GlobalResearch
Center for Research on Globalization

CIA Documents Reveal Agency Spying On Us Through Our Computers, Phones and TVs

By Washington's Blog
Global Research, March 08, 2017
Washington's Blog

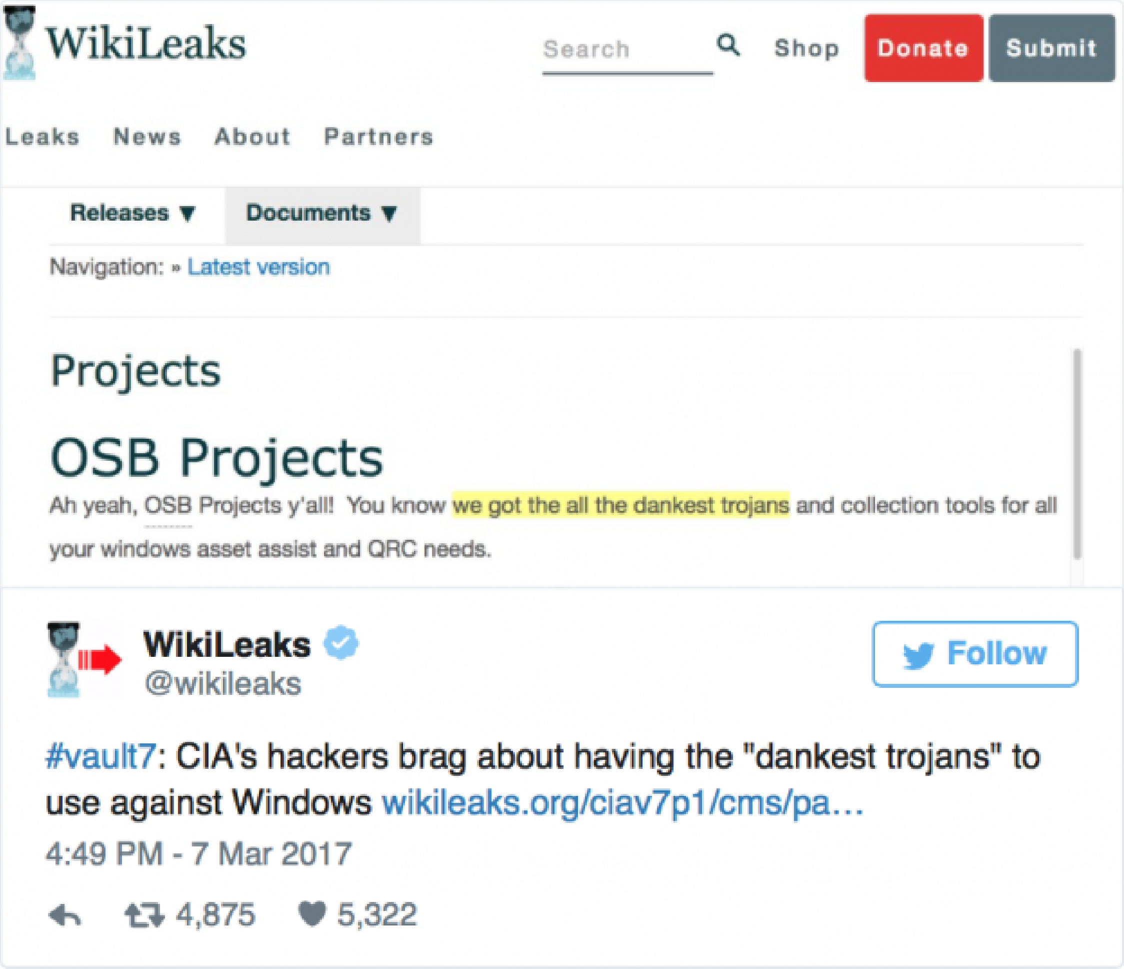
Region: USA
Theme: Intelligence, Police State & Civil Rights

We've previously documented that the government is spying on us through our computers, phones, cars, buses, streetlights, at airports and on the street, via mobile scanners and drones, through our credit cards and smart meters, televisions, dolls, and in many other ways.

