Cognizant Hit by MAZE Ransomware

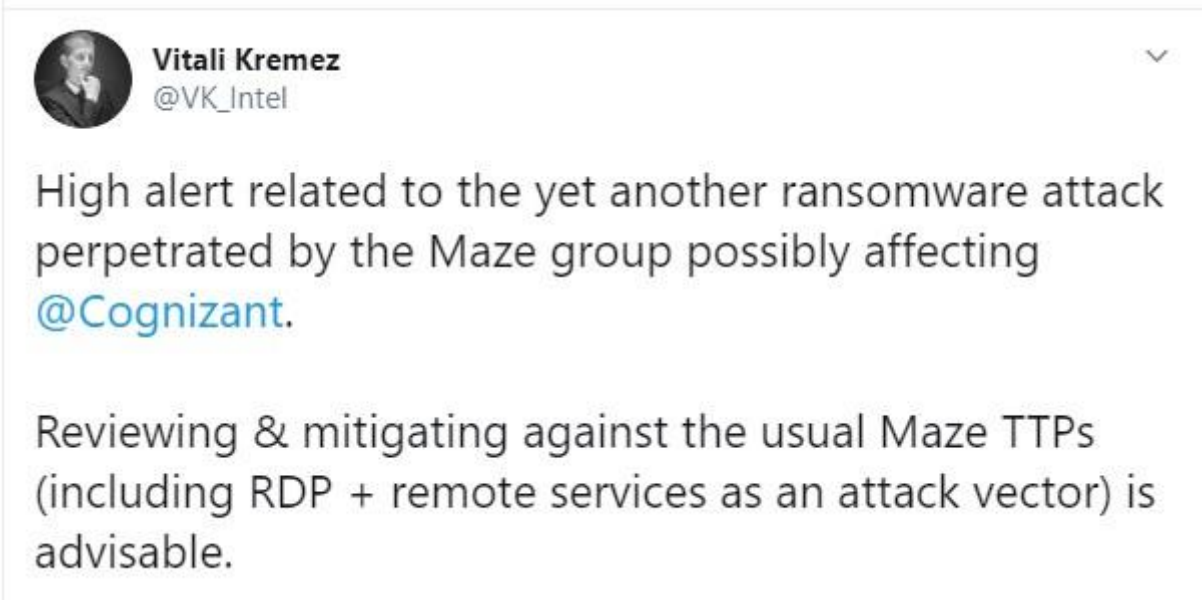
April 2020

Cyberint

TABLE OF CONTENTS

SUMMARY

On April 18th, Cognizant a major global IT service provider experienced an incident involving the Maze Ransomware.



Looking at our data we found several Maze Ransomware DLLs uploaded to VT on April 17th.

The group behind the Maze ransomware are very active and prolific and are in the habit of dumping stolen information from compromised organizations who fail to pay the ransom using their publicly available website https://mazenews.top/.

Typical TTP's that are frequently used by the actors behind the Maze Ransomware are exploiting exposed RDP servers and other remote access applications such as vulnerable VPN nods.

KEY FINDINGS

- Maze Ransomware continuous to be one of the most prolific and highly prevalent ransomwares
- Recently discovered samples using Valid code signing certificate
- The same code signing certificate used to sign two other malware samples we classify as information stealers

TECHNICAL ANALYSIS

On April 18th we received reports on various social media that Cognizant a global IT service provider has suffered an incident involving the Maze Ransomware. Doing some initial analysis, we discovered several files classified as Maze Ransomware uploaded to VT during April 2020.

The samples are DLL files where one specific file uploaded on April 17th is a legitimately signed file.

File Name	SHA-256	Size	Tags
kepstl32.dll	4218214f32f946a02b7a7bebe3059af3dd87bcd130c0469aeb21b58299e2ef9a	615624 bytes	DLL, Maze, Ransomware

When the DLL is loaded in memory it creates a file in the %TEMP% directory with a hidden attribute and copy the file to C:\ProgramData\ and save the file as memes.tmp.

The file contains loading instructions for the DLL.

