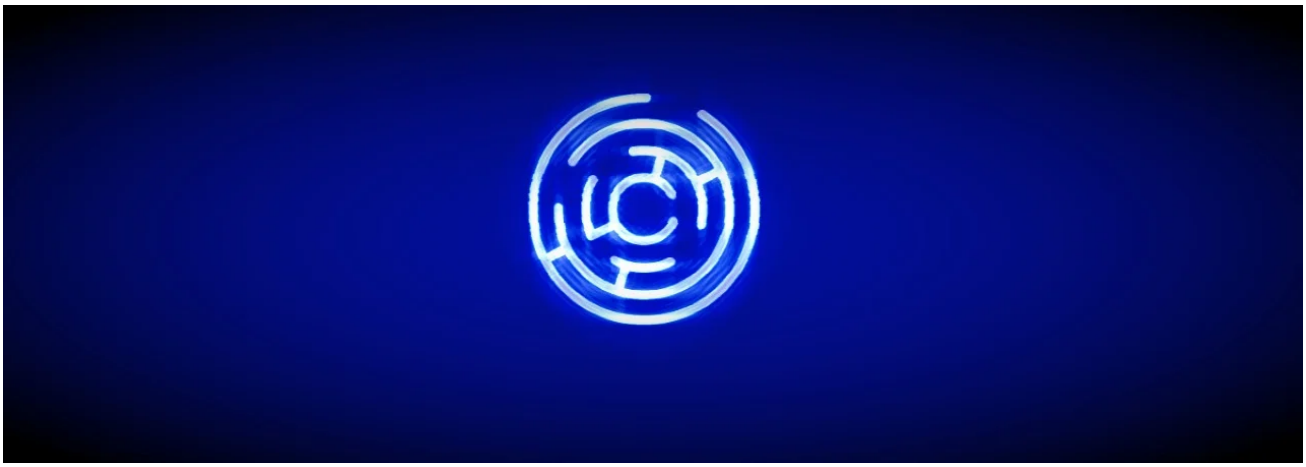
Maze Ransomware Now Delivered by Spelevo Exploit Kit

bleepingcomputer.com/news/security/maze-ransomware-now-delivered-by-spelevo-exploit-kit/

Sergiu Gatlan

By
Sergiu Gatlan

- October 18, 2019
- 02:02 PM
- 0



The Spelevo exploit kit has been spotted by security researchers while infecting victims with Maze Ransomware payloads via a new malicious campaign that exploits a Flash Player use after free vulnerability.

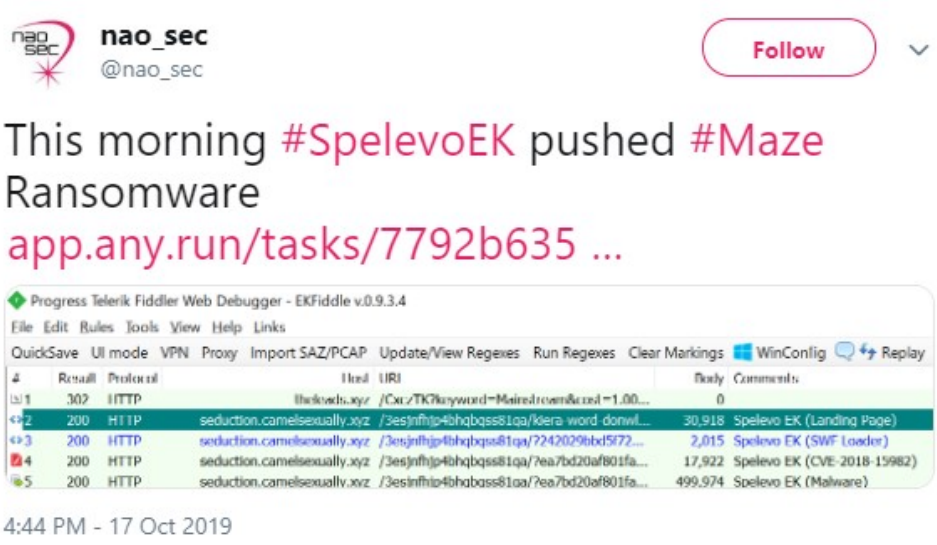
Maze Ransomware, a variant of Chacha Ransomware, was initially found by Malwarebytes security researcher Jérôme Segura in May.