And that the CIA wants to spy on you through your dishwasher and other "smart" appliances.

Indeed, spying in the U.S. is worse than under Nazi Germany, the Stasi, J. Edgar Hoover … or Orwell's 1984.

CIA documents leaked today by Wikileaks confirm that the CIA is spying on us through our Windows-based computers, phones and TVs.



Navigation: » Latest version

Projects

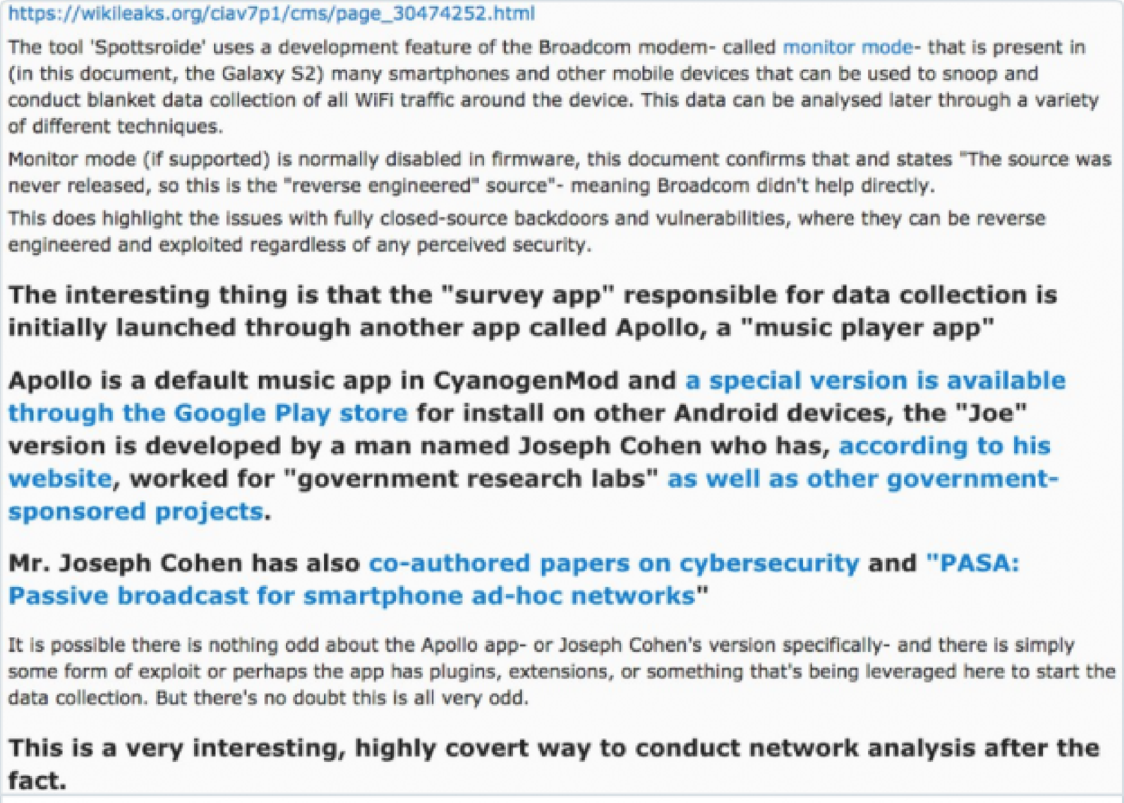
OSB Projects

Ah yeah, OSB Projects y'all! You know we got the all the dankest trojans and collection tools for all your windows asset assist and QRC needs.

