

Was Every 'Conspiracy Theorist' in America Just Vindicated?

Yes, the government can use your phone, your computer and even potentially your television to spy on what you are doing inside your own home.

On Tuesday, WikiLeaks released thousands of documents that prove what virtually every "conspiracy theorist" in America has been saying for years about government spying. And I don't even like to use the term "conspiracy theorist" much, because the truth is that most "conspiracy theorists" are simply citizen journalists who are attempting to expose things the mainstream media doesn't want to talk about. And one of the things that the mainstream media has always been hesitant to address is the unconstitutional surveillance that U.S. intelligence agencies systematically conduct on their own citizens.

But now the mainstream media is being forced to talk about government surveillance because WikiLeaks has just exposed it for all the world to see. According to WikiLeaks, the CIA has been secretly running "its 'own NSA' with even less accountability and without publicly answering the question as to whether such a massive budgetary spend on duplicating the capacities of a rival agency could be justified". It is known as the Central Intelligence Agency's Center for Cyber Intelligence, and it has produced "more than a thousand hacking systems, trojans, viruses and other 'weaponized' malware." In fact, the computer or phone that you are reading this article on may be infected with one of their programs right now.

The documents that were released by Wikileaks show that

government spooks can remotely take control of Apple iPhones, Google Android phones, Microsoft Windows operating systems and Samsung smart televisions, and once in control of those devices, they can use them to spy on their owners.

The ironic thing is that while Barack Obama and members of Congress have been accusing Russia of conducting cyberattacks, the truth is that U.S. intelligence agencies have been perhaps the biggest offenders of all.

This is an absolutely massive scandal, and I truly hope it gets the attention that it deserves in the days ahead. The following is a portion of the press release **Wikileaks issued on Tuesday:**

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.

“Year Zero” introduces the scope and direction of the CIA’s global covert hacking program, its malware arsenal and dozens of “zero day” weaponized exploits against a wide range of U.S. and European company products, include Apple’s iPhone, Google’s Android and Microsoft’s Windows and even Samsung TVs, which are turned into covert microphones.

Since 2001 the CIA has gained political and budgetary preeminence over the U.S. National Security Agency (NSA). The CIA found itself building not just its now infamous drone fleet, but a very different type of covert, globe-spanning force—its own substantial fleet of hackers. The agency’s hacking division freed it from having to disclose its often-

controversial operations to the NSA (its primary bureaucratic rival) in order to draw on the NSA's hacking capacities.

By the end of 2016, the CIA's hacking division, which formally falls under the agency's Center for Cyber Intelligence (CCI), had over 5000 registered users and had produced more than a thousand hacking systems, trojans, viruses and other "weaponized" malware. Such is the scale of the CIA's undertaking that by 2016, its hackers had utilized more code than that used to run Facebook.

After learning about this, you may never look at your smart TV the same way again.

In fact, according to the documents that Wikileaks has given us the CIA can even use your smart TV to spy on you when it appears to be turned off:

A program dubbed "Weeping Angel" after an episode of the popular British TV science fiction series Dr. Who, can set a Samsung smart TV into a fake "off" mode to fool the consumer into thinking the TV isn't recording room sounds when it still is. The conversations are then sent out via the user's server. The program was developed in conjunction with MI5, the British FBI equivalent of a domestic counterintelligence and security agency, according to the WikiLeaks documents.

And if your phone has been infected by the CIA, they can remotely turn on the camera and microphone whenever they want and use the phone as a GPS locator to track you wherever you go. The following comes from *USA Today*:

CIA-created malware can penetrate and then control the operating systems for both Android and iPhone phones, allege the documents. This software would allow the agency to see the user's location, copy and transmit audio and text from the phone and covertly turn on the phone's camera and

microphone and then send the resulting images or sound files to the agency.

Just two days ago, I wrote a major article warning that the government has the capability to do these sorts of things.

This stuff is really going on, and it needs to stop now. I warned about some of this advanced “Big Brother technology” in my apocalyptic novel, *The Beginning Of The End*, and many of us have been screaming about what U.S. intelligence agencies have been doing for years and years. Now that President Trump is extremely upset that the government was spying on him, let us hope that he steps up to the plate and puts an end to this unconstitutional surveillance for good.

In the documents WikiLeaks has just released, there is even discussion about the CIA potentially being able to infect a vehicle control system. Presumably, the goal would be to remotely take control of a vehicle and either spy on the occupants or kill them by driving into an obstacle at very high speed.

And if you can believe it, the CIA has also been developing ways to make it look like a cyberattack that they conducted actually came from the Russians. The following comes from an article by Jerome Corsi:

The Wikileaks “Vault 7” drop of CIA cyber-warfare documents contains the startling revelation that the CIA, under a project identified as “Umbrage,” maintained a substantial library of Russian cyber-attack techniques “stolen” from malware produced in other states including the Russian Federation.

Of course when it comes to violations of privacy, the NSA is even worse than the CIA.

The NSA systematically collects all forms of digital

communication and stores them in a giant data center out in Utah. So nothing you do on a digital device is ever truly private. If you don't believe the article that I posted the other day, perhaps you will believe a 36-year veteran of the NSA named William Binney:

President Donald Trump is "absolutely right" to claim he was wiretapped and monitored, a former NSA official claimed Monday, adding that the administration risks falling victim to further leaks if it continues to run afoul of the intelligence community.

"I think the president is absolutely right. His phone calls, everything he did electronically, was being monitored," Bill Binney, a 36-year veteran of the National Security Agency who resigned in protest from the organization in 2001, told Fox Business on Monday. Everyone's conversations are being monitored and stored, Binney said.

Did you catch that last sentence?

Binney knows very well that all of our conversations are systematically being monitored and stored because he helped build the systems that do it.

Now that all of this is out in the open, America has two choices.

We can end this unconstitutional surveillance and go back to being a nation that respects privacy, or we can allow it to continue and keep heading down the road toward becoming a "Big Brother" surveillance society far worse than anything that George Orwell ever warned about. {eoa}