The researcher found that the ransomware was being distributed using the Fallout exploit kit via a fake site camouflaged as a legitimate cryptocurrency exchange app.

Segura told BleepingComputer that the attackers created a fake Abra cryptocurrency site to buy ad network traffic which was later used to redirect visitors to the exploit kit landing page under certain conditions.

New Maze Ransomware campaign

Exploit kit expert nao_sec was the first to spot the new Maze Ransomware campaign yesterday, with GrujaRS also taking a closer look at it one hour later.

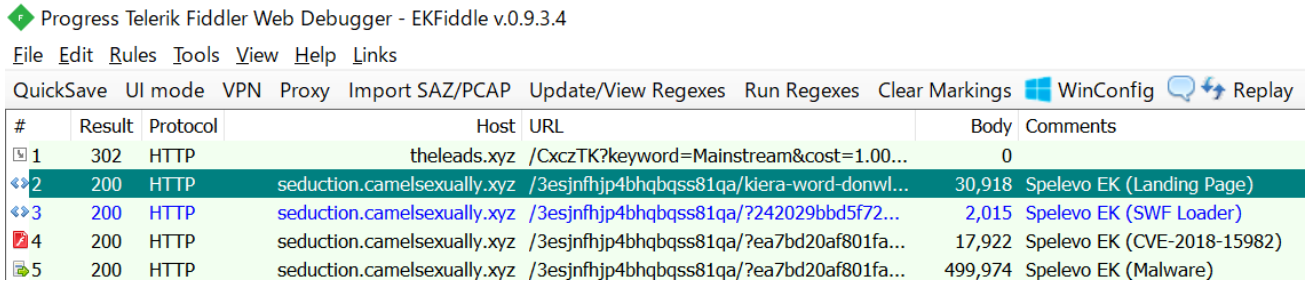


This campaign is redirecting users to the Spelevo exploit kit, as shown in the web requests captured by nao_sec and as shown in the screenshot below.

When redirected to the exploit, Spelevo will attempt to exploit the critical CVE-2018-15982 use after free vulnerability in the browser, with users of Flash Player versions 31.0.0.153 / 31.0.0.108 and earlier being the ones exposed.

Upon successful exploitation, the exploit kit will automatically download and install the Maze Ransomware payload via arbitrary code execution.