#vault7: CIA's hackers brag about having the "dankest trojans" to use against Windows wikileaks.org/ciav7p1/cms/pa…

4:49 PM - 7 Mar 2017

4,875 5,322



https://wikileaks.org/ciav7p1/cms/page_30474252.html

The tool 'Spottsroide' uses a development feature of the Broadcom modem- called monitor mode- that is present in (in this document, the Galaxy S2) many smartphones and other mobile devices that can be used to snoop and conduct blanket data collection of all WiFi traffic around the device. This data can be analysed later through a variety of different techniques.

Monitor mode (if supported) is normally disabled in firmware, this document confirms that and states "The source was never released, so this is the "reverse engineered" source"- meaning Broadcom didn't help directly.

This does highlight the issues with fully closed-source backdoors and vulnerabilities, where they can be reverse engineered and exploited regardless of any perceived security.

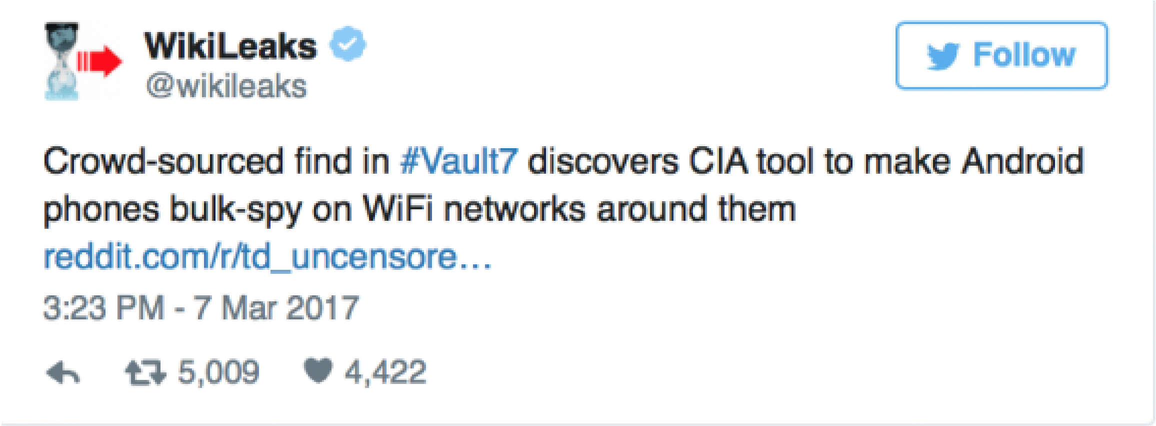
The interesting thing is that the "survey app" responsible for data collection is initially launched through another app called Apollo, a "music player app"

Apollo is a default music app in CyanogenMod and a special version is available through the Google Play store for install on other Android devices, the "Joe" version is developed by a man named Joseph Cohen who has, according to his website, worked for "government research labs" as well as other government-sponsored projects.

Mr. Joseph Cohen has also co-authored papers on cybersecurity and "PASA: Passive broadcast for smartphone ad-hoc networks"

It is possible there is nothing odd about the Apollo app- or Joseph Cohen's version specifically- and there is simply some form of exploit or perhaps the app has plugins, extensions, or something that's being leveraged here to start the data collection. But there's no doubt this is all very odd.

This is a very interesting, highly covert way to conduct network analysis after the fact.

