APT28 Uses LoJax, First UEFI Rootkit Seen in the Wild

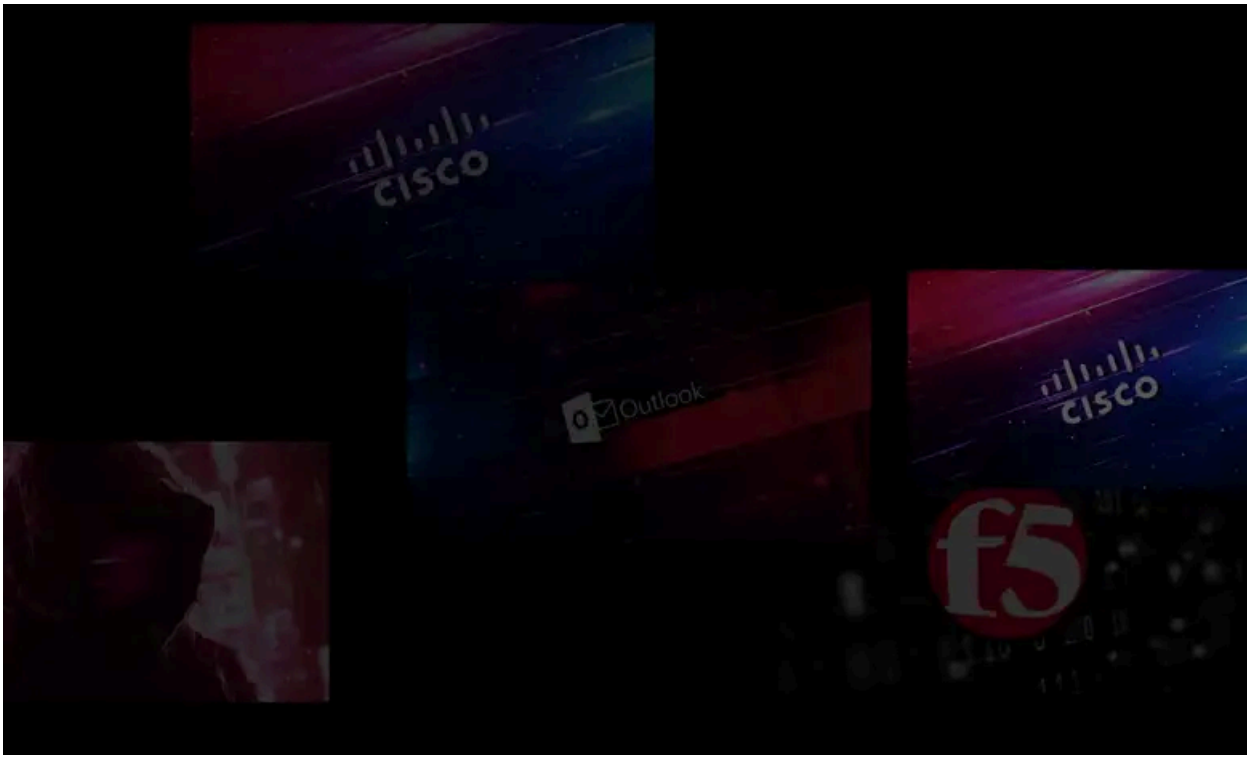
By Ionut Ilascu

Published: 2018-09-27 · Archived: 2026-04-02 12:42:06 UTC

Security researchers tracking the operations of a cyber-espionage group found the first evidence of a rootkit for the Unified Extensible Firmware Interface (UEFI) being used in the wild.

The threat actor, known in the infosec community by the names Sednit, Fancy Bear, APT28, Strontium, and Sofacy, was able to write a malicious component into a machine's UEFI firmware.

According to ESET, the threat actor embedded the rootkit in the SPI flash module of a target computer, which gives persistence not only against reinstallation of the operating system but also when the hard drive is replaced.


cisco
Outlook
cisco
f5

Visit Advertiser websiteGO TO PAGE

The researchers named the rootkit LoJax, after the malicious samples of the LoJack anti-theft software that were discovered earlier this year. That hijacking operation of the legitimate software was also the work of ATP28.

