Maze Ransomware Analysis and Protection

December 9, 2020 | Yaron Dinkin | Identity Protection

This blog was originally published on May 13, 2020.

Maze ransomware is a malware targeting organizations worldwide across many industries. It is believed that Maze operates via an affiliated network where Maze developers share their proceeds with various groups that deploy Maze in organizational networks. More concerning than just the penetration in the organization, Maze operators have a reputation for taking advantage of assets in one network to move laterally to other networks. Since the affected company is part of IT services provider, it is extremely likely that this breach could be leveraged to attack hundreds of customers that rely on their IT services.

Three years ago, we published a short blog post about NotPetya. The blog discussed some of the techniques employed by the ransomware and how these can be mitigated. Three years later, these techniques are still vulnerable to the same type of attacks. As we followed up with this Maze story, we thought it would be a good idea to share insights on why these types of ransomware attacks are prevalent and what actions you can take to mitigate them.

How organizations get infected with Maze

This blog post shares the tactics, techniques, and procedures used by Maze. The research lists which tools and techniques Maze is using in various stages of the attack cycle (initial access, reconnaissance, lateral movement, and privilege escalation). Reading the techniques list, it is clear that Maze does not typically employ 0-days (one exception is trying to use a 1-day: CVE-2018-8174). This is actually expected – attackers typically don't use 0-day vulnerabilities for two main reasons. They are extremely hard to find and very expensive and, when used in the wild, they get exposed and fixed very quickly.

Let's review the techniques:

Initial Access

We can see that in most cases the techniques used by Maze operators are valid credentials that log in to the network via internet-facing assets. It can be an open RDP server or a Citrix/VPN server. How the initial credential was compromised is unclear but standard attack methodologies include guessing default/weak passwords or spear-phishing through a targeted mail with a .docx attachment containing a malicious macro.

- T1133: Spear-phishing Attachment
- T1133: External Remote Services
- T1078: Valid Accounts

Reconnaissance

Once an initial machine in the network is compromised, the malware starts scanning the network to find vulnerabilities. The malware scans various facets such as open SMB shares, network configuration, and various Active Directory attributes such as permissions, accounts, and domain trusts. The scans could be performed with known open-source tools such as smbtools.exe, Adfind, BloodHound, PingCastle as well as built-in Windows commands.

- T1087: Account Discovery
- T1482: Domain Trust Discovery
- T1083: File and Directory Discovery
- T1135: Network Share Discovery
- T1069: Permission Groups Discovery
- T1016: Remote System Discovery
- T1018: System Network Configuration Discovery
- T1033: System Owner/User Discovery

Lateral Movement/Credential Access

After a few days of gaining intelligence on the network, the malware started moving laterally in the network. The easiest option was to find credentials in the compromised machine. These could have been Kerberos tickets or password hashes. Maze also scans compromised machines for files containing plaintext passwords. When these are not found, the malware tries moving laterally in the same network segment using LLMNR/NBT-NS Poisoning to steal network packets for later NTLM cracking and/or NTLM relay attacks. Finally, if none of these techniques work, the malware tries to find weak passwords by brute-forcing user/service accounts. Once a valid credential is found, the malware uses known Windows interfaces such as SMB, WinRM, and RDP to move laterally and execute code on remote machines.

- T1110: Brute Force
- T1003: Credential Dumping
- T1081: Credentials in Files
- T1171: LLMNR/NBT-NS Poisoning
- T1076: Remote Desktop Protocol
- T1028: Windows Remote Management
- T1097: Pass the Ticket
- T1105: Remote File Copy
- T1077: Windows Admin Shares

Privileges Escalation

Privilege escalation is a kind of dance. The attacker moves laterally to new machines. Once they're on new machines they can again use the same lateral movement techniques and find new credentials to compromise and move to additional machines. The process is typically over once domain admin credentials are found. At this point, the attacker can easily compromise any machine in the network.

- T1078: Valid Accounts
- T1055: Process Injection
- T1050 New Service

Persistence

As is often the case in these situations. The operator wants to maintain his presence in the network for as long as possible. This means adding various backdoors and ways to retake control over the network. This is done so if malware is detected and removed, the operator can compromise the network a second time. The method discovered in this case is mainly to capture as many user credentials as possible and potentially create new privileged accounts in the network.

- T1078: Valid Accounts
- T1050 New Service
- T1136: Create Account
- T1031: Modify Existing Service

The Root Cause

The critical point is that throughout the compromise, most of the malicious activity is executed using valid user credentials. The malware is stealing credentials in various ways. It is using tools like Mimikatz to harvest local credentials and later-performing Pass-the-Hash attacks. Maze attempts to find passwords that are stored in local drives, sometimes engaging in attacks to compromise accounts with weak passwords using brute force and credential scanning techniques.

I often engage with customers and review the security posture of their network. I've never encountered a network where I couldn't find any software vulnerability. In some cases, I find trivial security configuration issues allowing one-click elevation of privilege to domain admin. You can find another great talk on this subject by the BloodHound team at SpecterOps delivered last year at Blackhat.

How CrowdStrike Can Help

The following is a visual matrix representation of the MITRE ATT&CK techniques we've reviewed in the previous section and an analysis of what techniques are covered by the CrowdStrike Falcon® Zero Trust platform (formerly the Preempt platform).

Click image to enlarge

As can be seen, Falcon Zero Trust helps mitigate every step in the Maze attack chain. Additionally, it enforces/monitors every technique in Lateral Movement/Credential Access steps.

