



ACTIVITY ALERT

Cyber Activity Alert

AA20-017A

NUMBER

January 31, 2020

DATE

Threat Actor TA2101 (ProofPoint) using Maze Ransomware to target Government and Commercial Entities

CONTENTS

Key Takeaways.....	1
Executive Summary.....	1
Technical Details.....	2
Mitigations	5
Resources	5
Contact Information.....	6
Feedback.....	6

KEY TAKEAWAYS

- A threat actor known as TA2101 has been observed targeting government and commercial agencies with Maze ransomware since October 2019.ⁱ
- TA2101 leveraged unpatched vulnerabilities to compromise systems by using phishing emails to exfiltrate and encrypt the victim's data with Maze ransomware.
- CISA has identified multiple indicators that organizations can use to identify and block activity relating to TA2101/Maze ransomware.

EXECUTIVE SUMMARY

From open-source reporting, TA2101 has been observed using Maze ransomware to encrypt and exfiltrate the files of U.S. and international governments and commercial organizations in an attempt to extort money from their targets. TA2101 has also been identified implementing spam campaigns and impersonating foreign and domestic government agencies and security vendors.

DISCLAIMER: This report is provided "as is" for informational purposes only. The Department of Homeland Security (DHS) does not provide any warranties of any kind regarding any information contained within. The DHS does not endorse any commercial product or service, referenced in this bulletin or otherwise. This document is distributed as TLP:GREEN: Limited disclosure, restricted to the community. Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels. Information in this category can be circulated widely within a particular community. TLP:GREEN information may not be released outside of the community. For more information on the Traffic Light Protocol, see <http://www.us-cert.gov/tlp>.

WARNING: This document is UNCLASSIFIED//For Official Use Only (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with the DHS policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need to know" without prior approval of an authorized DHS office.



CISA
CYBER+INFRASTRUCTURE

TECHNICAL DETAILS

Description

A threat actor, named “TA2101” by ProofPoint,¹ has been using a variant of the ChaCha ransomware, known as Maze ransomware. Activity relating to this threat actor and type of ransomware has been identified as early as May 2019.² There were no public reports on Maze ransomware activity until an Italian media source reported the activity and ProofPoint assigned the activity to a new actor, which ProofPoint named TA2101. If a victim does not pay the initial ransomware within a certain timeframe, the threat actor publishes a percentage of the victim’s data to a public website. Data published has sensitive personally identifiable information (PII) and sensitive proprietary information.^{3,4}



Figure 1: Example screenshot from a system affected by Maze ransomware

The threat actor allows victims to decrypt a number of files for free to provide assurance to the victim that the encryption can be reversed. TA2101 uses Maze ransomware to encrypt directories separately and save them to two separate files: `DECRYPT-FILES.TXT` and a randomly generated filename.

Detection and Response

The Cybersecurity and Infrastructure Security Agency (CISA) recommends blocking all high confidence indicators, which are shown in **red**. Indicators in ***purple** can also be used for detection of Maze

¹ ProofPoint, “TA2101 plays government imposter to distribute malw are to German, Italian, and US organizations”, November 14, 2019, <https://www.proofpoint.com/us/threat-insight/post/ta2101-plays-government-imposter-distribute-malw-are-german-italian-and-us>

² BlogSpot, “Maze Ransomw are ChaCha Ransomw are”, May 13, 2019, <http://id-ransomw-are.blogspot.com/2019/05/chacha-ransomw-are.html>

³ Bleeping Computer, “Maze Ransomw are Publishes 14GB of Stolen Southw ire Files,” January 10, 2020, <https://www.bleepingcomputer.com/news/security/maze-ransomw-are-publishes-14gb-of-stolen-southw-ire-files/>

⁴ BlogSpot, “Guide to Remove Maze Ransomw are from Computer”, October 18, 2019, <https://pc-malw-are.blogspot.com/2019/10/remove-maze-ransomw-are.html>

ransomware; however, indicators in purple could be legitimate activity or may only be temporarily related to the threat actor. Therefore, CISA suggests using indicators in purple for detection only.

