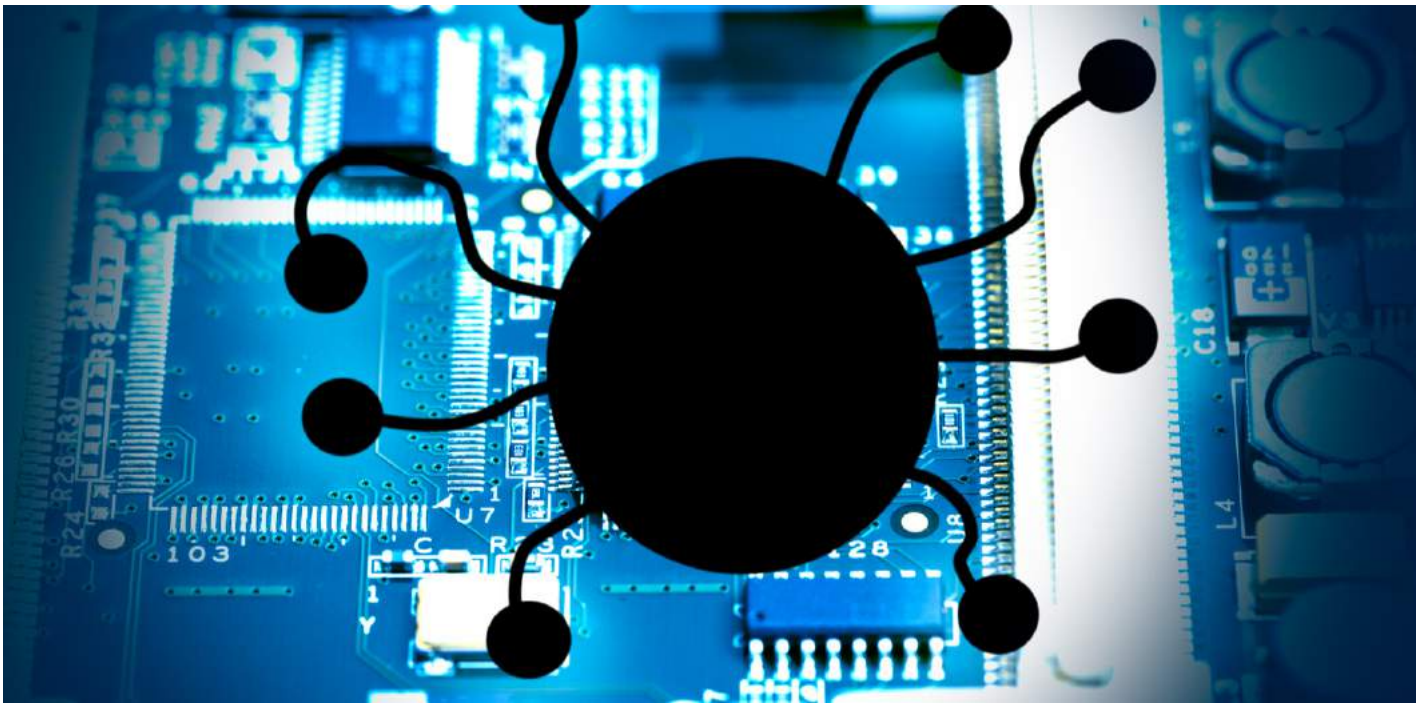
MAZE.RANSOMWARE
NEW DESTRUCTIVE MALWARE STRAIN



SUMMARY

Maze.Ransomware is a sophisticated file-encrypting windows strain and successor of ChaCha malware, identified in mid-May 2019. Maze uses a variety of malicious techniques and tactics in its code to give a legitimate impression.

Maze ransomware is a 32-bit file that often comes with '.EXE' or ".DLL" extensions. The malware uses two unique cipher keys (RSA and ChaCha20) to crypt data files, similar to ChaCha malware.

Once the data gets locked, the threat group behind Maze, demands the victim for a ransom to decrypt compromised files. Unlike other ransomware, the threat group exposes the stolen data on the public internet, when the victim did not pay the demanded ransom.

Since its first identification in October 2019, researchers have been identifying a persistent spike in the malicious Maze attacks across the world. Maze ransomware has been primarily targeting B2B service provider companies that engage other companies to provide data-driven services.

HOW MAZE WORKS?

INITIAL ACCESS

Researchers found that Maze uses a different means to gain initial access to data systems. Impersonation of systems with weak passwords, usage of exploit kits that scan for vulnerable applications to exploit, and phishing campaigns are popular ways of Maze distribution. Currently, a phishing campaign containing emails with macro-enabled word attachments has seen targeting organizations.