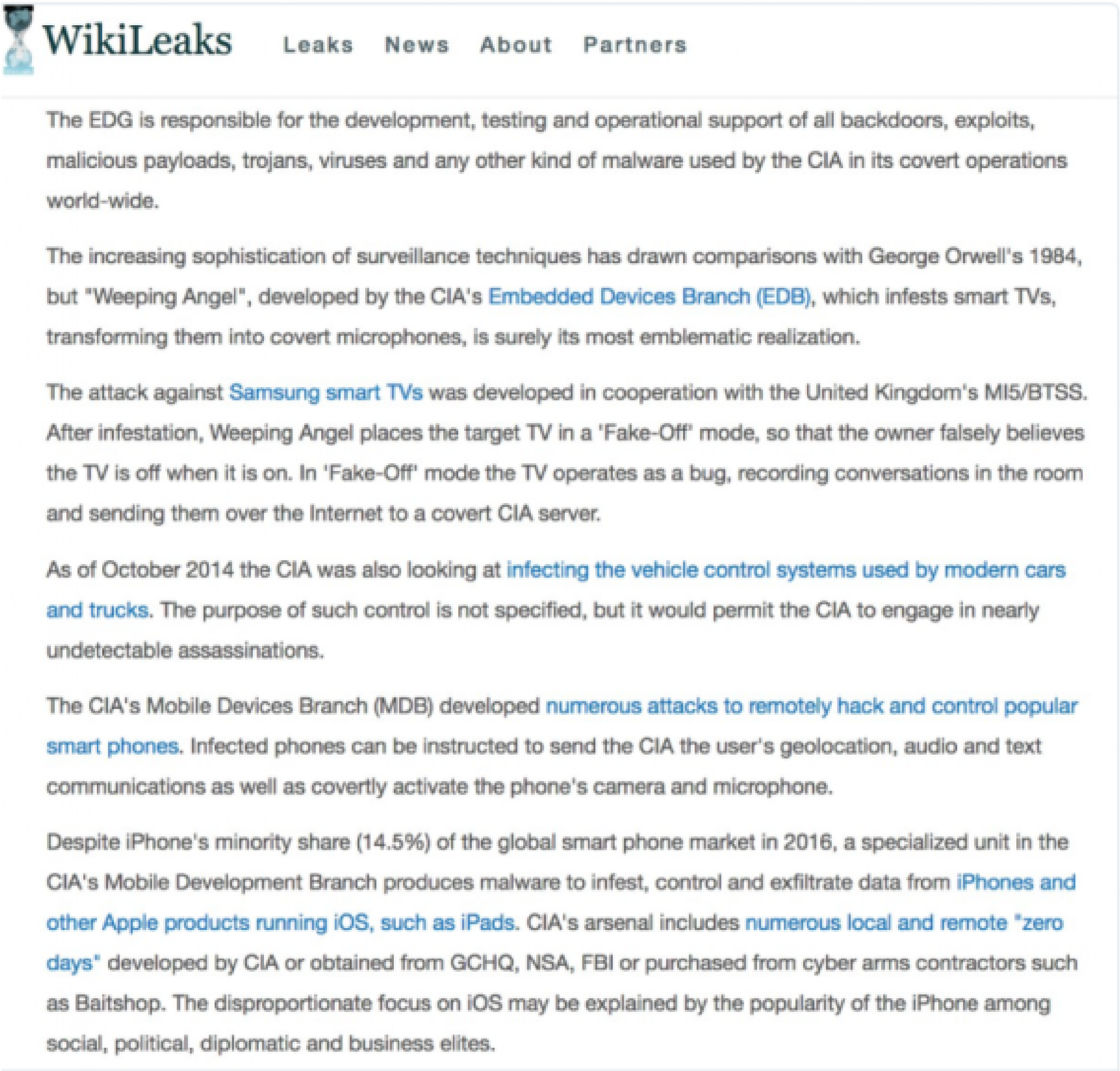


WikiLeaks
@wikileaks

Crowd-sourced find in #Vault7 discovers CIA tool to make Android phones bulk-spy on WiFi networks around them reddit.com/r/td_uncensore…

3:23 PM - 7 Mar 2017

5,009 4,422



The EDG is responsible for the development, testing and operational support of all backdoors, exploits, malicious payloads, trojans, viruses and any other kind of malware used by the CIA in its covert operations world-wide.

