Researchers showed remote style hack for new Macs

August 13 2018, by Nancy Owano

Credit: CC0 Public Domain

What could be a happier moment? You starting work with the setup process of a brand new Mac.

What could be an unhappier moment? You starting work with the setup process of a brand new Mac.

Excuse the quiz writers for puzzling over an answer key, as news unfolds that hacking would be possible via Apple's enterprise hardware management setup tools.

The result would be gaining remote access to the Mac.

It appeared that the new Mac could be compromised even before the user were to take it out of the box.

The researchers' findings were discussed at the recent Black Hat USA 2018 in Las Vegas. Jesse Endahl, chief security officer of Apple device management firm Fleetsmith, and Max Bélanger, a staff engineer at Dropbox, were at the show to explain their findings.

"We found a bug that allows us to compromise the device and install malicious software before the user is ever even logged in for the very first time," Endahl said, in *Cult of Mac*.

What's it all about?

Simply put, the mischief maker can construct, as Mikey Campbell in *AppleInsider* wrote, " a man-in-the-middle attack that downloads malware or other malicious software before a client logs in to a new Mac for the first time."

The "enterprise tools" involved and being talked about at length are the Device Enrollment Program and Mobile Device Management platform.

"The attack takes advantage of enterprise Macs using Apple's Device Enrollment Program (.pdf) and its Mobile Device Management platform," said Buster Hein at *Cult of Mac*. "The enterprise tools allow companies to completely customize a Mac shipped to an employee straight from Apple. However, a flaw in the system allows attackers to put malware on the Macs remotely."

These very tools work in tandem so that companies can look forward to easy IT setup regimens in deploying a large number of devices to their workers, said *AppleInsider*.

As *Wired* also said, "The idea is that a company can ship Macs to its workers directly from Apple's warehouses, and the devices will automatically configure to join their corporate ecosystem after booting up for the first time and connecting to Wi-Fi."

And that advantage would make sense for businesses where some of the workforce are in a satellite office or working from their homes.

A Black Hat conference briefing item on the same said, "Our talk walks through the various stages of bootstrapping, showing which binaries are involved, the IPC flows on the device, and evaluates the network (TLS) security of key client/server communications. We will follow with a live demo showing how a nation-state actor could exploit this vulnerability such that a user could unwrap a brand new Mac, and the attacker could root it out of the box the first time it connects to WiFi."

Hein in *Cult of Mac* went on to explain that "when enterprise Macs use MDM [Mobile Device Management] to see which apps to install off the Mac App Store, there is no certificate pinning to verify the manifest's authenticity. Hackers could use a man-in-the-middle exploit to install malicious apps to access data. Making matters worse, the flaw could be used to hack an entire company's computers."

Campbell also looked at "certificate pinning," which is intended to authenticate web servers through the configuration process. "In particular, the researchers found a bug in Apple's MDM sequence that, when the process hands the machine over to the Mac App Store, fails to complete pinning to confirm the authenticity of an app download manifest, the report said. The hole provides an opportunity for hackers to install malicious code on a target Mac remotely and without alerting the end user."

Lily Hay Newman referred to "certificate pinning" in *Wired* as "a method of confirming that particular web servers are who they claim."

A problem during one step was spotted by the researchers. "When MDM hands off to the Mac App Store to download enterprise software, the sequence retrieves a manifest for what to download and where to install it without pinning to confirm the manifest's authenticity."

Endahl said in his company 's news release that "under the hood, the DEP and MDM implementations involve many moving parts, and the bootstrapping process exposes vulnerabilities when a device is brought to a fully-provisioned state."

Apple's response? According to reports, Apple addressed the issue when notified by the researchers, in that the vulnerability was patched in macOS High Sierra 10.13.6.

Citation: Researchers showed remote style hack for new Macs (2018, August 13) retrieved 3 May 2024 from https://techxplore.com/news/2018-08-remote-style-hack-macs.html