IP addresses

5.199.167.188	91.218.114.38	92.63.32.2	104.168.201.35
45.76.149.204	91.218.114.77	*92.63.32.55	104.168.201.47
91.218.114.4	92.63.8.47	92.63.37.100	104.168.215.54
91.218.114.11	92.63.11.151	92.63.194.3	146.0.72.85
91.218.114.25	92.63.15.6	92.63.194.20	149.56.245.196
91.218.114.26	92.63.15.8	104.238.158.250	185.147.15.22
91.218.114.31	92.63.15.56	104.168.174.32	195.123.217.13
91.218.114.32	92.63.17.245	104.168.198.208	198.50.168.67
91.218.114.37	92.63.29.137	104.168.198.230	

Domains

introle[.]biz	zhengjuncai[.]monster	heatmoscover[.]xyz
plex[.]direct	healyproductbest[.]review	publistendick[.]xyz
agenziaentrate[.]jicu	download-invoice[.]site	thisrich[.]xyz
agenziaentrateinformazioni[.]jicu	malaysiaenterkini[.]site	succeptishough[.]xyz
agenziainformazioni[.]jicu	conbase[.]top	throposition[.]xyz
bzst-info[.]jicu	mazedecrypt[.]top	werenceptical[.]xyz
hilfe-center-1und1[.]jicu	condurises[.]xyz	yearinesents[.]xyz
intralian[.]jicu	emplementriaton[.]xyz	
usps-deliveryservice[.]jicu	fantimit[.]xyz	
1drivelive[.]com	canadian-overnite[.]com	activate[.]netonline[.]net
aloha-edc[.]net	info-delivery-notification[.]com	bayi.netonline[.]net
gsitestat[.]com	lj-kabel[.]net	beta-bayi[.]kibrisonline[.]com
nesinoder[.]com		dev-bayi[.]netonline[.]net
set-validator[.]com	hotspot.easygonet[.]com	dev-hotspotpanel[.]netonline [.]net
wwwcolnbase[.]com	webislem[.]kibrisonline[.]com	
gidra2web[.]shop	hidra2wep[.]com	hydro2wed[.]com
gidraruzxpnew4af[.]com	hudra2wed[.]com	hydro2wep[.]com
gudra2wed[.]com	hudra2wep[.]com	onion[.]business
gudra2wep[.]com	hybra2web[.]co	onion[.]capital
gybra2web[.]com	hydpa2web[.]com	onion[.]cards
gydra2web[.]co	hydr2aweb[.]com	onion[.]fish
gydra2web[.]shop	hydra2ewb[.]com	onion[.]limited
gydra2wed[.]com	hydra2ved[.]com	onion[.]management
gydra2wep[.]com	hydra2wed[.]co	onion[.]photo
hedra2wep[.]com	hydra2weg[.]com	onion[.]shopping
hibra2web[.]com	hydra2wep[.]co	
hidra2wed[.]com	hydra4web[.]com	
dependepeat[.]info	apkeseay[.]info	apkitsall[.]info
mostualled[.]info	apkfinder[.]info	apks-rec[.]info
all-apk[.]info	apk-get-update[.]info	apk-rool[.]info
apkbit[.]info	apkhila[.]info	apkrool[.]info

apk-tools[.]info
 apktool[.]info
 apktwin[.]info
 apk-update[.]info
 appsfans[.]info
 bit-apk[.]info

freshapk[.]info
 get-apk-update[.]info
 instaapk[.]info
 pure-apk[.]info
 qwecklyapk[.]info
 to-apk[.]info

true-apk[.]info
 trueapk[.]info
 upd-ur-apk[.]info
 update-ur-apk[.]info

sicurezza[.]me
 mx2[.]imgk [.]pl
 fermeri1[.]ru
 i1fermer[.]ru

lbi1[.]ru
 bayii[.]netcity[.]net[.]tr
 shop[.]nethouse[.]net[.]tr
 missiondirectorates[.]us

