MTR Casebook: Blocking a $15 million Maze ransomware attack

news.sophos.com/en-us/2020/09/22/mtr-casebook-blocking-a-15-million-maze-ransomware-attack/

Greg Iddon September 22, 2020

Customer profile: An organization with many hundreds of networked devices based in Asia Pacific.

The Sophos Managed Threat Response (MTR) team was called in to help an organization targeted with Maze ransomware. The attackers issued a ransom demand for US$15 million – if they had succeeded this would have been one of the most expense ransomware payments to date.

Background: Ransomware partners in crime

Maze is one of the most notorious ransomware families, active since 2019 when it evolved from ChaCha ransomware. It was among the first to combine data encryption with information theft.

The operators behind Maze have recently started colluding with other ransomware groups, including LockBit, SunCrypt and Ragnar Locker, providing them with access to their platform for posting stolen victim data.

This appears to have led to a reciprocal sharing of tactics, techniques and procedures (TTPs): in the attack covered here the Maze group borrowed a Ragnar Locker technique that involves using virtual machines.

For detailed technical analysis of this collaboration between attackers read Maze attackers adopt Ragnar Locker virtual machine technique.

Days 1-3: The attack begins

Prior to the attack becoming active, the operators compromised a computer on the target's network. This computer was then used as a 'beach head' in the network. On multiple occasions during the attack, the attackers connected from here to other computers over Remote Desktop Protocol (RDP).

On day three, the main part of the attack began. The attackers exploited a domain admin account with a weak password to take control of an unprotected Domain Controller (DC). They then spent several days moving across the network.

Using the legitimate network scanning tool Advanced IP Scanner to map the network, the attackers created lists of IP addresses to which they would later deploy ransomware. These included a list of the IP addresses of machines belonging to the target's IT administrators.

The attackers' attention then turned to the exfiltration of data.

They identified a file server and accessed it remotely over RDP using the compromised domain admin account. Using the legitimate archiving tools WinRar and 7zip, they started compressing folders located on it.

These archives were then copied back to the primary DC using the legitimate Total Commander FTP client that the attackers had installed on the file server.

The attackers tried to install the cloud storage application Mega on the DC. This was blocked as the target had added Mega to their blocked list using the application control capability in Sophos Intercept X endpoint protection. The attackers then switched to using the web-based version instead, uploading the compressed files.

Days 4-5: The calm before the storm

For two days, the attackers went quiet. It's likely they were waiting for a day when the target's IT security team wouldn't be working, like the weekend.

Day 6: The first ransomware attack is launched

The first Maze ransomware attack was launched on a Sunday, using the already compromised domain admin account and the lists of IP addresses that had been identified.

This first attack actually comprised three attacks as the operators deployed three copies of the Maze ransomware via batch scripts to the targeted computers:

- C:\ProgramData\enc6.exe
- C:\ProgramData\enc.exe
- C:\ProgramData\network.dll

Three scheduled tasks were created to execute the ransomware:

Name	Command
Windows Update Security Patches	C:\ProgramData\enc6.exe
Windows Update Security Patches 5	C:\ProgramData\enc.exe
Windows Update Security	regsvr32.exe /i c:\programdata\network.dll

Over 700 computers were targeted in the attack, which was detected and blocked by Sophos Intercept X.

Either the attackers didn't realize the attack had been blocked or they were hoping that the theft of the data would be enough for the target to pay up – but whatever the reason, upon launching the first attack attempt they issued a ransom demand for US$ 15 million.

Day 7: The MTR team gets to work

Realizing that they were under attack, the target's security team engaged the advanced incident response skills of the Sophos MTR team. Since they were not yet a Sophos MTR customer, the Sophos Rapid Response team was first engaged. The team quickly identified the compromised admin account, identified and removed several malicious files, and blocked attacker commands and C2 (command and control) communications.

Day 8: Investigation and neutralization continue

Over the following hours the MTR team found further tools and techniques used by the attackers, as well as evidence relating to the exfiltration of data. More files and accounts were blocked.

