Thunderstrike 2: Proof-of-concept worm could infect Macs

August 4 2015, by Nancy Owano

Two researchers, Xeno Kovah co-founder of LegbaCore and Trammell Hudson, a security engineer with Two Sigma Investments, have created a proof of concept worm capable of attacking Mac computers. The worm which they designed can spread from MacBook to MacBook without them even being networked. If one were to actually be a victim of this kind of attack, a solution would be nothing less than opening up the machine and electrically reprogramming the chip. For many users, that solution would be daunting. They might take the easier way out, which is to slip the machine into a gym bag and put it in the back of the closet, on top of the pile of broken exercise equipment and ironing board.

Kim Zetter, who covers cybercrime, privacy, and security for *Wired*, had a detailed report on Monday about what they found. Namely, they saw

that known vulnerabilities that can smack down firmware from the top PC makers can also hit the firmware of Mac's.

Security scanners would not pick up on the attack; machines, even air-gapped ones, could be targeted. Even through operating system and firmware updates, the attack would keep hold. Zetter said, "any malware in the firmware could block new updates from being installed or simply write itself to a new update as it's installed." The firmware would persist, in short, even if the operating system were wiped and re-installed.

One would need to re-flash the chip that contains the firmware, said *Wired*.

Why a firmware problem is so nasty lies in why a firmware problem is so resilient against detection and removal. Firmware, noted *Wired*, "operates at a level below the level where antivirus and other security products operate and therefore does not generally get scanned by these products, leaving malware that infects the firmware unmolested."

Kovah was already aware that firmware vulnerabilities in PCs could allow attackers to reflash the BIOS to plant malicious code in it. He and Hudson sought to know if such vulnerabilities were applicable to Apple's firmware. They saw that "untrusted code could indeed be written to the MacBook boot flash firmware," *Wired* said.

Readers' comments on the *Wired* site included Darryl, who said "firmware should have a switch that is defaulted to read-only. Only when you need to update it should it be changed to allow writing."

Another reader said, "this is not an 'Apple issue'- this is a hardware design issue much of which is OSmfg agnostic. "

Kovah, in the article, talked about how most of these firmwares are built

—from the same reference implementations. "When someone finds a bug in one that affects Lenovo laptops, there's a really good chance it's going to affect the Dells and HPs," said Kovah. "What we also found is that there is really a high likelihood that the vulnerability will also affect Macbooks. Because Apple is using a similar EFI firmware."

Out of six vulnerabilities examined, five affected Mac firmware, said *Wired*. The researchers notified Apple of the vulnerabilities, and the company has fully patched one and partially patched another. *Wired* said three of the vulnerabilities remained unpatched.

Kovah said they were trying to make it clear "that any time you hear about EFI firmware attacks, it's pretty much all x86 [computers]."

Zetter wrote about some possible safeguards: "Hardware makers could guard against firmware attacks if they cryptographically signed their firmware and firmware updates and added authentication capabilities to hardware devices to verify these signatures. They could also add a write-protect switch to prevent unauthorized parties from flashing the firmware."

The researchers will be discussing their findings at the upcoming Black Hat security conference in Las Vegas.

The Briefings notes from the conference said that the number of vulnerabilities in firmware disclosed as affecting Wintel PC vendors has been rising over the past few years, but this talk "will provide conclusive evidence that Mac's are in fact vulnerable to many of the software only firmware attacks that also affect PC systems." The presentation is by Hudson, Kovah and Corey Kallenberg, and it is titled "Thunderstrike 2: Sith Strike."