- DllInstall
- DllRegisterServer
- DllUnregisterServer
- DllInstall 0
- DllRegisterServer 0
- DllUnregisterServer 0
- DllInstall 1
- DllRegisterServer 1
- DllUnregisterServer 1
- DllInstall Install
- DllRegisterServer Install
- DllUnregisterServer Install
- DllInstall DefaultInstall
- DllRegisterServer DefaultInstall
- DllUnregisterServer DefaultInstall
- DllInstall 127.0.0.1

- DllRegisterServer 127.0.0.1
- DllUnregisterServer 127.0.0.1
- DllInstall explorer.exe
- DllRegisterServer explorer.exe
- DllUnregisterServer explorer.exe
- DllInstall iexplore.exe
- DllRegisterServer iexplore.exe
- DllUnregisterServer iexplore.exe
- DllInstall %Temp%\IXP000.TMP\
- DllRegisterServer %Temp%\IXP000.TMP\
- DllUnregisterServer %Temp%\IXP000.TMP

The DllInstall and DllRegisterServer are responsible for the installation and registration of DLL in the Windows operating system.

- DllUnregisterServer
- DllRegisterServer
- DllInstall

are exported by the malicious DLL, the Malware then deletes the volume shadow copy by calling the following command.

C:\mbep\t\twdgk\..\..\..\Windows\sxqe\g\..\..\system32\qb\ohhs\..\..\wbem\f\..\wmic.exe" shadowcopy delete

The malware also uses some Anti-Analysis mechanisms such as hooking the DbgUiRemoteBreakin function by inserting a single byte hook at 0x0 and changing a simple cmp instruction opcode A6 to RET opcode C3. this will cause the function to immediately return from execution.

The malware also calls IsDebuggerPresent to check for the presence of a debugger in an attempt to hinder analysis.

The malware also dynamically resolves its IAT and directly calling native API functions. the malware encrypts files on the infected machine and with a random 4-7-character extension.

The malware then overwrites the MBR (Master Boot Record) by writing 512 bytes and drops the ransom note decrypt-files.txt to the startup directory.

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*

After the payment, the data will be removed from our disks and decryptor will be given to you, so you can restore all your files.

How to contact us and get my files back?

The only method to restore your files and be safe from data leakage 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:

[Recommended] Using hidden TOR network.

Download a special TOR browser: https://www.torproject.org/

Install the TOR Browser.

Open the TOR Browser.

Open our website in the TOR browser: http://aoacugmutagkwctu.onion/d39d0d96f0d19656

Follow the instructions on this page.

If you have any problems connecting or using TOR network

Open our website: https://mazedecrypt.top/d39d0d96f0d19656

Follow the instructions on this page.

Warning: the second (2) method can be blocked in some countries. That is why the first (1) method is recommended to use.

On this page, you will see instructions on how to make a free decryption test and how to pay.

It also has a live chat with our operators and support team.

What about guarantees?

We understand your stress and worry.

So, you have a FREE opportunity to test a service by instantly decrypting for free three files from every system in your network.

If you have any problems our friendly support team is always here to assist you in a live chat!

P.S. Dear system administrators do not think you can handle it by yourself. Inform leadership as soon as possible.

By hiding the fact of the breach, you will be eventually fired and sometimes even sued.

THIS IS A SPECIAL BLOCK WITH A PERSONAL AND CONFIDENTIAL INFORMATION! DO NOT TOUCH IT WE NEED IT TO IDENTIFY AND AUTHORIZE YOU

