The Shadow Brokers

By Contributors to Wikimedia projects

Published: 2016-08-18 · Archived: 2026-04-05 13:12:38 UTC

From Wikipedia, the free encyclopedia

The Shadow Brokers (**TSB**) are a hacker group that emerged during the summer of 2016.[1][2] They published several leaks containing hacking tools, including several zero-day exploits,[1] from the "Equation Group" who are widely suspected to be a branch of the National Security Agency (NSA) of the United States.[3][4] Specifically, these exploits and vulnerabilities[5][6] targeted enterprise firewalls, antivirus software, and Microsoft products.[7] The Shadow Brokers originally attributed the leaks to the Equation Group threat actor, who have been tied to the NSA's Tailored Access Operations unit.[8][9][10][4]

Several news sources noted that the group's name was likely in reference to a character from the *Mass Effect* video game series.[11][12] Matt Suiche quoted the following description of that character: "The Shadow Broker is an individual at the head of an expansive organization which trades in information, always selling to the highest bidder. The Shadow Broker appears to be highly competent at its trade: all secrets that are bought and sold never allow one customer of the Broker to gain a significant advantage, forcing the customers to continue trading information to avoid becoming disadvantaged, allowing the Broker to remain in business."[13]

Equation Group leaks

[edit]

While the exact date is unclear, reports suggested that the preparation of the leak started at least in the beginning of August,[14] and that the initial publication occurred August 13, 2016 with a Tweet from a Twitter account "@shadowbrokerss" announcing a Pastebin page[6] and a GitHub repository containing references and instructions for obtaining and decrypting the content of a file supposedly containing tools and exploits used by the Equation Group. The initial response to the publication was met with some uncertainty about its authenticity.[15]

On October 31, 2016, The Shadow Brokers published a list of servers supposedly compromised by the Equation Group, as well as references to seven supposedly undisclosed tools (DEWDROP, INCISION, JACKLADDER, ORANGUTAN, PATCHICILLIN, RETICULUM, SIDETRACK AND STOICSURGEON) also used by the threat actor.[16]

On April 8, 2017, the Medium account used by The Shadow Brokers posted a new update.[17] The post revealed the password `CrDj"(;Va.*NdlnzB9M?@K2)#>deB7mN` to encrypted files released the previous year, which allegedly had more NSA hacking tools.[18] This posting explicitly stated that the post was partially in response to President Trump's attack against a Syrian airfield, which was also used by Russian forces.

April 14 hacking tool leak

[edit]

On April 14, 2017, The Shadow Brokers released, amongst other things, the tools and exploits codenamed: DANDERSPRITZ, ODDJOB, FUZZBUNCH, DARKPULSAR, ETERNALSYNERGY, ETERNALROMANCE, ETERNALBLUE, EXPLODINGCAN and EWOKFRENZY.[19][20][21]

The leak was suggested to be the "most damaging release yet"[19] and CNN quoted Matthew Hickey saying, "This is quite possibly the most damaging thing I've seen in the last several years".[22]

Some of the exploits targeting the Microsoft Windows operating system had been patched in a Microsoft Security Bulletin on March 14, 2017, a month before the leak occurred.[23][24] Some speculated that Microsoft may have been tipped off by the NSA about the release of the exploits.[25]

Over 200,000 systems were infected with tools from this leak within the first two weeks,[26] and in May 2017, the major WannaCry ransomware attack used the ETERNALBLUE exploit on Server Message Block (SMB) to spread itself.[27] The exploit was also used to help carry out the 2017 NotPetya cyberattack on June 27, 2017.[28]

ETERNALBLUE contains kernel shellcode to load the non-persistent DoublePulsar backdoor.[29] This allows for the installation of the PEDDLECHEAP payload which would then be accessed by the attacker using the DanderSpritz Listening Post (LP) software.[30][31]

Speculations and theories on motive and identity

[edit]

James Bamford along with Matt Suiche speculated[32] that an insider, "possibly someone assigned to the [NSA's] highly sensitive Tailored Access Operations", stole the hacking tools.[33][34] 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. Martin had worked with the NSA's Tailored Access Operations from 2012 to 2015 in a support role. He pleaded guilty to retaining national defense information in 2019, but it is not clear whether the Shadow Brokers obtained their material from him. The Shadow Brokers continued posting messages that were cryptographically-signed and were interviewed by media while Martin was detained.[35]

Alleged Russian ties

[edit]

Edward Snowden stated on Twitter on August 16, 2016 that "circumstantial evidence and conventional wisdom indicates Russian responsibility"[36] and that the leak "is likely a warning that someone can prove US responsibility for any attacks that originated from this malware server"[37] summarizing that it looks like "somebody sending a message that an escalation in the attribution game could get messy fast".[38][39]