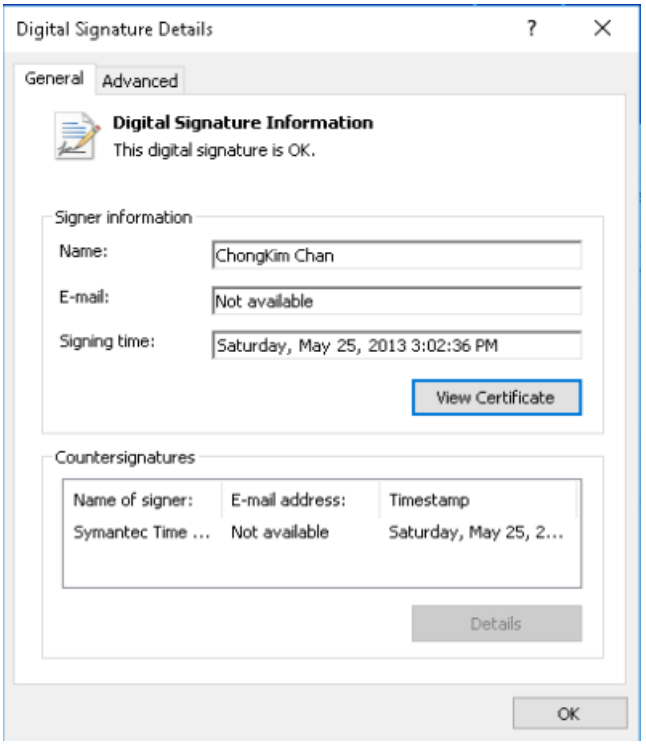
"On systems that were targeted by the LoJax campaign, we found various tools that are able to access and patch UEFI/BIOS settings," ESET says in a report shared with BleepingComputer.

Signed driver opens access to firmware

Security researchers explain that they found three different types of tools on a victim's computer. Two of them are responsible for gathering details about the system firmware and for creating a copy of the system firmware by reading the SPI flash memory module, where the UEFI firmware is located.

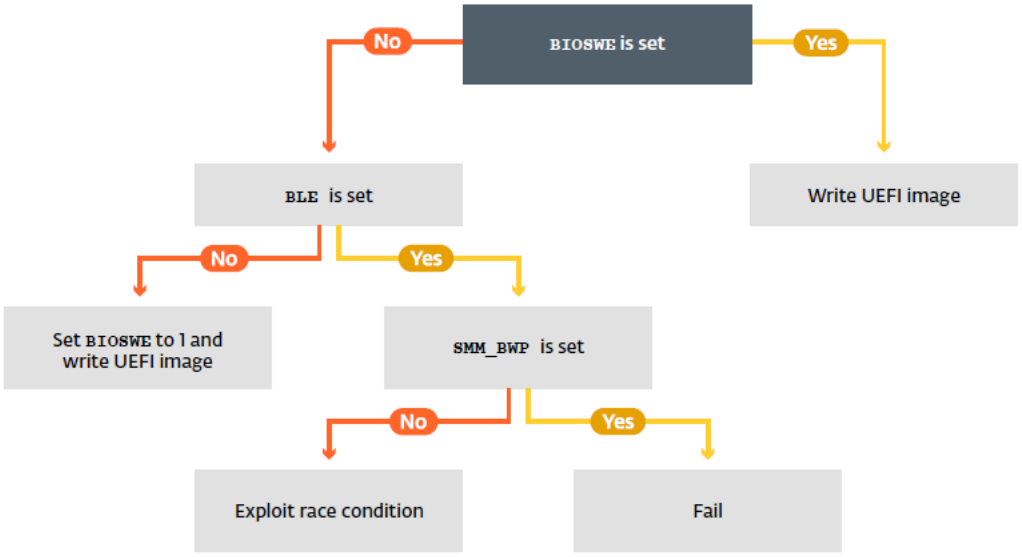
The third one injects the malicious module and writes the compromised firmware back to the SPI flash memory, creating persistence for the malware.

To reach the UEFI/BIOS settings, all tools use the kernel driver of the RWEverything tool that allows modification of the settings in the firmware of almost any hardware. The driver is signed with a valid certificate.



