EuRepoC

ADVANCED PERSISTENT THREAT profile

Equation Group

Associated APT designations

- **Equation Group** (Kaspersky)
- **Tilded Team, Lamberts, EQGRP, Longhorn** (Symantec)
- **PLATINUM TERMINAL** (CTU)
- **G0020** (MITRE ATT&CK)

Sources: [1] [2]

Country of origin

Time period of activity

1996 (alternatively 2001) - **today**

Sources: [1]

Political affiliations

Technical threat intelligence reporting has named the Equation Group as one of the most sophisticated cyber threat actors worldwide. These assessments have associated the group with the National Security Agency (NSA), the US foreign signals intelligence (SIGINT) agency; it has specifically been linked to the former Office of Tailored Access Operations (TAO). Elements of TAO were restructured into the Computer Network Operations unit and integrated into the Information Assurance Directorate under the reorganization plan NSA21, initiated in 2016. Subsequently, parts of TAO may have been absorbed into the Cybersecurity Directorate. Created in 2019 to fuse signals intelligence and cyber defense missions, the Cybersecurity Directorate is headed by Rob Joyce, who previously served as Deputy Director of the now-defunct Information Assurance Directorate and also as Director of Tailored Access Operations. The Equation Group was likely involved in the development of Stuxnet, which is widely considered to be part of the cyber operation "Olympic Games," initiated by former US President George W. Bush and continued by his successor, Barack Obama. Reports by Kaspersky, the IT security firm which first discovered the group, suggested a close connection to actors involved in Stuxnet. An NSA spokesperson declined to comment on these findings. However, at least one unnamed former NSA official has since confirmed this information. Through the connection to the NSA, the Equation Group is also linked to the Five Eyes intelligence alliance.

Sources: [2] [3] [4] [5] [6] [31] [32] [33]

By Kerstin Zettl-Schabath, Lena Rottinger and Camille Borrett

November 2022

Agency type

State-integrated group (military intelligence service/agency members; NSA's TAO Unit)

Sources: [1] [2] [3]

Most frequent targets:

- Afghanistan
- Algeria
- Bangladesh
- Belgium
- Brazil
- Cambodia
- China
- Ecuador
- France
- Germany
- Hong Kong
- India
- Indonesia
- Iran
- Iraq
- Kazakhstan
- Libya
- Malaysia
- Mali
- Mexico
- Nigeria
- Pakistan
- Philippines
- Qatar
- Russia
- Singapore
- Somalia
- South Africa
- Sudan
- Switzerland
- Syria
- UAE
- United Kingdom
- USA
- Vietnam
- Yemen

Sources: [1] [3]

Group composition/organisational structure

There is not much information on the group's organization and structure, but due to their extreme sophistication and technical capabilities, the group was attributed to the NSA. An article in The New York Times reported that US President Obama was regularly informed about the progress of the "Olympic Games"/Stuxnet-Operation, suggesting that the US government was in control of key operational decisions.

Sources: [2] [5]

Impact type(s)

Direct

- **Intelligence impact**
- **Functional impact (physical effects)**
  (Stuxnet – see Landmark incidents p.6)

Sources: [2] [3] [4] [5] [6] [7]

Incident type(s)

- **Cyber espionage**
- **Physical destruction through data manipulation**

EuRepoC codes: *Hijacking with misuse; data theft; disruption*

Sources: [3] [7]

Threat Level Index

14.5/24 high threat

Index scoring scale

Score	Label
≤6	Low
>6 - ≤12	Medium
>12 - ≤18	High
>18 – 24	Very high

The Threat Level Index is derived from the EuRepoC dataset 1.0. It is a composite indicator covering five dimensions: the **sectorial** and **geographical scope** of the APT's attacks, the **intensity** of the attacks, the **frequency** of attacks and the **use of zero-days**. Please note that only attacks that have been publicly attributed to the APT group during its period of activity and which meet the specific EuRepoC criteria for inclusion are considered. The scores account for the practice of other APT groups analysed by EuRepoC, as thresholds used for determining low/high scores are based on the range of scores obtained across multiple APT groups. For more detailed information on the methodology underpinning the Threat Level Index see here.

