-crime organizations operate like companies, with experts specialized in each area and position. Yet unlike most companies, they don't have timetables, holidays or weekends. They cyber criminal professional are part of organized syncicate.

Black Market Products



Cyber Criminals

Sale Item	Underground Price
Credit Card: Consists of a credit card's 16-digit PAN, CVV2 code, expiration date, billing address	\$1.50 - \$3.00
SSN / DOB / MMN personal details are very often used by banks to authenticate an individual's identity	MMN \$5 - \$6 SSN \$1 - \$3 DOB \$1 - \$3
Track 2 Data (aka "Dumps") "Track-2" information is found on a payment card's magnetic stripe.	Standard cards: \$15 - \$20 Gold/ Platinum: \$20 - \$80 Business/ Corporate: \$30 - \$40
Online Banking Logins: Consist of a consumer's username, password, and in some cases additional information.	\$50 - \$1,000 per account
Full Data Sets: Details of consumer's online banking credentials (e.g., username and password), mailing address, card No., CVV2 code, expiration date, MMN, DOB, SSN.	\$5 - \$20 per set
Bulletproof Hosting: Hosting service for cybercriminals to host malicious content.	\$87 - \$400 per month depending on the service level
Zeus Trojan Kit One of today's most pervasive banking Trojans. With an infection rate of thousands of computers per day	Zeus Kit: \$3K - \$4K - Firefox form grabber \$2000 - Windows 7 Support \$2000
SpyEye Trojan Kit One of the most advanced current-day Trojans	- Basic kit - \$1,000 - Firefox Tool - \$1,000 - \$2000

Credit cards. Of course, credit cards still figure largely. Yet the illicit sale of these has become much more professional:

Delivery details. In the past, the credit card number was delivered with the PIN. Now however, the amount of data needed has increased considerably, and the information delivered covers all the needs for any online or offline operation. The following data is supplied when buying credit card details:

The Cyber Crime Underground



The Zombie Army



BOTNET

- A **botnet** (aka Zombie Army) is a collection of compromised computers, each of which is known as a '**bot**'
- Hackers to take control of the compromised PCs & turn them into **zombie** computers
- Zombie PCs then operate as part of a powerful "**botnet**" to spread viruses, generate spam, and commit various online crime and fraud

Jericho Botnet



Target Banks

- The Jericho botnet is taking aim at banks and financial institutions
- This stealthy program which piggybacks on common applications allows Jericho to avoid detection by most antivirus software
- 42 samples analyzed by Palo Alto Networks, the top AV solutions only achieved a 3.2% detection rate on the day of discovery
- 12 of the 42 signatures were not detected at all over a seven-day span

Jericho demonstrates a number of behaviors that are designed for stealth, persistence, and avoidance of traditional signature-based approaches to malware detection, the researchers say.

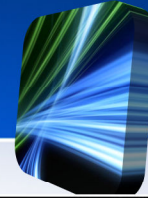
Using a combination of a stealthy program and piggybacking on common applications, Jericho has avoided the scrutiny of most antivirus vendors, the researchers said.

"Of the 42 samples analyzed by Palo Alto Networks, the top AV solutions only achieved a 3.2 percent detection rate on the day [of discovery]," Palo Alto Networks says. Twelve of the 42 signatures were not detected at all over a seven-day span.

"This trend seems to indicate that this particular criminal operation is cognizant of the AV coverage for their malware, and has established a delivery strategy that minimizes collection by AV vendors," the researchers say.

<http://www.darkreading.com/threat-intelligence/167901121/security/vulnerabilities/232901514/jericho-botnet-targets-banks-and-financial-institutions.html>

Get You Malware w/ support



Cyber Tools

- **Commercial “dual-use”**
Trojan creator
- V.4 New features
 - Remote Desktop
 - Webcam Streaming
 - Audio Streaming
 - Remote passwords
 - MSN Sniffer
 - Remote Shell
 - Advanced File Manager
 - Online & Offline keylogger
 - Information about remote computer
 - Etc..
- Three versions
 - Gold, Silver & Bronze

