DSCI
PROMOTING DATA PROTECTION
A NASSCOM® Initiative

MAZE RANSOMWARE

TECHNICAL REPORT

About Maze Ransomware

The **Maze ransomware** attack is an example of advancing malware that tends to move laterally in the network and has the potential to cause disruptions and information stealing for extortion**,** as per the available information.

Maze Ransomware has been spotted being distributed by the **Fallout exploit kit earlier,** also known as the **ChaCha ransomware** distributed through a fake site pretending to be a **cryptocurrency exchange app.** Been around for a year but possibly this time, infection might have started from spear phishing email/spam and someone might have clicked a malicious attachment.

Observations

Below are the observations on maze group ransomwares, basis internal static and dynamic analysis.

- Maze ransomware is Anti VM or Sandbox evading malware. It doesn't run on most of the virtual machines and sandboxes
- Maze Ransomware encrypts different file formats with different files extensions
- Reads the cookies from browser and other places
- Intruders also offer decryption of 3 files for free as a proof of work

Modus Operandi

Possibility 1:

1. Spear phishing email /regular Spam email
2. On click, it drops file and runs
3. Deletes shadow copies
4. Writes files to word start up folder
5. Follow ransomware instructions & encrypt files
6. Connects to server without Host Name

Possibility 2:

1. Possibly used free crypto currency/social ads
2. On click, it drops file and runs
3. Deletes shadow copies
4. Writes files to word start up folder
5. Follow ransomware instructions & encrypt files
6. Connects to server without Host Name

Indicators of Compromise (IOCs)

MD5

- 8205a1106ae91d0b0705992d61e84ab2

SHA1

- 49cdc85728bf604a50f838f7ae941977852cc7a2

SHA256

- 91514e6be3f581a77daa79e2a4905dcbdf6bdcc32ee0f713599a94d453a26fc1

SSDEEP

- 6144:66dXYUNkTVW1ibG9WDPeocKZLqNUPitzHzO6YIBFFQQXtP/C62814nbncULJJ2ne:66NYSWVxEU2Gp0tzQIBTbXGzzLf

Network Communication

- http [:]//92[.]63[.]8[.]47
- http [:]//92[.]63[.]32[.]2
- http [:]//92[.]63[.]37[.]100
- http [:]//92[.]63[.]194[.]20
- http [:]//92[.]63[.]17[.]245
- http [:]//92[.]63[.]32[.]55
- http [:]//92[.]63[.]11[.]151
- http [:]//92[.]63[.]194[.]3
- http [:]//92[.]63[.]15[.]8
- http [:]//92[.]63[.]29[.]137
- http [:]//92[.]63[.]32[.]57
- http [:]//92[.]63[.]15[.]56
- http [:]//92[.]63. [.]11[.]151
- http [:]//92[.]63[.]32[.]52
- http [:]//92[.]63[.]15[.]6

The Maze Ransomware is a variant of Chacha Ransomware, whose affiliates, identified as the **TA2101 threat actor.**

Hash

- 91514e6be3f581a77daa79e2a4905dcbdf6bdcc32ee0f713599a94d453a26fc1

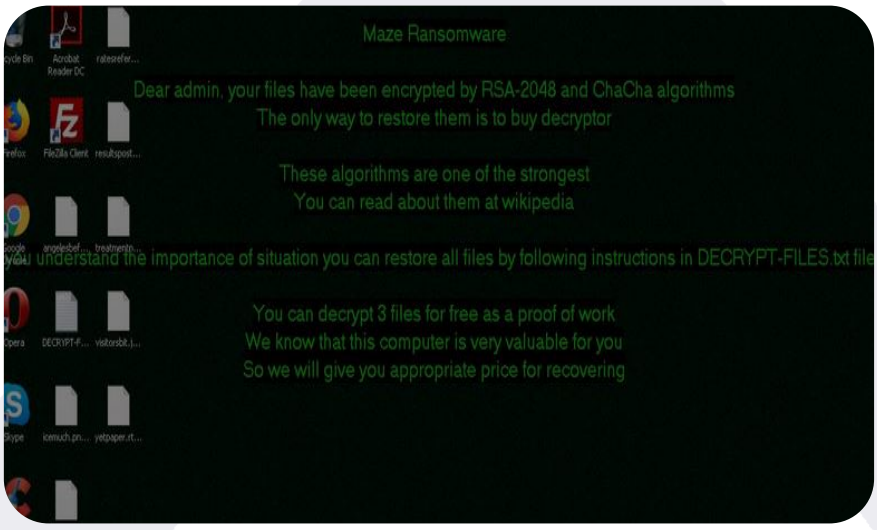
Network

- Domain mazedecrypt.top
- IP 91.218.114.11
- IP 91.218.114.25
- IP 91.218.114.26
- IP 91.218.114.31
- IP 91.218.114.32
- IP 91.218.114.37
- IP 91.218.114.38
- IP 91.218.114.4
- IP 91.218.114.77
- IP 91.218.114.79

Sandboxing

Dynamic Analysis (on running sample in Cuckoo and Any Run)

1. **Desktop after Infection**



2. Ransomware Note

```
Attention!

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

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 have a
chance! It is easy to recover in a few steps.

----------------------------
| How to get my files back?
----------------------------

The only method to restore your files is to purchase a unique for you
private key which is securely stored on our servers.
To contact us and purchase the key you have to visit our website in a
hidden TOR network.

There are general 2 ways to reach us:

1) [Recommended] Using hidden TOR network.

  a) Download a special TOR browser: https://www.torproject.org/
  b) Install the TOR Browser.
  c) Open the TOR Browser.
  d) Open our website in the TOR browser:
http://aoacugmutagkwctu.onion/17dd0b47869e7270
  e) Follow the instructions on this page.

2) If you have any problems connecting or using TOR network

  a) Open our website: https://mazedecrypt.top/17dd0b47869e7270
  b) Follow the instructions on this page.
```

