https://wikileaks.org/vault7/?marble9#Marble%20Framework

Wikileaks: CIA Program That Hide Dirty Work

Marble Framework

31 March, 2017

Today, March 31st 2017, WikiLeaks releases Vault 7 "Marble" -- 676 source code files for the CIA's secret anti-forensic Marble Framework. Marble is used to hamper forensic investigators and anti-virus companies from attributing viruses, trojans and hacking attacks to the CIA.

Marble does this by hiding ("obfuscating") text fragments used in CIA malware from visual inspection. This is the digital equivallent of a specalized CIA tool to place covers over the english language text on U.S. produced weapons systems before giving them to insurgents secretly backed by the CIA.

Marble forms part of the CIA's anti-forensics approach and the CIA's Core Library of malware code. It is "*[D]esigned to allow for flexible and easy-to-use obfuscation*" as "*string obfuscation algorithms (especially those that are unique) are often used to link malware to a specific developer or development shop.*"

The Marble source code also includes a *deobfuscator* to reverse CIA text obfuscation. Combined with the revealed obfuscation techniques, a pattern or signature emerges which can assist forensic investigators attribute previous hacking attacks and viruses to the CIA. Marble was in use at the CIA during 2016. It reached 1.0 in 2015.

The source code shows that Marble has test examples not just in English but also in Chinese, Russian, Korean, Arabic and Farsi. This would permit a forensic attribution double game, for example by pretending that the spoken language of the malware creator was not American English, but Chinese, but then showing attempts to conceal the use of Chinese, drawing forensic investigators even more strongly to the wrong conclusion, --- but there are other possibilities, such as hiding fake error messages.

The Marble Framework is used for obfuscation only and does not contain any vulnerabilties or exploits by itself.

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.