Zeppelin

Threat: **Ransomware-As-A-Service**

Author: **Jeffrey Farnan** Date Originally Published: **August 31st, 2022**

1. SUMMARY

- A new strain of ransomware called Zeppelin has been detected recently by the FBI which uses multiple attack vectors to gain access to victim's networks. The latest campaigns also show threat actors using a new tactic associated with Zeppelin to execute the malware multiple times within a victim's network, which means a victim would need not one but multiple decryption keys to unlock files. The threat actors also implement a double extortion model, threatening to leak stolen files in case the victims refuse to pay the ransom.

2. MALWARE FAMILY

- **Type** = Ransomware-as-a-service (RasS).
- **Sub-type** = Data Theft.

- **Ransomware-as-a-service (RasS**) – Malicious software designed to encrypt all files on a device until a sum of money has been paid. The cybercriminals create this software to sell or rent it to other cybercriminals and take a portion of any bounty collected after a successful attack.
- **Data Theft:** Some ransomware variants include a data theft component, used to incentivize victims to pay the ransom demand. The ransomware will search for valuable data and send copies to the attacker before encrypting the files on the victim's computer.

3. MALWARE CHARATERISTICS

- **Suspected country of origin** = Russia.
- **First seen date/period** = Zeppelin identified in June 2022.
- **Still active** = Yes.
- **Last submitted sample as of writing this article** = August 20th, 2022.

4. MALWARE HISTORY

- Zeppelin is the latest member of the Delphi-based Ransomware-as-a-Service (RaaS) family initially known as Vega or VegaLocker. VegaLocker began in 2019 but went through many name changes from VegaLocker, Buran, Jamer to eventually Zeppelin. These are different strains of the ransomware, which may have different capabilities and target different countries.
- The actors behind Zeppelin are well organized and have been incredibly strategic in carefully targeting their ransomware attacks which began first taking aim at tech and healthcare companies in Europe and the United States. Recent attacks indicate that real estate firms are their latest targets.

5. MALWARE DESCRIPTION

- The actors behind Zeppelin are well organized and have been incredibly strategic in carefully targeting their ransomware attacks.
- **Entry onto the system:** The Zeppelin ransomware group uses a number of tactics, techniques and procedures to use in their attack framework such as exploit remote desktop protocol to gain entry on their targets network. Exploit vulnerabilities found in SonicWall applications, crafting phishing emails and fake advertisements with malicious links and attachments to trick users into executing malicious payloads and infect target networks. The Cybercriminals can spent one to two weeks mapping the victim's network with the aim of identifying valuable data.
- **Execution:** Zeppelin can be easily configurable and can be deployed as a exe file or a .dll file or wrapped in a PowerShell loader. Once Zeppelin gets installed on a device it places itself in a temporary folder named .zeppelin and spreads throughout infecting the device and encrypting files. The Threat actor can configure what is encrypted but by default it encrypts all Windows operating system directories, web browser applications, system boot files and users files in that order to preserve system functions.
- **Data Theft:** Before encryption the cybercriminals steals any valuable or sensitive company data to sell or publish in at event the ransom is not paid.
- **Encryption**: A randomized nine-digit hexadecimal number is appended to each encrypted file as a file extension. An example, "1.jpg" might appear as something similar to "1.jpg.126-D7C-E67", and so on for all affected files. Additionally, it adds file markers ("ZEPPELIN") to the encrypted files. Zeppelin also appears to have a new multi-encryption tactics, executing the malware more than once within a victim's network and creating different IDs and file extensions for multiple instances attack. A note appears on the victim's desktop in Notepad informing the victims they have been attacked and the ransom must be pain in Bitcoin for the return of their data. Sometimes there is an offer of free decryption of a single file offered as proof that decryption is possible, this is to encourage payment for all the data.
- **Persistence and Privilege Escalation:** Persistence is gained by adding malicious binaries to the registry allowing the ransomware to be executed each time a user logs into the host. The UAC prompt option or the registry key allow it to run with elevated privileges.
- **Defence and Evasion:** Strings in the malware binaries are encrypted with a 32-byte RC4 key. A Delphi packer is used to pack the malicious files making detecting and analysing hard for defenders.

6. POTENTIAL CUSTOMER DEFENSE

- When ransomware attacks an organization there is really only two options to follow: Pay the ransom or rebuild from backups. If you pay the ransom you may not get a decryption key and still end up in the same situation. The only solution is to rebuild from backups, but this can be a very slow and cumbersome method. The best solution is prevention.
- **Prevention:** Ransomware attacks are primary aimed at employees as a way into an organization. Phishing scams are the primary source of most of the attacks while overly permissive access policies and poor password hygiene are other attack vectors. Other measures can be taken to prevent an attack:
    - **System Updates:** A common source of ransomware attacks is out-of-data Software, organizations must apply software patches quickly.
    - **Back Up:** Backups are essential in defending against ransomware, while not preventing attacks can limit the negative impact of a successful attack and minimize the damage.
    - **Security Tools:** Most free tools such as antivirus programs and firewall offer insufficient protection against ransomware attacks. The best and most effective protection come from advanced antivirus programs which use machine learning and artificial intelligence to deep packet inspection tools used to hone in on anomalous activity.
- **Training:** Training employees to be vigilant and look for signs of an attack is now vital for most organizations. Preventing employees from clicking on suspicious looking emails and changing passwords regularly with strong passwords can better improve their security posture.

Research Sources:

- https://www.picussecurity.com/resource/zeppelin-ransomware-analysis-simulation-and-mitigation
- https://www.cisa.gov/uscert/ncas/alerts/aa22-223a
- https://www.bleepingcomputer.com/news/security/fbi-zeppelin-ransomware-may-encrypt-devices-multiple-times-in-attacks/
- https://www.coresecurity.com/core-labs/articles/what-zeppelin-ransomware-steps-prepare-respond-and-prevent-infection