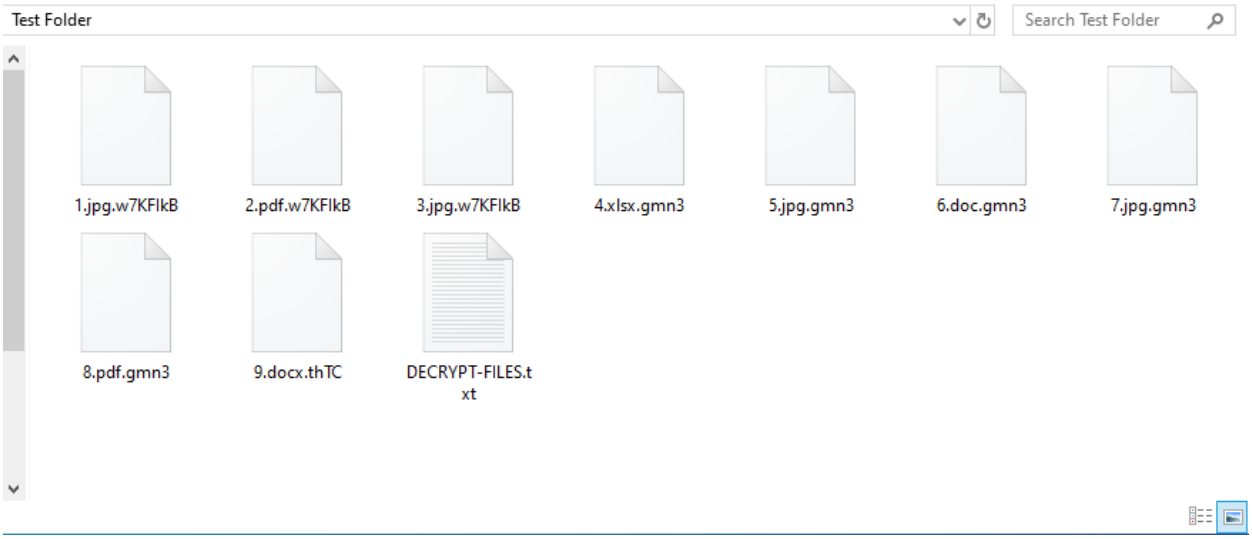
Spelevo was previously seen by Cisco Talos while dropping the infamous IceD and Dridex banking trojans via a compromised business-to-business (B2B) website.



Spelevo exploit kit in action

The Maze Ransomware

When the Maze Ransomware payload is installed and executed, it will start scanning for interesting files (e.g., documents, photos, databases, and more) to encrypt them using RSA encryption and the ChaCha20 stream cipher, and append several extensions as shown below.