soresponsiblesd[.]us
 nano-care[.]vn

MD5 Hashes

0F841C6332C89EAA7CAC14C9D5B1D35B
 21A563F958B73D453AD91E251B11855C
 27C5ECBB94B84C315D56673A851B6CF9
 2FBD10975EE65845A18AF6B7488A5236
 44B21AF75880AF21BAD9FDA1DD953815
 5774F35D180C0702741A46D98190FF37
 5DF79164B6D0661277F11691121B1D53
 79D137D91BE9819930EEB3876E4FBE79
 87239CE48FC8196A5AB66D8562F48F26
 A0DC59B0F4FDF6D4656946865433BCCE
 A0C5B4ADBCD9EB6DE9D32537B16C423B
 A3A3495AE2FC83479BAEAF1878E1EA84
 B3E674E85A9BB5ACA3ABBC17FD99F603
 BE537A66D01C67076C8491B05866C894
 BF2E43FF8542E73C1B27291E0DF06AFD
 D2DDA72FF2FBBB89BD871C5FC21EE96A
 D727F747F5D1F6C88FC0032B8B1B8BA9
 E69A8EB94F65480980DEAF1FF5A431A6
 F5ECDA7DD8BB1C514F93C09CEA8AE00D
 F83FB9CE6A83DA58B20685C1D7E1E546

- wordupd.tmp
 - wordupd.tmp
 - wordupd.tmp
 - USPS_Delivery.doc
 - peexe
 - peexe
 - peexe
 - peexe
 - winupd.tmp, peexe
 - peexe
 - wordupd.tmp
 - peexe
 - peexe
 - peexe
 - peexe
 - peexe
 - peexe
 - peexe
 - wordupd.tmp
 - peexe

1304606861C8D05f5BBA92D225ADC69A
 1FFECD461B3D4B65E44fAFF8537F68D6
 3BFCBA2DD05E1C75F86C008F3D245F62
 53D5BDC6BD7904B44078CF80E239D42B
 54C9A5FC6149007E9B727FCCCDAFBBD4
 65CF08FFAF12E47DE8CD37098AAC5B33
 80043A5B285DA88FB63D469243655751
 8205A1106AE91D0B0705992D61E84AB2
 916D7838CD5A30015D75D1D783053EF7
 9ABAD04C13B62E379642EEEC6E55C712
 A2D631FCB08A6C840C23A8F46F6892DD
 A3386E5D833C8DC5DFBB772D1D27C7D1
 AA87D4E3133F9E4591EA6179CA7AFF3C
 AD30987A53B1B0264D806805CE1A2561
 B40A9EDA37493425782BDA4A3D9DAD58
 B4D6CB4E52BB525EBE43349076A240DF

- VERDI.DOC
 - Steuerbescheid-8508884191-78843000-140.doc
 - eset.exe
 - VERDI.doc
 - Coupon_91658155.exe
 - peexe, 01NYX3xs.tmp
 - Steuerbescheid.doc
 - 1473359.exe, peexe
 - Windowsupdate.bat
 - ball.exe, peexe
 - cure.doc
 - 7.dd, peexe
 - Invoice_97544835.exe, peexe
 - VERDI.doc
 - Invoice_29557473.exe, peexe
 - dospizdos.tmp, peexe

C09AF442E8C808C953F4FA461956A30F	- Steuerbescheid.doc
C3341B7DFB9D43BCA8C812E07B4299F	- pass.exe
D552BE44A11D831E874E05CADAFE04B6	- LOAD_ENC DLL.EXE, peexe
DEEBBEA18401E8B5E83C410C6D3A8B4E	- ESET32.EXE, peexe
EE26E33725B14850B1776A67BD8F2D0A	- R19340003422.doc
F04D404D84BE66E64A584D425844B926	- out2.exe, peexe
FBA4CBB7167176990D5A8D24E9505F71	- 1-1.exe, peexe

Note: if organizations detect any of the hashes above on their systems, the filenames associated with the hashes may be different than those identified in purple text. The filenames in purple text are expected to be short-lived or possibly matching legitimate filenames.

There are many Maze ransomware URLs that can be found from open-source reporting and tools, but CISA does not suggest using URLs for blocking as there are very few URLs that use a repeatable or defined pattern. CISA suggests concentrating on domain, IP address, and hash indicators for prevention and detection.