The New York Times put the incident in the context of the Democratic National Committee cyber attacks and hacking of the Podesta emails. As US intelligence agencies were contemplating counter-attacks, the Shadow Brokers code release was to be seen as a warning: "Retaliate for the D.N.C., and there are a lot more secrets, from the hackings of the State Department, the White House and the Pentagon, that might be spilled as well. One senior official compared it to the scene in *The Godfather* where the head of a favorite horse is left in a bed, as a warning."[40]

In 2019, David Aitel, a computer scientist formerly employed by the NSA, summarized the situation with: "I don't know if anybody knows other than the Russians. And we don't even know if it's the Russians. We don't know at this point; anything could be true."[41]

1. ^ Jump up to: **a** **b** *Ghosh, Agamoni (April 9, 2017). "'President Trump what the f**k are you doing' say Shadow Brokers and dump more NSA hacking tools". International Business Times UK. Archived from the original on May 14, 2017. Retrieved April 10, 2017.*
2. ^ *"'NSA malware' released by Shadow Brokers hacker group". BBC News. April 10, 2017. Archived from the original on July 22, 2025. Retrieved April 10, 2017.*
3. ^ *Brewster, Thomas. "Equation = NSA? Researchers Uncloak Huge 'American Cyber Arsenal'". Forbes. Archived from the original on July 20, 2025. Retrieved November 25, 2020.*
4. ^ Jump up to: **a** **b** *Sam Biddle (August 19, 2016). "The NSA Leak is Real, Snowden Documents Confirm". The Intercept. Archived from the original on May 25, 2017. Retrieved April 15, 2017.*
5. ^ *Nakashima, Ellen (August 16, 2016). "Powerful NSA hacking tools have been revealed online". The Washington Post. Archived from the original on May 19, 2017. Retrieved August 18, 2016.*
6. ^ Jump up to: **a** **b** *"Equation Group - Cyber Weapons Auction - Pastebin.com". August 16, 2016.* `{{cite web}}` : CS1 maint: deprecated archival service (link)
7. ^ *Dan Goodin (January 12, 2017). "NSA-leaking Shadow Brokers lob Molotov cocktail before exiting world stage". Ars Technica. Archived from the original on May 24, 2017. Retrieved January 14, 2017.*
8. ^ *Goodin, Dan (August 16, 2016). "Confirmed: hacking tool leak came from "omnipotent" NSA-tied group". Ars Technica. Retrieved January 14, 2017.*
9. ^ *"The Equation giveaway - Securelist". August 16, 2016. Archived from the original on August 15, 2017. Retrieved May 19, 2020.*
10. ^ *"Group claims to hack NSA-tied hackers, posts exploits as proof". August 16, 2016. Archived from the original on May 24, 2017. Retrieved June 15, 2017.*
11. ^ *"The 'Shadow Brokers' NSA theft puts the Snowden leaks to shame - ExtremeTech". Extremetech. August 19, 2016. Archived from the original on May 3, 2017. Retrieved January 20, 2017.*
12. ^ *"Shadow Brokers: Hackers Claim to have Breached NSA's Equation Group". The Daily Dot. August 15, 2016. Archived from the original on May 27, 2017. Retrieved January 20, 2017.*
13. ^ *"Shadow Brokers: NSA Exploits of the Week". Medium.com. August 15, 2016. Archived from the original on February 14, 2017. Retrieved January 20, 2017.*
14. ^ *"The Shadow Brokers: Lifting the Shadows of the NSA's Equation Group?". August 15, 2016. Archived from the original on June 28, 2017. Retrieved August 18, 2016.*
15. ^ *Rob Price (August 15, 2016). "'Shadow Brokers' claim to have hacked an NSA-linked elite computer security unit". Business Insider. Archived from the original on June 20, 2025. Retrieved April 15, 2017.*

