Exploited!!

Jose Ramirez

University of Advancing Technology

Exploited!!

MAZE ransomware incidents have been seen throughout 2019 and 2020, the group behind the ransomware does not seem to be slowing down either. MAZE is a sophisticated Windows ransomware that has been plaguing businesses, mainly those located in the United States. The group behind the ransomware attacks have been focused on targeting financial services, healthcare, and manufacturing organizations. This report will talk about how they are able to deploy MAZE and the techniques the threat actors use to blackmail the companies affected.

# The Vulnerabilities

The MAZE ransomware threat actors have been seen taking advantage of 4 different intrusion methods. The first method is a very common method used by ransomware threat actors, phishing emails. The emails will look legitimate, but they are not, the email’s sender will be a fake domain created to mimic a legitimate company email domain. For example, an attacker will create a fake account under the name google-team-support@gmail.com, and will use the account to send fake emails impersonating Google’s support team. These emails will contain malicious links that when clicked will download a malicious attachment. MAZE has been seen using a Microsoft Word document with a macro, an automates scrip, attached to the fake emails. Once someone opens the document, they will become infected. The second method used by MAZE threat actors is using publicly accessible RDP servers. FireEye has not been able to identify how they are able to obtain the passwords for the accounts, but some of the RDP servers are not even password protected. Once they are inside the sever they will deploy the MAZE ransomware.

Two other methods the threat actors use involve taking advantage of misconfigurations and weak passwords. The servers being affected are the publicly available ones, sometimes the actors will find Citrix servers with weak passwords. These servers are then used as footholds for the MAZE deployment. Meterpreter shells and web shells are used to create the connections between the actors and the servers. There are also instances in which the actors will create domain accounts and add themselves to the administration group once they are in the servers.

# The Exploit

Once the threat actors had a foothold on the systems they would use programs such as Mimikatz and Bloodhound to find more credentials accessible from their newly created accounts. Mimikatz is known for dumping the SAM and SYSTEM file on Windows systems, these files contain hashes for account credentials. These hashes can then be cracked with tools like John and Hashcat. Bloodhound was used to analyze the active directory environments. Once the threat actors had a good foothold on the servers, they were seen (after three days of being in the systems) scanning the network for other hosts and servers through a series of nslookup commands. They would also use Bloodhound and smbtools.exe to look for other accounts that could be logged into in the environment.

The threat actors would use a 7zip utility to archive as much information they could before deploying the ransomware. The data would be zipped up and since the program being used was 7zip, the extensions to these archives was .7z. Not only were the threat actors deploying the malware, but they were also exfiltrating the information they had gathered. This information was then used to blackmail the organizations affected. I will talk about this more in the next section. The exfiltration was done through the file transfer protocol (FTP port 20-21) and it was done with a Base-64 encoded PowerShell script that looked for .7z files. The script would then reach out to an FTP server where the information was fed to and stored. There were also some instances in which the threat actors would use a cloning utility instead of 7zip, then the cloned files would be sent to a cloud-based file hosting service.

After five days of the all the files found being extracted, the threat actors would start to drop the MAZE ransomware onto machines. The attack would start with 15 infected hosts, then it would spread to tens of other hosts in the environment. The process started with batch scripts encrypting all the data then some other scripts copying itself onto other hosts. The replication was done through shared folders. A batch script led to more batch scripts being executed, some of them where for replication, some of them where kill scripts. MAZE uses RSA and ChaCha20 for its encryption.

# The Fallout

Some of the threat actors behind MAZE ransomware have been using the exfiltrated data as blackmail. Not only will they ask for more money, to make sure the documents don’t get exposed, they will also contact news organizations about the breach to expose security flaws. There was an interesting case with a company called Chubb, a cybersecurity insurance company, that was exposed publicly by the threat actor. The actor went to Bleeping Computer to expose the company before Chubb could respond publicly. The actor also exposed the company on twitter, showing the open RDP server they used to gain access on the environment. This has become a common technique used by ransomware groups. They will exfiltrate the data before they encrypt it, then they will use any juicy documents found as blackmail. I think this has happened because companies were not paying for the decryption costs. Most ransomware will demand a ransom for decrypting the information, whether the threat actor will actually decrypt the information once payed is still something to consider. Now companies will have backups of their information and they can re-install operating systems on mass with network-based installations. Ransomware groups needed a new way of getting money off their victims. What’s the next best option? Blackmailing the victims using any of the information exfiltrated. They will even expose the vulnerabilities used to compromise the victim. What a time to be a part of the industry!

References

References

Abrams, L. (2020, March 26). Chubb cyber insurer allegedly hit by maze ransomware attack. Retrieved from https://www.bleepingcomputer.com/news/security/chubb-cyber-insurer-allegedly-hit-by-maze-ransomware-attack/

Kennelly, J., Goody, K., & Shilko, J. (2020, May 7). Navigating the MAZE: Tactics, techniques and procedures associated With MAZE ransomware incidents. Retrieved from https://www.fireeye.com/blog/threat-research/2020/05/tactics-techniques-procedures-associated-with-maze-ransomware-incidents.html