Wikileaks Warns: Your Bitcoins Are Open To CIA And Criminals

Little by little, everything that is supposed to be secure is getting broken open or hacked by the Intelligence community, in this case Bitcoin's blockchain. TN Editor

Wikileaks has exposed the CIA's hacking tools and techniques in "the largest ever publication of confidential documents on the agency." Some readers are probably compromised without knowing it – if not by the government, then by criminals who have acquired the non-secured tools. Here's how to assess your vulnerability and what to do about it.

"Vault7" is Wikileaks' codename for a series of massive document releases on the e-surveillance and cyber-warfare techniques of the CIA. It is not known how many releases will occur but four have so far.

- March 7: "Year Zero" contains over 8,000 documents or "more than several hundred million lines of code" – that render the

CIA's entire hacking capacity.

- March 23: "Dark Matter" documents several CIA projects to infect Apple Mac firmware and explains how the CIA gains "persistence" on "Apple Mac devices, including Macs and Iphones" and how it uses "EFI/UEFI and firmware malware."
- March 31: "Marble Framework" offers 676 source code files for the CIA's program that aims "to hamper forensic investigators and anti-virus companies from attributing viruses, trojans and hacking attacks to the CIA."
- April 7: "Grasshopper" contains 27 documents from the CIA regarding "a platform used to build customized malware payloads for Microsoft Windows operating systems."

"Year Zero" is the most interesting to Bitcoin users because it documents proximate dangers. "Grasshopper" is also important to examine.

Which Devices are Vulnerable to CIA 'Infection'?

This Wikileaks dump reiterated something we already knew; Our devices are fundamentally unsafe. No matter what kind of encryption we use, no matter which secure messaging apps we take care to run, no matter how careful we are to sign up for two-factor authentication, the CIA—and, we have to assume, other hackers—can infiltrate our operating systems, take control of our cameras and microphones, and bend our phones to their will. The same can be said of smart TVs, which could be made to surreptitiously record our living-room conversations.

Consider just three.

Smartphones

Reason magazine states the danger simply. “According to Wikileaks, the documents show the CIA has a specialized unit specifically for stealing data from Apple products like the Iphone and the Ipad, and another unit for Google’s Android mobile operating system. These units create malware based on ‘zero- day’ exploits that the companies that develop the compromised systems are not aware of.”

PC Backdoors

CIA can reputedly infect computers which run on Windows XP, Windows Vista and Windows 7. Mac OS or Linux – those are reported to be affected as well.

Weeping Angel

C/net reports that Weeping Angel is an “alleged spying tool, co-developed by the CIA and the UK’s MI5 security agency, which lets a Samsung Smart TV (specifically, the F8000 Smart TV) *pretend* to turn itself off — and record your conversations — when you’re not using the screen.” Although there is evidence of development since 2014, there is no hard evidence of completion. Note: Samsung drew sharp criticism in 2015 when its smart TVs were shown to be recording private conversations.

Weeping Angel may not affect Bitcoin use directly but it demonstrates the pervasive surveillance being pursued by the CIA.

A Truly Troublesome Wrinkle – Criminals

Most people will not be targeted by the CIA or even by government agencies with which the hacking tools may have been shared, like the IRS. But the CIA seems to have lost control of their own tools including weaponized viruses, malware, and trojans. The tools, code, and strategies apparently circulated freely among former contractors and hackers for the U.S. government, who were not authorized to view them.

NBC News reported on an interview with Wikileaks founder Julian Assange. “Assange ridiculed the CIA for failing to guard information about its online arsenal, allowing it to be passed around within the

intelligence community. That is how the material ended up in Wikileaks' hands − and, possibly, criminals', he said." Wikileaks has "held off publishing viruses and other weapons"; it has delayed publication in order to first "disarm" the tools.

You should assume that weaponized hacking tools are in private hands. The CIA may not consider you "worthy" of targeting but criminals are less discriminating.

Read full story here...