

[← Go to listing page](#)



Malware

Maze Ransomware: A Devious Combination of Data Theft and Encryption Targeting US Organizations

SHARE BLOG POST



Malware Profile

- Origin:** May 2019
- Alias:** ChaCha Ransomware, FileRepMalware, Win32/Filecoder.NVY, Trojan-Ransom.Win32.Gen.tno
- Infection Vectors:** Spelevo EK, Fallout EK, Spam Emails
- Attack Sector:** Real Estate, Enterprise Services, Manufacturing, Information Technology, Government
- Targeted Region:** Eastern and Western Europe, North America
- Motive:** Ransom, Data Theft
- Threat Level:** High

Origin

Maze is a strain of ransomware that was first spotted in an attack campaign targeting Italian-speaking users in October 2019. However, the earliest infection of this ransomware, which is a variant of the ChaCha ransomware, can be tracked to early-2019. Systems infected with this ransomware cannot access their data or files, because it encrypts files and locks them until a ransom is paid. Originally, Maze was seen as a typical data-encrypting ransomware and behaved like one, but later it evolved into more elaborate extortion campaigns. Since October 2019, Maze has become increasingly more aggressive and more widespread. So far in 2020, the ransomware has continued to make headlines with a string of high-profile cyberattacks, including a number of law firms, the city of Pensacola, FL., a large US staffing company (Allied Universal), a Fortune 500 company (Cognizant), French industrial giant “Bouygues Construction” and others.

Propagation Method

Maze ransomware is typically delivered or spread via spam emails and exploits kits (such as Fallout and Spelevo).

- In May 2019, it was observed spreading via Fallout exploit kit using a fake site pretending to be a cryptocurrency exchange app. The attackers designed a fake Abra cryptocurrency site to buy traffic from ad networks. Visitors to this site were redirected to the exploit kit landing page under certain conditions and got infected.
- Later, in October 2019, Spelevo exploit was used to infect victims that exploited a Flash Player 'use-after-free' vulnerability. The attack campaign was redirecting users to the Spelevo exploit kit, which utilized the critical "CVE-2018-15982" vulnerability in the browser, with users of Flash Player versions 31.0.0.153 / 31.0.0.108 and earlier. Upon successful exploitation or infection, the exploit kit automatically downloaded and installed the Maze ransomware payload via arbitrary code execution.
- A month later, a new attack campaign from a new threat actor, "TA2101", was seen targeting German organizations and companies to deliver and install backdoor malware along with Maze ransomware. Hundreds of spam emails were used to deliver malicious Microsoft Word attachments with German lures impersonating the German Federal Ministry of Finance and Federal Central Tax Office.

After the typical ransom tactic of infecting and targeting organizations around the world, the operators behind this ransomware started leaking the data online for those who did not pay the ransom. They began to threaten the victims to pay the ransom, or their sensitive data would be exposed online.

- In November 2019, after a deadline was missed for receiving a ransom payment, criminals behind Maze ransomware had leaked almost 700 MB worth of data, and files that were stolen from the security staffing firm "Allied Universal."
- The same thing happened in the case of Southwire (a leading wire and cable manufacturer from Carrollton, GA), where a ransom demand of 850 bitcoins (\$6 million) was not paid, and the criminals leaked a portion (around 14GB out of 120GB) of their stolen data on a "news" site they created.

Technical Info

Maze ransomware uses 2048 bit Rivest-Shamir-Adleman (RSA) and the ChaCha20 stream cipher to encrypt individual files. It adds different extensions to the files during the encryption process. It then changes the user's desktop wallpaper to a message about the encrypted files and the file name of the dropped ransom note.

- A notable feature of Maze ransomware is that it sets the ransomware amount based on the type of device it detects. This is uncommon among other types of ransomware.
- Maze operators have used the following labels to indicate the user's computer type in the wallpaper message: standalone server or in a corporate network, workstation in a corporate network, home computer, primary domain controller, backup server, etc.

