Security Newsletter

October 2018

Security Vulnerabilities – LoJax Rootkit

Phoenix is an industry leading provider of secure UEFI firmware solutions to computing device manufacturers. Phoenix works closely with semiconductor chip manufacturers and operating system vendors, including Intel, AMD, and Microsoft, to help provide the most secure firmware available for computing devices.

On September 27, 2018, security researchers from ESET publicly disclosed the discovery of a UEFI rootkit named "LoJax" that was "found in the wild". LoJax is installed by using OS-level tools to modify the UEFI platform firmware in the system's SPI flash memory. The LoJax rootkit installs malicious code into the operating system that allows a remote attacker to gain access to the system without the user's knowledge.

Phoenix UEFI firmware provides protection against the LoJax attack by locking the SPI flash memory and implementing additional protections against the bypass mechanism described in the ESET public disclosure. We work closely with our valued customers and authorized distributors to help ensure their computing devices that include Phoenix UEFI firmware are safeguarded.

You may notice that the ESET whitepaper references an early version of Absolute Software Corporation's anti-theft solution, Computrace (or LoJack small agent), and includes an image from a Lenovo ThinkPad laptop. Please note that LoJax is not an attack against Computrace, and the ThinkPad image was used to provide context for describing the legitimate Computrace component. Indeed, the researchers have named the rootkit "LoJax" because it uses a maliciously modified version of the Computrace OS agent software (also called LoJack small agent) to bypass OS-level anti-malware detection.

End users should also note that Secure Boot does not protect against LoJax, as previously stated in the first iteration of the ESET public disclosure. Phoenix recommends applying all firmware updates provided by your computing device manufacturer.

While no software can be guaranteed to be bug free, Phoenix makes every effort to monitor and discover emerging computing device security vulnerabilities and work with industry partners to quickly deliver solutions to help keep computing devices secure.

If you have any questions, please contact Phoenix using our secure reporting webpage located at https://www.phoenix.com/security/index.html.