Day 9: The second attack

The attackers launched a second attack via a different compromised account. This attack was similar to the first one: commands were executed on a DC, looping through the lists of IP addresses contained in txt files.

However, this time they coped a file called license.exe to C:\ProgramData:

```
FOR /f "usebackq delims=" %a IN ("c:\programdata\s1.txt")
DO XCOPY /F /Y "c:\programdata\license.exe" \\%a\C$\programdata\"
```

This was followed by a scheduled task to execute it. In this attack attempt the task was called “Google Chrome Security Update”:

```
FOR /f "usebackq delims=" %a IN ("c:\programdata\s1.txt")
do cmd /c SCHTASKS /s %a /RU "SYSTEM" /create /tn "Google Chrome Security Update"
/tr "C:\programdata\license.exe" /sc ONCE /sd 01/01/1910 /st 00:00 /f
```

The attack was quickly identified and stopped. Intercept X detected the ransomware, and the MTR team disabled and deleted both the compromised account and the license.exe file. No files were encrypted.

Day 9: Third time lucky?

Just a few hours after the second attempt, the attackers tried again.

By now they seemed to be growing desperate. This attack targeted a single machine, the main file server that the exfiltrated data had been taken from, and used a completely different technique to the previous attacks.

In the third attempt, the attackers distributed the ransomware payload inside a virtual machine (VM).

Fortunately the MTR investigators recognized this new approach immediately as they had also responded to the Ragnar Locker ransomware attack where the technique was first seen.

The Maze operators had enhanced the technique, but it was undoubtedly the same. The attack was detected and stopped and no files were encrypted.

Defeating adversaries in human-led attacks

This casebook highlights how agile and adaptable human-operated attacks can be, with the attackers able to quickly substitute and reconfigure tools and return to the ring for another round. It also demonstrates how, to minimize likelihood of detection, attackers take advantage of multiple legitimate IT tools in their attacks.

Sophos endpoint products detect components of this attack as Troj/Ransom-GAV or Troj/Swrort-EG. Indicators of compromise can be found on the SophosLabs Github.

What can defenders do?

The most important things an IT security team can do is to reduce the attack surface, implement strong security software, including specialist anti-ransomware security, educate employees, and consider setting up or engaging a human threat hunting service to spot the clues that software can’t.

Any organization can be a ransomware target, and any spam or phishing email, exposed RDP port, vulnerable exploitable gateway device or stolen remote access credentials will be enough for such adversaries to gain a foothold.

MITRE ATT&CK Mapping

The MITRE ATT&CK framework is a globally accessible knowledge base of known adversary tactics, techniques and procedures (TTPs). It can help security teams as well as threat hunters and analysts to better understand, anticipate and mitigate attacker behavior.

Initial Access

- T1078.002 – Valid Accounts: Domain Accounts
- T1133 – External Remote Services

Execution

- T1059.001 – Command & Scripting Interrupter: PowerShell
- T1059.003 – Command and Scripting Interpreter: Windows Command Shell
- T1047 – Windows Management Instrumentation
- T1053.005 – Scheduled Task/Job: Scheduled Task

Defense Evasion

T1564.006 – Hide Artifacts: Run Virtual Instance

Credential Access

T1003.003 – OS Credential Dumping

Discovery

T1016 – System Network Configuration Discovery

Lateral Movement

- T1021.001 – Remote Services: Remote Desktop Protocol
- T1021.002 – Remote Services: SMB/Windows Admin Shares

Command & Control

T1071.001 – Application Layer Protocol: Web Protocols

Exfiltration

T1567.002 – Exfiltration Over Web Service: Exfiltration to Cloud Storage

Impact

T1486 – Data Encrypted for Impact

Sophos Managed Threat Response and threat hunting

For more information on the Sophos MTR service visit our website or speak with a Sophos representative.

If you prefer to conduct your own threat hunts Sophos EDR gives you the tools you need for advanced threat hunting and IT security operations hygiene. Start a 30-day no obligation trial today.