Roughly speaking the Zero Trust platform offers three types of mitigations:

- Security Assessment: Statically analyzing current configuration and security practices to find security vulnerabilities and holes.
- Threat detection: Monitoring network traffic and data continuously and detecting malicious activity in real time.
- Threat Prevention: Define real-time custom Conditional Access policies to block access or trigger MFA based on changing behavior and increasing risk, allowing you to proactively thwart malicious activity in real time. This deterministic approach reduces user friction when accessing applications/resources.

Let's review how can CrowdStrike Identity Protection helps with every mitigation.

Security Assessment

Knowing your vulnerabilities is preventative medicine. CrowdStrike® Falcon Zero Trust can help you not just to detect an attack but also to avoid it altogether by presenting a smooth attack surface. Here are a few Maze-vulnerable configurations Falcon Zero Trust can scan for in your network:

1. Weak Passwords
2. Privileged Accounts
3. Detect various GPO misconfiguration:
   - Open RDP servers with no NLA
   - Servers with no SMB signing
   - Servers supporting NTLMv1

Threat Detection

Most of the initial reconnaissance of Maze can be detected by Falcon Zero Trust. BloodHound, credentials scanning, SMB share enumeration, and LLMNR/NBT-NS Poisoning all have detection modules. Privilege escalation usually involves noisy operations such as dumping domain hashes, creation of new privileged accounts, or executing code on the domain controller. All these are detected by the Falcon Zero Trust platform. For ongoing security, any anomalous resource account can be monitored for suspicious/anomalous behavior. Vendor or otherwise sensitive accounts should be closely monitored and have their activity logs reviewed periodically.

Threat Prevention

Policies are the key to automating a security response and are critical to blocking and preventing malicious attacks. The following is a quote from a blog post we released three years ago: "All it takes to cause serious harm to your network is a few minutes. By the time you see the alerts in your security analytics solution or SIEM, the NotPetya of the world will have already scrambled all your data". Detection is important, but sometimes you want to simply block the attack and not allow it to happen at all.

As described above, most of the activity performed in Maze ransomware attacks are existing, valid accounts. The Falcon Zero Trust solution has the ability to deploy a flexible and extensive policy and to block or MFA any actions using valid credentials. Simple policies challenging privileged accounts with MFA and triggering an MFA for anomalous activities can mitigate most of the ways lateral movement is being performed.

We also recommend creating an additional policy to further segment and limit the operations allowed to be performed by external vendors.

Maze Ransomware Summary

Ransomware operators are using old techniques and open-source tools such as BloodHound and Mimikatz to compromise and move laterally in networks. They have been doing so for a while with great success. Enterprise networks are getting hacked mostly by compromised credentials and credentials-based attacks. Simple steps like monitoring for weak passwords, limiting account privileges, detecting stealthy admins, and enforcing adaptive authentication can reduce most of the risk of being the next ransomware victim.

Additional Resources

- *Learn more by reading the white paper, "Defending the Enterprise with Conditional Access Everywhere."*
- *Visit the CrowdStrike Falcon Identity Protection solutions webpage.*
- *Request a demo of CrowdStrike Falcon Zero Trust or Falcon Identity Threat Detection products.*
- *Read expert insights and analysis on other complex threats — download the CrowdStrike 2020 Global Threat Report.*

Related Content

Security Advisory: MSRPC Printer Spooler Relay (CVE-2021-1678)

On Patch Tuesday, January 12, 2021, Microsoft released a patch for CVE-2021-1678, an important vulnerability discovered by CrowdStrike® researchers. This vulnerability allows an attacker to relay NTLM authentication sessions to an attacked machine, and use a printer spooler MSRPC interface to remotely execute code on the attacked machine. A similar MSRPC relay first appeared in […]

Six Tips for Securing Privileged Accounts in the Enterprise

This blog was originally published on March 2, 2016. Protecting privileged accounts and actively responding to key potential compromises has become a critical initiative for many CISOs. Stolen credentials are at the heart of most modern attacks and breaches. Attackers can easily obtain credentials via phishing attacks, brute force, keyloggers, pass-the-hash techniques or using a […]

Your Session Key Is My Session Key: How to Retrieve the Session Key for Any Authentication

This blog was originally published on June 11, 2018. As announced in our recent security advisory, Preempt (now CrowdStrike) researchers discovered a critical vulnerability that allows attackers to retrieve the session key for any NTLM authentication and establish a signed session against any server. Any domain environment which does not entirely block NTLM traffic is […]

← Catching Blood Hound Before It Bites

The Imperative to Secure Identities: Key Takeaways from Recent High-Profile Breaches →

CATEGORIES

Endpoint & Cloud Security (260)
Engineering & Tech (64)
Executive Viewpoint (102)
From The Front Lines (153)
Identity Protection (14)
Observability & Log Management (67)
People & Culture (74)
Remote Workplace (27)
Research & Threat Intel (334)
Tech Center (132)

CONNECT WITH US

FEATURED ARTICLES

2022 Global Threat Report: A Year of Adaptability and Perseverance
February 16, 2022

Falcon XDR: Extending Detection and Response – The Right Way
February 10, 2022

Falcon XDR: Why You Must Start With EDR to Get XDR
February 10, 2022

February 2022 Patch Tuesday: Windows Kernel Zero-Day and Servicing Stack Updates
February 9, 2022