When it infects home workstations, it encrypts files, alters them by adding a random extension (for example, "one.jpg" file will become "one[.].jpg.sA16PA"), creates the "DECRYPT-FILES[.]txt" file, and also changes the desktop wallpaper. The modified wallpaper includes a ransom message stating that the victim's files have been encrypted using RSA-2048 and ChaCha encryption algorithms. The only way to decrypt them is to

purchase a decryptor by following instructions provided in the "DECRYPT-FILES[.]txt" text file (a ransom message).

- The message shows that the infected victims must pay the ransom using a website link, which can be opened with only the Tor browser. The Tor website informs the victim that they must pay \$500 in Bitcoins using the BTC wallet address provided.
- Another way to make payment is to use another website (the link included in a ransom message), which can be opened with any web browser. It is also mentioned that, unless the victims pay the ransom within a particular time frame (a countdown timer is shown at the top of the Tor web page), the size of the ransom will be doubled.
- It is possible to unlock three files free of charge using the same website to prove that criminals have a valid decryption key. However, the ransom demand varies when it infects big organizations or enterprises where its ransom demand goes up to \$1 million.

Recent Incidents

- In December 2019, a Georgia-based wire and cable manufacturer "Southwire" was attacked, and after five days for not paying the \$6 million ransom, the criminal group leaked the data online.
- The same month, they also targeted the City of Pensacola's finance, executive, treasury, risk management, housing, legal, and human resources departments for ransom.
- In January 2020, the Maze cybercriminal group targeted a London-based company London Offshore Consultants. The criminal group claimed that 300GB of information was stolen from London Offshore Consultants (LOC) Group, and some of it was leaked online to force LOC Group to pay a ransom.
- Just a month later, in February, Maze ransomware attacks targeted five law firms and a French industrial giant "Bouygues Construction." The French firm released a brief statement admitting a "ransomware-type virus" was detected on its network. The group charged the firm twice, as it asked for \$1 million for the decryption key and another \$1 million for the 'deletion' of data they stole.
- In March 2020, a cybersecurity insurance provider for businesses known as "Chubb" was targeted and their data was also stolen.
- In April 2020, the American multinational corporation "Cognizant," was targeted by Maze in an attack that resulted in service disruptions. In the same month, the Maze ransomware also targeted the Canadian accounting firm "MNP", the London-based medical center Hammersmith Medicines Research, Texas-based Affordacare Urgent Care Clinic, Groupement Berkine, as well as two law firms in Manitoba.

Prevention

At present, there is no decryption tool or software available for Maze ransomware. Organizations should follow strong cybersecurity practices to prevent or stop the infection. Users should frequently update their browsers and plugins with the latest security and vulnerability patches. Since this malware spreads via exploit kits, users should install and use anti-malware and ad-blocker software to stop the distribution of EKs via malicious advertising. To prevent infection from spam email, deploy powerful email security software that can detect or spot malicious Word attachments embedded with macros. Also, make a habit of routine data backup, being sure to back up important files and data in a timely manner so they can be used to restore lost data in the event of a ransomware infection like Maze.

Indicators of Compromise

SHA256

E8a091a84dd2ea7ee429135ff48e9f48f7787637ccb79f6c3eb42f34588bc684

MD5

8205a1106ae91d0b0705992d61e84ab2

SHA1

49cdc85728bf604a50f838f7ae941977852cc7a2

SSDEEP

6144:66dXYUNkTVW1ibG9WDPeockZLqNUPitzHzO6YIBFFQQXtP/C62814nbncULJJ2ne:66NYSWVxEU2Gp0tzQIB

