
SHADOW
BROKERS
AXIAL

A SURVEY ON TSB: ABOUT, WEAPON OF CHOICE, TECHNIQUES & ENGAGEMENTS

-NERDS OF AX1AL

I. ABOUT

The Shadow Brokers (TSB) is a financially motivated hacker group who first appeared in the summer of 2016. They published several leaks containing hacking tools from the National Security Agency (NSA), including several zero-day exploits. The Shadow Brokers originally attributed the leaks to the Equation Group threat actor, who has been tied to the NSA's Tailored Access Operations unit. They had breached a server where zero-days accumulated by Equation Group were held, leaked a large section on the internet, and tried to sell the rest afterward. Most of the published vulnerabilities have since been fixed by the respective vendors, but many have been used by other threat actors. Most notably among the dumps were zero-days such as ETERNALBLUE that were used for the creation of infamous ransomware explosions such as WannaCry and NotPetya. Shadow Brokers turned out to be an ex-NSA contractor named Harold T. Martin III.

II. OPERATIONS

- 2016
  - Shadow Brokers came to light when they initially publically auctioned tools obtained from NSA-based "Equation Group". The dump contained a set of exploits, implants, and tools for hacking firewalls (“firewall operations”).
  - Shadow Brokers released a second dump of tools in October as well as whining about how no one is buying their hacked NSA files.
- 2017
  - In March, ShadowBrokers published a chunk of stolen data that included two frameworks: DanderSpritz and FuzzBunch. DanderSpritz consists entirely of plugins to gather intelligence, use exploits, and examine already controlled machines. Fuzzbunch on the other hand provides a framework for different utilities to interact and work together. It contains various types of plugins designed to analyze victims, exploit vulnerabilities, schedule tasks, etc.
  - Shadow Brokers leaked NSA documents that provided a rare insight into the clandestine digital espionage operations pursued by the spy agency over the past few years, including information on operations aimed at Iran and Russia. They also released U.S. government files that show the National Security Agency may have spied on banks across the Middle East.
  - In September, Shadow Brokers are offering the exploits for $3,914,080 and promising to deliver two data dumps a month as part of its monthly dumps.
  - In the same month, they unveiled the UNITEDRAKE NSA exploit, which is a remote access and control tool that can remotely target Windows-based systems to capture desired information and transfer it to a server.

AX1AL

III. COUNTER OPERATIONS

- In October 2016, The Washington Post reported that Harold T. Martin III, a former contractor for Booz Allen Hamilton accused of stealing approximately 50 terabytes of data from the National Security Agency (NSA), was the lead suspect. The Shadow Brokers continued posting messages that were cryptographically-signed and were interviewed by media while Martin was detained.

IV. REFERENCES

- https://www.hackread.com/nsa-data-dump-shadowbrokers-expose-unitedrake-malware/
- http://securityaffairs.co/wordpress/62770/hacking/shadowbrokers-return.html
- https://www.csoonline.com/article/3190055/new-nsa-leak-may-expose-its-bank-spying-windows-exploits.html
- https://www.cyberscoop.com/nsa-shadow-brokers-leaks-iran-russia-optimusprime-stoicsurgeon/
- https://securelist.com/darkpulsar/88199/
- https://musalbas.com/blog/2016/08/16/equation-group-firewall-operations-catalogue.html