Lojax

Threat: **UEFL Firmware Rootkit**

Author: **Jeffrey Farnan** Date Originally Published: **April 27th, 2021**

1. SUMMARY

- Lojax was first found in the wild by security researchers in 2018. Lojax affects the Unified Extensible Firmware Interface (UEFI), which is the interface for the operating system to connect with the firmware. This attack is designed to exploit vulnerabilities in UEFI implementations allowing Hackers to modify the UEFI in an unauthorized manner. UEFI rootkits are extremely difficult to detect, and costly to remove. These attacks can grant Hackers near control of the infected PC, including access to corporate networks. Reinstalling operating systems or replacing drives will not remove this infection. Lojax is a new and growing trend of attack and many layers of security is needed to defend against this type of attack.

2. MALWARE FAMILY

Type = UEFL Firmware Rootkit.

- Lojax comes from the UEFL firmware rootkit family, it is technical advanced and is used in cyber espionage attacks.
- Security researchers believe this new type of rootkit came from the Russian group calling themselves Fancy Bear. Lojax uses several capabilities found it other malware coming from this group. Fancy Bear allegedly utilized Lojax against several high-profile targets in Central and Eastern Europe. Fancy Bear hackers target high profile elections, aerospace, defence, energy, government and media organizations. Fancy Bear typically employ both phishing messages and credential harvesting using spoofed websites.

3. MALWARE CHARATERISTICS

- **Suspected country of origin** = Russia.
- **First seen date/period** = 2018.
- **Still active** = Yes.
- **Last submitted sample as of writing this article** = April 24^{h}, 2021.

4. MALWARE HISTORY

- Like most of the first rootkits, the UEFI rootkit started out as a theory based rootkit. Some security professionals presented the UEFI rootkit as a proof-of-concept at security conferences. Up until August in 2018 no UEFI rootkit was ever detected in a real cyberattack.

5. MALWARE DESCRIPTION

Lojax is the first rootkit to be detected that directly attacks the Unified Extensible Firmware Interface (UEFI), it provides the interface for the operating system to connect with the firmware.

The Lojax Rootkit is separated into components (tools) each designed with a specific purpose.

- The payload, a set of binaries to achieve persistence and to compromise the UEFI at a later stage.
- The malware that runs on the system to deliver the payload. This malware consists of tools that read the existing UEFI binary on the system, modify it by adding the malicious payload, and inject the "modified" UEFI back into the system.

There are various ways Lojax can gain access onto the system, such as phishing, malicious documents, removable media, or downloaded binaries.

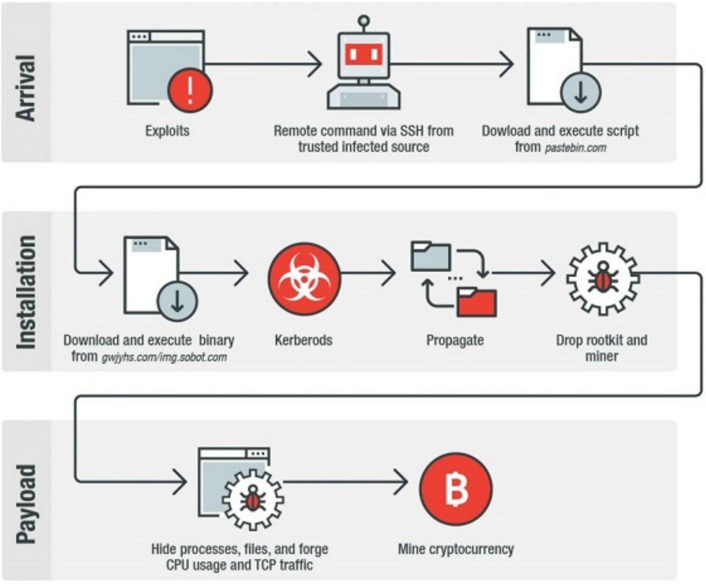
- **Phishing Infection Method:** The infection can be distributed via phishing email message. The phishing email contains a Microsoft Word document, when clicked the user is prompted to engage the built-in macros. Embedded in the word document is a PowerShell dropper, when executed downloads a malicious code which flashes the rootkit to the UEFI firmware.
    - **First-stage of the attack (OS User-Mode) –** The first stage involves bypassing security measures to get the payload to run on system, escalating privileges, such as admin control.
    - **Second-stage attack (OS Kernel-Mode) –** The payload now infects the hardware Abstraction Services
    - **UEFI Infection –** The final stage involves writing the malicious code, to the UEFI firmware which flashes the rootkit to the UEFI firmware.
- **Trojan Infection Method:** Lojax was also found bundled together with a toolset called LoJack, also where Lojax got its name. LoJack is an anti-theft software package, which helped to protect Pc's by working its way deep inside the UEFI. LoJack helps to connect a Pc's operating system to its firmware. Lojax has taken advantage of this technology and modified it so it can remain hidden inside a PC. Lojax uses most of the components from LoJack, but it connect to command-and-control servers are operated by Fancy Bear. The Hackers can use the tool to monitor the computer with little risk of detection.

