Firmware Attacks: An Endpoint Timeline

2011
Mebromi

One of the first observed malware to attack the BIOS directly.

2015-2017
Equation Group & Vault 7 Leaks

Two separate instances led to tools and techniques for firmware attacks being leaked to the public. In 2015 we learned of EquationDrug and Grayfish. Later in 2017, we learned of Dark Matter and Sonic Screwdriver.

October 2020
MosaicRegressor

Researchers at Kaspersky disclosed a new UEFI implant being used in the wild dubbed MosaicRegressor. This implant has been used in targeted attacks as a way to maintain a persistent foothold in target organizations and evade most detection controls while delivering malicious payloads to compromised systems. You can find more information about MosaicRegressor and other UEFI implants here.

September 2021
FinSpy

A UEFI component belonging to the FinFisher surveillance toolset. Although researchers have tracked the spy tool since at least 2011, the bootkit didn't surface until 2021. You can find our full write-up, including a video breakdown, of FinSpy here.

January 2022
MoonBounce

Discovered in January and attributed to APT41, or an actor closely affiliated to the group, which researchers say is part of the Winnti Umbrella.

July 2022
CosmicStrand

One of the most recent examples of malware that "hooks" UEFI at an early stage to infect all subsequent operations in the boot process. The end result is malware stealthy infecting the Windows kernel, evading most protections. You can find our write-up on CosmicStrand here.

2011 | 2012 | 2013 | 2014 | 2015 | 2016 | 2017 | 2018 | 2019 | 2020 | 2021 | 2022

2015
Hacking Team

Hacking Team had a UEFI rootkit that was used to maintain persistent access to target systems. It is believed that this was installed with physical access, however, it is possible that physical access was not required to implant the malware.

2018
Lojax

Russian hacking group Fancy Bear is found using a UEFI rootkit to install Lojax, independent of the kernel and operating system, even a complete wipe of the hard drive will not remove the malware (patched UEFI modules of the LoJack anti-theft software (also known as Computrace) were used). (You can find our discussion of LoJax here.)

December 2020
Trickboot

Trickbot contains code to read, write, and erase firmware dubbed Trickboot. This was discovered in a collaborative research effort between Advanced Intelligence (AdvIntel) and Eclypsium.

October 2021
ESpecter

A bootkit persisting in the EFI System Partition that can bypass Windows Driver Signature Enforcement to load its own unsigned driver. You can find our article on detecting ESpector (and FinSpy) here.

June 2022
Conti Group Found Actively Looking For Firmware Vulnerabilities

Leaked chat logs show that the Conti ransomware group is actively looking for firmware vulnerabilities, specifically in Intel ME technologies.

October 2022
BlackLotus

Researchers observed a UEFI bootkit sold online called "BlackLotus". Commanding a $5,000 price tag the sellers claim this malware can bypass Secure Boot.