# Equation Group

By Contributors to Wikimedia projects

Published: 2015-02-16 · Archived: 2026-04-05 18:06:46 UTC

From Wikipedia, the free encyclopedia

Equation Group

| | |
|---|---|
| **Type** | Advanced persistent threat |
| **Products** | • Stuxnet<br>• Flame<br>• EternalBlue |
| **Parent organization** | • National Security Agency<br>◦ Signals Intelligence Directorate<br>▪ Tailored Access Operations |

The **Equation Group**, also known in China as **APT-C-40**,[1][2] is a highly sophisticated threat actor suspected of being tied to the Tailored Access Operations (TAO) unit of the United States National Security Agency (NSA).[3][4][5] Kaspersky Labs describes them as one of the most sophisticated advanced persistent threats in the world and "the most advanced (...) we have seen", operating alongside the creators of Stuxnet and Flame.[6][7] Most of their targets have been in Iran, Russia, Pakistan, Afghanistan, India, Syria and Mali.[7]

The name originated from the group's extensive use of encryption. By 2015, Kaspersky documented 500 malware infections by the group in at least 42 countries, while acknowledging that the actual number could be in the tens of thousands due to its self-terminating protocol.[7][8]

In 2017, WikiLeaks published a discussion held within the CIA on how it had been possible to identify the group.[9] One commenter wrote that "the Equation Group as labeled in the report does not relate to a specific group but rather a collection of tools" used for hacking.[10]

At the Kaspersky Security Analysts Summit held in Mexico on February 16, 2015, Kaspersky Lab announced its discovery of the Equation Group. According to Kaspersky Lab's report, the group has been active since at least 2001, with more than 60 actors.[11] The malware used in their operations, dubbed EquationDrug and GrayFish, was found to be capable of reprogramming hard disk drive firmware.[6] Because of the advanced techniques involved and high degree of covertness, the group is suspected of ties to the NSA, but Kaspersky Lab has not identified the actors behind the group.

## Probable links to Stuxnet and the NSA

[edit]

In 2015 Kaspersky's research findings on the Equation Group noted that its loader, "GrayFish", had similarities to a previously discovered loader, "Gauss",[repository] from another attack series, and separately noted that the Equation Group used two zero-day attacks later used in Stuxnet; the researchers concluded that "the similar type of usage of both exploits together in different computer worms, at around the same time, indicates that the EQUATION group and the Stuxnet developers are either the same or working closely together".[12]:13

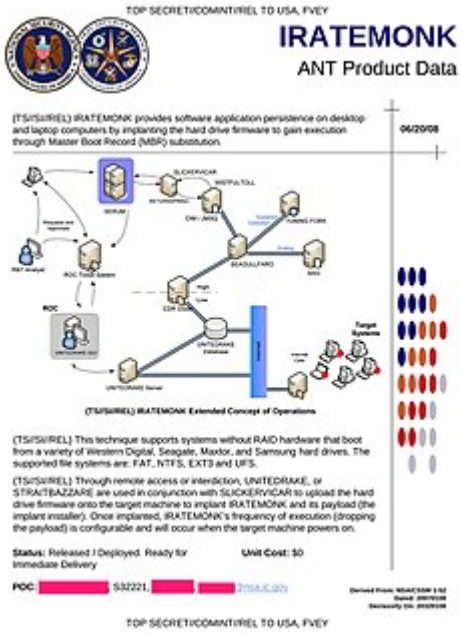
They also identified that the platform had at times been spread by interdiction (interception of legitimate CDs sent by a scientific conference organizer by mail),[12]:15 and that the platform had the "unprecedented" ability to infect and be transmitted through the hard drive firmware of several major hard drive manufacturers, and create and use hidden disk areas and virtual disk systems for its purposes, a feat which would require access to the manufacturer's source code to achieve,[12]:16–18 and that the tool was designed for surgical precision, going so far as to exclude specific countries by IP and allow targeting of specific usernames on discussion forums.[12]:23–26

### Codewords and timestamps

[edit]

The NSA codewords "STRAITACID" and "STRAITSHOOTER" have been found inside the malware. In addition, timestamps in the malware seem to indicate that the programmers worked overwhelmingly Monday–Friday in what would correspond to an 08:00–17:00 (8:00 AM - 5:00 PM) workday in an Eastern United States time zone.[13]