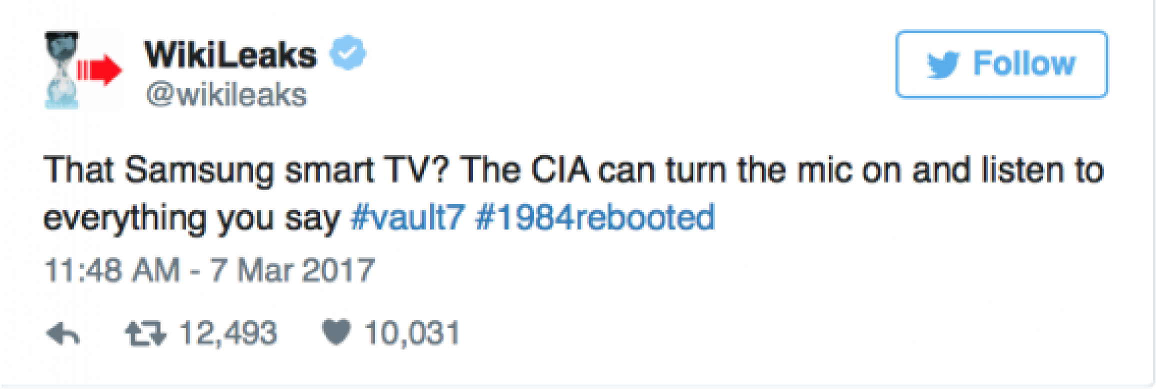
The increasing sophistication of surveillance techniques has drawn comparisons with George Orwell's 1984, but "Weeping Angel", developed by the CIA's Embedded Devices Branch (EDB), which infests smart TVs, transforming them into covert microphones, is surely its most emblematic realization.

The attack against Samsung smart TVs was developed in cooperation with the United Kingdom's MI5/BTSS. After infestation, Weeping Angel places the target TV in a 'Fake-Off' mode, so that the owner falsely believes the TV is off when it is on. In 'Fake-Off' mode the TV operates as a bug, recording conversations in the room and sending them over the Internet to a covert CIA server.

As of October 2014 the CIA was also looking at infecting the vehicle control systems used by modern cars and trucks. The purpose of such control is not specified, but it would permit the CIA to engage in nearly undetectable assassinations.

The CIA's Mobile Devices Branch (MDB) developed numerous attacks to remotely hack and control popular smart phones. Infected phones can be instructed to send the CIA the user's geolocation, audio and text communications as well as covertly activate the phone's camera and microphone.

Despite iPhone's minority share (14.5%) of the global smart phone market in 2016, a specialized unit in the CIA's Mobile Development Branch produces malware to infest, control and exfiltrate data from iPhones and other Apple products running iOS, such as iPads. CIA's arsenal includes numerous local and remote "zero days" developed by CIA or obtained from GCHQ, NSA, FBI or purchased from cyber arms contractors such as Baitshop. The disproportionate focus on iOS may be explained by the popularity of the iPhone among social, political, diplomatic and business elites.



