The Shadow Brokers

From Wikipedia, the free encyclopedia

[Jump to navigation](https://en.wikipedia.org/wiki/The_Shadow_Brokers#mw-head)[Jump to search](https://en.wikipedia.org/wiki/The_Shadow_Brokers#searchInput)

**The Shadow Brokers** is a [hacker group](https://en.wikipedia.org/wiki/Hacker_group) who first appeared in the summer of 2016.[[1]](https://en.wikipedia.org/wiki/The_Shadow_Brokers#cite_note-:0-1)[[2]](https://en.wikipedia.org/wiki/The_Shadow_Brokers#cite_note-2) They published several leaks containing hacking tools from the [National Security Agency](https://en.wikipedia.org/wiki/National_Security_Agency) (NSA)[[3]](https://en.wikipedia.org/wiki/The_Shadow_Brokers#cite_note-ConfirmsNSA-3), including several [zero-day exploits](https://en.wikipedia.org/wiki/Zero-day_(computing)).[[1]](https://en.wikipedia.org/wiki/The_Shadow_Brokers#cite_note-:0-1) Specifically, these exploits and vulnerabilities[[4]](https://en.wikipedia.org/wiki/The_Shadow_Brokers#cite_note-4)[[5]](https://en.wikipedia.org/wiki/The_Shadow_Brokers#cite_note-pastebin.com-5) targeted enterprise [firewalls](https://en.wikipedia.org/wiki/Firewall_(computing)), [antivirus software](https://en.wikipedia.org/wiki/Antivirus_software), and [Microsoft](https://en.wikipedia.org/wiki/Microsoft) products.[[6]](https://en.wikipedia.org/wiki/The_Shadow_Brokers#cite_note-6) The Shadow Brokers originally attributed the leaks to the [Equation Group](https://en.wikipedia.org/wiki/Equation_Group) threat actor, who have been tied to the NSA's [Tailored Access Operations](https://en.wikipedia.org/wiki/Tailored_Access_Operations) unit.[[7]](https://en.wikipedia.org/wiki/The_Shadow_Brokers#cite_note-7)[[8]](https://en.wikipedia.org/wiki/The_Shadow_Brokers#cite_note-8)[[9]](https://en.wikipedia.org/wiki/The_Shadow_Brokers#cite_note-9)[[3]](https://en.wikipedia.org/wiki/The_Shadow_Brokers#cite_note-ConfirmsNSA-3)



**Contents**

* [1Name and alias](https://en.wikipedia.org/wiki/The_Shadow_Brokers#Name_and_alias)
* [2Leak history](https://en.wikipedia.org/wiki/The_Shadow_Brokers#Leak_history)
  + [2.1First leak: "Equation Group Cyber Weapons Auction - Invitation"](https://en.wikipedia.org/wiki/The_Shadow_Brokers#First_leak:_%22Equation_Group_Cyber_Weapons_Auction_-_Invitation%22)
    - [2.1.1Publication and speculation about authenticity](https://en.wikipedia.org/wiki/The_Shadow_Brokers#Publication_and_speculation_about_authenticity)
  + [2.2Second leak: "Message #5 - TrickOrTreat"](https://en.wikipedia.org/wiki/The_Shadow_Brokers#Second_leak:_%22Message_#5_-_TrickOrTreat%22)
  + [2.3Third leak: "Message #6 - BLACK FRIDAY / CYBER MONDAY SALE"](https://en.wikipedia.org/wiki/The_Shadow_Brokers#Third_leak:_%22Message_#6_-_BLACK_FRIDAY_/_CYBER_MONDAY_SALE%22)
  + [2.4Fourth leak: "Don't Forget Your Base"](https://en.wikipedia.org/wiki/The_Shadow_Brokers#Fourth_leak:_%22Don't_Forget_Your_Base%22)
  + [2.5Fifth leak: "Lost in Translation"](https://en.wikipedia.org/wiki/The_Shadow_Brokers#Fifth_leak:_%22Lost_in_Translation%22)
    - [2.5.1Eternalblue](https://en.wikipedia.org/wiki/The_Shadow_Brokers#Eternalblue)
* [3Speculations and theories on motive and identity](https://en.wikipedia.org/wiki/The_Shadow_Brokers#Speculations_and_theories_on_motive_and_identity)
  + [3.1NSA insider threat](https://en.wikipedia.org/wiki/The_Shadow_Brokers#NSA_insider_threat)
  + [3.2Theory on ties to Russia](https://en.wikipedia.org/wiki/The_Shadow_Brokers#Theory_on_ties_to_Russia)
* [4References](https://en.wikipedia.org/wiki/The_Shadow_Brokers#References)
* [5External links](https://en.wikipedia.org/wiki/The_Shadow_Brokers#External_links)