1

2

Gold Edition

- 6 months (unlimited) or 9 months(maximum 3 times) replacement warranty if it gets detected by any antivirus (you can choose 6 months or 9 months)
- 724 online support via e-mail and instant messengers
- Supports Windows 95/98/ME/NT/2000/2003/XP/Vista
- Remote Shell (Managing with Ms-Dos Commands)
- Webcam - audio streaming and msn sniffer
- Controlling remote computer via keyboard and mouse
- Notifies changes on clipboard and save them
- Technical support after installing software
- Viewing pictures without any download(Thumbnail Viewer)

Price : 249\$ (United State Dollar)

Wow 24/7 Online Support



Cyber Tools

- **Commercial "dual-use"**
Trojan creator
- V.4 New features
- Remote Desktop



Gold Edition

- 6 months (unlimited) or 9 months(maximum 3 times) replacement warranty if it gets detected by any antivirus (you can choose 6 months or 9 months)
- 7/24 online support via e-mail and instant messengers
- Supports Windows 95/98/ME/NT/2000/2003/XP/Vista
- Remote Shell (Managing with Ms-Dos Commands)
- Webcam - audio streaming and msn sniffer
- Controlling remote computer via keyboard and mouse
- Notifies changes on clipboard and save them
- Technical support after installing software
- Viewing pictures without any download(Thumbnail Viewer)

Price : 249\$ (United State Dollar)

Price : 249\$ (United State Dollar)

Passive

Social Engineering



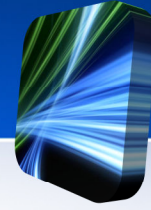
Loose Lips

- Cyber Criminals do not just rely on Malware, they attack us!
- Social Engineering is a non-technical kind of intrusion that relies heavily on human interaction.
- It often involves tricking other people to break normal security procedures.
- Social Engineering can use email, Social Media, faxes, text message, phone calls, or in person.

Social Engineering



Social Engineering



Loose Lips

- People are constantly being duped into installing malicious malware or giving up confidential information
- **Phone Call:** You may get a Fake Tech Support Call or vendor requesting Info
- **Email:** Phishing or spam request info
- **Fake Anti-Virus:** Require you to run a scan or fix a fake problem

CSB Phishing / Spam



From: Facebook [\[mailto:alert@facebookmail.com\]](mailto:alert@facebookmail.com)
Sent: Thursday, May 03, 2012 9:54 AM
To: jfazio@commercestebank.com; jbackhaus@commercestebank.com; jbaum@commercestebank.com; mhaaherriges@commercestebank.com; bkuhn@commercestebank.com; dborchardt@commercestebank.com; cwo
Subject: Someone has commented your status update

facebook

Hi jfazio,

You have disabled your Facebook account. You can reopen your account whenever you wish by logging into Facebook using your former login email address and password. After that you will be able to use the site in the same way as before.

Sign in to Facebook
and start connecting

Sign in

Thanks and regards,
The Facebook Team

<http://3dmobilegamingcontest.com/maiderargazkiak/fb.html>

Follow the link below:

Click to follow link

<http://www.facebook.com/home.php>

This message was sent to jfazio@commercestebank.com. If you don't want to receive these emails from Facebook in the future, please click: [unsubscribe](#).
Facebook, Inc. Attention: Department 415 P.O. Box 10005 Palo Alto CA 94303

Social Engineering



Defense in Depth



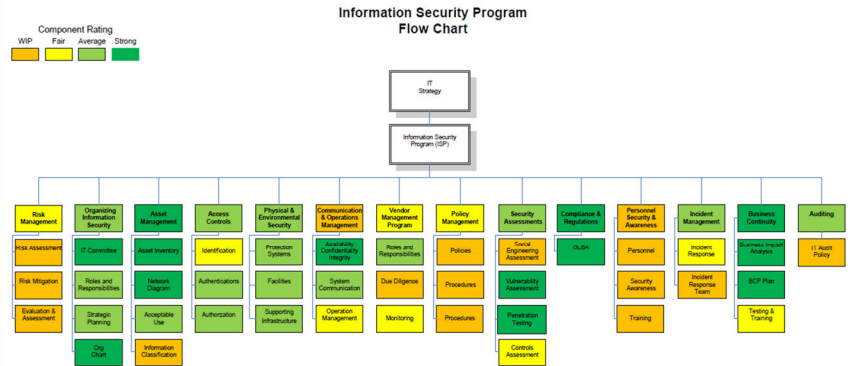
Concept

- **Defense in Depth** is the coordinated use of multiple security countermeasures to protect the integrity of the information assets in an enterprise.