3. Registry Activity - Modification Event

PID	Process	Operation	Key	Name	Value
1324	91514e6be3f581a77daa79e2a4905dcbdf6bdcc32ee0f713599a94d453a26fc1.exe	write	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\RASAPI32	EnableFileTracing	0
1324	91514e6be3f581a77daa79e2a4905dcbdf6bdcc32ee0f713599a94d453a26fc1.exe	write	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\RASAPI32	EnableConsoleTracing	0
1324	91514e6be3f581a77daa79e2a4905dcbdf6bdcc32ee0f713599a94d453a26fc1.exe	write	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\RASAPI32	FileTracingMask	4294901760
1324	91514e6be3f581a77daa79e2a4905dcbdf6bdcc32ee0f713599a94d453a26fc1.exe	write	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\RASAPI32	ConsoleTracingMask	4294901760
1324	91514e6be3f581a77daa79e2a4905dcbdf6bdcc32ee0f713599a94d453a26fc1.exe	write	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\RASAPI32	MaxFileSize	1048576
1324	91514e6be3f581a77daa79e2a4905dcbdf6bdcc32ee0f713599a94d453a26fc1.exe	write	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\RASAPI32	FileDirectory	%windir%\tracing
1324	91514e6be3f581a77daa79e2a4905dcbdf6bdcc32ee0f713599a94d453a26fc1.exe	write	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\RASMANCS	EnableFileTracing	0

4. File Activities – Dropped Files

	Process	Filename	Type
1324	91514e6be3f581a77daa79e2a4905dcbdf6bdcc32ee0f713599a94d453a26fc1.exe	C:\Users\admin\AppData\Local\Temp\000.bmp **MD5:** 36C543B351F5E9ABFD057292F243DE8D **SHA256:** 41894E29936B344B0A3FFAA1438E7B6FC1B865A08350FA8AEC119956628D8019	image
1324	91514e6be3f581a77daa79e2a4905dcbdf6bdcc32ee0f713599a94d453a26fc1.exe	C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\qldyz51w.default\gmp-gmpopenh264\1.8.1\DECRYPT-FILES.txt **MD5:** A74666C5586D8B288E508A979998C3E6 **SHA256:** E2A93EEFCA86E4AC99EEEEA2A0BFC7EAAE64E31F3BF23F4B4B9D69C6731FE7F0	text
1324	91514e6be3f581a77daa79e2a4905dcbdf6bdcc32ee0f713599a94d453a26fc1.exe	C:\Users\Public\Videos\Sample Videos\Wildlife.wmv.bvFN **MD5:** — **SHA256:** —	—
1324	91514e6be3f581a77daa79e2a4905dcbdf6bdcc32ee0f713599a94d453a26fc1.exe	C:\Users\Public\Videos\Sample Videos\Wildlife.wmv **MD5:** — **SHA256:** —	—
1324	91514e6be3f581a77daa79e2a4905dcbdf6bdcc32ee0f713599a94d453a26fc1.exe	C:\Users\Public\Videos\Sample Videos\DECRYPT-FILES.txt **MD5:** A74666C5586D8B288E508A979998C3E6 **SHA256:** E2A93EEFCA86E4AC99EEEEA2A0BFC7EAAE64E31F3BF23F4B4B9D69C6731FE7F0	text

5. Connections

PID	Process	IP	ASN	CN	Reputation
1324	91514e6be3f581a77daa79e2a4905dcbdf6bdcc32ee0f713599a94d453a26fc1.exe	91.218.114.4:80	Mir Telematiki Ltd	RU	malicious
1324	91514e6be3f581a77daa79e2a4905dcbdf6bdcc32ee0f713599a94d453a26fc1.exe	91.218.114.11:80	Mir Telematiki Ltd	RU	malicious
1324	91514e6be3f581a77daa79e2a4905dcbdf6bdcc32ee0f713599a94d453a26fc1.exe	91.218.114.25:80	Mir Telematiki Ltd	RU	malicious
1324	91514e6be3f581a77daa79e2a4905dcbdf6bdcc32ee0f713599a94d453a26fc1.exe	91.218.114.26:80	Mir Telematiki Ltd	RU	malicious
1324	91514e6be3f581a77daa79e2a4905dcbdf6bdcc32ee0f713599a94d453a26fc1.exe	91.218.114.31:80	Mir Telematiki Ltd	RU	malicious

Recommendations

1. Install ad blockers to combat exploit kits such as Fallout that are distributed via malicious advertising.
2. Protect your personal/official devices with licensed Antivirus.
3. Implement strong email security software that detects Word attachments that are potentially embedded with malicious macros.
4. Lockdown Remote Desktop Protocol, if not in use or follow RDP best practices such as rate limiting, 2FA, etc.
5. Deploy effective backup strategies including keeping the backup safe; so that they can be used to recover lost data in the event of an infection.
6. Please refer remote connection guidelines and best practices:
    a. Make use of legitimate VPN services instead of free services.
    b. Configure strong firewalls; at least VPN must have capability to test underlying machine for basic security before it connects.
    c. Don't allow user to keep logged in for a long period of time. Enforce sessions with specific time periods.
    d. Adopt better protocols like IPSEC/L2TP to establish a connection.
    e. Enforce multifactor authentication before every user activity/action.