Kaspersky's global research and analysis team, otherwise known as GReAT, claimed to have found a piece of malware that contained Stuxnet's "privLib" in 2008.[14] Specifically it contained the LNK exploit found in Stuxnet in 2010. Fanny is classified as a worm that affects certain Windows operating systems and attempts to spread laterally via network connection or USB storage.[repository] Kaspersky stated that they suspect that the Equation Group has been around longer than Stuxnet, based on the recorded compile time of Fanny.[6]




The NSA's listing of its Tailored Access Operations program named IRATEMONK from the NSA ANT catalog.

F-Secure claims that the Equation Group's malicious hard drive firmware is TAO program "IRATEMONK",[15] one of the items from the NSA ANT catalog exposed in a 2013 *Der Spiegel* article. IRATEMONK provides the attacker with the ability to have their software application persistently installed on desktop and laptop computers, despite the disk being formatted, its data erased or the operating system re-installed. It infects the hard drive firmware, which in turn adds instructions to the disk's master boot record that causes the software to install each time the computer is booted up.[16] It is capable of infecting certain hard drives from Seagate, Maxtor, Western Digital, Samsung,[16] IBM, Micron Technology and Toshiba.[6]

## 2016 breach of the Equation Group

[edit]

In August 2016, a hacking group calling itself "The Shadow Brokers" announced that it had stolen malware code from the Equation Group.[17] Kaspersky Lab noticed similarities between the stolen code and earlier known code from the Equation Group malware samples it had in its possession including quirks unique to the Equation Group's way of implementing the RC6 encryption algorithm, and therefore concluded that this announcement is legitimate.[18] The most recent dates of the stolen files are from June 2013, thus prompting Edward Snowden to speculate that a likely lockdown resulting from his leak of the NSA's global and domestic surveillance efforts stopped The Shadow Brokers' breach of the Equation Group. Exploits against Cisco Adaptive Security Appliances and Fortinet's firewalls were featured in some malware samples released by The Shadow Brokers. EXTRABACON, a Simple Network Management Protocol exploit against Cisco's ASA software, was a zero-day exploit as of the time of the announcement. Juniper also confirmed that its NetScreen firewalls were affected.[20] The EternalBlue exploit was used to conduct the damaging worldwide WannaCry ransomware attack.

## 2022 alleged Northwestern Polytechnical University hack

[edit]

In 2022, an investigation conducted by the Chinese National Computer Virus Emergency Response Center [zh] (CVERC) and computer security firm Qihoo 360 attributed an extensive cyber attack on China's Northwestern Polytechnical University (NPU) to the NSA's Office of Tailored Access Operations (TAO),[2][21] compromising tens of thousands of network devices in China over the years and exfiltrating over 140GB of high-value data.[21]

The CVERC alleged that the attack involved a "longer period of preparatory work", setting up an anonymized attack infrastructure by leveraging SunOS zero-days to compromise institutions with large network traffic in 17 countries, 70% of which neighbored China. Those compromised machines were used as "springboards" to gain access into the NPU by leveraging man-in-the-middle and spear-phishing attacks against students and teachers. The report also claims the NSA had used two cover companies, "Jackson Smith Consultants" and "Mueller Diversified Systems", to purchase US-based IP addresses that would later be used in the FOXACID platform to launch attacks on the Northwestern.[2][21]

CVERC and 360 identified 41 different tools and malware samples during forensic analysis, many of which were similar or consistent with TAO weapons exposed in the Shadow Brokers leak. Investigators also attributed the attack to the Equation Group due to a mixture of attack times, human errors and American English keyboard inputs. Forensic analysis on one of the tools, called "NOPEN", which required human input, indicated that 98% of all attacks occurred during U.S. working hours, with no cyber-attacks being logged during weekends or during American holidays such as Memorial Day and Independence Day.[2]

- Global surveillance disclosures (2013–present)
- United States intelligence operations abroad
- Firmware hacking