Name and alias[[edit](https://en.wikipedia.org/w/index.php?title=The_Shadow_Brokers&action=edit&section=1)]

Several news sources noted that the group's name was likely in reference to a character from the [*Mass Effect*](https://en.wikipedia.org/wiki/Mass_Effect_(series)) video game series.[[10]](https://en.wikipedia.org/wiki/The_Shadow_Brokers#cite_note-10)[[11]](https://en.wikipedia.org/wiki/The_Shadow_Brokers#cite_note-11) [Matt Suiche](https://en.wikipedia.org/wiki/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."[[12]](https://en.wikipedia.org/wiki/The_Shadow_Brokers#cite_note-12)

Leak history[[edit](https://en.wikipedia.org/w/index.php?title=The_Shadow_Brokers&action=edit&section=2)]

**First leak: "Equation Group Cyber Weapons Auction - Invitation"**[[edit](https://en.wikipedia.org/w/index.php?title=The_Shadow_Brokers&action=edit&section=3)]

While the exact date is unclear, reports suggest that the preparation of the [leak](https://en.wikipedia.org/wiki/Internet_leak) started at least in the beginning of August,[[13]](https://en.wikipedia.org/wiki/The_Shadow_Brokers#cite_note-13) and that the initial publication occurred August 13, 2016 with a Tweet from a [Twitter](https://en.wikipedia.org/wiki/Twitter) account "@shadowbrokerss" announcing a [Pastebin](https://en.wikipedia.org/wiki/Pastebin.com) page[[5]](https://en.wikipedia.org/wiki/The_Shadow_Brokers#cite_note-pastebin.com-5) and a [GitHub](https://en.wikipedia.org/wiki/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](https://en.wikipedia.org/wiki/Equation_Group).

**Publication and speculation about authenticity**[[edit](https://en.wikipedia.org/w/index.php?title=The_Shadow_Brokers&action=edit&section=4)]

The Pastebin[[5]](https://en.wikipedia.org/wiki/The_Shadow_Brokers#cite_note-pastebin.com-5) 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](https://en.wikipedia.org/wiki/Cyber_weapon)? Not malware you find in networks. Both sides, [RAT](https://en.wikipedia.org/wiki/Remote_access_trojan) + LP, full state sponsor tool set? We find cyber weapons made by creators of [stuxnet](https://en.wikipedia.org/wiki/Stuxnet), [duqu](https://en.wikipedia.org/wiki/Duqu), [flame](https://en.wikipedia.org/wiki/Flame_(malware)). [Kaspersky](https://en.wikipedia.org/wiki/Kaspersky_Lab) 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](https://en.wikipedia.org/wiki/Zip_(file_format)) contains seven files, two of which are the [GPG](https://en.wikipedia.org/wiki/GNU_Privacy_Guard)-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](https://en.wikipedia.org/wiki/Online_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,[[14]](https://en.wikipedia.org/wiki/The_Shadow_Brokers#cite_note-businessinsider_2016_NSA_TSB-14) as to whether or not the content actually would be "...many many Equation Group cyber weapons."[[5]](https://en.wikipedia.org/wiki/The_Shadow_Brokers#cite_note-pastebin.com-5)

**Second leak: "Message #5 - TrickOrTreat"**[[edit](https://en.wikipedia.org/w/index.php?title=The_Shadow_Brokers&action=edit&section=5)]

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 STOCSURGEON) also used by the threat actor.[[15]](https://en.wikipedia.org/wiki/The_Shadow_Brokers#cite_note-15)