---BEGIN MAZE KEY---

V4DG7h8EyZMrRhyNOOMYaXmw0E41HsKPECj3DWpGdy6C/3blYHIRwWMERJC61W08Oz4897AdJxCxTMN9iXhBsJU5vmO
q7dEN+LKk7vLxsDkhGtnM8dFgKUICI5CW/oOeebfFg2tx6r0xfVfd2ZZI0sBVnlBA5uEGnO6/VsmXGPtTfEMGTDJz/i1znJVSIXEbk
tJGPslcLoLFoDEmeOVYjZM7SV1esYfC+VzKpaVz2Vb7GNopWBZ/trDcgoJflQySHaJxtSQVfNZBbOkhY9H2hCVaFc8hCf6eWHsO
gTcR7s8FXKK/w0/STWdpZsjzvBrt6UWbRmLicB4JjyE+uYGkFKqPd8ETkspLAtBGOss9kkUIqyfZIaxKA8LDWfAEz3bQ3yuGjQe0a
KhMDlg4lOnH+pw5a3Z8Sy/lofXQVm7Cbb1GgcfqQe9rk1fjKpApmeD2RzyP0qCG37NSUmE8fTOYODJJRs+CGvgAn5KiDKR+tQ
zhlaCCb8qTJ55LZfLkdxX6QUJQK+JM3FtDNaiZfBdHr21qo0vL2XMCFAgiYgW1QnYWF6uL7bhH2nsc2EYWVwPLYBJGUSl6LvZ
ASyscoIWEUR5WuuDO9/ixyCmp8VrlViRG/N+4eZACSbnaOCl/9SB9zWuOauB+gGS4W4ypagmXTHLd2TappPfnymx6slmAt2sN
RI6g6BcBJcPNkPNh+CE7+I9RTFhk3QTGobvoPxEIWYbtOnKxQjo8bDjW2SIPAZBlQGbp66rEEWJCx8gF6Vdn4m0UxGX2VIRAg
NT0nBQDA8f2bAUNFcO59ZGYv2aZplhlvYVjzKzELkuWLb0huV107rr2iYd3el838SoiRhED2yVEzsj95BKKKBVH7bkHDCBf4YSs
AntM4WbrtKx4stqBulc6GOn9ijCLuKEbcJmFSoyOIB/xKylRQU495ajwtt9IYfKzFcr7iabatuW4Az4GDvDPo76hxyGJgvrIBe7Bi/eo
8DJkh6gH7RSwWAZXNHkubGyJL9u25/6C0YsKzst3fk3ichJOENnclp6dBljzXKfZsGLQFjn0iPGUWJXSCOUy70gDHMLaKkp/JXC
pZ+K1DdDHdWXRu8jQF9hfAI0EfgSQoNAwPJhV+nBYFRne1bEdgiT4fTnjCOu+v9fzn9vUvBxu3q0Q2KHTVCd0r3+0nyPy1BK6
KLRyby7eh/QEHWxl0DUhMs4PeKMzmzHPowZzhVy2eeQ9wb/2XW6iQ6CJG6ugHJwrVzNpFBjKUyXJdL0nY9Q8JsqS+ZhLM4+
NbqEsMotilxue72vAJUu99yCCWbkmHSGTaWy8qKJiKCQqhWdla22ecde67JjH7n5RbYbcowf1ihbpQrRQdq3qVXZgJOk3UcU49
hOPYhTAvqCCUnHXhoFS8o+a9Jnb6zkOwMSwPJhzjpTIWeJSMpV34+Yt1masg093MaTdwaOBro5LB5X1+SBfe94uG0rwaATdz
ZqgwYYYfKYHMarQneDYG1Lxflgp5wABGKTi0JYr4K7ogShWUeuuCJsICE0R/4PxHyzWRExgi9BAdrwfdeiDbNHf1irxGWIk9hn7J
5c5EY15z42diyEXAQuJRg8j16rq/kfLPRNIIrcE50Eo/6wK6oPrjcOVaVUrdcOXeIYwa/0vjPs+tPSZfofivxjbbs7xQ0fZz/OXuttaDfIcK
dLK998ero+QmXox0kCPEgsrN2lVtqDmjolc+HGGkzp+/zWSG0p3LlMdysWQeXrc1jtamErv8VqDyRl+SupeliSvyUbh7ygyV+66lI1y
i15nX5whEW2OkMP9pvxsbKRNfEbQThlmJ9B1UJ5Toufs0A3F9PRduzXq628isehG8tx+K+SvKn3bwWErI2IlzrtXvqf6oTPzvNJ4B
6vuhxJjq4AGeY6iWD7QJimNRXg0iu/7c2hpNrQuI6txM4fVVcqERKSvHaOrYkBKQxRZkCvRKSh1TyvfhNgyEtwsLWeg1o9vnPgU
nSTLWDVVukaz2j901EJXZV8jvSpJH8Xfq9tciHnOYOf5tg6cUMH4W5gFudLv7xTUEiEMhb4wg6WMWXo8V6UG4vF0bIqbl8uS
08br33MDmoBL+D3KdSCQEGMsSW1MLtfO/Ag9CKNhDXlgS44Tsrj4GmlV2tB6F5FC/gYMTxnK2ENDS7ii0PrDOunqUyhPdA5
wvy9pY/6m44mE6gqIOgiI98ZabW0d+jEKd203MywIIundLMkt5M2mIkfOGq4FS4FvdFqkb7iPlwoiZAAzADkAZAAwAGQAOQA2
AGYAMABkADEAOQA2ADUANgAAABCAYBoSVwBoAHUATwBYAFkAcwBEAAAAIi5XAE8AUgBLAEcAUgBPAFUAUABcAEUARw
BMAEEARgBUAEIAMQBOADgAWQBBAAAAKgxuAG8AbgBlAHwAAAAyLlcAaQBuAGQAbwB3AHMAIAA3ACAAUAByAG8AZgBl
AHMAcwBpAG8AbgBhAGwAAAA6KHwAZABlAHAAcgBlAGMAYQB0AGUAZAAgAD4AIAB2ADIALgAzAHwAAABCKHwAQwBfA
EYAXwA0ADkANwAyADQAMQAvADUAMgAzADcANQAyAHwAAABIAFBAWIkIYIkIaIkIcJq76g14DoABAYoBBTIuMy4y