1. ^ *Ionut Arghire (21 February 2025). "How China Pinned University Cyberattacks on NSA Hackers". Security Week. Retrieved 10 May 2025.*
2. ^ Jump up to: **a b c d** *Lina Lau (18 February 2025). "An inside look at NSA (Equation Group) TTPs from China's lense". Retrieved 10 May 2025.*
3. ^ *Fox-Brewster, Thomas (February 16, 2015). "Equation = NSA? Researchers Uncloak Huge 'American Cyber Arsenal'". Forbes. Retrieved November 24, 2015.*
4. ^ *Menn, Joseph (February 17, 2015). "Russian researchers expose breakthrough U.S. spying program". Reuters. Retrieved November 24, 2015.*
5. ^ *"The nsa was hacked snowden documents confirm". The Intercept. 19 August 2016. Retrieved 19 August 2016.*
6. ^ Jump up to: **a b c d** *GReAT (February 16, 2015). "Equation: The Death Star of Malware Galaxy". Securelist.com. Kaspersky Lab. Retrieved August 16, 2016. "SecureList, Costin Raiu (director of Kaspersky Lab's global research and analysis team): "It seems to me Equation Group are the ones with the coolest toys. Every now and then they share them with the Stuxnet group and the Flame group, but they are originally available only to the Equation Group people. Equation Group are definitely the masters, and they are giving the others, maybe, bread crumbs. From time to time they are giving them some goodies to integrate into Stuxnet and Flame.""*

7. ^ Jump up to: *a b c* Goodin, Dan (February 16, 2015). *"How "omnipotent" hackers tied to NSA hid for 14 years—and were found at last"*. *Ars Technica*. Retrieved November 24, 2015.
8. ^ Kirk, Jeremy (17 February 2015). *"Destroying your hard drive is the only way to stop this super-advanced malware"*. *PCWorld*. Retrieved November 24, 2015.
9. ^ Goodin, Dan (7 March 2017). *"After NSA hacking exposé, CIA staffers asked where Equation Group went wrong"*. *Ars Technica*. Retrieved 21 March 2017.
10. ^ *"What did Equation do wrong, and how can we avoid doing the same?"*. Vault 7. *WikiLeaks*. Retrieved 21 March 2017.
11. ^ *"Equation Group: The Crown Creator of Cyber-Espionage"*. Kaspersky Lab. February 16, 2015. Retrieved November 24, 2015.
12. ^ Jump up to: *a b c d* *"Equation Group: Questions and Answers (Version: 1.5)"* (PDF). *Kaspersky Lab*. February 2015. Archived from *the original* (PDF) on February 17, 2015. Retrieved November 24, 2015.
13. ^ Goodin, Dan (March 11, 2015). *"New smoking gun further ties NSA to omnipotent "Equation Group" hackers"*. Ars Technica. Retrieved November 24, 2015.
14. ^ *"A Fanny Equation: "I am your father, Stuxnet""*. Kaspersky Lab. February 17, 2015. Retrieved November 24, 2015.
15. ^ *"The Equation Group Equals NSA / IRATEMONK"*. *F-Secure* Weblog : News from the Lab. February 17, 2015. Retrieved November 24, 2015.
16. ^ Jump up to: *a b* Schneier, Bruce (January 31, 2014). *"IRATEMONK: NSA Exploit of the Day"*. Schneier on Security. Retrieved November 24, 2015.
17. ^ Goodin, Dan (August 15, 2016). *"Group claims to hack NSA-tied hackers, posts exploits as proof"*. Ars Technica. Retrieved August 19, 2016.
18. ^ Goodin, Dan (August 16, 2016). *"Confirmed: hacking tool leak came from "omnipotent" NSA-tied group"*. Ars Technica. Retrieved August 19, 2016.
19. ^ Pauli, Darren (August 24, 2016). *"Equation Group exploit hits newer Cisco ASA, Juniper Netscreen"*. *The Register*. Retrieved August 30, 2016.
20. ^ Jump up to: *a b c* *"西北工业大学遭美国NSA网络攻击事件调查报告（之一）"* (in Chinese). National Computer Virus Emergency Response Center. 5 September 2022. Retrieved 11 May 2025.

- *Equation Group: Questions and Answers* by Kaspersky Lab, Version: 1.5, February 2015
- A Fanny Equation: "I am your father, Stuxnet" by Kaspersky Lab, February 2015
- fanny.bmp source - at GitHub, November 30, 2020
- Technical Write-up - at GitHub, February 10, 2021


---