Maze Ransomware

"**Maze Ransomware**" is a not-so-familiar term for many of us. With the advent of media penetration, most of us have heard the term Ransomware and it truly can send a cold wave through the spine of the IT professionals, particularly those who are responsible for maintaining the IT infrastructure of any organisation.

Now what is this "**Maze Ransomware**" ?

The Cyber Security – Centre of Excellence (CS-CoE), functioning under the Dept. of IT & Electronics, has a team of extremely knowledgeable IT professionals who are experts in cyber related issues too. To extract a best literature from them, the CS-CoE Management decided to call for a competition where all CS-CoE members participated.

Shri Mainak Sen, a certified ethical hacker and a network architect, working as an Assistant Manager in the internal IT cell of WBEIDC Ltd. (Webel) has come out with the best output. Being an engineer by profession, and during his stint with Webel for 9 years, he was part of many successful projects.

We are happy to bring out the article by Shri Mainak Sen for your knowledge update and reading pleasure.

Maze Ransomware

History | Impact | Attack Chain | Uniqueness | Mitigation

Original Issue Date: April 26, 2020

Severity Rating: High

What is Ransomware?

Ransomware is a form of malware that targets your critical data and systems for the purpose of extortion. Ransomware is frequently delivered through spearphishing emails with infected link or macro-enabled documents as attachments. After the user has been locked out of the data or system, the cyber actor demands a ransom payment.

What is the impact?

Ransomware targets home users, businesses and government networks and can lead to temporary or permanent loss of sensitive or proprietary information, disruption to regular operations, financial losses incurred to restore systems and files, and potential harm to an organization's reputation.

Common types of ransomware

The first ransomware virus was thought to be PC Cyborg, which appeared in 1998. It used simple symmetric encryption, and it was relatively easy to produce tools to decrypt files that PC Cyborg had encrypted. But it wasn't until 2012, with the arrival of the Reveton worm that attempts to hold users'

computers for ransom payments became commonplace. Reveton locked users out of their computers unless they paid a "fine" through a payment service such as Ukash. Two years later, CryptoLocker was released, encrypting user files and demanding a ransom for the key to decrypt them. This became the template for most subsequent types of ransomware that have appeared since.

There are two main types of ransomware:

- Locker ransomware, which locks the computer or device
- Crypto ransomware, which prevents access to files or data, usually through encryption.

Now, the third one has evolved which not only encrypt the files but threatens to release the data in various medium if the ransom has not been paid.

Details of Maze Ransomware

The Maze ransomware, previously known in the community as “ChaCha ransomware”, was discovered on May the 29th 2019 by Jerome Segura. Like other ransomware seen in the past, Maze can spread across a corporate network, infect computers it finds and encrypts data so it cannot be accessed. But what makes Maze more dangerous is that it also steals the data it finds and exfiltrates it to servers controlled by malicious hackers who then threaten to release it if a ransom is not paid. Increasingly, other ransomware (e.g., REvil (also known as Sodinokibi) Nemty, Clop etc.) have been observed using similar tactics. **SO THIS IS A COMBINATION OF A RANSOMWARE ATTACK AND A DATA BREACH.**

Maze ransomware is targeting companies across sectors, including Healthcare, IT/ITeS and Banking across the globe. A website operated by the criminals behind the Maze attacks claims, if the ransom is not paid, they will:

- Release public details of your security breach and inform the media
- Sell stolen information with commercial value on the darkweb.
- Tell any stock exchanges on which your company might be listed about the hack and the loss of sensitive information
- Use stolen information to attack clients and partners as well as inform them that your company was hacked.

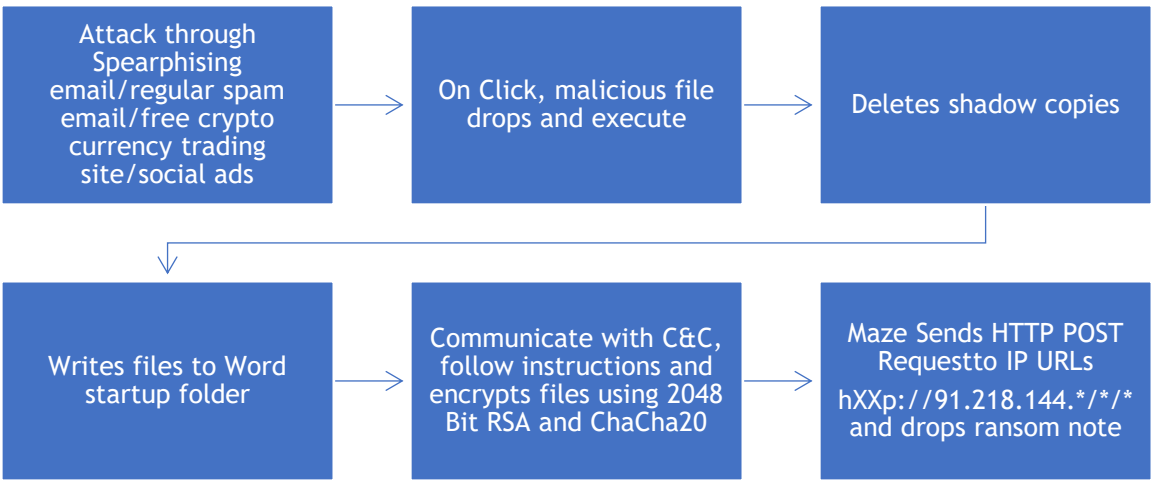
Below are the observations on maze group ransomwares, basis internal static and dynamic analysis.