MITIGATIONS

To protect systems from Maze ransomware, CISA recommends organizations ensure:

- Personnel know how to identify phishing emails, and
- Internal protections are in place to protect systems.

Internal protections include ensuring antivirus software, operating systems, and other programs are up to date to the current released version or a level at which the organization is willing to accept the risk in accordance with information assurance (IA) policies and CISA [Binding Operational Directives \(BODs\)](#).⁵ For additional general guidance on ransomware, see:

- CISA's Tip on [Protecting Against Ransomware](#) and
- CISA's [Ransomware page](#).

RESOURCES

Media Reports

1. Ransomware blog resource (in Russian) (CISA recommends blocking all javascript on this site with a script blocker)
<http://id-ransomware.blogspot.com/2019/05/chacha-ransomware.html> (May 13, 2019)
 - a. English translation of above site
<https://translate.google.ru/translate?hl=ru&tab=wT&sl=ru&tl=en&u=https%3A%2F%2Fid-ransomware.blogspot.com%2F2019%2F05%2Fchacha-ransomware.html>
2. <https://www.abuseipdb.com/check/70.96.202.66> (May 30, 2019)
3. <https://www.metacompliance.com/blog/onedrive-users-hit-with-sneaky-phishing-scam/> (July 4, 2019)
4. <https://pc-malware.blogspot.com/2019/10/remove-maze-ransomware.html> (October 18, 2019)

⁵ CISA, Cybersecurity Directives, <https://cyber.dhs.gov/directives/>

5. <https://www.cybersecurity360.it/nuove-minacce/ransomware/maze-il-ransomware-nascosto-dietro-finte-comunicazioni-dellagenzia-delle-entrate-come-difendersi/> (October 29, 2019)
6. <https://newsbeezer.com/italyeng/maze-the-virus-that-comes-with-a-fake-e-mail-from-the-inland-revenue-and-infects-the-devices/> (November 11, 2019)
7. <https://www.proofpoint.com/us/threat-insight/post/ta2101-plays-government-imposter-distribute-malware-german-italian-and-us> (November 14, 2019)
8. <https://blog.talosintelligence.com/2019/12/IR-Lessons-Maze.html> (December 17, 2019)
9. <https://krebsonsecurity.com/2019/12/ransomware-gangs-now-outing-victim-businesses-that-dont-pay-up/#more-49994> (December 19, 2019)
10. <https://labs.sentinelone.com/maze-ransomware-update-extorting-and-exposing-victims/> (December 19, 2019)

Whitepaper from National Cyber-Forensics and Training Alliance

- https://1f3r982zgpjh2wuihs3suki9-wpengine.netdna-ssl.com/wp-content/uploads/2019/12/Maze_Whitepaper.pdf (December 2, 2019)

Suricata Signatures relating to Maze Ransomware

- <https://doc.emergingthreats.net/bin/view/Main/2027392>

CONTACT INFORMATION

CISA encourages recipients of this report to contribute any additional information that they may have related to this threat. For any questions related to this report, please contact CISA at

- 1-888-282-0870 (From outside the United States: +1-703-235-8832)
- CISAServiceDesk@cisa.dhs.gov (UNCLASS)
- us-cert@dhs.sgov.gov (SIPRNET)
- us-cert@dhs.ic.gov (JWICS)

CISA encourages you to report any suspicious activity, including cybersecurity incidents, possible malicious code, software vulnerabilities, and phishing-related scams. Reporting forms can be found on the CISA homepage at <http://www.us-cert.gov/>.

FEEDBACK

CISA strives to make this report a valuable tool for our partners and welcomes feedback on how this publication could be improved. You can help by answering a few short questions about this report at the following URL: <https://www.us-cert.gov/forms/feedback>.

ⁱ Bleeping Computer, "Maze Ransomware Behind Pensacola Cyberattack, \$1M Ransom Demand," December 11, 2019, <https://www.bleepingcomputer.com/news/security/maze-ransomware-behind-pensacola-cyberattack-1m-ransom-demand/>