Defense in Depth



Info Sec Program



Defense in Depth



Technology & YOU

- Commerce State Bank uses various products to protect the network:
 - Firewall - Perimeter
 - Antivirus software - Desktop
 - Intrusion Protection Systems - Malware
 - Patch Management – Exploits
 - Web Filter – Perimeter
 - Logs – Forensic
 - Monitoring – Proactive

Human Firewall



Or Weakest Link

- A very important part of security is You..
...YES YOU!
- We have various security technology in place but cyber criminals can trick you to install malware for them!!!
- **44.8** percent of malware attacks required Human Interaction

Human Firewall



Trick or Treat

- You are a BIG Factor in security and you can be the weakest link or a strong one
- Your actions can greatly REDUCE the risk of a security breach or cause a breach
- Criminals use social engineering, phishing, drive-by attacks, social media sites, compromised emails as avenue of attacks
- Web surfing, open attachments or clicking links can unleash malware onto the network.

Passwords



Strong & Complex

- Passwords are the lock to the computer and protect the sensitive data
- A stolen password gives others the power to:
 - Access Secured Systems
 - Modify or destroy your files
 - Send electronic mail in your name
- Malware can crack a weak passwords in seconds!
- Weak: Packers1, Cabbage2, Banking3 or Password4...

Long Live Conficker Worm



Weak Passwords

- A **3-year-old 'dead' Windows worm** infection is still spreading via **weak or stolen passwords**
- The Orphaned botnet worm spread to **1.7 million** Windows PCs worldwide last year
- 92% of the Conficker infections came through bad passwords and 8% via unpatched systems
- The worm was found 220 million times during the past two-and-a-half years

Security patching is still an important strategy for preventing infection. Another easier method to secure your PC is **STRONG** passwords! Yet people still use weak or easy to guess passwords, which is allowing an 3 year old Windows worm to still spread via the internet. What about the newer threat that are harder to detect can break in with a weak password.

More than three years after its initial release, the Conficker worm is still the most commonly encountered piece of malicious software, representing 14.8% of all infection attempts seen by Sophos customers in the last six months. Evidently, plenty of infected PCs are still trying to spread this old worm.

The orphaned botnet worm Conficker spread to 1.7 million Windows machines worldwide by the end of last year despite a major industry initiative led by Microsoft over the past three years that neutered it.

Password – Make'm Strong!



Is it Safe.....Heck No!



Reduce the Risk

- Is the web safe- NO! A PC can be infected with malware via many avenue
- An unsecured computer connected to the internet becomes infected 5 to 15 minutes
- Can you greatly reduce the risk of malware invading your computer- YES!

Use Protection



Fix the holes

- Secure your browser
 - <https://browsercheck.qualys.com/>
- Patch, Patch and Patch – Turn on Auto updates on your PC
- Patch you third party software – Adobe Reader & Flash, Quicktime, iTunes, Java
- Numerous malware attacks use older exploits & a patched PC can avoid these

At Home are you safe....



Home Defense

- Use an Internet Security Suite
 - Anti-Virus/Malware, Anti-Phishing, Firewall
 - Keep it up to date (Renew the subscription)
- Enable the software Firewall
- Use a hardware firewall (internet router)
- Secure your Wireless
- Set strong passwords on you PC
 - You can enable auto login

Mobile Malware Threats



The Next Frontier

- From 2012 to 2011, the Juniper identified a 155% increase in mobile malware across all device platforms
- In the last 7 months of 2011 alone Juniper found, malware targeting the Android platform rose **3,325%** to 13,302 samples.
- 30% of all mobile applications have the ability to obtain device locations without consent
- 14.7% of all applications have the ability to make phone calls without the user's consent

Conclusion



Security Awareness

- Every minute, 232 computers are infected by malware.
- Cybercriminals develop lightning fast attacks and create new malware code thus making it harder for organizations to manage risk
- One of the most important lines of defense is Security Awareness, patching your PC, Don't click it....and so on....
- **Be Aware, Be Secure!**

Q & A