Associated File Names

DECRYPT-FILES[.]html
%ProgramData%\foo[.]dat
C:\hutchins[.]txt

Network Communication

hXXp://92[.]63[.]8[.]47
hXXp://92[.]63[.]3[.]2
hXXp://92[.]63[.]37[.]100
hXXp://92[.]63[.]194[.]20
hXXp://92[.]63[.]17[.]245
hXXp://92[.]63[.]32[.]55
hXXp://92[.]63[.]11[.]151
hXXp://92[.]63[.]194[.]3
hXXp://92[.]63[.]15[.]8
hXXp://92[.]63[.]29[.]137
hXXp://92[.]63[.]32[.]57
hXXp://92[.]63[.]15[.]56
hXXp://92[.]63[.]11[.]151
hXXp://92[.]63[.]32[.]52
hXXp://92[.]63[.]15[.]6
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[.]4
91[.]218[.]114[.]77
91[.]218[.]114[.]79

Associated Email Addresses

filedecryptor@nuke[.]africa

File Extension

.sA16PA

Domain

mazedecrypt.top

April 2020 (Indicators of Compromise)

Registry Keys

SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\LegalNoticeCaption
SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\LegalNoticeText
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal
Server subkey fDenyTSConnections

Files Created

C:\Windows\Temp\ered[.]tmp
C:\Windows\Temp\wupd12[.]14[.]tmp
DECRYPT-FILES[.]txt

MD5 Hashes

Dropper

a2d631fcb08a6c840c23a8f46f6892dd, Name: "Cure[.]doc"
2fbd10975ee65845a18af6b7488a5236, Name: "USPS_Delivery[.]doc"
ee26e33725b14850b1776a67bd8f2d0a , Name: R19340003422[.]doc
2fbd10975ee65845a18af6b7488a5236 , Name: USPS_Delivery[.]doc
a2d631fcb08a6c840c23a8f46f6892dd , Name: Cure[.]doc
ad30987a53b1b0264d806805ce1a2561 , Name: VERDI[.]doc
53d5bdc6bd7904b44078cf80e239d42b , Name: VERDI[.]doc

Second Stage

Eset[.]exe
3bfcba2dd05e1c75f86c008f4d245f62

Loaders - wordupd[.]tmp

21a563f958b73d453ad91e251b11855c
27c5ecbb94b84c315d56673a851b6cf9
0f841c6332c89eaa7cac14c9d5b1d35b
F5ecda7dd8bb1c514f93c09cea8ae00d
0f841c6332c89eaa7cac14c9d5b1d35b
a0c5b4adbcd9eb6de9d32537b16c423b

Loaders - Other

B40a9eda37493425782bda4a3d9dad58
5df79164b6d0661277f11691121b1d53
79d137d91be9819930eeb3876e4fbe79
65cf08ffaf12e47de8cd37098aac5b33
Fba4cbb7167176990d5a8d24e9505f71
Deebbea18401e8b5e83c410c6d3a8b4e
87239ce48fc8196a5ab66d8562f48f26
A3a3495ae2fc83479baeaf1878e1ea84
8205a1106ae91d0b0705992d61e84ab2
B4d6cb4e52bb525ebe43349076a240df
A3386e5d833c8dc5dfbb772d1d27c7d1
D552be44a11d831e874e05cadafe04b6
Bf2e43ff8542e73c1b27291e0df06afd
e69a8eb94f65480980deaf1ff5a431a6

Extracted Malware

5774f35d180c0702741a46d98190ff37
F04d404d84be66e64a584d425844b926
Be537a66d01c67076c8491b05866c894
d2dda72ff2fbbb89bd871c5fc21ee96a

Additional Hashes

910aa49813ee4cc7e4fa0074db5e454a
8205a1106ae91d0b0705992d61e84ab2

IP Addresses (Dropper)

hxxp://104[.]168[.]215[.]54/wordupd[.]tmp
hxxp://149[.]56[.]245[.]196/wordupd[.]tmp
hxxps://104[.]168[.]198[.]208/wordupd[.]tmp
hxxp://104[.]168[.]198[.]230/wordupd[.]tmp
hxxp://104[.]168[.]201[.]47/wordupd[.]tmp

Maze URLs

hxxps://mazedecrypt[.]top/c3100a28b009e7a9
hxxp://aoacugmutagkwctu[.]onion/c3100a28b009e7a9

