MOONBOUNCE UEFI MALWARE UNCOVERED IN TARGETED ATTACK

By Lindsey O'Donnell-Welch

Share

The China-linked APT41 threat actor has launched a targeted attack using UEFI malware that researchers call MoonBounce.

Researchers with Kaspersky discovered the firmware bootkit being leveraged last year in a single incident. Mark Lechtik, senior security researcher with the Global Research and Analysis Team (GReAT) at Kaspersky, said that while researchers cannot disclose any details on the victim itself, they can reveal that "given its nature and the overall details of the campaign, the attackers were likely seeking to conduct long standing espionage activity against it."

As part of the attack, threat actors tampered with the Unified Extensible Firmware Interface (UEFI) - a leading technology that's embedded in chips of modern devices and links the firmware to the operating system - in order to embed the malicious MoonBounce implant. UEFI level implants give sophisticated attackers a full range of control over devices, and they are also difficult to detect and remove.

The attackers behind MoonBounce focused on a known attack vector within UEFI: Serial Peripheral Interface (SPI) flash, which is a storage and data transfer component external to the hard drive. Because SPI flash is located on the motherboard instead of the hard disk, attackers can gain persistence even after disk formatting or replacement, said researchers. That sets this type of malware apart from other UEFI implants - such as the UEFI bootkit loading the FinSpy surveillance toolset and the ESPectre bootkit - that instead use the EFI System Partition (ESP), which is storage space designated for some UEFI components that is generally based in the computer's hard drive or SSD.

"Such bootkits are not only stealthier (partially because of limited visibility by security products into this hardware component), but also more difficult to mitigate: flashing a clean firmware image in place of a malicious one can prove to be more difficult than formatting a hard drive and reinstalling an OS, which would typically eliminate ESP level threats," Kaspersky researchers said.