WikiLeaks publishes 'entire hacking capacity of the CIA'

07/03/2017

WikiLeaks has published what it claims is the largest ever batch of confidential documents on the CIA, revealing the breadth of the agency's ability to hack smartphones and popular social media messaging apps such as WhatsApp.

A total of 8,761 documents have been published as part of 'Year Zero', the first part in a series of leaks on the agency that the whistleblower organization has dubbed 'Vault 7.'

In a statement WikiLeaks said 'Year Zero' revealed details of the CIA's "global covert hacking program," including "weaponized exploits" used against company products including "Apple's iPhone, Google's Android and Microsoft's Windows and even Samsung TVs, which are turned into covert microphones."

@wikileaks RELEASE: Vault 7 Part 1 "Year Zero": Inside the CIA's global hacking force https://wikileaks.org/ciav7p1

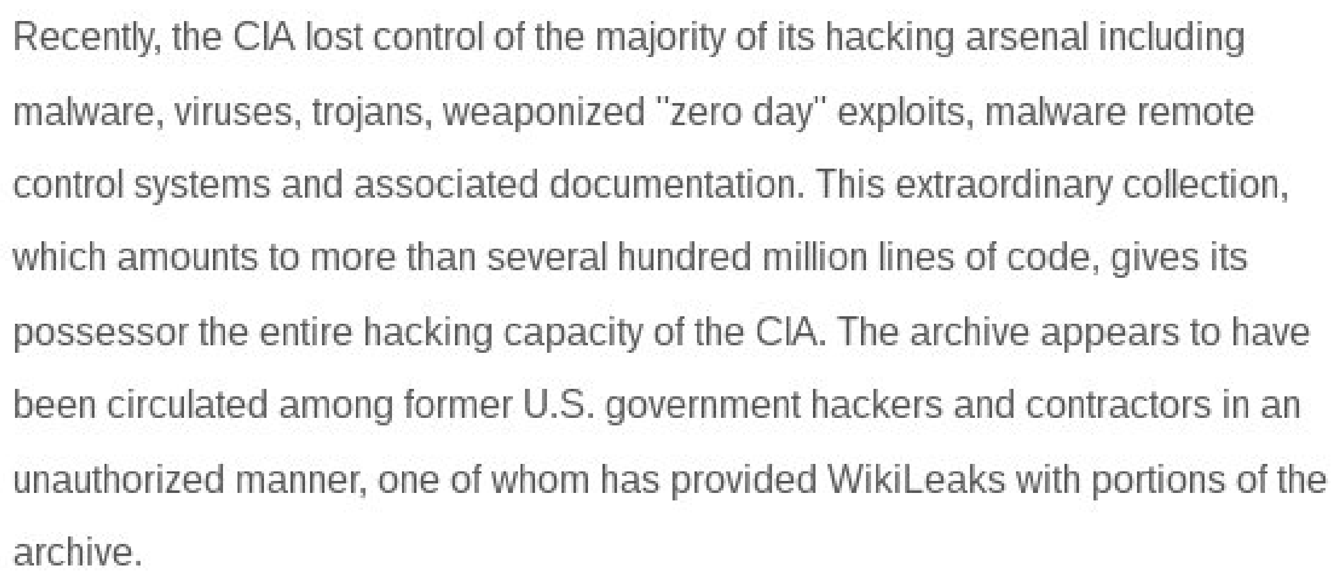
According to the cache of documents released, the CIA's Mobile Devices Branch (MDB) has developed multiple tools and systems to hack popular smart phones and remotely order them to send both location data as well as audio and text communications.

The phones’ cameras and microphones can also be remotely activated at will.

Such tools and techniques allow the CIA to hack social media platforms such as WhatsApp, Signal, Telegram, Wiebo, Confide and Cloackman before encryption can be applied, WikiLeaks claims in the statement on their website.

The time period covered in the latest leak is 2013 to 2016, according to the CIA timestamps on the documents themselves.

@wikileaks CIA negligence sees it losing control of all cyber weapons arsenal sparking serious proliferation concerns **#Vault7** https://wikileaks.org/ciav7p1/#PRESS



Recently, the CIA lost control of the majority of its hacking arsenal including malware, viruses, trojans, weaponized "zero day" exploits, malware remote control systems and associated documentation. This extraordinary collection, which amounts to more than several hundred million lines of code, gives its possessor the entire hacking capacity of the CIA. The archive appears to have been circulated among former U.S. government hackers and contractors in an unauthorized manner, one of whom has provided WikiLeaks with portions of the archive.

The source of the information told WikiLeaks in a statement that they wish to initiate a public debate about the “security, creation, use, proliferation and democratic control of cyberweapons.”

Policy questions that should be debated in public include “whether the CIA's hacking capabilities exceed its mandated powers and the problem of public oversight of the agency,” WikiLeaks claims the source said.

READ MORE: Revelations of CIA spying on NATO-ally France 'a nuclear bombshell’

Commenting on the leak, WikiLeaks co-editor Julian Assange said the cache showed the *“extreme proliferation risk in the development of cyber 'weapons.”*

“The significance of ‘Year Zero’ goes well beyond the choice between cyberwar and cyberpeace. The disclosure is also exceptional from a political, legal and forensic perspective," he said.

The FAQ section of the release yields some key details which highlight the true extent of the leak: firstly, the information was *“obtained recently and covers through 2016”.*

Secondly, WikiLeaks has asserted that it has not mined the entire leak and has only verified it, asking that journalists and activists do the leg work.

READ MORE: WikiLeaks releases 'CIA espionage orders' for 2012 French presidential election

In WikiLeaks’ analysis of ‘Year Zero’ it detailed ‘Weeping Angel’, a surveillance technique which infiltrates smart TV’s, transforming them into microphones.

An attack against Samsung TV’s used ‘Weeping Angel’ in cooperation with MI5, placing them into a ‘Fake-Off’ mode, recording conversations even when the device appears to be off.

In the released batch “Things you might do” with ‘Weeping Angel’ is detailed in a document. *“Investigate any listening ports & their respective services”* is listed, along with *“extract browser credentials or history.”*

@KimDotcomBREAKING: CIA turns Smart TVs, iPhones, gaming consoles and many other consumer gadgets into open microphones. **#Vault7**

@KimDotcom BREAKING: CIA turned every Microsoft Windows PC in the world into spyware. Can activate backdoors on demand, including via Windows update.

The release came after a planned press conference suffered a cyberattack, according to the whistleblowing organization. WikiLeaks has since rescheduled its press conference.