IP Addresses

91[.]218[.]114[.]37
91[.]218[.]114[.]77
91[.]218[.]114[.]14


91[.]218[.]114[.]11
91[.]218[.]114[.]31
91[.]218[.]114[.]79
91[.]218[.]114[.]25
91[.]218[.]114[.]26
91[.]218[.]114[.]38
91[.]218[.]114[.]32

[View live updates on Maze Ransomware related cybersecurity alerts](#)

TAGS

- Filerepmalware
- Chacha Ransomware
- Maze Ransomware

Posted on: April 27, 2020

← PREVIOUS

APT36 Taking Advantage of COVID-19 Fear ...

→ NEXT

Mitigate Threats with Actionable Th...



Recent Posts



May 01, 2020

Manage Custom Threat Indicators (IOCs) with CFTR version 2.1

What are Custom Threat Indicators? Custom threat indicators are...

- Indicators Of Compromise locs
- Cyware Fusion And Threat Response
- + 2 more



May 01, 2020

Cyware Adds STIX 2.1 Support for Custom Threat Intelligence Feeds

What is STIX 2.1? STIX is a language and serialization format that ena...

- Stix 20
- Stix 1x
- + 2 more



May 01, 2020

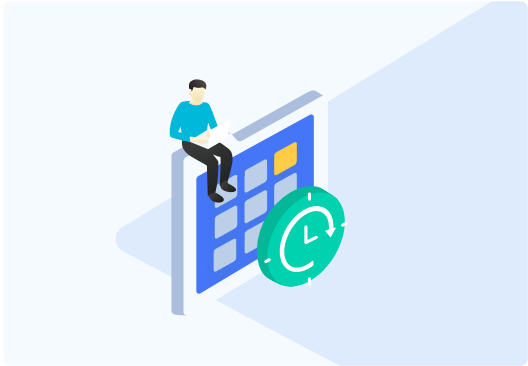
Mitigate Threats with Actionable Threat Intelligence Sharing

Cyware Situational Awareness Platform (CSAP) version 2.1 comes with a new ...

- Threat Intelligence
- Cyware Situational Awareness Platform

More from Cyware

Stay updated on the security threat landscape and technology innovations at Cyware with our threat intelligence briefings and blogs.



Daily Threat Briefing

Cyware Daily Threat Intelligence, May 01, 2020



Weekly Threat Briefing

Cyware Weekly Threat Intelligence, April 27 - May 01, 2020



Monthly Threat Briefing

Cyware Monthly Threat Intelligence, March 2020

Join Thousands of Other Cyware Followers!

Enter your email address

Subscribe

PRODUCTS

[Cyware Situational Awareness Platform \(CSAP\)](#)

[Cyware Threat Intelligence eXchange \(CTIX\)](#)

[Cyware Fusion and Threat Response \(CFTR\)](#)

[Cyware Security Orchestration Layer \(CSOL\)](#)

[Product FAQs](#)

[Get a Demo →](#)

SOLUTIONS

[ISACs](#)

[MSSPs](#)

[CERTs](#)

[Enterprise](#)

RESOURCES

[Cyware Blog](#)

[Daily Threat Briefing](#)

[Weekly Threat Briefing](#)

[Monthly Threat Briefing](#)

[Educational Guides](#)

[Cyware Insights](#)

COMMUNITY

[Cyware Social](#)

FREE

[eXchange Lite](#)

FREE

[Cyware Threat Intelligence Feeds](#)

FREE

[Open APIs](#)

PARTNERS & SUPPORT

[Technical Support Plans](#)

[Technology Partners](#)

[Channel Partners](#)

[Tool Integrations](#)

[Environments](#)

[Subscribe →](#)

COMPANY

[Leadership](#)

[Press & Media](#)

[Careers](#)

[Press Kit](#)

[Contact Us](#)



Cyware Labs, 1460 Broadway, New York, NY 10036 [Get Directions](#)

Call Us at [1-855-692-9927](#)

[Terms of Use](#)

[Privacy Policy](#)
© 2020