- 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 some files for free as a proof of work

Attack Chain

Maze has been using emails, RDP along with exploit kits like Fallout EK, Spelevo EK. Payloads have been downloaded through Word documents as attachments through email. Each Word document was embedded with a macro that downloaded Maze ransomware from the actor-controlled server. The macro then wrote the ransomware payload to C:\Windows\Temp\wordupd.tmp and executed it.

After Maze encrypted the victim’s files, it made HTTP POST requests to several IP-based URLs that began with the first octet 91. Only a few of these requests returned a 200 response code, indicating a successful connection.



The interesting difference with this version is that it attempts to detect whether the victim is using a home computer, workstation, domain controller, or server and adjusts its ransomware accordingly. When the victim is successfully infected, the Maze Ransomware displays a wallpaper on the victim's screen with instructions and what type of system the victim is using.

Indicators of Compromise

MD5 Hashes

- 8205a1106ae91d0b0705992d61e84ab2

SHA1 Hashes

- 49cdc85728bf604a50f838f7ae941977852cc7a2

SHA256 Hashes

- 91514e6be3f581a77daa79e2a4905dcbdf6bdcc32ee0f713599a94d453a26fc1
- 19AAA6C900A5642941D4EBC309433E783BEFA4CCCD1A5AF8C86F6E257BF0A72E
- B950DB9229DB2F37A7EB5368308DE3AAFCEA0FD217C614DAEDB7F334292D801E
- 5d59b107448b2c61849dd0f41fc179df9d60c35355e2d8d0ac9e19b97a3b96dd

SSDEEP

- 6144:66dXYUNkTVW1ibG9WDPeocKZLqNUPitzHzO6YIBFFQQXtP/C62814nbncULJJ2ne:66NYSWVxEU2Gp0tzQIBTbXGzzLf

Ransomware Note

Difference between popularly known other ransomware

As new ransomware variants arise on a regular basis, it can be difficult to keep track of the different strains. While each of these strains of malware are different, they often rely on similar tactics to take advantage of users and hold encrypt data hostage. Let's take a look at the common ransomware examples and their different approach:

NAME OF RANSOMWARE	DESCRIPTION / ATTACK METHODOLOGY
PETYA	**Petya overwrites the master boot record, leaving their operating system in an unbootable state.** The virus is delivered via email, designed to look like an applicant seeking a job. The email contains a hyperlink to Dropbox to download a resume.
GOLDENEYE	It is similar to the prolific Petya ransomware. Hackers spread GoldenEye ransomware through a massive campaign targeting human resources departments. After the file is downloaded, a macro is launched which encrypts files on the computer. For each file it encrypts, **GoldenEye adds a random 8-character extension at the end. The ransomware then also modifies the user's hard drive MBR (Master Boot Record) with a custom boot loader.**
WANNACRY	Like other forms of ransomware, the malware is commonly **spread via phishing emails** prompting users to unknowingly download the file and encrypt their data. WannaCry uses SAMBA to connect remotely and add their malware to the exploited machine. **Once WannaCry has gotten onto the network, it can spread like a worm**. If the ransom goes unpaid, after a couple of days it

	increases, and after a slightly longer amount of time **the decryption algorithm is deleted and data is lost**.
CRYSIS	Crysis ransomware encrypts files on fixed, removable, and network drives with a strong encryption algorithm making it difficult to crack in a reasonable amount of time. **It's typically spread via emails containing attachments with double-file extension, which make the file appear as a non-executable file.** In addition to emails, it can also be disguised as a legitimate installer for applications.
TORRENTLOCKER	TorrentLocker is typically distributed through spam email campaigns and is geographically targeted with email messages delivered to specific regions. It uses an AES algorithm to encrypt file types. **In addition to encoding files, it also collects email addresses from the victim's address book to spread malware beyond the initially infected computer—this is unique to TorrentLocker.**

Recommendation

Common infection vectors used by Maze Ransomware are phishing emails with MS Office attachments and fake/phishing websites laced with Exploit Kits. Hence, we advise users to exercise caution while handling emails from unknown sources, downloading MS Office attachments, enabling macros and clicking on suspicious links.

Here are a few additional guidelines which will help to minimize the attack surface & possible damage to IT infrastructure.

- Security researchers have seen the Spelevo exploit kit delivering Maze ransomware. Since Spelevo exploits outdated browser plugins, users should frequently update their browsers and plugins with the latest security patch.
- Install ad blockers to combat exploit kits such as Fallout that are distributed via malicious advertising.
- Implement strong email security software that detects Word attachments that are potentially embedded with malicious macros.
- Frequently back up files so they can be used to recover lost data in the event of a ransomware infection. Create an effective backup strategy by following the 3-2-1 rule.
- Lockdown Remote Desktop Protocol (RDP), if not in use or follow RDP best practices such as rate limiting, 2FA, etc.
- Ensure segmentations of the network to limit the spread
- Conduct regular phishing awareness campaign to alert the users and contain the spread of spammed emails and attachments

References

- https://www.mcafee.com/blogs/other-blogs/mcafee-labs/ransomware-maze/
- https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view
- https://www.dsci.in/sites/default/files/Maze_Ransomware_Technical_Report.pdf
- https://www.sciencedirect.com/science/article/abs/pii/S0167739X18307325
- https://www.esecurityplanet.com/malware/types-of-ransomware.html

- https://www.tripwire.com/state-of-security/featured/maze-ransomware-what-you-need-to-know/
- https://www.datto.com/blog/common-types-of-ransomware
- https://blog.malwarebytes.com/detections/ransom-maze/
- https://www.binarydefense.com/threat_watch/maze-ransomware/
- https://nationalcybersecuritynews.today/computersecurity-computernews-hacker-a-guide-for-defending-against-maze-ransomware/