Once the malware lands on a system, it needs to run with administrative privileges, which will allow the malware to use a particular kernel mode driver for reading and writing the UEFI image.

- The malware checks to see if the UEFI firmware protections are configured or not (old configurations or updated configurations are in place).

- Read the contents of the computer's Serial Peripheral Interface (SPI) memory where the UEFI is, then save it into a file (as a firmware image).

- Install the rootkit by embedding a malicious UEFI module into the saved image, then write the modified firmware back to the SPI flash memory.


Arrival
Exploits
Remote command via SSH from trusted infected source
Dowload and execute script from pastebin.com
Installation
Download and execute binary from gwjyhs.com/img.sobot.com
Kerberods
Propagate
Drop rootkit and miner
Payload
Hide processes, files, and forge CPU usage and TCP traffic
Mine cryptocurrency

Once the malware is embedded in the UEFI firmware, it can be executed the next time the computer is booted up. Once the infection is successful the Hackers can use Lojax to get remote access constantly and install and execute additional malware on it. The domains in the Lojax samples the researchers analyzed were used for command-and-control (C&C) communication for a known Fancy Bear backdoor, which is used for cyberespionage.

6. POTENTIAL CUSTOMER DEFENSE

Lojax is aimed at and a threat to high-value targets, so normal users should not be worried at this time. It's important to note that anti-virus and other third-party solutions are insufficient to protect against this type of infection. Hardware enforced security is needed, to reliably protect against BIOS/UEFI attacks, check the security configurations of the hardware provider. Other steps can be taken:

- Enable "Secure Boot" mechanism which ensures that everything that's loaded in the system firmware comes up with a valid certificate. Since Lojax is not signed it won't load during "Secure Boot".
- Confirm that the latest version of firmware is on your motherboard is genuine. If not it should be updated. It is advisable to get more experienced users to update the firmware as it can be difficult to configure. The current version of Lojax does not resist a firmware update. The current updated version of the firmware is password protected, so any future malicious or unauthorized updates will not be installed.
- Another option is to replace the computers motherboard with a new one, since Lojax only affects older chipsets.

Research Sources:

- https://www.osradar.com/lojax-first-uefi-rootkit-in-the-wild/
- https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/lojax-uefi-rootkit-used-in-cyberespionage
- https://press.hp.com/us/en/blogs/2018/the-lojax-attack--what-you-need-to-know.html?jumpid=in_r12129_us/en/psg/computer_security/sure-start/blog
- https://www.bleepingcomputer.com/news/security/apt28-uses-lojax-first-uefi-rootkit-seen-in-the-wild/

Disclaimer: All opinions expressed in this article are the opinions solely of the author.