Dark Matter

23 March, 2017

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.

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.

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 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.