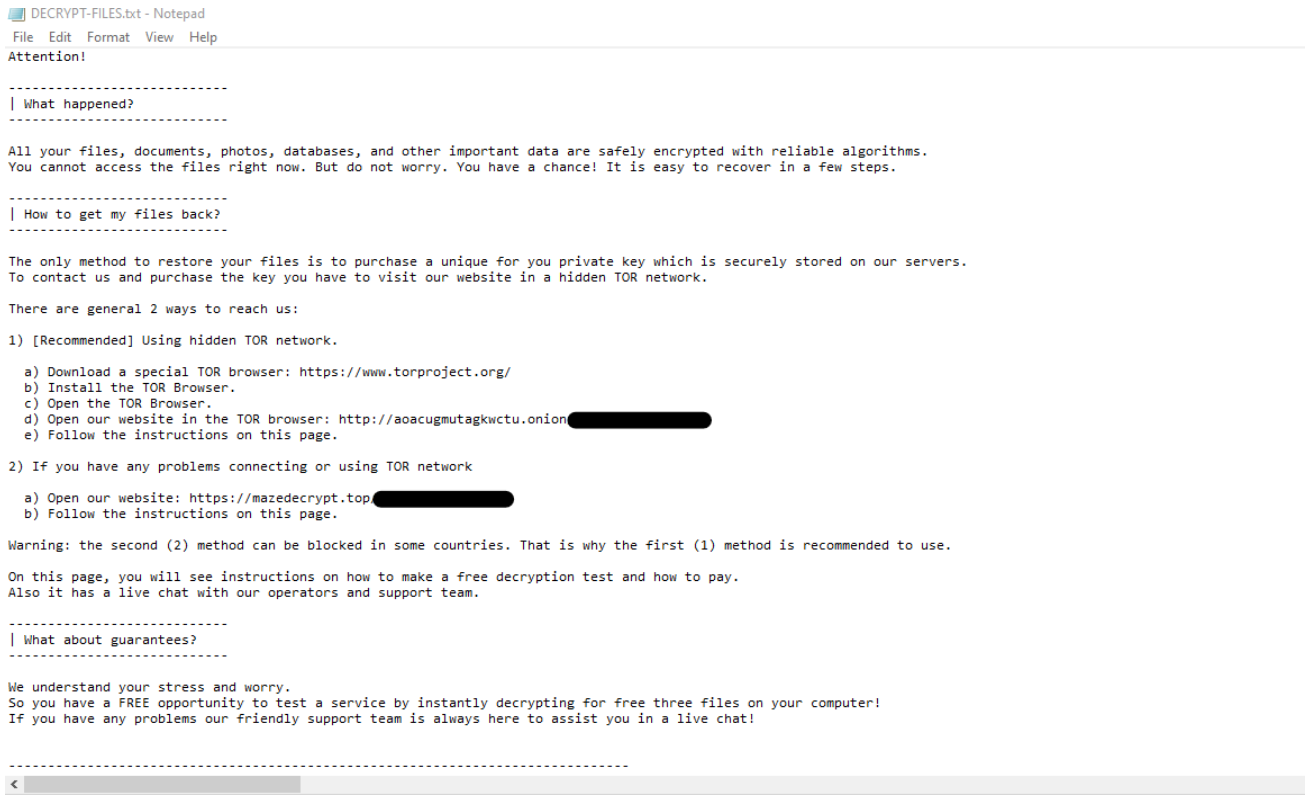
Encrypted files *(Image: GrujaRS)*

The ransomware will also create a ransom note named DECRYPT-FILES.txt in each of the scanned folders, instructing the victims to open a website hosted on the TOR network for payment instructions to purchase a private key to decrypt the files.

Victims are also provided with an online decryption interface which allows them to decrypt three of their now locked files as proof that decryption is indeed possible.

According to the ransomware's support site, the ransom value automatically doubles if the victim does not pay within approximately a week after the ransom note was uploaded.

A second website available over the clear web is also provided, with the mention that it might be blocked in some countries and thus leaving the TOR site as the only option.



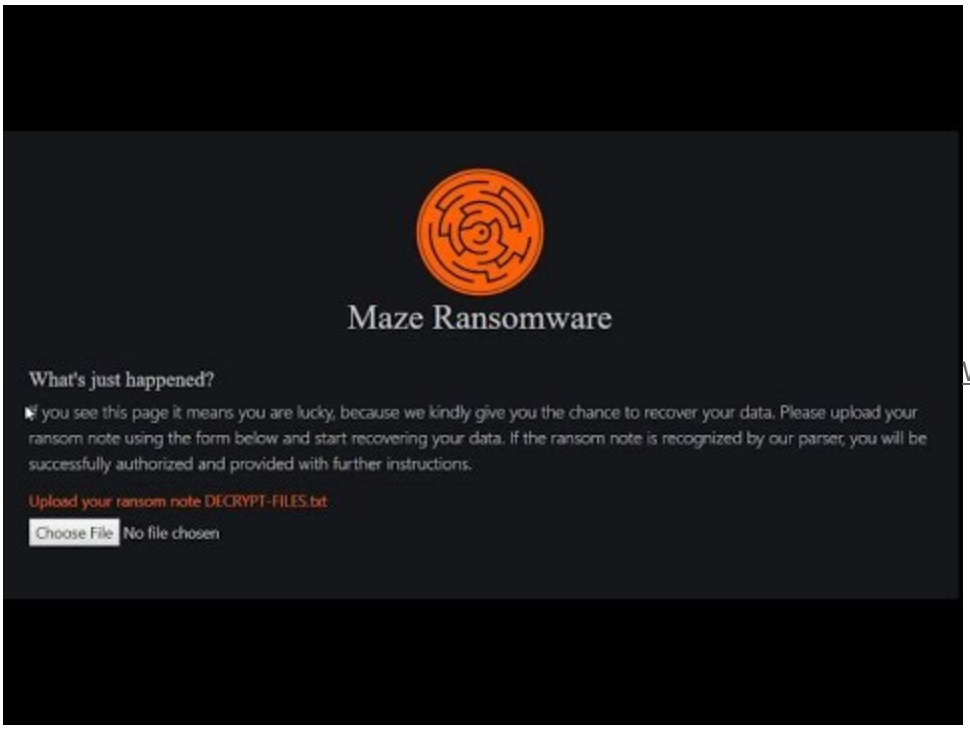
Ransom note*(Image: GrujaRS)*

On this support website, the victims will be asked to upload their ransom note to get further instructions on how to recover their data.

