Maze Ransomware Campaign Spoofs Italian Revenue Agency Correspondence

Author: Christopher Kim

Overview

On 29 October, we detected a campaign distributing Maze ransomware (a variant of ChaCha ransomware) to Italian-speaking users. The emails impersonated the Agenzia della Entrate, or Italian Revenue Agency, and instructed users to open an attached Microsoft Word document, claiming that it contained new usage guidelines for financial services.

Maze ransomware is often delivered via emails or exploit kits such as Fallout[1] and Spelevo.[2] The malware was first discovered in May 2019,[3] but the security community has recently seen an uptick in Maze ransomware activity.[4]

Customer Impact

Maze ransomware uses 2048 bit Rivest-Shamir-Adleman (RSA) and the ChaCha20 stream cipher to encrypt individual files. It appends different extensions to the files during the encryption process. It then changes the user's desktop wallpaper to a message about the encrypted files and the file name of the dropped ransom note.

A notable feature of Maze ransomware is that it sets the ransomware amount based on the type of device it detects. This is uncommon among other types of ransomware. Maze operators have used the following labels to indicate the user's computer type in the wallpaper message:

- standalone server
- server in corporate network
- workstation in corporate network
- home computer
- primary domain controller
- backup server
- very valuable for you

Campaign Analysis

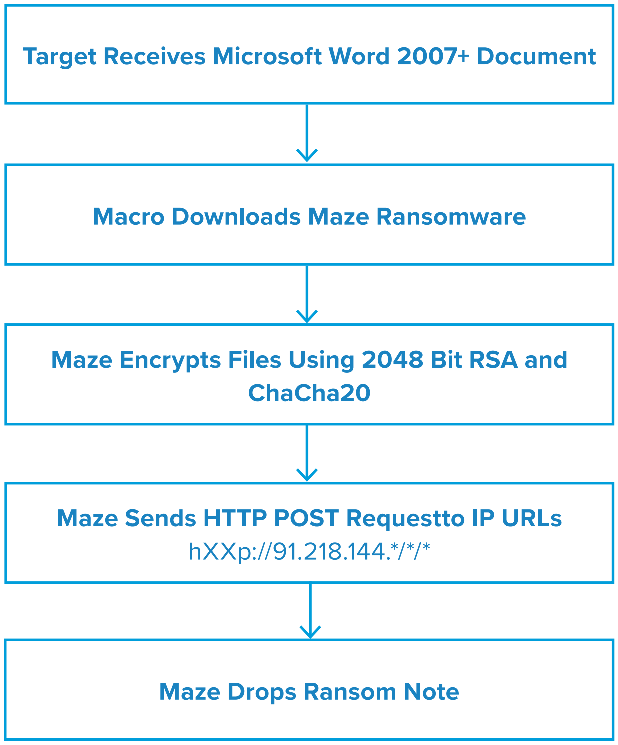
The emails we saw were sent by one of two email accounts designed to appear to be from an official Italian government organization. Both email domains were actor controlled and registered with PublicDomainRegistry on 25 October. The domains resolved to IP addresses that hosted the Maze ransomware samples for this campaign.[5] At the time of this writing, the registrar had suspended both domains.

We found two unique Word documents across the 28 emails. All of the emails imitated the Agenzia della Entrate and used the subject "AGGIORNAMENTO: Attivita di contrasto all'evasione. Aggiornamento," which translates to "UPDATE: Activities to combat evasion. Update." The body of the email directed users to open the attachment and comply with its guidelines relating to online financial services.

Attack Chain

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.


Target Receives Microsoft Word 2007+ Document
Macro Downloads Maze Ransomware
Maze Encrypts Files Using 2048 Bit RSA and ChaCha20
Maze Sends HTTP POST Requestto IP URLs
hXXp://91.218.144.*/*/*
Maze Drops Ransom Note

Vulnerabilities & Mitigation

At this time, there is no publicly available decryption tool for Maze ransomware. Therefore, organizations should implement strong cyber security practices to prevent infection. We recommend the following:

- Security researchers have seen the Spelevo exploit kit delivering Maze ransomware.[2] 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.

Endnotes

1. https://labs.bitdefender.com/2019/10/a-close-look-at-fallout-exploit-kit-and-raccoon-stealer/
2. https://securityintelligence.com/news/spelevo-ek-exploits-flash-player-vulnerability-to-deliver-maze-ransomware/
3. https://twitter.com/jeromesegura/status/1133767240686288896
4. https://www.bleepingcomputer.com/news/security/maze-ransomware-says-computer-type-determines-ransom-amount/
5. https://www.virustotal.com/gui/ip-address/104.168.198.208/relations

Infoblox enables next level network experiences with its Secure Cloud-Managed Network Services. As the pioneer in providing the world's most reliable, secure and automated networks, we are relentless in our pursuit of network simplicity. A recognized industry leader, Infoblox has 50 percent market share comprised of 8,000 customers, including 350 of the Fortune 500.

Corporate Headquarters | 3111 Coronado Dr. | Santa Clara, CA | 95054
+1.408.986.4000 | 1.866.463.6256 (toll-free, U.S. and Canada) | info@infoblox.com | www.infoblox.com