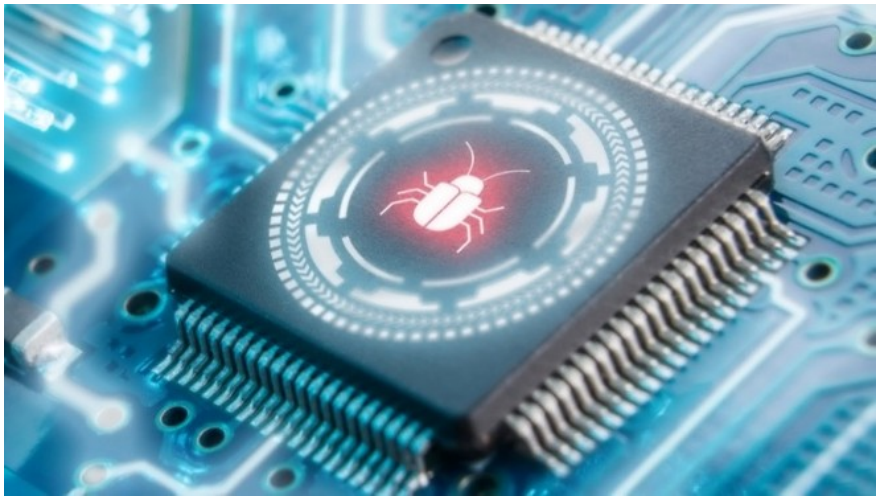
UEFI CosmicStrand Malware Found in ASUS and Gigabyte Firmware

The security threat research team at antivirus software maker Kaspersky has discovered a rootkit malware called CosmicStrand.

The security threat research team at antivirus software maker Kaspersky has discovered a rootkit malware called CosmicStrand. In fact, this is not a new malware but a variant of the Spy Shadow trojan that appeared in 2016 - 2017.

CosmicStrand is a UEFI rootkit malware and it was found in ASUS and Gigabyte firmware. That's why it's called an Advanced Persistent Threat (APT) because it's so hard to remove. No matter how many times you reinstall Windows, you can't remove this type of UEFI rootkit.



Regarding operating systems, Kaspersky found that so far only Windows operating systems have been attacked and penetrated.

"All the attacked computers were running Windows. Every time the computer rebooted, the malicious code would be executed after Windows finished booting. Its purpose was to connect to the C2 server and download additional malicious files ," Kaspersky shared.

While Kaspersky has identified the malware, it does not know how it was initially transmitted. Some users have reported that second-hand motherboards they ordered online were infected when they received them.

For those using Gigabyte and ASUS motherboards running Windows, enabling Secure Boot is a viable option to protect against any malicious effects. Of course, if you have some computer knowledge, you can reset your

BIOS. However, remember to download the official firmware from the manufacturer's website.

So far, CosmicStrand's victims have been primarily consumers in China, Vietnam, Iran and Russia.