Former CIA engineer leaked to WikiLeaks the hacking tools used by the Agency

Security Newspaper | May 18, 2018 | Important, Incidents | No Comments

A former CIA engineer is being accused of handing the documents from the Vault 7 series to WikiLeaks.

The US government claims to have identified the malicious actor who allegedly stole a data package belonging to the Central Intelligence Agency (CIA) detailing hacking tools and secret cyberespionage campaigns aimed at governments, unsuspected users and companies around the world, commented **information security** researchers.

The character has been identified as the 29-year-old former CIA engineer Joshua A. Schulte. It is believed that Schulte not only stole data but also gave them to be published to WikiLeaks.

According to researchers, the hacking tools have already been published by WikiLeaks on their website under the control of Vault 7. The stolen packages contained 8,000 documents and 943 attachments that showed how the CIA developed tools to hack their targets and convert them in espionage devices.

The list of CIA objectives has been published, it is quite broad and covers many devices, the list includes Windows, Linux and Mac-based computers, air-gapped PCs, security cameras, smart TVs, web browsers, iPhones and Android smartphones, webcams, headphones, microphones, notebooks, video players, trucks and other devices connected to the Internet. These documents showed the entire hacking capacity of the CIA.

Joshua A. Schulte is no stranger to the CIA, worked for the agency's Engineering Development Group, and helped develop malware and other hacking tools for cybernetic intelligence, information security researchers said. In 2016, Schulte left the agency and worked for a private software firm.

In 2017, a week after WikiLeaks began publishing Vault 7 documents; Schulte's department was raided by the FBI. Schulte was not formally charged, but the FBI confiscated his personal computer, notes, notebooks and passport, which prohibited him from leaving the country.

In a court statement, US attorney Matthew Laroch commented that Schulte used the Tor browser to transfer classified information, but no evidence was provided. The Tor browser allows users to hide their real IP address and browse anonymously, experts in **information security** said.

Schulte's attorneys have asked prosecutors to make a final decision on charges related to Vault 7 filtering.

"This case has been dragging on since August 2017," said Schulte's attorney, Sabrina P. Shroff. "The government is required to bring an indictment so that Mr. Schulte has an opportunity to defend himself."

Information security professionals said that when WikiLeaks published the Vault 7 series documents, it was doubtful whether these documents were authentic. Edward Snowden and Wall Street Journal confirmed its authenticity; the government investigated one of the agency's former engineers about the leak, indicating that the Vault 7 series was authentic.

List Of Leaked Vault 7 Documents

- BothanSpy and Gyrfalcon: Steals SSH credentials from Linux & Windows devices
- OutlawCountry and Elsa: Malware targeting Linux devices and tracking user geolocation

- Brutal Kangaroo: CIA hacking tools for hacking air-gapped PCs
- Cherry Blossom: CherryBlossom & CherryBomb: Infecting WiFi routers for years
- Pandemic: A malware hacking Windows devices
- AfterMidnight and Assassin: CIA remote control & subversion malware hacking Windows
- Dark Matter: CIA hacking tool infiltrating iPhones and MacBooks
- Athena: A malware targeting Windows operating system
- Archimedes: A program helping CIA to hack computers inside a Local Area Network
- HIVE: CIA implants to transfer exfiltrated information from target machines
- Grasshopper: A malware payloads for Microsoft Windows operating systems
- Marble: A framework used to hamper antivirus companies from attributing malware
- Dark Matter: A CIA project that infects Apple Mac firmware
- Highrise: An Android malware spies on SMS Messages
- Aeris, Achilles, SeaPea: 3 malware developed by CIA targeting Linux and macOS
- Dumbo Project: CIA's project hijacking webcams and microphones on Windows devices
- CouchPotato Tool: Remotely Collects Video Streams from Windows devices
- ExpressLane implant: CIA Collected Biometric Data from Partner Agencies