WikiLeaks unveils how Apple products have been hacked for years

By Ilse van den Berg

24 Mar 2017

NEWSWATCH: Yesterday, 23 March 2017, saw the release of WikiLeaks' Vault 7 "Dark Matter", a cache of documents which explains the techniques used by the CIA to gain 'persistence' on Apple Mac devices, including Macs and iPhones. The documents also demonstrate the use of EFI/UEFI and firmware malware.

It is reported that Vault 7 "Dark Matter" 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).

> *Apple's claim that it has "fixed" all "vulnerabilities" described in DARKMATTER is duplicitous. EFI is a systemic problem, not a zero-day.— WikiLeaks (@wikileaks) March 24, 2017*

According to WikiLeaks founder, Julian Assange, the organisation only published 1% of the information it has discovered.

> *#Julain_Assange: The #CIA has become a giant #hacker #spy agency! We Only published 1% of #Vault7 @wikileaks @YosriFouda @dw_arabic pic.twitter.com/0yopB6VUpN— □□□□□□□ □□□□□□ (@dw_Sulta5) March 23, 2017*

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.

> *Full recording: WikiLeaks press conference this afternoon on CIA / Vault7 / "Dark Matter" https://t.co/gGQgMzjLIL #Vault7 #cia #darkmatter— WikiLeaks (@wikileaks) March 23, 2017*

> The press release states that "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 organisation's supply chain including by interdicting mail orders and other shipments (opening, infecting, and resending) leaving the United States or otherwise."

> *WikiLeaks #Vault7 shows CIA has been infecting supply chains for at least 8 yearshttps://t.co/Dn22OPrlr9*

> *More: https://t.co/oGV212GlCL pic.twitter.com/8APJricEWo— WikiLeaks (@wikileaks) March 24, 2017*

For more:

- Dark Matter via WikiLeaks
- WikiLeaks unveils how CIA reportedly hacked our Apple products via The Next Web
- WikiLeaks' New Dump Shows How The CIA Allegedly Hacked Macs and iPhones Almost a Decade Ago via Motherboard

ABOUT ILSE VAN DEN BERG

Ilse is a freelance journalist and editor with a passion for people & their stories (check out Passing Stories). She is also the editor of Go & Travel, a platform connecting all the stakeholders in the travel & tourism industry. You can check out her work here and here. Contact Ilse through her website here.

- #StartupStory: Aura security app to aid beleaguered Uber drivers - 13 Jul 2018
- #StartupStory: BlockMesh - 12 Jun 2018
- Taking telecoms to the next level: Who needs a long-term contract? - 4 Jun 2018
- Nokia makes a comeback in South Africa with new phones - 24 Apr 2018
- New Cape Town/Brazil subsea cable to boost SA broadband - 18 Apr 2018

View my profile and articles...