---END MAZE KEY---

The file is signed by a legitimate code signing certificate with the following details.

Name GO ONLINE d.o.o.

Status Valid

Issuer Sectigo RSA Code Signing CA

Valid From 01:00 AM 03/10/2020

Valid To 12:59 AM 03/11/2021

Valid Usage Code Signing

Algorithm sha256RSA

Thumbprint AF2A70604EF0FD0A2511FB5795DCF810754B97D9

Serial Number "26 91 74 F9 FE 7C 6E D4 E1 D1 9B 26 C3 F5 B3 5F

MITRE ATT&CK MAPPING

Techniques	Tactics
T1067 - Bootkit	Persistence
T1060 - Registry Run Keys / Startup Folder	Persistence
T1158 - Hidden Files and Directories	Defense Evasion, Persistence
T1045 - Software Packing	Defense Evasion
T1112	Defense Evasion
T1081 - Credentials in Files	Credential Access
T1083 - File and Directory Discovery	Discovery
T1057 - Process Discovery	Discovery
T1119 - Automated Collection	Collection
T1005 - Data from Local System	Collection
T1486 - Data Encrypted for Impact	Impact

T1490 - Inhibit System Recovery	Impact
T1491 - Defacement	Impact

The file compile time is 2020-04-15 23:09:33 and the file was signed using the code signing certificate at 1:35 AM 4/16/2020 a day before it was submitted to VT.

Further analysis pivoting on the code signing certificate serial number we discovered two additional executable files we classify as information stealing malware.

FILES

File Name	SHA-256	File Size	Tags
IRS_Documents.exe	6fc48d3429e817e52c38c8d17fc2c7740acaae 563a90ebad8e0391a9e9742aee	259784 bytes	Malware, Packed, Signed
mapdata.exe	aad2869ebbd92c22c3366bccf857522686e 70c8f541d9164bc483dc44244dbcc	153288 bytes	Malware, Packed, Signed

IRS_Documents.exe compile time is *2019-08-20 09:08:07* and it was signed by the legitimate code signing certificate at *4:18 PM 4/16/2020*. which is around three hours after the Maze Ransomware sample

mapdata.exe compile time is *2018-12-15 17:23:31* and it was signed by the legitimate code signing certificate at *1:02 AM 4/9/2020* which is 23 minutes before the Maze Ransomware Sample.

