Written by **C. Mitchell Shaw** on March 30, 2017

Can the CIA Hack iPhones and Macs?

The most recent WikiLeaks disclosures, published last week, detail hacks developed by the CIA to penetrate iPhones and Mac laptops. The leaks — codenamed "Dark Matter" by WikiLeaks — show that the CIA had developed methods for installing surveillance malware on "factory fresh" iPhones as early as 2008. They also reveal that the agency has methods for injecting persistent malware into the firmware of Mac laptops.

As WikiLeaks' press release from last week says:

> Also included in this release is the manual for the CIA's "NightSkies 1.2" a "beacon/loader/implant tool" for the Apple iPhone. Noteworthy is that NightSkies had reached 1.2 by 2008, and is expressly designed to be physically installed onto factory fresh iPhones. i.e the CIA has been infecting the iPhone supply chain of its targets since at least 2008.

While this deepens the rabbit hole of the CIA's hacking program, it is also fairly good news — if you read between the lines. Because this hack requires physical access to the device. Again, this is a shift away from the *mass surveillance* revealed almost four years ago by Ed Snowden; this is *targeted surveillance* of select devices. Because of the wide adoption of powerful encryption standards, the surveillance hawks are forced to take the more costly, time consuming, and detectable route of bugging individual devices.

While this means that the CIA and other agencies (or for that matter, anyone who has been able to get their hands on the cyberweapons the CIA let loose in the wild) would need to actually get their hands on an iPhone to install the malware, the CIA would not likely have allowed that to serve as much of an obstacle. Agents could simply break in to a home or office and infect the device. And, since many people and organizations order their phones via the Internet and have them delivered by either the U.S. mail service or a delivery company such as FedEx or UPS, the CIA would have little trouble intercepting the phone en route, installing the malware, and sending the phone on to the unsuspecting customer. As the WikiLeaks press release said:

> While CIA assets are sometimes used to physically infect systems in the custody of a target it is likely that many CIA physical access attacks have infected the targeted organization's supply chain including by interdicting mail orders and other shipments (opening, infecting, and resending) leaving the United States or otherwise.

Also in the good-news column is the fact that this CIA hack, like others, requires unpatched vulnerabilities. Apple — while confirming the vulnerability that the CIA hack depends on — explained in a statement that the vulnerability this hack exploited has been patched for years. Part of that statement said:

> Based on our initial analysis, the alleged iPhone vulnerability affected iPhone 3G only and was fixed

> in 2009 when iPhone 3GS was released.

The recent WikiLeaks dump also pointed to vulnerabilities in the firmware (software embedded into the hardware of devices) of Mac laptops. By exploiting those vulnerabilities, the CIA discovered ways to inject those devices with surveillance malware that was "persistent" and would remain even if the hard drive was formatted (or even replaced) and the operating system reinstalled (or even replaced). As the press release states:

> Today, March 23rd 2017, WikiLeaks releases Vault 7 "Dark Matter", which contains documentation for several CIA projects that infect Apple Mac firmware (meaning the infection persists even if the operating system is re-installed) developed by the CIA's Embedded Development Branch (EDB). These documents explain the techniques used by CIA to gain "persistence" on Apple Mac devices, including Macs and iPhones and demonstrate their use of EFI/UEFI and firmware malware.
>
> Among others, these documents reveal the "Sonic Screwdriver" project which, as explained by the CIA, is a "mechanism for executing code on peripheral devices while a Mac laptop or desktop is booting" allowing an attacker to boot its attack software for example from a USB stick "even when a firmware password is enabled". The CIA's "Sonic Screwdriver" infector is stored on the modified firmware of an Apple Thunderbolt-to-Ethernet adapter.
>
> "DarkSeaSkies" is "an implant that persists in the EFI firmware of an Apple MacBook Air computer" and consists of "DarkMatter", "SeaPea" and "NightSkies", respectively EFI, kernel-space and user-space implants.

While Apple — enjoying recent fame for its successful standoff with the FBI over demands to create a backdoor to compromise the encryption of iPhone and iPad devices — claims that those vulnerabilities have also been patched as of 2013, WikiLeaks claims otherwise. The statement from Apple — quoted above — goes on to say:

> Additionally, our preliminary assessment shows the alleged Mac vulnerabilities were previously fixed in all Macs launched after 2013.

If that is true and Apple hasn't missed something, it would mean that any Mac computer less than four years old should be fine. But, according to WikiLeaks — and the documents it released — that may not be the case. The press release stated:

> Documents on the "Triton" MacOSX malware, its infector "Dark Mallet" and its EFI-persistent version "DerStarke" are also included in this release. While the DerStarke1.4 manual released today dates to 2013, other Vault 7 documents show that as of 2016 the CIA continues to rely on and update these systems and is working on the production of DerStarke2.0.

Of course it may be that the CIA is simply updating its malware for greater functionality on those Macs that were made prior to the update that it claims patched those vulnerabilities. It is also possible that Apple is not aware of the full scope of vulnerabilities existing in its firmware and other proprietary software.

In either case, the facts remain that the CIA has devoted time, talent, and (national) treasure to developing ways to hack specific endpoint devices and that the CIA — by ineptitude or worse — lost control of those methods and allowed them to become available for hackers all over the world (both state-sponsored and otherwise) to use.

The takeaway here is that anyone using a Mac laptop produced in 2013 or before or an older iPhone 3G

(though that number is probably very small) can now know with certainty that their devices are vulnerable. Those with newer devices are left to wonder whether Apple has sufficiently patched those vulnerabilities or if new vulnerabilities exist. Of course, since proprietary firmware is the norm for PCs, and Android devices as well, owners of non Mac devices are not out of the woods.

The best course of action — though it would have seemed like the extreme advice of a "conspiracy theory" advocate just a couple of months ago — would be to only buy phones and computers in stores and take delivery right away. Never leave them unattended. And — most importantly — if an agent of the government (a TSA agent, for example) ever, for one second, takes one of those devices out of your sight, get rid of it. If it is a computer, remove (and destroy) the hard drive and sell the computer for parts. Buy a new computer and restore your data from the backup you should be keeping.

Oh, and *encrypt everything*.

The surveillance hawks have shown (again) that they will stop at nothing. Encryption is the bane of their tyrannical attack on liberty and the privacy it protects. Those concerned about preserving privacy and liberty have to be willing to bring pressure to bear on their elected officials to begin investigating and dismantling the surveillance state. They should also take the necessary steps to do all they can to protect themselves and their devices against the surveillance state. To that end, this article (which contains some out-of-date information) is a good starting place.