Link to [message](https://www.reddit.com/r/DarkNetMarkets/comments/5a9wnc/message_5_trick_or_treat/)[[*dead link*](https://en.wikipedia.org/wiki/Wikipedia:Link_rot)]

Link to [material](https://mega.nz/#F!D1Q2EQpD!Lb09shM5XMZsQ_5_E1l4eQ) (Password = payus)

**Third leak: "Message #6 - BLACK FRIDAY / CYBER MONDAY SALE"**[[edit](https://en.wikipedia.org/w/index.php?title=The_Shadow_Brokers&action=edit&section=6)]

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.[[16]](https://en.wikipedia.org/wiki/The_Shadow_Brokers#cite_note-16)

This leak[[17]](https://en.wikipedia.org/wiki/The_Shadow_Brokers#cite_note-17) 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"**[[edit](https://en.wikipedia.org/w/index.php?title=The_Shadow_Brokers&action=edit&section=7)]

On April 8, 2017, the [Medium](https://en.wikipedia.org/wiki/Medium_(website)) account used by The Shadow Brokers posted a new update.[[18]](https://en.wikipedia.org/wiki/The_Shadow_Brokers#cite_note-18) 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.[[19]](https://en.wikipedia.org/wiki/The_Shadow_Brokers#cite_note-19) This posting explicitly stated that the post was partially in response to President Trump's [attack against a Syrian airfield](https://en.wikipedia.org/wiki/2017_Shayrat_missile_strike), 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.[[20]](https://en.wikipedia.org/wiki/The_Shadow_Brokers#cite_note-20)

**Fifth leak: "Lost in Translation"**[[edit](https://en.wikipedia.org/w/index.php?title=The_Shadow_Brokers&action=edit&section=8)]

On April 14, 2017, the [Twitter](https://en.wikipedia.org/wiki/Twitter) account used by The Shadow Brokers posted a tweet with a link[[21]](https://en.wikipedia.org/wiki/The_Shadow_Brokers#cite_note-steemit_TSB-21) 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".[[22]](https://en.wikipedia.org/wiki/The_Shadow_Brokers#cite_note-22) The fifth leak is suggested to be the "...most damaging release yet"[[23]](https://en.wikipedia.org/wiki/The_Shadow_Brokers#cite_note-Ars_Technica-23) and CNN quoted Matthew Hickey saying, "This is quite possibly the most damaging thing I've seen in the last several years,".[[24]](https://en.wikipedia.org/wiki/The_Shadow_Brokers#cite_note-24)

The leak includes, amongst other things, the tools and exploits codenamed: DANDERSPIRITZ, ODDJOB, FUZZBUNCH, DARKPULSAR, ETERNALSYNERGY, ETERNALROMANCE, [ETERNALBLUE](https://en.wikipedia.org/wiki/ETERNALBLUE), EXPLODINGCAN and EWOKFRENZY.[[23]](https://en.wikipedia.org/wiki/The_Shadow_Brokers#cite_note-Ars_Technica-23)[[25]](https://en.wikipedia.org/wiki/The_Shadow_Brokers#cite_note-25)[[26]](https://en.wikipedia.org/wiki/The_Shadow_Brokers#cite_note-26)

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.[[27]](https://en.wikipedia.org/wiki/The_Shadow_Brokers#cite_note-27)[[28]](https://en.wikipedia.org/wiki/The_Shadow_Brokers#cite_note-28) Some speculated that Microsoft may have been tipped off about the release of the exploits.[[29]](https://en.wikipedia.org/wiki/The_Shadow_Brokers#cite_note-29)

**Eternalblue**[[edit](https://en.wikipedia.org/w/index.php?title=The_Shadow_Brokers&action=edit&section=9)]

*Main article:*[*EternalBlue*](https://en.wikipedia.org/wiki/EternalBlue)

Over 200,000 machines were infected with tools from this leak within the first two weeks,[[30]](https://en.wikipedia.org/wiki/The_Shadow_Brokers#cite_note-30) and in May 2017, the major [WannaCry ransomware attack](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack) used the ETERNALBLUE exploit on [Server Message Block](https://en.wikipedia.org/wiki/Server_Message_Block) (SMB) to spread itself.[[31]](https://en.wikipedia.org/wiki/The_Shadow_Brokers#cite_note-31) The exploit was also used to help carry out the [2017 Petya cyberattack](https://en.wikipedia.org/wiki/2017_Petya_cyberattack) on June 27, 2017.[[32]](https://en.wikipedia.org/wiki/The_Shadow_Brokers#cite_note-32)

