ACTIVITY ALERT

Cyber Activity Alert

AA20-017Av2 NUMBER

February 27, 2020 DATE

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

CONTENTS

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.

***Note**: This Activity Alert updates Activity Alert AA20-017A. See the Domains section for more information on the update.*

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 personably 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 malware to German, Italian, and US organizations", November 14, 2019, https://www.proofpoint.com/us/threat-insight/post/ta2101-plays-government-imposter-distribute-malware-german-italian-and-us
[2] BlogSpot, "Maze Ransomware ChaCha Ransomware", May 13, 2019, http://id-ransomware.blogspot.com/2019/05/chacha-ransomware.html
[3] Bleeping Computer, "Maze Ransomware Publishes 14GB of Stolen Southwire Files," January 10, 2020, https://www.bleepingcomputer.com/news/security/maze-ransomware-publishes-14gb-of-stolen-southwire-files/
[4] BlogSpot, "Guide to Remove Maze Ransomware from Computer", October 18, 2019, https://pc-malware.blogspot.com/2019/10/remove-maze-ransomware.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
45.76.149.204
91.218.114.4
91.218.114.11
91.218.114.25
91.218.114.26
91.218.114.31
91.218.114.32
91.218.114.37
91.218.114.38
91.218.114.77
92.63.8.47
92.63.11.151
92.63.15.6
92.63.15.8
92.63.15.56
92.63.17.245
92.63.29.137
92.63.32.2
*92.63.32.55
92.63.37.100
92.63.194.3
92.63.194.20
104.238.158.250
104.168.174.32
104.168.198.208
104.168.198.230
104.168.201.35
104.168.201.47
104.168.215.54
146.0.72.85
149.56.245.196
185.147.15.22
195.123.217.13
198.50.168.67

Domains

introle[.]biz
agenziaentrate[.]icu
agenziaentrateinformazioni[.]icu
agenziainformazioni[.]icu
bzst-info[.]icu
hilfe-center-1und1[.]icu
intralian[.]icu
usps-deliveryservice[.]icu
zhengjuncai[.]monster
healtyproductbest[.]review
download-invoice[.]site
malaysiaterkini[.]site
conbase[.]top
mazedecrypt[.]top
condurises[.]xyz
emplementriaton[.]xyz
fantimit[.]xyz
heatmoscover[.]xyz
publistendick[.]xyz
thistrich[.]xyz
succeptishough[.]xyz
thropossion[.]xyz
werenceptical[.]xyz
yearinesents[.]xyz

1drivelive[.]com
aloha-edc[.]net
gsitestat[.]com
nesinoder[.]com
set-validator[.]com
wwwcolnbase[.]com
canadian-overnite[.]com
info-delivery-notification[.]com
lj-kabel[.]net
hotspot.easygonet[.]com
webislem[.]kibrisonline[.]com
activate[.]netonline[.]net
bayi.netonline[.]net
beta-bayi[.]kibrisonline[.]com
dev-bayi[.]netonline[.]net
dev-hotspotpanel[.]netonline [.]net

gidra2web[.]shop
gidraruzxpnew4af[.]com
gudra2wed[.]com
gudra2wep[.]com
gybra2web[.]com
gydra2web[.]co
gydra2web[.]shop
gydra2wed[.]com
gydra2wep[.]com
hedra2wep[.]com
hibra2web[.]com
hidra2wed[.]com
hidra2wep[.]com
hudra2wed[.]com
hudra2wep[.]com
hybra2web[.]co
hydpa2web[.]com
hydr2aweb[.]com
hydra2ewb[.]com
hydra2ved[.]com
hydra2wed[.]co
hydra2weg[.]com
hydra2wep[.]co
hydra4web[.]com
hydro2wed[.]com
hydro2wep[.]com
onion[.]business
onion[.]capital
onion[.]cards
onion[.]fish
onion[.]limited
onion[.]management
onion[.]photo
onion[.]shopping

dependepeal[.]info
mostualled[.]info
all-apk[.]info
apkbit[.]info
apkeseay[.]info
apkfinder[.]info
apk-get-update[.]info
apkhila[.]info
apkitsall[.]info
apks-rec[.]info
apk-rool[.]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[.]mgk [.]pl
fermeri1[.]ru
i1fermer[.]ru
lbi1[.]ru
bayi[.]netcity[.]net[.]tr
shop[.]nethouse[.]net[.]tr
missiondirectorates[.]us
soresponsiblesd[.]us
nano-care[.]vn