"This patching tool uses different techniques either to abuse misconfigured platforms or to bypass platform SPI flash memory write protections," ESET says.

If write operations are denied, the malicious tool exploits a four-year-old race condition vulnerability in UEFI (CVE-2014-8273) to bypass the defenses.



The purpose of the rootkit is just to drop malware into the Windows operating system and make sure that it executes at startup.

Defending against LoJax UEFI rootkit

Protecting against LoJax infection is possible by enabling the Secure Boot mechanism, which checks that every component loaded by the system firmware is signed with a valid certificate.

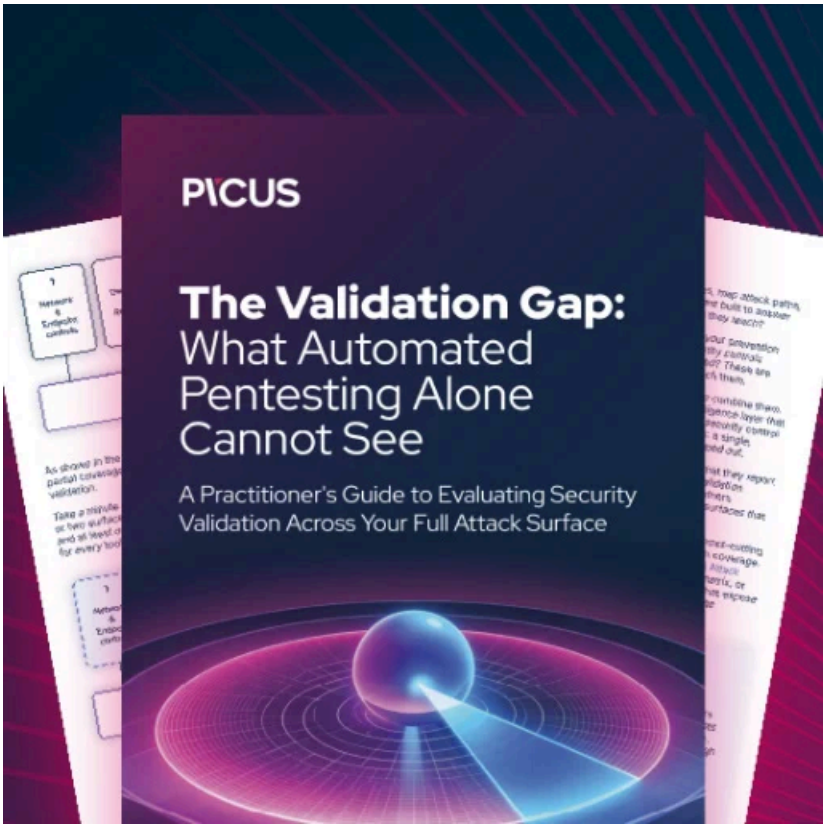
Since LoJax rootkit is not signed, Secure Boot can prevent it from dropping the malware in the first place.

Another way to protect against Sednit's rootkit is to make sure the motherboard has the latest firmware version from the manufacturer. The patching tool can do its job only if the protections for the SPI flash module are vulnerable or misconfigured. An updated firmware should render fruitless the malicious update operation.

Reflashing the firmware, however, is a task most users are unfamiliar with. It is a manual operation that typically involves downloading the latest firmware version from the motherboard manufacturer, saving it on an external storage device, booting into the UEFI menu and installing it.

An alternative is to replace the motherboard with a newer generation since LoJax affects older chipsets. This requires some technical knowledge, to ensure hardware compatibility, and most users find it easier to replace the entire station.

LoJax is a rare threat, designed for high-value targets. ESET presented their discovery today at the Microsoft BlueHat security conference. A detailed analysis of LoJax UEFI rootkit is available here.



Automated Pentesting Covers Only 1 of 6 Surfaces.

Automated pentesting proves the path exists. BAS proves whether your controls stop it. Most teams run one without the other.

This whitepaper maps six validation surfaces, shows where coverage ends, and provides practitioners with three diagnostic questions for any tool evaluation.

Source: https://www.bleepingcomputer.com/news/security/apt28-uses-lojax-first-uefi-rootkit-seen-in-the-wild/