LATERAL MOVEMENT

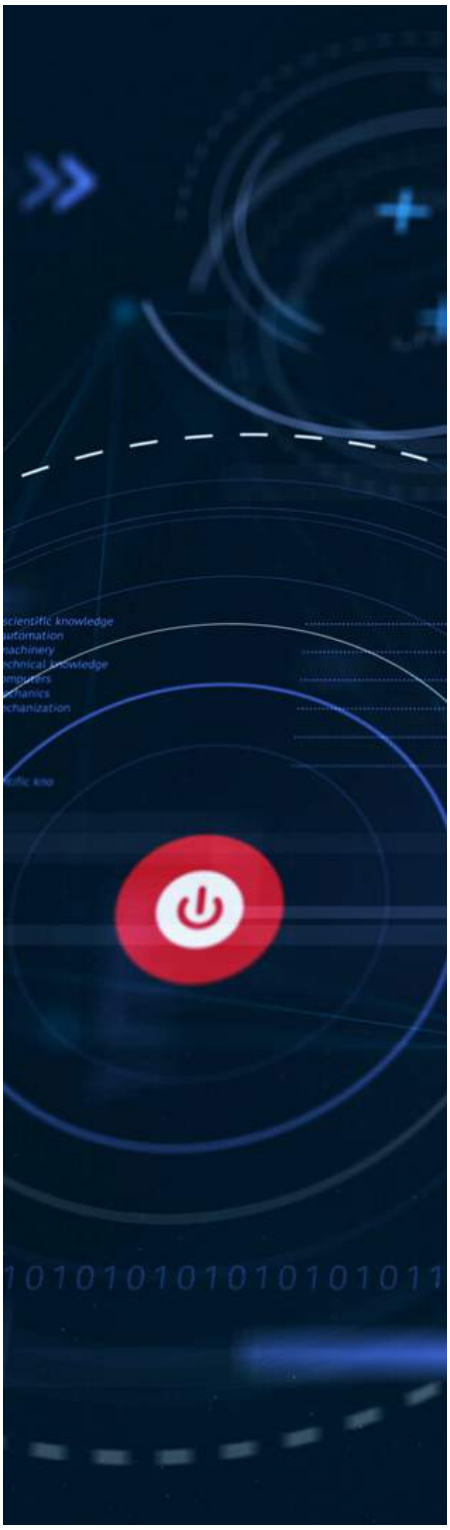
After succeeding in its initial intrusion, Maze starts executing its malicious payload without knowledge of the victim and starts encrypting the files.

At first, the malware checks for the existence of the data files and once it confirms that the file exists, it then allocates memory to store the file along with obtaining permission to open, read, and write.

Maze generates a random 32-byte key and a new random extension for the victim file, unique for each file, and appends the new extension to the old. The ransomware appends a string of length 4-7 random characters and a marker at the end of each compromised data file. After making necessary changes, Maze crypts the infected file with ChaCha algorithm and RSA public key. Later, the malware uses anti-forensics to evade detection.

The malware overwrites encrypted files on the same sector (a subdivision of a track on a magnetic disk) of the raw disk as the original files and makes recovery impossible.

After successfully encrypting data files, the malware drops DECRYPT-FILES.html message to the victim, asking for ransom in bitcoins. The file DECRYPT-FILES.html further contains information about proceeding with the ransom payment.



TYPES OF FILES IGNORED BY MAZE

Based on the malware samples analysed until now, Maze ransomware ignores a few types of data files from locking. The malware ignores data present in the files with extensions, .LNK, .EXE, .SYS, and .DLL.

The malware has a list of files that it leaves non-encrypted, which includes inf, ini, dat, db, bak, dat.log, bin, DECRYPT-FILES.txt. Below is the list of folders ignored by Maze:

- Windows main directory
- Games
- Top Browser
- ProgramData
- cache2\entries
- Low\Content.IE5
- All Users
- Local Settings
- AppData\Local
- Program Files
- User Data\Default\Cache

Threat Intelligence Feed

Here is the list of Indicators of Compromise for Maze Ransomware detected across the globe.

Know more

MITIGATION MEASURES:

HERE IS THE SEQUENCE OF MITIGATION STEPS FOR PROACTIVE DETECTION AND HUNTING OF MAZE RANSOMWARE:

1. Remove infected or suspicious devices from respective networks to disable lateral movement of the malware from one system to another.
2. Run IR Scripts such as Fast IR/ SISA IR for collecting artifacts and acquiring forensic images of the critical systems.
3. Identify the Command and Control (C2) server of the malware, communicating with the infected system, and block its IP address or domain.
4. Use NetFlow logs to scope other systems that communicated with the systems infected or suspected of Maze infection
5. Boot the infected or suspected systems in safe mode and launch a deep scan mode of Anti-Virus/ Anti-Malware software. Replicate the step across scoped systems.
6. Also, repeat the step for backups (onsite and offsite) and restoration points. Ensure regular scanning of backups with updated Anti-Virus/ Anti-Malware solutions
7. Try executing data recovery software on acquired images for data discovery and encryption, a good practice to minimize the effects of data loss

Security Best Practices

In cybersecurity, prevention is beyond just better than cure. Below are a few security best practices that ensure good network health and block Maze ransomware's intrusion:

1. Ensure capturing the following logs with a SIEM
   - DNS logs
   - Netflow logs or equivalent
   - Web server access logs
   - Proxy logs
   - Server logs

   A SIEM solution can analyze the above logs on a real-time basis and generate alerts when there occurs a suspicious activity.

2. Have a team of security monitoring experts to monitor network traffic 24/7 and identify incident/ ingress points within minutes. Also, train the security monitoring team on Incident Response activity.

3. Monitor egress traffic for data exfiltration events

4. Deploy the Intrusion Prevention System/ Intrusion Detection System and regularly update signatures.

5. Deploy a Web Application Firewall and monitor all public web applications, web services, public exposure, etc.

6. Perform a regular backup of critical and sensitive data

7. Host-Based controls:
   - Implement Multi-Factor Authentication for all console/non-console access
   - Configure a strict access control list on a firewall to allow only necessary traffic
   - Use application whitelisting software to whitelist permitted software
   - Deploy Anti-Virus/ Anti-Malware solutions. Update the signatures regularly, perform a regular full system scan and enable real-time protection
   - Patch all critical, high severity and medium severity exploitable vulnerabilities (operating system, applications, etc.) every week for endpoint systems and monthly basis for servers
   - Deploy File Integrity Monitoring tool and configure it to monitor all critical files

8. Improve end-user security awareness with security awareness training. Also, test the knowledge of end-users from time to time using phishing simulators.