Once the attackers' parser recognizes the ransom note, the victims will be redirected to a page where they can test the attackers' decryption tool (supports only BMP, JPG, GIF, and PNG image files) and get info on how to buy Bitcoins to pay the ransom.

The Maze Ransomware 'support' site also comes with a live support chat as detailed in the ransom note and as GrujaRS also found.

He created a video to demo the attack, to show how Maze Ransomware encrypts its victims' files, how the live chat works, and to take a look at the Maze Ransomware test decrypt tool.



Watch Video At:

https://youtu.be/MTed3ffpmNY

At this time, there is no way to decrypt for free the files that Maze Ransomware encrypts.If anything changes, we will publish a new article with additional findings.

How to protect yourself from Maze Ransomware

To protect yourself from Maze Ransomware, or from any other ransomware family, it is important to use good computing habits and security software. The most important thing is to always have a reliable and tested backup of your data that you can quickly restore in case of an emergency, like a ransomware attack.

Since Maze is being dropped via exploit kits, you need to make sure that all the latest Windows security updates are installed and that all your software is up to date. By doing this you will prevent exploit kits from abusing previously patched vulnerabilities to infect your computer.

Given that ransomware is also known to be delivered via hacked Remote Desktop services, you should make sure that computers running remote desktop services in your network are not directly connected to the Internet by placing them behind VPNs to only allow access to trusted users.

Running security software with a built-in behavioral detection engine like Emsisoft Anti-Malware and Malwarebytes Anti-Malware is also important when defending your data against ransomware infections.

Last, but not least, you also need to follow good online security habits, since, in many cases, are the most important measures of all:

- Backup, Backup, Backup!
- Do not open attachments if you do not know who sent them.
- Do not open attachments until you confirm that the person actually sent you them,
- Scan attachments with tools like VirusTotal.
- Make sure all Windows updates are installed as soon as they come out! Also make sure you update all programs, especially Java, Flash, and Adobe Reader. Older programs contain security vulnerabilities that are commonly exploited by malware distributors. Therefore it is important to keep them updated.
- Make sure you use have some sort of security software installed.
- Use hard passwords and never reuse the same password at multiple sites.
- If you are using Remote Desktop Services, do not connect it directly to the Internet. Instead make it accessibly only via a VPN.

For a complete guide on how to protect your computer against ransomware infections, you can read our How to Protect and Harden a Computer against Ransomware article.

Related Articles:

BlackCat/ALPHV ransomware asks $5 million to unlock Austrian state

Windows 11 KB5014019 breaks Trend Micro ransomware protection

Industrial Spy data extortion market gets into the ransomware game

New ‘Cheers’ Linux ransomware targets VMware ESXi servers

SpiceJet airline passengers stranded after ransomware attack

IOCs

Hashes:

```
91514e6be3f581a77daa79e2a4905dcbdf6bdcc32ee0f713599a94d453a26fc1
```

File Names:

```
DECRYPT-FILES.txt
```

Network Communication:

```
91.218.114.4
91.218.114.11
91.218.114.25
91.218.114.26
91.218.114.31
91.218.114.32
91.218.114.37
91.218.114.38
91.218.114.77
91.218.114.79
```

- Exploit Kit
- Maze
- Ransomware
- Spelevo Exploit Kit

Sergiu Gatlan

Sergiu Gatlan is a reporter who covered cybersecurity, technology, Apple, Google, and a few other topics at Softpedia for more than a decade. Email or Twitter DMs for tips.

- Previous Article
- Next Article

Post a Comment Community Rules

You need to login in order to post a comment

Not a member yet? Register Now

You may also like: