The Shadow Brokers

en.wikipedia.org/wiki/The_Shadow_Brokers

Contributors to Wikimedia projects

The Shadow Brokers (**TSB**) is a hacker group who first appeared in 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]

Name and alias

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]

Leak history

First leak: "Equation Group Cyber Weapons Auction - Invitation"

While the exact date is unclear, reports suggest 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.

Publication and speculation about authenticity

The Pastebin[6] introduces a section titled "Equation Group Cyber Weapons Auction - Invitation", with the following content:

> Equation Group Cyber Chase Weapons Auction - Invitation
>
> - --
>
> !!! Attention government sponsors of cyber warfare and those who profit from it !!!!
>
> How much you pay for enemies cyber weapons? Not malware you find in networks. Both sides, RAT + LP, full state sponsor tool set? We find cyber weapons made by creators of stuxnet, duqu, flame. Kaspersky calls Equation Group. We follow Equation Group traffic. We find Equation Group source range. We hack Equation Group. We find many many Equation Group cyber weapons. You see pictures. We give you some Equation Group files free, you see. This is good proof no? You enjoy!!! You break many things. You find many intrusions. You write many words. But not all, we are auction the best files. .

The Pastebin includes various references for obtaining the file, named "EQGRP-Auction-Files.zip". This zip file contains seven files, two of which are the GPG-encrypted archives "eqgrp-auction-file.tar.xz.gpg" and "eqgrp-free-file.tar.xz.gpg". The "eqgrp-free-file.tar.xz.gpg" archive's password was revealed in the original Pastebin to be `theequationgroup`. The "eqgrp-auction-file.tar.xz" archive's password was revealed in a later Medium post to be `CrDj"(;Va.*NdlnzB9M?@K2)#>deB7mN`.

The Pastebin continues with instructions for obtaining the password to the encrypted auction file:

> Auction Instructions
>
> - --------------------
>
> We auction best files to highest bidder. Auction files better than stuxnet. Auction files better than free files we already give you. The party which sends most bitcoins to address: 19BY2XCgbDe6WtTVbTyzM9eR3LYr6VitWK before bidding stops is winner, we tell how to decrypt. Very important!!! When you send bitcoin you add additional output to transaction. You add OP_Return output. In Op_Return output you put your (bidder) contact info. We suggest use bitmessage or I2P-bote email address. No other information will be disclosed by us publicly. Do not believe unsigned messages. We will contact winner with decryption instructions. Winner can do with files as they please, we not release files to public.

The initial response to the publication was met with some skepticism,[15] as to whether or not the content actually would be "...many many Equation Group cyber weapons."[6]

Second leak: "Message #5 - TrickOrTreat"

This publication, made on October 31, 2016, contains a list of servers, supposedly compromised by 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]

Third leak: "Message #6 - BLACK FRIDAY / CYBER MONDAY SALE"

Message #6 reads as follows:

> TheShadowBrokers is trying auction. Peoples no like. TheShadowBrokers is trying crowdfunding. Peoples is no liking. Now TheShadowBrokers is trying direct sales. Be checking out ListOfWarez. If you like, you email TheShadowBrokers with name of Warez you want make purchase. TheShadowBrokers is emailing you back bitcoin address. You make payment. TheShadowBrokers emailing you link + decryption password. If not liking this transaction method, you finding TheShadowBrokers on underground marketplaces and making transaction with escrow. Files as always being signed.[17]

This leak[18] contains 60 folders named in a way to serve as reference to tools likely used by Equation Group. The leak doesn't contain executable files, but rather screenshots of the tools file structure. While the leak could be a fake, the overall cohesion between previous and future leaks and references as well as the work required to fake such a fabrication, gives credibility to the theory that the referenced tools are genuine.

Fourth leak: "Don't Forget Your Base"

On April 8, 2017, the Medium account used by The Shadow Brokers posted a new update.[19] The post revealed the password to encrypted files released last year to be `CrDj"(;Va.*NdlnzB9M?@K2)#>deB7mN`. Those files allegedly reveal more NSA hacking tools.[20] 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.