ETERNALBLUE contains kernel shellcode to load the non-persistent [DoublePulsar](https://en.wikipedia.org/wiki/DoublePulsar) [backdoor](https://en.wikipedia.org/wiki/Backdoor_(computing)).[[33]](https://en.wikipedia.org/wiki/The_Shadow_Brokers#cite_note-33) This allows for the installation of the PEDDLECHEAP payload which would then be accessed by the attacker using the DanderSpritz Listening Post (LP) software.[[34]](https://en.wikipedia.org/wiki/The_Shadow_Brokers#cite_note-34)[[35]](https://en.wikipedia.org/wiki/The_Shadow_Brokers#cite_note-35)

Speculations and theories on motive and identity[[edit](https://en.wikipedia.org/w/index.php?title=The_Shadow_Brokers&action=edit&section=10)]

**NSA insider threat**[[edit](https://en.wikipedia.org/w/index.php?title=The_Shadow_Brokers&action=edit&section=11)]

[James Bamford](https://en.wikipedia.org/wiki/James_Bamford) along with [Matt Suiche](https://en.wikipedia.org/wiki/Matt_Suiche) speculated[[36]](https://en.wikipedia.org/wiki/The_Shadow_Brokers#cite_note-36) that an insider, "possibly someone assigned to the [NSA's] highly sensitive [Tailored Access Operations](https://en.wikipedia.org/wiki/Tailored_Access_Operations)", stole the hacking tools.[[37]](https://en.wikipedia.org/wiki/The_Shadow_Brokers#cite_note-37)[[38]](https://en.wikipedia.org/wiki/The_Shadow_Brokers#cite_note-38) In October 2016, [*The Washington Post*](https://en.wikipedia.org/wiki/The_Washington_Post) reported that [Harold T. Martin III](https://en.wikipedia.org/wiki/Harold_T._Martin_III), a former contractor for [Booz Allen Hamilton](https://en.wikipedia.org/wiki/Booz_Allen_Hamilton) accused of stealing approximately 50 terabytes of data from the [National Security Agency](https://en.wikipedia.org/wiki/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.[[39]](https://en.wikipedia.org/wiki/The_Shadow_Brokers#cite_note-39)

**Theory on ties to Russia**[[edit](https://en.wikipedia.org/w/index.php?title=The_Shadow_Brokers&action=edit&section=12)]

[Edward Snowden](https://en.wikipedia.org/wiki/Edward_Snowden) stated on [Twitter](https://en.wikipedia.org/wiki/Twitter) on August 16, 2016 that "circumstantial evidence and conventional wisdom indicates Russian responsibility"[[40]](https://en.wikipedia.org/wiki/The_Shadow_Brokers#cite_note-twitter_Snowden_2016-40) and that the leak "is likely a warning that someone can prove responsibility for any attacks that originated from this malware server"[[41]](https://en.wikipedia.org/wiki/The_Shadow_Brokers#cite_note-41) summarizing that it looks like "somebody sending a message that an escalation in the attribution game could get messy fast".[[42]](https://en.wikipedia.org/wiki/The_Shadow_Brokers#cite_note-42)[[43]](https://en.wikipedia.org/wiki/The_Shadow_Brokers#cite_note-43)

[*The New York Times*](https://en.wikipedia.org/wiki/The_New_York_Times) put the incident in the context of the [Democratic National Committee cyber attacks](https://en.wikipedia.org/wiki/Democratic_National_Committee_cyber_attacks) and hacking of the [Podesta emails](https://en.wikipedia.org/wiki/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*](https://en.wikipedia.org/wiki/The_Godfather) where the head of a favorite horse is left in a bed, as a warning."[[44]](https://en.wikipedia.org/wiki/The_Shadow_Brokers#cite_note-44)

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."[[45]](https://en.wikipedia.org/wiki/The_Shadow_Brokers#cite_note-45)