Breakdown of the scores for the Equation Group:

Sub-indicator	Score	Explanation
Intensity of attacks	1 /5	This sub-indicator represents the average "Weighted Cyber Intensity" score from the EuRepoC codebook for all attacks attributed to the APT for its period of activity. It assesses the type of attacks, their potential physical effects, and their socio-political severity – see here for more information.
Sectorial scope of attacks	4.5 /8	This sub-indicator calculates average number of targeted sectors per attack attributed to the APT groups over its period of activity. If the majority of the targeted sectors are critical to the functioning of the targeted societies (i.e. political systems and critical infrastructure) a multiplier is applied. On average, attacks attributed to the Equation Group within the EuRepoC database, targeted two types of sectors (leading to a converted score of 3/4). In addition, as 81% of the attacks were against political systems and/or critical infrastructure, the score was multiplied by 1.5.
Geographical scope of attacks	3 /4	This sub-indicator considers the average number of targeted countries per attack attributed to the APT group. Whole regions or continents affected during one attack are weighted higher. In the case of the Equation Group, for most of the attacks attributed to the group within the EuRepoC database, multiple countries and in some cases entire regions were targeted.
Frequency of attacks	3 /4	This sub-indicator is calculated by dividing the total number of attacks attributed to the APT group within the EuRepoC database by the number of years of activity of the APT group. The obtained scores are then converted to a four-level scale. On average, the Equation Group was held responsible for 1 attack per year of activity.
Exploitation of Zero days	3 /3	This indicator calculates the percentage of attacks attributed to the APT that make use of one or multiple zero days. The obtained score is then converted to a three-level scale. 12% of the attacks attributed to the Equation Group exploited zero-days.

→ Overall, the Equation Group obtains a high-level threat score compared to other APT groups. The attacks analysed within the EuRepoC framework often targeted multiple countries/regions in one go; were comparatively frequent, and a comparatively high proportion of these attacks exploited zero-days.

TECHNICAL CHARACTERISTICS / PECULIARITIES / SOPHISTICATION

According to the Russian IT-security firm Kaspersky, the Equation Group is "one of the most sophisticated cyber-attack groups in the world" due to their ability to infect hard drive firmware. They use a specific implementation of the RC5 and other versions of the encryption algorithm as obfuscation strategy. The group is known for their surgical precision during a target infection, indicating that they are capable of conducting thorough target intelligence and analysis before the actual payload delivery.

Basic attack pattern

(1) **Victim infection:** the group uses different techniques; among them are: web-based exploits, self-replicating worms (e.g., "Fanny"), interdiction and manipulation of legitimate physical media and electronics, USB-sticks in combination with exploits.

(2) Use of **DoubleFantasy (validator-style plugin) to infiltrate a network** and to discover whether the victim is "interesting" enough for further activity.

(3) If the target is rated important, **Equationdrug or Grayfish** (depending on the target's operating system) is installed via a backdoor created in step (2). Both malwares are considered to be the most complex espionage platforms to date and allow the groups **to have full control over the infiltrated operating system**.

Zero-Day exploits

The Equation Group has deployed zero-day-exploits against four of the following vulnerabilities; reporting by Kaspersky did not specify the exact targeting: CVE-2010-2568 (used for Stuxnet), MS09-025 (used for Flame and Stuxnet), CVE-2012-0159 (possibly), CVE-2013-3894 (possibly), CVE-2012-1723, CVE-2012-4681.

Malware used (non-exhaustive)

Equation Laser	EquationDrug	DoubleFantasy
DoubleFeature	TripleFantasy	Fanny
Grayfish	Gauss	Equestre
Stuxnet	Flame	

Techniques used (non-exhaustive)

Persistence: Pre-OS Boot (Component Firmware); **Defense Evasion:** Execution Guardrails (Environmental Keying), Hide Artifacts (Hidden File System); **Discovery:** Peripheral Device Discovery

Sources: [1] [7] [8] [9] [10] [11]

Select tactics and techniques leveraged by the group based on the MITRE ATT&CK Framework