The decrypted file, eqgrp-auction-file.tar.xz, contained a collection of tools primarily for compromising Linux/Unix based environments.[21]

Fifth leak: "Lost in Translation"

On April 14, 2017, the Twitter account used by The Shadow Brokers posted a tweet with a link[22] to the Steem blockchain. Herein, a message with a link to the leak files, encrypted with the password `Reeeeeeeeeeeeeee`.

The overall content is based around three folders: "oddjob", "swift" and "windows".[23] The fifth leak is suggested to be the "...most damaging release yet"[24] and CNN quoted Matthew Hickey saying, "This is quite possibly the most damaging thing I've seen in the last several years,".[25]

The leak includes, amongst other things, the tools and exploits codenamed: DANDERSPIRITZ, ODDJOB, FUZZBUNCH, DARKPULSAR, ETERNALSYNERGY, ETERNALROMANCE, ETERNALBLUE, EXPLODINGCAN and EWOKFRENZY.[24][26][27]

Some of the exploits targeting the Windows operating system had been patched in a Microsoft Security Bulletin on March 14, 2017, one month before the leak occurred.[28][29] Some speculated that Microsoft may have been tipped off about the release of the exploits.[30]

Eternalblue

Main article: EternalBlue
Over 200,000 machines were infected with tools from this leak within the first two weeks,[31] and in May 2017, the major WannaCry ransomware attack used the ETERNALBLUE exploit on Server Message Block (SMB) to spread itself.[32] The exploit was also used to help carry out the 2017 Petya cyberattack on June 27, 2017.[33]

ETERNALBLUE contains kernel shellcode to load the non-persistent DoublePulsar backdoor.[34] This allows for the installation of the PEDDLECHEAP payload which would then be accessed by the attacker using the DanderSpritz Listening Post (LP) software.[35][36]

Speculations and theories on motive and identity

NSA insider threat

James Bamford along with Matt Suiche speculated[37] that an insider, "possibly someone assigned to the [NSA's] highly sensitive Tailored Access Operations", stole the hacking tools.[38][39] 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.[40]

Theory on ties to Russia

Edward Snowden stated on Twitter on August 16, 2016 that "circumstantial evidence and conventional wisdom indicates Russian responsibility"[41] and that the leak "is likely a warning that someone can prove responsibility for any attacks that originated from this malware server"[42] summarizing that it looks like "somebody sending a message that an escalation in the attribution game could get messy fast".[43][44]

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."[45]

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."[46]

References

1. ^ *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. Retrieved April 10, 2017.*
2. ^
3. ^ *Brewster, Thomas. "Equation = NSA? Researchers Uncloak Huge 'American Cyber Arsenal'". Forbes. Retrieved November 25, 2020.*
4. ^ *a* *b* *Sam Biddle (August 19, 2016). "The NSA Leak is Real, Snowden Documents Confirm". The Intercept. Retrieved April 15, 2017.*
5. ^ *Nakashima, Ellen (August 16, 2016). "Powerful NSA hacking tools have been revealed online". The Washington Post.*
6. ^ *a* *b* *c* *d* *"Equation Group - Cyber Weapons Auction - Pastebin.com". August 16, 2016. Archived from the original on August 15, 2016.*
7. ^ *Dan Goodin (January 12, 2017). "NSA-leaking Shadow Brokers lob Molotov cocktail before exiting world stage". Ars Technica. 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".*
10. ^ *"Group claims to hack NSA-tied hackers, posts exploits as proof". August 16, 2016.*
11. ^ *"The 'Shadow Brokers' NSA theft puts the Snowden leaks to shame - ExtremeTech". Extremetech. August 19, 2016.*
12. ^
13. ^
14. ^ *"The Shadow Brokers: Lifting the Shadows of the NSA's Equation Group?". August 15, 2016.*
15. ^ *Rob Price (August 15, 2016). "'Shadow Brokers' claim to have hacked an NSA-linked elite computer security unit". Business Insider. 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. Retrieved January 14, 2017.*
17. ^ *"MESSAGE #6 - BLACK FRIDAY / CYBER MONDAY SALE". bit.no.com. bit.no.com.*
18. ^ *"unix_screenshots.zip". bit.no.com.*

