

WikiLeaks docs allege CIA can hack smartphones, expose Frankfurt listening post

The CIA would not verify the documents' authenticity.

WikiLeaks released on Tuesday what the whistleblower group claimed were thousands of secret CIA files showing how U.S. spies hack smartphones, as well as exposing a major secret listening post in Germany.

The Office of the Director of National Intelligence declined to comment, and in a statement the CIA would not say whether the files are authentic.

"We do not comment on the authenticity or content of purported intelligence documents," said CIA spokesperson Jonathan Liu.

However, several current and former intelligence officials, speaking on condition of anonymity, told ABC News the documents appear to be authentic and likely have origins at the National Security Agency, where most national security hacking of overseas targets occurs.

"Somebody really screwed up to let this get out," a former official familiar with the activities outlined in the WikiLeaks-released files told ABC News.

WikiLeaks said a former government contractor leaked the tranche of files.

"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," WikiLeaks said in a statement accompanying more than 8,000 pages of documents.

The WikiLeaks files also revealed that the U.S. Consulate in Frankfurt is a major

hacker outpost for the most important and sensitive operations, and a former official confirmed that it is the major nerve center for covert joint CIA and National Security Agency voice collection around the globe. The official said it was the likely origin of the hacking of German Chancellor Angela Merkel's personal phone — which was revealed in a leak by NSA whistleblower Edward Snowden in 2013.

In fact, many of the hacker tools and files referred to in the documents appear to be the NSA's, in the possession of the CIA rather than the CIA's capabilities, an official said.

"There are only specific people at [the CIA's Center for Cyber Intelligence] who are allowed to see tailored access operations products by NSA hackers," the official told ABC News.

The U.K.'s signals intelligence spy agency GCHQ, for example, is known to conduct proxy cyberactivities in places where the U.S. faces legal restrictions the British government does not have to contend with, a former official involved in hacking said. That intelligence is often shared with or gathered at the behest of American spy services.

The current and former officials could not corroborate WikiLeaks' claim that a former contractor was behind the massive security breach but said it was very possible, if not highly likely.

"I'm not denying there are people leaking information," Tyler Wood, a former senior Defense Intelligence Agency cyberprograms official, told ABC News today.

The leaked files show a large effort undertaken by CIA's Center for Cyber Intelligence to find ways to turn consumer electronic devices — from smart TVs to Google Android and Apple IOS devices, including smartphones and tablets — into remotely activated spy devices. The files detail efforts made to access messages before they are encrypted by security apps and to turn on phones and activate tablet cameras and microphones without owners' awareness. An entire office at CCI is devoted to exploiting mobile smart devices, the documents suggest.

While Snowden, in hiding in Russia and still wanted by U.S. authorities for his breach, tweeted today that the CIA files reveal a "security hole the CIA left open to break into any iPhone in the world," an official familiar with such intelligence

activities said usually a human spy is necessary — a “cyber middleman” — who can first gain physical access to a device. That is an often dangerous task and is rarely accomplished, the official told ABC News.

The programs revealed today have a series of cover names, such as BrutalKangaroo, RickyBobby, AfterMidnight and WeepingAngel — the last being the name of a set of characters in the BBC sci-fi drama “Dr. Who.”

Countless intelligence programs with similar cover names — approved by the Office of the Director of National Intelligence in a lengthy process — had to be renamed after Snowden blew the lid on those activities.

“And everything will have to be renamed after this,” an official familiar with many of the named programs told ABC News.

Senate Armed Services Committee Chairman John McCain, R-Ariz., said Americans should pay attention to such breaches that reveal vulnerabilities to privacy and national security.

“This is of the utmost seriousness. If they can hack into the CIA, they can hack into anybody,” he said today.

Many cybersecurity experts on social media after the leaks focused attention on the apparent capability of U.S. intelligence to hack smart devices such as Samsung smart TVs, which the leaked files said can be in “fake off mode” when in reality the microphone is turned into a room-listening device without anyone nearby knowing it because the TV appears to be off.

“Pretty much anything can be made into an eavesdropping device,” said a former official.

Samsung, in its user manuals’ privacy statement, warns users that their speech can be transmitted through the internet to third parties.

In the last 10 years, WikiLeaks has published an incredible amount of secret U.S. information — about military operations in Iraq, Guantanamo Bay and, more recently, Democratic National Committee emails hacked by Russian intelligence.

Devin Nunes, R-Calif., the chairman of the House Intelligence Committee, said he is “extremely concerned” by the WikiLeaks publications on Tuesday, telling

reporters his panel has reached out to the intelligence community for more information.

“We’ve had initial inquiries into the [intelligence community]. Look, this is early on in the investigation, but these appear to be very, very serious. But at this time, that’s really all the information that I have on it,” he said. “I’ve long said this — that emails and many of our electronic devices are not safe, and they’re primarily not safe from our adversaries like the Russians and the Chinese and others who are actively trying to get into government institutions and private businesses.”

Asked about supposed security vulnerabilities detailed in the documents that are relevant to its devices, Apple said, “While our initial analysis indicates that many of the issues leaked today were already patched in the latest iOS, we will continue work to rapidly address any identified vulnerabilities. We always urge customers to download the latest iOS to make sure they have the most recent security updates.”

“As we’ve reviewed the documents, we’re confident that security updates and protections in both Chrome and Android already shield users from many of these alleged vulnerabilities,” Heather Adkins, Director of Information Security and Privacy at Google, said in a statement to ABC News after original publication of this story. “Our analysis is ongoing and we will implement any further necessary protections. We’ve always made security a top priority and we continue to invest in our defenses.”

Samsung, when asked for comment, said, “Protecting consumers’ privacy and the security of our devices is a top priority at Samsung. We are aware of the report in question and are urgently looking into the matter.”

Last October, Trump as a presidential candidate said, “WikiLeaks, I love WikiLeaks. And I said, write a couple of them down. Let’s see.”

In the regular White House press briefing on Tuesday, press secretary Sean Spicer declined to comment on the matter.

ABC News’ Matthew Mosk, Alexander Hosenball, Paul Blake, Cho Park, Benjamin Siegel and Elizabeth McLaughlin contributed to this report.

This story was originally published on March 7, 2017 and has been updated as new information has become available.

Source:

<https://abcnews.go.com/International/wikileaks-docs-allege-cia-hack-smartphones-exposes-frankfurt/story?id=45977302>

[Disclaimer]