CIA acknowledges its trove of cyber warfare tools was exposed by WikiLeaks in 2017

Kevin Reed
19 June 2020

A newly-released 2017 internal review of security practices at the Central Intelligence Agency (CIA) confirms that the top secret agency had developed an arsenal of cyber espionage tools and would not have known about the massive "Vault 7" data hack of them had WikiLeaks not made it public.

Vault 7 is the name given to a trove of hacked documents from the CIA's Center for Cyber Intelligence (CCI) that were anonymously shared with WikiLeaks, which the online site began publishing information about on March 7, 2017. The hack obtained nearly the entire arsenal of espionage tools and the methods by which the CIA was conducting illegal electronic surveillance and cyber warfare around the world.

The internal report says that the CIA could not determine the precise scope of the data breach, "We assess that in spring 2016 a CIA employee stole at least 180 gigabytes to as much as 34 terabytes of information. This is roughly equivalent to 11.6 million to 2.2 billion pages in Microsoft Word." It was the largest unauthorized disclosure of classified information in the history of the CIA.

Significantly, the heavily redacted and partially released, "WikiLeaks Task Force Final Report" from October 17, 2017 says, "Because the stolen data resided on a mission system that lacked user activity monitoring and a robust server audit capability, we did not realize the loss had occurred until a year later, when WikiLeaks publicly announced it in March 2017. Had the data been stolen for the benefit of a state adversary and not published, we might still be unaware of the loss—as would be true for the vast majority of data on Agency mission systems."

The CIA report also says that WikiLeaks published primarily "user and training guides" from a collaboration and communication platform called Confluence along with "limited source code" from a repository called DevLan: Stash and that "All of the documents reveal, to varying degrees, CIA's tradecraft in cyber operations."

The task force report was initially provided to the *Washington Post* on Tuesday by the office of Democratic Party Senator from Oregon Ron Wyden, a member of the Senate Intelligence Committee, who obtained the incomplete document—pages 15 through 44 have been removed—from the Justice Department.

The same limited version of the report had been introduced as evidence in the trial of Joshua Schulte, a former CIA employee who worked at CCI and has been accused of stealing the Vault 7 documents and handing them over to WikiLeaks. Schulte pled not guilty to eleven charges covered by the US Espionage Act and went to trial in early February.

The federal case ended in a hung jury in early March on the most serious eight charges against Schulte and convicted him only on the lesser charges of contempt of court and making false statements to the Federal Bureau of Investigation. As the *World Socialist Web Site* explained at the time, the failure to convict Schulte of leaking the Vault 7 trove created a stumbling block for the US government in its attempt to extradite WikiLeaks founder and editor Julian Assange, who is currently being held in London's Belmarsh Prison in violation of his rights.

The mistrial in the case of Schulte has so far prevented the US from adding anything about the Vault 7 breach into the already trumped up US charges against Assange. However, Assistant US Attorney David Denton told a judge in the Southern District of New York on May 18 that the Department of Justice "does intend to retry Mr. Schulte on the espionage

© World Socialist Web Site

charges.”

The Vault 7 release by WikiLeaks exposed the CIA’s use of special software to take control of cars, smart TVs, web browsers, smartphones and personal computers for the purpose of spying on individuals and organizations. The exposure of the CIA’s cyber espionage and warfare repository yielded extensive information about these programs by their code names and what function they perform.

An example is a malware tool called Athena which was developed in conjunction with the release of Microsoft Windows operating system 10 in 2015. The Athena malware, which was jointly developed by the CIA and a New Hampshire software company called Siege Technologies, hijacks the Windows Remote Access services utility on Windows 10 computers, enabling an unauthorized user to gain access to the PC and steal and delete private data or install additional malicious software.

Another tool developed by the CIA called Scribbles is designed to track whistleblowers and journalists by embedding “web beacon” tags into classified documents in order to trace who leaked them. This tool was designed to interact with Microsoft Office documents whereby when any CIA watermarked document is opened, an invisible document hosted on the agency’s server is loaded into it, generating an HTTP request that gathers information about who is opening the file and where it is being opened.

It has been estimated that training and user information as well as the source code for as many as 91 such CIA tools were released in the Vault 7 breach.

The majority of corporate media coverage of the newly released document has focused on the vulnerability of the CIA servers and what the agency intends to do about it, the purpose of the Senate Intelligence Committee attempt to make the report public in the first place, to the exclusion of any mention of the tools that were being developed and the blatantly criminal activity of the CIA associated with them.

They have also not drawn attention to the fact that the CIA had, until the Schulte trial and release of the redacted review document, refused to officially acknowledge the existence of the cyber espionage and warfare tools. At the time of the WikiLeaks Vault 7 revelations, when asked about the authenticity of the trove, former Director of the Central Intelligence Agency, Michael Hayden, replied that the organization does “not comment on the authenticity or content of purported intelligence documents.”

The only other government official to mention the enormous hack of the CIA was President Donald Trump, who, on March 15, 2017, stated during an interview with Fox News host Tucker Carlson that “the CIA was hacked, and a lot of things taken.” In typical fashion, Democratic Representative Adam Schiff of California, then the Ranking Member of the House Intelligence Committee, issued a news release the next day that said, “In his effort to once again blame Obama, the President appeared to have discussed something that, if true and accurate, would otherwise be considered classified information.”

To contact the WSWS and the Socialist Equality Party visit:

wsws.org/contact

© World Socialist Web Site