19. ^ theshadowbrokers (April 8, 2017). "Don't Forget Your Base". Medium. Retrieved April 9, 2017.
20. ^ Cox, Joseph (April 8, 2017). "They're Back: The Shadow Brokers Release More Alleged Exploits". Motherboard. Vice Motherboard. Retrieved April 8, 2017.
21. ^ "GitHub - x0rz/EQGRP: Decrypted content of eqgrp-auction-file.tar.xz". GitHub. February 26, 2022.
22. ^ "Lost in Translation". Steemit. April 14, 2017. Retrieved April 14, 2017.
23. ^ "Share". Yandex.Disk. Retrieved April 15, 2017.
24. ^ a b "NSA-leaking Shadow Brokers just dumped its most damaging release yet". Ars Technica. Retrieved April 15, 2017.
25. ^ Larson, Selena (April 14, 2017). "NSA's powerful Windows hacking tools leaked online". CNNMoney. Retrieved April 15, 2017.
26. ^ "Latest Shadow Brokers dump — owning SWIFT Alliance Access, Cisco and Windows". Medium. April 14, 2017. Retrieved April 15, 2017.
27. ^ "misterch0c". GitHub. Retrieved April 15, 2017.
28. ^ "Microsoft says users are protected from alleged NSA malware". AP News. Retrieved April 15, 2017.
29. ^ "Protecting customers and evaluating risk". MSRC. Retrieved April 15, 2017.
30. ^ "Microsoft says it already patched 'Shadow Brokers' NSA leaks". Engadget. Retrieved April 15, 2017.
31. ^ "Leaked NSA tools, now infecting over 200,000 machines, will be weaponized for years". CyberScoop. April 24, 2017. Retrieved April 24, 2017.
32. ^ "An NSA-derived ransomware worm is shutting down computers worldwide". May 12, 2017.
33. ^ Perlroth, Nicole; Scott, Mark; Frenkel, Sheera (June 27, 2017). "Cyberattack Hits Ukraine Then Spreads Internationally". The New York Times. p. 1. Retrieved June 27, 2017.
34. ^ Sum, Zero (April 21, 2017). "zerosum0x0: DoublePulsar Initial SMB Backdoor Ring 0 Shellcode Analysis". zerosum0x0. Retrieved November 15, 2017.
35. ^ "Shining Light on The Shadow Brokers". The State of Security. May 18, 2017. Retrieved November 15, 2017.
36. ^ "DanderSpritz/PeddleCheap Traffic Analysis" (PDF). Forcepoint. February 6, 2018. Retrieved February 7, 2018.
37. ^ "Shadow Brokers: The insider theory". August 17, 2016.
38. ^ "Commentary: Evidence points to another Snowden at the NSA". Reuters. August 23, 2016.
39. ^ "Hints suggest an insider helped the NSA "Equation Group" hacking tools leak". Ars Technica. August 22, 2016.
40. ^ Cox, Joseph (January 12, 2017). "NSA Exploit Peddlers The Shadow Brokers Call It Quits". Motherboard.
41. ^

42. ^ "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.
43. ^ Price, Rob (August 16, 2016). "Edward Snowden: Russia might have leaked alleged NSA cyberweapons as a 'warning'". Business Insider. Retrieved August 22, 2016.
44. ^ Eric Lipton, David E. Sanger and Scott Shane (December 13, 2016). "The Perfect Weapon: How Russian Cyberpower Invaded the U.S." New York Times. Retrieved April 15, 2017. `{{cite news}}`: CS1 maint: uses authors parameter (link)
45. ^ 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.