This suggests that the actors behind the Maze Ransomware might have access to a stolen legitimate code signing certificate shared with them by a different threat actor or perhaps someone part of the group behind the Maze Ransomware is also taking part of other eCrime activities.

The fact that all files were signed in a very close time frame suggests that the threat actors with access to the code signing certificate attempt to reuse older malware signed with a legitimate certificate to reduce the chance of it being detected. Both files exhibit the same behavioral activities.

When first executes the malware copies itself to the *%AppData%\Roaming* directory the malware then enumerates running processes by calling.

CreateToolhelp32Snapshot

Process32First

Process32Next

Looking for explorer.exe, the malware then injects code into the explorer.exe by mapping is sections using NtMapViewOfSection and creating a threat in explorer.exe using RtlCreateUserThread the injected explorer.exe then collects information form internet explorer using

VaultOpenVault

VaultEnumerateItems

VaultFree

The malware also collects information from Mozilla Firefox by reading its profile.ini file and chrome browser information by accessing

%AppData%\Local\Google\Chrome\User Data\Local State

%AppData%\Local\Google\Chrome\User Data\Default\Cookies

%AppData%\Local\Google\Chrome\User Data\Default\Cookies-journal

The malware also reads the outlook registry setting by calling RegOpenKeyW to the following registry key

HKCU\Software\\Microsoft\\Windows NT\\CurrentVersion\\Windows Messaging Subsystem\\Profiles\\Outlook\\9375CFF0413111d3B88A00104B2A6676

The malware then beacons to its C2 at http[:]//shopmarketbase[.]com/ by an HTTP POST request using a User-Agent string

Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E; InfoPath.3)

MITRE ATT&CK MAPPING

Techniques	Tactics
T1053 - Scheduled Task	Defense Evasion, Execution, Persistence
T1096 - NTFS File Attributes	Defense Evasion
T1045 - Software Packing	Defense Evasion

T1214 - Credentials in Registry	Credential Access
T1081 - Credentials in Files	Credential Access
T1003 - Credential Dumping	Credential Access
T1083 - File and Directory Discovery	Discovery
T1012 - Query Registry	Discovery
T1057 - Process Discovery	Discovery
T1119 - Automated Collection	Collection
T1005 - Data from Local System	Collection
T1071 - Standard Application Layer Protocol	Command and Control

RECOMMENDATIONS

1. Configure Strong encryption when using RDP Protocol
2. Use Strong Passwords for users who are using RDP to access servers remotely
3. Use Two Factor Authentication when using RDP to access servers remotely
4. Use the latest software patches for Operating systems and 3rd party software
5. Restrict access only to authorized users and hosts using RDP to access servers remotely by applying restrictive firewall policy
6. Enable NLA (Network Level Authentication for more information check: https://www.notion.so/cyberintmdr/Cognizant-hit-by-MAZE-Ransomware-eabc73e000bb40328927a6defb54d7a1#e00c3fa2afd64bdd894daaacfbc0d8bd
7. Set restrictive account lockout policy for RDP sessions
8. enforce session timeouts
9. Limit Access to vssadmin.exe and other administrative utilities such as wmic.exe on non-administrative workstations
10. Enforce 'Least Privileges' policy by disabling local administrative permission to logged on users

CONTACT US

www.cyberint.com | sales@cyberint.com | blog.cyberint.com

USA

Tel: +1-646-568-7813
214 W 29th St, 2nd Floor New York, NY 10001

ISRAEL

Tel: +972-3-7286-777
17 Ha-Mefalsim St 4951447 Petah Tikva

UNITED KINGDOM

Tel: +44-203-514-1515
Fox Court 14 Grays Inn Rd, Holborn, WC1X 8HN, Suite 2068 London

SINGAPORE

Tel: +65-3163-5760
135 Cecil St. #10-01 MYP PLAZA 069536

LATAM

Tel: +507-395-1553
Panama City