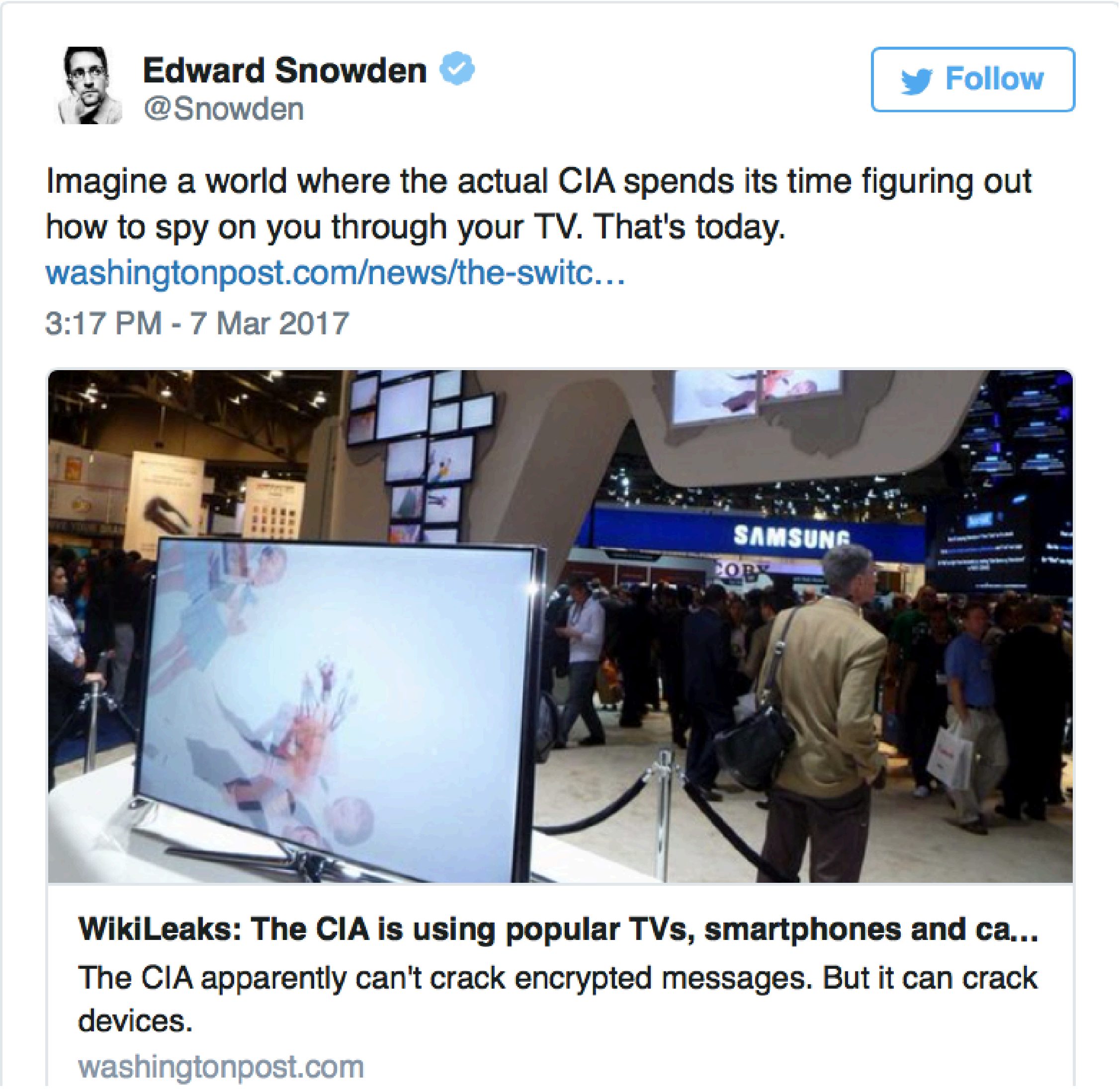
WikiLeaks
@wikileaks

That Samsung smart TV? The CIA can turn the mic on and listen to everything you say #vault7 #1984rebooted

11:48 AM - 7 Mar 2017

12,493 10,031

Edward Snowden notes the similarities to George Orwell's novel *1984*:



Edward Snowden
@Snowden

Imagine a world where the actual CIA spends its time figuring out how to spy on you through your TV. That's today. washingtonpost.com/news/the-switc…

3:17 PM - 7 Mar 2017

WikiLeaks: The CIA is using popular TVs, smartphones and ca…

The CIA apparently can't crack encrypted messages. But it can crack devices.

washingtonpost.com

The original source of this article is Washington's Blog

Comment on Global Research Articles on our Facebook page

Become a Member of Global Research

Articles by: **Washington's Blog**

Disclaimer: The contents of this article are of sole responsibility of the author(s). The Centre for Research on Globalization will not be responsible for any inaccurate or incorrect statement in this article. The Centre of Research on Globalization grants permission to cross-post Global Research articles on community internet sites as long the source and copyright are acknowledged together with a hyperlink to the original Global Research article. For publication of Global Research articles in print or other forms including commercial internet sites, contact: publications@globalresearch.ca