Hacking in the 2010s

Timeline

Major incidents

2010	Operation Aurora Australian cyberattacks Operation ShadowNet Operation Payback
2011	DigiNotar DNSChanger HBGary Federal Operation AntiSec Operation Tunisia PlayStation RSA SecurID compromise
2012	LinkedIn hack Stratfor email leak Operation High Roller
2013	South Korea cyberattack Snapchat hack Cyberterrorism Attack of June 25 2013 Yahoo! data breach Singapore cyberattacks

2014	• Anthem medical data breach • Operation Tovar • 2014 celebrity nude photo leak • 2014 JPMorgan Chase data breach • Sony Pictures hack • Russian hacker password theft • 2014 Yahoo! data breach
2015	• Office of Personnel Management data breach • Hacking Team • Ashley Madison data breach • VTech data breach • Ukrainian Power Grid Cyberattack • SWIFT banking hack
2016	• Bangladesh Bank robbery • Hollywood Presbyterian Medical Center ransomware incident • Commission on Elections data breach • Democratic National Committee cyber attacks • Vietnam Airport Hacks • DCCC cyber attacks • Indian Bank data breaches • Surkov leaks • Dyn cyberattack • Russian interference in the 2016 U.S. elections • 2016 Bitfinex hack
2017	• 2017 Macron e-mail leaks • WannaCry ransomware attack • Westminster data breach • Petya cyberattack 2017 cyberattacks on Ukraine • Equifax data breach • Deloitte breach • Disqus breach
2018	• Trustico • Atlanta cyberattack • SingHealth data breach
2019	• Sri Lanka cyberattack • Baltimore ransomware attack • Bulgarian revenue agency hack • Jeff Bezos phone hacking

Hacktivism	• Anonymous associated events • CyberBerkut • GNAA • Goatse Security • Lizard Squad • LulzRaft • LulzSec • New World Hackers • NullCrew • OurMine • PayPal 14 • RedHack • TeaMp0isoN • TDO • UGNazi • Ukrainian Cyber Alliance
Advanced persistent threats	• Bureau 121 • Charming Kitten • Cozy Bear • Dark Basin • Elfin Team • Equation Group • Fancy Bear • Guccifer 2.0 • Hacking Team • Helix Kitten • Iranian Cyber Army • Lazarus Group (BlueNorOff) (AndAriel) • NSO Group • PLA Unit 61398 • PLA Unit 61486 • PLATINUM • Pranknet • Red Apollo • Rocket Kitten • Syrian Electronic Army • Tailored Access Operations • The Shadow Brokers • Yemen Cyber Army

Individuals	• George Hotz • Guccifer • Jeremy Hammond • Junaid Hussain • Kristoffer von Hassel • Mustafa Al-Bassam • MLT • Ryan Ackroyd • Sabu • Topiary • Track2 • The Jester
Major vulnerabilities publicly disclosed	• Evercookie (2010) • iSeeYou (2013) • Heartbleed (2014) • Shellshock (2014) • POODLE (2014) • Rootpipe (2014) • Row hammer (2014) • JASBUG (2015) • Stagefright (2015) • DROWN (2016) • Badlock (2016) • Dirty COW (2016) • Cloudbleed (2017) • Broadcom Wi-Fi (2017) • EternalBlue (2017) • DoublePulsar (2017) • Silent Bob is Silent (2017) • KRACK (2017) • ROCA vulnerability (2017) • BlueBorne (2017) • Meltdown (2018) • Spectre (2018) • EFAIL (2018) • Exactis (2018) • Speculative Store Bypass (2018) • Lazy FP State Restore (2018) • TLBleed (2018) • SigSpoof (2018) • Foreshadow (2018) • Microarchitectural Data Sampling (2019) • BlueKeep (2019) • Kr00k (2019)
Malware	

2010	Bad Rabbit SpyEye Stuxnet
2011	Alureon Duqu Kelihos Metulji botnet Stars
2012	Carna Dexter FBI Flame Mahdi Red October Shamoon
2013	CryptoLocker DarkSeoul
2014	Brambul Carbanak Careto DarkHotel Duqu 2.0 FinFisher Gameover ZeuS Regin
2015	Dridex Hidden Tear Rombertik TeslaCrypt
2016	Hitler Jigsaw KeRanger MEMZ Mirai Pegasus Petya (NotPetya) X-Agent

2017	- BrickerBot - Kirk - LogicLocker - *Rensenware* ransomware - Triton - WannaCry - XafeCopy
2019	- Grum - Joanap - NetTraveler - R2D2 - Tinba - Titanium - Vault 7 - ZeroAccess botnet