The malware detection is extremely dangerous, unable to destroy even if the operating system is reinstalled and the hard drive is replaced

An extremely dangerous malware called Lojax has just been discovered by ESET security firm. This malware is infecting a victim computer with malicious code.

An extremely dangerous malware called Lojax has just been discovered by ESET security firm. This malware is infecting a victim computer with malicious code. According to security experts at ESET, it is likely that Lojax was created by a famous hacker group from Russia called Fancy Bea.

These dangerous malware target UEFI software - the Unified Extensible Firmware Interface, which is used to boot the computer's system. Lojax rewrites UEFI so they can survive long in the flash memory of the computer, even when reinstalling the operating system and replacing the hard drive can not be destroyed.

ESET said, if you want to remove this malware, users will have to overwrite the memory of the flash storage drive, and this is definitely not for general users.

Security researchers have discovered the various components of the Lojax malware on computers belonging to government organizations in countries in Central and Eastern Europe and the Balkan region.

According to ESET, previously the type of rootkit attack targeting UEFI is only considered a form of attack in theory. And this is the first time this UEFI rootkit has appeared in the real world.

Fancy Bea hacker group is also known as Sednit because it has carried out a series of attacks on government groups. Including the leak of information in the National Democratic Committee's computer network in the 2016 US presidential campaign.

ESET said that Lojax's method of mimicking an anti-theft system protection product is also difficult to remove from a PC called Lojack. The hacker group has weaponized Lojack to help them attack computers and overcome security software.

Now, security experts still do not know how Fancy Bear put the malware on a victim's computer. But maybe Lojax is used to download other malware modules into infected computers.

Maybe Fancy Bear has developed parts of Lojax based on commands and control servers communicating with malware. Previously, domain names for these servers were also used to store other hacking tools developed by Fancy Bear.

Fortunately, this Lojax attack can be completely blocked through a standard feature that is usually enabled by the PC, called Secure Boot. All parts in the PC, including the firmware, will be Secure Boot checked to see if they are validated with a valid code signed by the manufacturer. This test can block Lojax Malware.

To enable or disable this feature, you can restart the computer and access the BIOS section.

In addition, security experts at ESET also advise PC users to constantly update the firmware for the motherboard of the device to prevent hackers from exploiting the vulnerabilities.

See more:

1. 5 things to do to avoid malware
2. Researchers create malware based on artificial intelligence
3. Warning, the botnet campaign called GhostDNS is taking over more than 100000 routers