MITRE Persistence

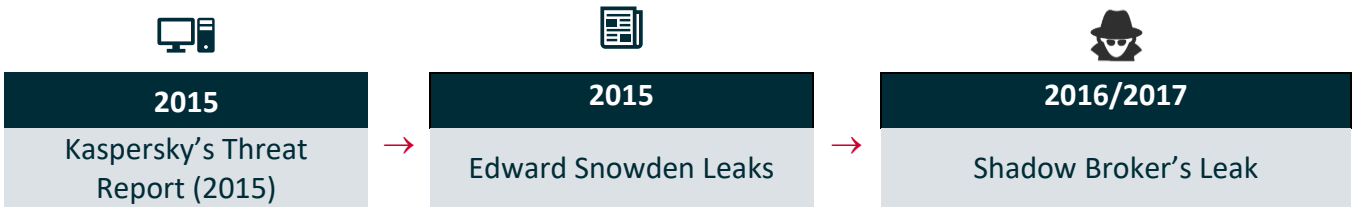
Pre-OS boot

MITRE Defense Evasion

Execution guardrails
Hide Artifacts
Pre-OS boot

ATTRIBUTION

Attribution milestones



Sources: [1] [2] [6] [12] [13]

Attribution controversies

Equation Group behind Regin?

The Cyber Operations Tracker by the Council on Foreign Relations indicates a relationship/association between the Regin malware and the Equation Group. However, in its extensive report about the Equation Group, Kaspersky did not indicate that it is the same as the group responsible for Regin. Instead, the Regin malware is usually associated with the Five Eyes intelligence alliance, but not the Equation Group in particular.

Equation Group equivalent to TAO?

Public reporting, including by Nicole Perlroth in 2021, indicates that the Equation Group is the private sector designation for NSA´s TAO as a whole. Nevertheless, given the reported size of more than 1000 employed hacking specialists (estimate as of June 2022), it seems plausible that the unit is divided into smaller sub-units, of which Equation Group could be just one of many.

Sources: [1] [14] [24] [25] [26] [28]

Attribution-/detection sensitivity

The group is known for their extremely sophisticated encryption and obfuscation techniques, thereby increasing the difficulty to detect them. Some of their operations were running for 15-20 years without being detected, which speaks to their unparalleled capabilities in terms of detection-evasion.

Sources: [1] [2]

LEGAL AND POLITICAL ACTIONS TAKEN AGAINST THE GROUP

Political/Legal/Law enforcement actions

There are no concrete political/legal or law enforcement actions tied to this particular group. However, their discovery shed light on the far-reaching US cyber espionage operations, which target not only their political enemies, but also their political allies (e.g., EU member states), which has caused some political tension between the US and its partners. An example is the so-called "no-spy deal" that the German (and French) government(s) tried to establish after an unidentified leak disclosed that chancellor Angela Merkel`s mobile phone had been spied on by the NSA.

Sources: [3] [27] [28]

Indicted individuals / sanctioned (associated) entities

There have been no indictments against members of the group so far (July 2022).

Landmark incidents

Fanny:

Fanny was created by the group in 2008 with the purpose of mapping air-gapped networks. The worm was distributed via a unique USB command-and-control technique in Asia and the Middle East. The countries mostly affected by Fanny were Pakistan, Indonesia, and Vietnam.

Sources: [1] [7] [15]

“Flame” (2007-2012):

According to public attributions, the US and Israeli intelligence agencies developed the sophisticated computer virus for wide-reaching cyber espionage campaigns. This virus was also created to prepare cyber-sabotage acts in Iran and is therefore considered a precursor of Stuxnet. It was spread via the abuse of Microsoft's software update mechanism. The Russian IT-security firm Kaspersky reported that Flame contained parts of the same code as Stuxnet, which is why at least a cooperation in the early stages of code development is very likely. Shortly after the discovery of Flame, its creators sent an updated command to many affected computers, which was designed to remove the malware and the command entirely. Although the Equation group hasn't been linked directly to Flame, they likely interacted and cooperated with the actors behind Flame from a position of superiority, since they had access to several zero-days before they were used in this operation.

Sources: [14] [15] [16] [17] [18] [19] [20] [21] [22]

“Stuxnet” (2008-2010):

It is plausible that Equation group malware was used to deliver later versions of the Stuxnet worm to Iran's Natanz facility, after the attackers had lost insider access, given the group's experience in infiltrating air-gapped computer networks. Stuxnet is considered to be the most sophisticated cyber-attack to this day (July 2022). The attackers were able to infiltrate the high-security nuclear facility in Natanz and managed to sabotage several gas centrifuges over time in such a way that uranium enrichment had to be interrupted. Many experts believe US-American and Israeli intelligence agencies (NSA and Unit 8200) were responsible for the attack, more precisely NSA's TAO, which New York Times journalist Nicole Perlroth describes as equivalent to the Equation Group. These connections appear to be corroborated by the fact that the Equation group had access to several zero-day exploits and utilized them even before they were used in the Stuxnet operation.

