Ex-CIA Engineer Who Leaked “Vault 7” Tools Convicted Of Biggest Theft In Agency History

Description

USA: A former CIA software engineer who leaked the so-called “Vault 7” tools **was convicted Wednesday of causing the largest theft of classified information in the history of the agency**.

Joshua Schulte, who has been sitting behind bars without bail since 2018 and chose to defend himself at trial, told the jury that the CIA and FBI made him a scapegoat for the 2017 WikiLeaks release of **up to 34 terabytes of information**.

Separately, Schulte awaits trial on possession of child ponography and transport charges, which he has pleaded not guilty to, according to *Military.com*.

As part of his defense, Schulte claimed he was **singled out** because “hundreds of people had access to (the information),” adding “Hundreds of people could have stolen it.”

“The government’s case is riddled with reasonable doubt,” he said. “There’s simply no motive here.”

> ***Assistant U.S. Attorney David Denton countered that there was plenty of proof that Schulte pilfered a sensitive backup computer file.***
>
> *“**He’s the one who broke into that system,**” Denton said. “**He’s the one who took that backup, the backup he sent to WikiLeaks**.”*
>
> *The prosecutor also encouraged jurors to consider evidence of an attempted cover-up, including a list of chores Schulte drew up that had an entry reading, “Delete suspicious emails.”*
>
> *“**This is someone who’s hiding the things that he’s done wrong**,” Denton said.*
>
> *Once the jury got the case, Furman complimented Schulte on his closing argument. - Military.com*

The judge complimented Schulte on his defense, saying “that was impressively done.”

“**Depending on what happens here, you may have a future as a defense lawyer.**”

In March of 2020, the trial of former CIA computer engineer Joshua Schulte ended in a hung jury on **eight counts**, including illegal gathering and transmission of national defense information, according to the *New York Times*.

As we noted two years ago, according to a 2017 report created by the CIA's WikiLeaks Task Force and released in June 2020, **there were major security lapses at** the CIA's Center for Cyber Intelligence (CCI), which made cyber weapons – including tools to crack into smartphones, hijack smart TVs, or make it look like a foreign adversary hacked someone.

"In a press to meet growing and critical mission needs, CCI had prioritized building cyber weapons at the expense of securing their own systems," reads the report. "**Day-to-day security practices had become woefully lax.**"

"**CCI focused on building cyber weapons and neglected to also prepare mitigation packages if those tools were exposed**. These shortcomings were emblematic of a culture that evolved over years that too often prioritized creativity and collaboration at the expense of security," the report continues.

> **The leak marked the largest data breach in the CIA's history** and included information on hacking tools used by the agency to break into smartphones and other internet-connected devices.
>
> The task force noted that due to failures to address vulnerabilities in IT systems, **if WikiLeaks had not published the stolen information, the CIA "might still be unaware of the loss** — as would be true for the vast majority of data on Agency mission systems."
>
> In a letter to Director of National Intelligence John Ratcliffe on Tuesday, Wyden criticizedthe intelligence community for its "widespread cybersecurity problems." –The Hill

The Vault 7 release – a series of 24 documents which began to publish on March 7, 2017 – reveal that the CIA has a giant arsenal of tools to use against adversaries, including **the ability to "spoof" its malware to appear as though it was created by a foreign intelligence agency**, as well as the ability to take control of **Samsung Smart TV's** and surveil a target using a "Fake Off" mode in which they appear to be powered down while eavesdropping.

The CIA's toy chest also includes:

- Tools code named "**Marble**" – which can misdirect forensic investigators from attributing viruses, trojans and hacking attacks to their agency by inserted code fragments in foreign languages. The tool was in use as recently as 2016. Per the WikiLeaks release:

  "The source code shows that Marble has test examples not just in English but also in **Chinese, Russian, Korean, Arabic and Farsi. This would permit a forensic attribution double game,** for example by pretending that the spoken language of the malware creator was not American English, but Chinese, **but then showing attempts to conceal the use of Chinese, drawing forensic investigators even more strongly to the wrong conclusion,** — but there are other possibilities, such as hiding fake error messages."

  CIA's "Marble Framework" shows its hackers use potential decoy languages https://t.co/Hm3pTPSXIS

  Background: https://t.co/GsoN4BuyTz pic.twitter.com/ZT66doCnfY

  — WikiLeaks (@wikileaks) March 31, 2017

- iPads / iPhones / Android devices and Smart TV's are all susceptible to hacks and malware. The agency's **"Dark Matter"** project reveals that the CIA has been bugging "factory fresh" iPhones since at least 2008 through suppliers. Another, "**Sonic Screwdriver**" allows the CIA to execute code on a Mac laptop or desktop while it's booting up.

> RELEASE: CIA #Vault7 "Dark Matter" https://t.co/pgnfeODXVB pic.twitter.com/vkI16f3vMD
>
> — WikiLeaks (@wikileaks) March 23, 2017

> RELEASE: CIA #Vault7 "Sonic Screwdriver" https://t.co/pgnfeODXVB pic.twitter.com/18BcVdqkqd
>
> — WikiLeaks (@wikileaks) March 23, 2017

- 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 Obama administration promised to disclose all serious vulnerabilities they found to Apple, Google, Microsoft, and other US-based manufacturers. The US Government broke that commitment.

  "Year Zero" documents show that the CIA breached the Obama administration's commitments. Many of the vulnerabilities used in the CIA's cyber arsenal are pervasive and some may already have been found by rival intelligence agencies or cyber criminals.

  In addition to its operations in Langley, Virginia the CIA also uses the U.S. consulate in Frankfurt as a covert base for its hackers covering Europe, the Middle East and Africa.

  CIA hackers operating out of the Frankfurt consulate ("Center for Cyber Intelligence Europe" or CCIE) are given diplomatic ("black") passports and State Department cover.
- The CIA laughs at Anti-Virus / Anti-Malware programs.

  CIA hackers developed successful attacks against most well known anti-virus programs. These are documented in AV defeats, Personal Security Products, Detecting and defeating PSPs and PSP/Debugger/RE Avoidance. For example, Comodo was defeated by CIA malware placing itself in the Window's "Recycle Bin". While Comodo 6.x has a "Gaping Hole of DOOM".

Quite the suite of toys, no?

by Tyler Durden

Category

1. Crime-Justice-Terrorism-Corruption

2. Main
3. NWO-Deep State-Dictatorship-Tyrrany

Date Created
07/16/2022