16. ^ *"'Shadow Brokers' Reveal List Of Servers Hacked By The NSA; China, Japan, And Korea The Top 3 Targeted Countries; 49 Total Countries, Including: China, Japan, Germany, Korea, India, Italy, Mexico, Spain, Taiwan, & Russia"*. Fortuna's Corner. November 1, 2016. Archived from the original on January 16, 2017. Retrieved January 14, 2017.
17. ^ theshadowbrokers (April 8, 2017). *"Don't Forget Your Base"*. Medium. Retrieved April 9, 2017.
18. ^ Cox, Joseph (April 8, 2017). *"They're Back: The Shadow Brokers Release More Alleged Exploits"*. Motherboard. Vice Motherboard. Retrieved April 8, 2017.
19. ^ Jump up to: **a** **b** *"NSA-leaking Shadow Brokers just dumped its most damaging release yet"*. Ars Technica. Archived from the original on May 13, 2017. Retrieved April 15, 2017.
20. ^ *"Latest Shadow Brokers dump — owning SWIFT Alliance Access, Cisco and Windows"*. Medium. April 14, 2017. Archived from the original on May 18, 2017. Retrieved April 15, 2017.
21. ^ *"misterch0c"*. GitHub. Archived from the original on April 9, 2022. Retrieved April 15, 2017.
22. ^ Larson, Selena (April 14, 2017). *"NSA's powerful Windows hacking tools leaked online"*. CNNMoney. Archived from the original on May 1, 2025. Retrieved April 15, 2017.
23. ^ *"Microsoft says users are protected from alleged NSA malware"*. AP News. Archived from the original on July 6, 2022. Retrieved April 15, 2017.
24. ^ *"Protecting customers and evaluating risk"*. MSRC. Archived from the original on October 24, 2017. Retrieved April 15, 2017.
25. ^ *"Microsoft says it already patched 'Shadow Brokers' NSA leaks"*. Engadget. April 15, 2017. Archived from the original on August 22, 2019. Retrieved April 15, 2017.
26. ^ *"Leaked NSA tools, now infecting over 200,000 machines, will be weaponized for years"*. CyberScoop. April 24, 2017. Retrieved April 24, 2017.
27. ^ *"An NSA-derived ransomware worm is shutting down computers worldwide"*. May 12, 2017. Archived from the original on July 11, 2017. Retrieved May 12, 2017.
28. ^ Perlroth, Nicole; Scott, Mark; Frenkel, Sheera (June 27, 2017). *"Cyberattack Hits Ukraine Then Spreads Internationally"*. The New York Times. p. 1. Archived from the original on April 13, 2018. Retrieved June 27, 2017.
29. ^ Sum, Zero (April 21, 2017). *"zerosum0x0: DoublePulsar Initial SMB Backdoor Ring 0 Shellcode Analysis"*. zerosum0x0. Archived from the original on August 12, 2017. Retrieved November 15, 2017.
30. ^ *"Shining Light on The Shadow Brokers"*. The State of Security. May 18, 2017. Archived from the original on September 26, 2022. Retrieved November 15, 2017.
31. ^ *"DanderSpritz/PeddleCheap Traffic Analysis"* (PDF). Forcepoint. February 6, 2018. Archived from the original (PDF) on March 27, 2023. Retrieved February 7, 2018.
32. ^ *"Shadow Brokers: The insider theory"*. August 17, 2016.
33. ^ *"Commentary: Evidence points to another Snowden at the NSA"*. Reuters. August 23, 2016. Archived from the original on February 24, 2022. Retrieved July 2, 2017.
34. ^ *"Hints suggest an insider helped the NSA "Equation Group" hacking tools leak"*. Ars Technica. August 22, 2016. Archived from the original on May 18, 2017. Retrieved June 15, 2017.
35. ^ Cox, Joseph (January 12, 2017). *"NSA Exploit Peddlers The Shadow Brokers Call It Quits"*. Motherboard.
36. ^ *"Circumstantial evidence and conventional wisdom indicates Russian responsibility. Here's why that is significant"*. Twitter. August 16, 2016. Archived from the original on August 16, 2016. Retrieved August 22,

2016.

37. ^ *"This leak is likely a warning that someone can prove US responsibility for any attacks that originated from this malware server". August 16, 2016. Retrieved August 22, 2016.*
38. ^ *"TL;DR: This leak looks like a somebody sending a message that an escalation in the attribution game could get messy fast". twitter.com. Archived from the original on August 26, 2016. Retrieved August 22, 2016.*
39. ^ *Price, Rob (August 16, 2016). "Edward Snowden: Russia might have leaked alleged NSA cyberweapons as a 'warning'". Business Insider. Archived from the original on May 1, 2025. Retrieved August 22, 2016.*
40. ^ *Eric Lipton; David E. Sanger; Scott Shane (December 13, 2016). "The Perfect Weapon: How Russian Cyberpower Invaded the U.S." New York Times. Archived from the original on May 27, 2017. Retrieved April 15, 2017.*
41. ^ *Abdollah, Tami; Tucker, Eric (July 6, 2019). "Mystery of NSA leak lingers as stolen document case winds up". Associated Press. Archived from the original on July 6, 2019.*
