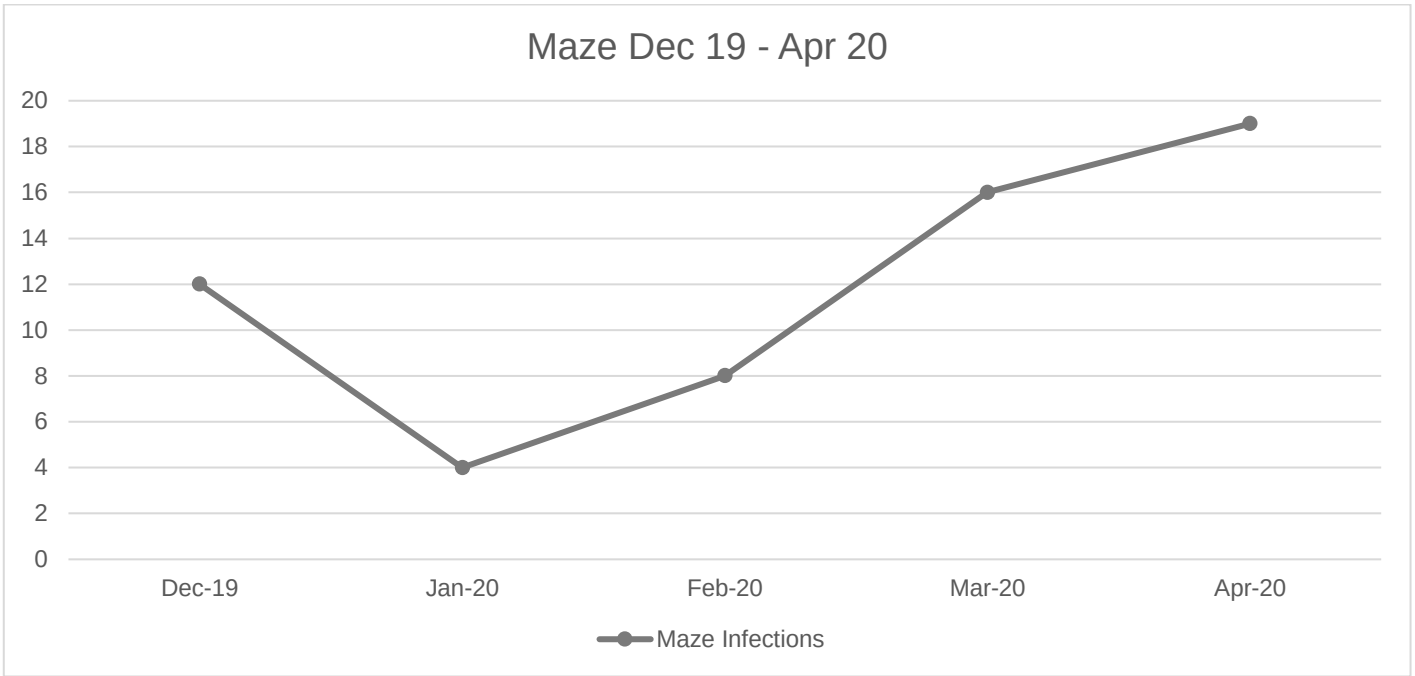
SPELLSECURITY

THREAT ADVISORY REPORT

Maze Ransomware

INTRODUCTION

In this Advisory we will take a look at the infamous Maze Ransomware that has been targeting organizations worldwide. This Ransomware made its debut in late May 2019. While it's currently unclear who exactly is behind this family actors such as TA-2101 (A group that targets German government agencies and US tax professionals) has been observed employing it in its campaigns. SpellSecurity Threat Research team has been tracking this family since December 2019.



EXECUTIVE SUMMARY

In early January 2020, FBI released a flash alert cautioning private businesses against possible rise in Maze campaigns. This family has been observed in targeted attacks against corporations.

There are a couple of things that differentiate Maze from traditional ransomware: -

- This family employs a data exfiltration module from infected machines. This makes sense as even organizations with backup and recovery strategies would still be held at "ransom" with the stolen data.
- The authors have publicly released the stolen data from victim's environment on failure to pay the ransom.
- The authors will also publicly disclose their victims to further pressure the victim.

There is no guarantee that the attackers delete the acquired data after payment. These "extortion" tactics have since been adopted by other ransomwares like REvil, DopplPaymer, Ragnar Locker, and Nefilim.

DESCRIPTION

Infection Vector and Lateral Movement

This ransomware is known to typically spread via: -

- Exploit Kits: Fallout and Spleevo drive by downloads.
- Exploit Frameworks: Cobalt Strike.
- Malspam.

