Joshua Adam Schulte

- U.S. Citizen
- Former CIA employee, Computer Engineer and Software Developer
- Age 35 at time of conviction

CDSE

Center for Development of Security Excellence

CASE STUDY

Espionage

WHAT HAPPENED

From approximately April of 2016 to November of 2017, a former Central Intelligence Agency (CIA) employee, Joshua Adam Shulte, leaked classified information to WikiLeaks that entailed cyber warfare and electronic surveillance tools developed by the CIA. The classified documents labeled “Vault 7” and “Vault 8” were considered one of the largest orchestrated data breaches in the history of the CIA. It was also attributed as the largest unauthorized disclosure of classified information accounts in U.S. history.

From 2012 to 2016, Shulte was employed as a computer engineer software developer at the CIA’s Center for Cyber Inntelligence (CCI). Schulte helped create the hacking tools as a coder at the Operations Support Branch at the agency’s headquarters in Langley, Virginia and had administrator privileges to one of the servers that contained the programs used to build cyber tools. It was detected that Schulte abused administrator privileges. As a result, leadership removed his privileges and transferred Schulte to another division. Schulte was also previously given a warning about granting privileges to himself that were previously revoked. Before his privileges were removed, Schulte secretly transmitted stolen CIA files to his custom desktop computer at his residence. Schulte then transferred those files to WikiLeaks and deleted any internal hard drives to cover his tracks. During the FBI’s investigation, child pornography, disturbing images from the dark web, and Russian websites were found on Schulte’s computer in encrypted files.

Schulte was arrested on August 24, 2017, and in September of 2023, he was found guilty of espionage, computer hacking, contempt of court, making false statements to the FBI and child pornography. On February 1, 2024, Schulte was sentenced to serve 40 years in prison.

INDICATORS

Access Attributes: Schulte used placement and access, while having adminstrator privileges to CIA files, to transmit classified information that revealed cyber warfare and electronic surveillance tools developed by the CIA.

Technical Activity (Security Violations): Schulte abused administrator privileges when he knowingly and willingly transmitted classified information that could be used to cause injury to the United States. This was after receiving a warning regarding self-granting privileges that were previously revoked.

Criminal Conduct:
The FBI investigation used digital forensics to discover that Schulte downloaded child pornography from the dark web and visited Russian websites.

IMPACT

U.S. Attorney Damian Williams for the Southern District of New York stated that Mr. Schulte's actions had a devastating effect on our intelligence community by providing critical intelligence to those who wish to do us harm. Mr. Williams called it "one of the most brazen and damaging acts of espionage in U.S. history."

Following the conviction of child pornography, William's stated, "Joshua Schulte has already been held accountable for endangering our nation's security, and today's verdict holds him accountable for endangering our nation's children as well."

ADDITIONAL INFO

- Due to what was considered a hostile work environment that escalated between Schulte and coworkers, Shulte left the CIA in November of 2016 and moved to New York for new employment prior to his arrest.
- Schulte's original 2020 court trial was declared a mistrial after jurors were unable to reach a verdict concerning serious criminal counts of Illegally Gathering and Transmission of National Defense Information.
- Prosecutors alleged that Schulte's motivation was retaliation for ignoring complaints about the work environment. Shulte was depicted as being uncontrollable and having extreme behaviors.
- Vault 7 and Vault 8 revealed how the CIA hacked smartphones in overseas operations, attempted to turn internet connected televisions into listening devices, and infiltrated computer networks used by foreign governments and terrorist organizations.
- While Schulte was being held at the Brooklyn Metropolitan Detention Center awaiting trial, he obtained access to cellphones that were unauthorized jail contraband. Schulte created anonymous encrypted email and social media accounts to transmit protected court discovery materials to WikiLeaks in an attempt to publish a manifesto.

Questions to consider:

- What Technical Activity can an organization use to perform checks and balances for privileged users?
- How can organizations respond to hostile work environments that have the potential to escalate?

Resources for further exploration:

- Job Aid: Insider Threat Potential Risk Indicators (PRI) (https://www.cdse.edu/Portals/124/Documents/jobaids/insider/INTJ0181-insider-threat-indicators-job-aid.pdf?ver=_HedcDtQk9sSEZItNMLQzA==)
- Counterintelligence Awareness Toolkit: FBI Economic Espionage Awareness Campaign (https://www.cdse.edu/Training/Toolkits/Counterintelligence-Awareness-Toolkit/)/)

Supporting Through Reporting!

Contact the appropriate POC to report any observed potential risk indicators:

Name: ____________________________ Agency/Department: ____________________________
Title: Supervisor/Security Officer/ITP Senior Official/ITP Manager