***Note**: this Activity Alert has been updated to remove indicator plex[.]direct because it is a legitimate domain; however, CISA recommends reviewing activity related to plex[.]direct that does not not use port 32400. This type of activity should be considered suspicious.*

MD5 Hashes

0F841C6332C89EAA7CAC14C9D5B1D35B - wordupd.tmp
21A563F958B73D453AD91E251B11855C - wordupd.tmp
27C5ECBB94B84C315D56673A851B6CF9 - wordupd.tmp
2FBD10975EE65845A18AF6B7488A5236 - USPS_Delivery.doc
44B21AF75880AF21BAD9FDA1DD953815 - peexe
5774F35D180C0702741A46D98190FF37 - peexe
5DF79164B6D0661277F11691121B1D53 - peexe
79D137D91BE9819930EEB3876E4FBE79 - peexe
87239CE48FC8196A5AB66D8562F48F26 - winupd.tmp, peexe
A0DC59B0F4FDF6D4656946865433BCCE - peexe
A0C5B4ADBCD9EB6DE9D32537B16C423B - wordupd.tmp
A3A3495AE2FC83479BAEAF1878E1EA84 - peexe
B3E674E85A9BB5ACA3ABBC17FD99F603 - peexe
BE537A66D01C67076C8491B05866C894 - peexe
BF2E43FF8542E73C1B27291E0DF06AFD - peexe
D2DDA72FF2FBBB89BD871C5FC21EE96A - peexe
D727F747F5D1F6C88FC0032B8B1B8BA9 - peexe
E69A8EB94F65480980DEAF1FF5A431A6 - peexe
F5ECDA7DD8BB1C514F93C09CEA8AE00D - wordupd.tmp
F83FB9CE6A83DA58B20685C1D7E1E546 - peexe

1304606861C8D05f5BBA92D225ADC69A - VERDI.DOC
1FFECD461B3D4B65E44fAFF8537F68D6 - Steuerbescheid-8508884191-78843000-140.doc
3BFCBA2DD05E1C75F86C008F3D245F62 - eset.exe
53D5BDC6BD7904B44078CF80E239D42B - VERDI.doc
54C9A5FC6149007E9B727FCCCDAFBBD4 - Coupon_91658155.exe
65CF08FFAF12E47DE8CD37098AAC5B33 - peexe, 01NYX3xs.tmp
80043A5B285DA88FB63D469243655751 - Steuerbescheid.doc
8205A1106AE91D0B0705992D61E84AB2 - 1473359.exe, peexe
916D7838CD5A30015D75D1D783053EF7 - Windowsupdate.bat
9ABAD04C13B62E379642EEEC6E55C712 - ball.exe, peexe
A2D631FCB08A6C840C23A8F46F6892DD - cure.doc
A3386E5D833C8DC5DFBB772D1D27C7D1 - 7.dd, peexe
AA87D4E3133F9E4591EA6179CA7AFF3C - Invoice_97544835.exe, peexe
AD30987A53B1B0264D806805CE1A2561 - VERDI.doc

B40A9EDA37493425782BDA4A3D9DAD58 - Invoice_29557473.exe, peexe
B4D6CB4E52BB525EBE43349076A240DF - dospizdos.tmp, peexe
C09AF442E8C808C953F4FA461956A30F - Steuerbescheid.doc
C3341B7DFBB9D43BCA8C812E07B4299F - pass.exe
D552BE44A11D831E874E05CADAFE04B6 - LOAD_ENCDLL.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)

[5] CISA, Cybesrsecurity Directives, https://cyber.dhs.gov/directives/

4. https://pc-malware.blogspot.com/2019/10/remove-maze-ransomware.html (October 18, 2019)

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/