Spellsecurity Threat Research team has observed this ransomware operating in two different ways.

TARGETED CAMPAIGNS

The attackers initially gain access to a corporate environment and spend significant time spreading internally. The common techniques observed in their lateral spread were: -

- Bruteforcing weak RDP credentials.
- Named pipe techniques.

Once the attacker has acquired enough data, they deploy Maze to encrypt and extort the victims.

NON-TARGETED WIDESPREAD CAMPAIGNS

In some campaigns the attackers directly drop Maze, as observed in the Fallout Exploit Kit campaign. One of the vulnerabilities used was Flash Player CVE-2018-15982 [1] which targeted versions 31.0.0.153 and earlier, and 31.0.0.108 and earlier. Another vulnerability being exploited in the wild by this ransomware to escalate privilege is CVE-2016-7255 [3].

Encryption Algorithm

This ransomware uses RSA 2048 and Cha Cha algorithms. There is no known publicly available decryptor for this ransomware as of 20th April 2020. After encryption the malware deletes the shadow copy on the system.

Exfiltration Tactics

The exfiltration tactics used by this ransomware family are: -

- Powershell Scripts to connect to FTP servers.
- POST to C2 from a list of hosts encrypted in the binary.

SPELLRADAR

In this section, we look at some of the latest incidents involving Maze Ransomware as observed on the SpellWorkbench threat intelligence platform. Spell Radar Strategic Intel Reports provides a security analyst with a quick and comprehensive view of the latest security incidents and trends.

Incidents

S.no	Title	Target	Industry	Location	Impact	Reference
1	Cognizant falls prey to Maze Ransomware	Cognizant	IT	-	-	Link
2	Manitoba Law firms falls victim to Maze Ransomware.	Manitoba Law Firms	Legal	Canada	-	Link
3	Maze Gang leaks Hammersmith Medicines Research data.	Hammersmith Medicines Research	Health	UK	Medical records of volunteers undergoing trials.	Link
4	Berkine Oil Giant hit by Maze Ransomware.	Berkine	Petroleum	Algeria	500 MB of critical data.	Link
5	BetUS infected by Maze.	BetUS	Gambling	USA	3 emails + additional data.	Link
6	Chubb Insurance hit by Maze	Chubb	Financial	-	-	Link
7	SouthWire hit by Maze Ransomware	SouthWire	Cable	USA	14GB	Link
8	Bouygues Construction falls victim to Maze Ransomware.	Bouygues Construction	Construction	France	-	Link
9	Maze ransomware release files stolen from City of Pensacola.	Pensacola Infrastructure	Government	USA	2GB	Link

Malware & Campaigns

S.no	Description	Actor	Threat Type	Reference
1	Malware Analysis of Maze Ransomware. A Ransomware with data exfiltration capabilities that spreads via remote services and RDP.	Maze Gang	Ransomware	Link
2	Maze Delivered via Cobalt Strike.	Maze Gang	Ransomware	Link
3	Fallout Exploit Kit dropping Maze Ransomware	Maze Gang	Ransomware	Link

RECOMMENDATIONS

SpellSecurity recommends the following steps to mitigate the risk of Maze Ransomware: -

- Blacklist the IOCs listed in Appendix [2].
- Strong password policies across the environment.
- Scan systems for registry persistence.
- Check logs/systems against regularly updated Intel Feeds for Maze IOCs.

SpellSecurity recommends the following best practices for diminishing ransomware imapct: -

- Patch System and Applications wherever possible.
- Deploy AV and/or EDR wherever possible.
- Consider a VDI solution, especially in the current environment with prevalent use of Work From Home and users using their personal systems.
- SIEM solution/detections on the environment logs, especially the VPN and proxy logs.
- Employ a data backup and recovery policy for critical information. Running mock backup recovery can help prepare the team for an attack.
- Apply the principle of least privilege to applications, services and users.
- Use email security products to identify emails with potential malicious attachments or suspicious sources.
- Network segmentation to lessen the spread of infection.

SPELLHUNT

SpellHunt is a next generation, multi-tenant threat hunting platform that provides security teams with the deep visibility they need to perform routine threat hunting activities in your environment, monitor systems, investigate, respond and document incidents.

APPENDIX

IOCs

S.no	Type	Reference
1	Hashes	https://spellsecuritystaging.s3.amazonaws.com/artifact%2F1587468778.xlsx
2	IP	https://spellsecuritystaging.s3.amazonaws.com/artifact%2F1587396095.xlsx
3	URL	https://spellsecuritystaging.s3.amazonaws.com/artifact%2F1587475563.xlsx

[redacted]

Questions

research@spellsecurity.com

SpellSecurity Inc