Sources: [1] [5] [7] [14] [23] [26] [29] [30]

SOURCES

[1] Kaspersky (2015), *Equation Group: Questions and Answers*, Version 1.5. Available at: https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/08064459/Equation_group_questions_and_answers.pdf [Last accessed: 20.10.2022]

[2] Brewster, T. (2015), *Equation = NSA? Researchers Uncloack Huge 'American Cyber Arsenal'*, Forbes. Available at: https://www.forbes.com/sites/thomasbrewster/2015/02/16/nsa-equation-cyber-tool-treasure-chest/ : [Last accessed: 20.10.2022]

[3] Menn, J. (2015), *Russian researchers expose breakthrough U.S. spying program*, Reuters. Available at: https://www.reuters.com/article/us-usa-cyberspying-idUSKBN0LK1QV20150216 : [Last accessed: 20.10.2022]

[4] Cimpanu, C. (2017), *Longhorn Cyber-Espionage Group Is Actually the CIA*, Bleeping Computer. Available at: https://www.bleepingcomputer.com/news/security/longhorn-cyber-espionage-group-is-actually-the-cia/ [Last accessed: 14.11.2022]

[5] Sanger, E., D. (2012), *Obama Order Sped Up Wave of Cyberattacks Against Iran,* New York Times. Available at: https://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?_r=2&smid=tw-nytimes&seid=auto&pagewanted=all [Last accessed: 14.11.2022]

[6] Biddle, S. (2016), *The NSA Leak Is Real, Snowden Documents Confirm, The Intercept*. Available at: https://theintercept.com/2016/08/19/the-nsa-was-hacked-snowden-documents-confirm/ [Last accessed: 14.11.2022]

[7] Goodin, D. (2015), *How "omnipotent" hackers tied to NSA hid for 14 years—and were found at last*, ARS Technica. Available at: https://arstechnica.com/information-technology/2015/02/how-omnipotent-hackers-tied-to-the-nsa-hid-for-14-years-and-were-found-at-last/ [Last accessed: 14.11.2022]

[8] Securelist (2015), A Fanny Equation: "I am your father, Stuxnet", Kaspersky. Available at: https://securelist.com/a-fanny-equation-i-am-your-father-stuxnet/68787/ [Last accessed: 14.11.2022]

[9] MITRE (2017), Equation. Available at: https://attack.mitre.org/groups/G0020/ [Last accessed: 14.11.2022]

[10] Goodin, D. (2016), *Confirmed: hacking tool leak came from "omnipotent" NSA-tied group*, ARS Technica. Available at: https://arstechnica.com/information-technology/2016/08/code-dumped-online-came-from-omnipotent-nsa-tied-hacking-group/

[11] Checkpoint (2021), *A Deep Dive into DoubleFeature, Equation Group's Post-Exploitation Dashboard*. Available at: https://research.checkpoint.com/2021/a-deep-dive-into-doublefeature-equation-groups-post-exploitation-dashboard/ [Last accessed: 14.11.2022]

[12] Cimpanu, C. (2017), *Shadow Brokers Release New Files Revealing Windows Exploits, SWIFT Attacks, Bleeping Computer*. Available at: https://www.bleepingcomputer.com/news/security/shadow-brokers-release-new-files-revealing-windows-exploits-swift-attacks/ [Last accessed: 14.11.2022]

[13] Menn, J. (2015), *Russian researchers expose breakthrough U.S. spying program*, Reuters. Available at: https://www.reuters.com/article/idUSL1N0VN15J20150216 [Last accessed: 14.11.2022]

[14] Kaspersky (2015), *Equation Group: The Crown Creator of Cyber-Espionage*. Available at: https://www.kaspersky.com/about/press-releases/2015_equation-group-the-crown-creator-of-cyber-espionage [Last accessed: 14.11.2021]

[15] Securelist (2015), *Equation: The Death Star of Malware Galaxy*. Available at: https://securelist.com/equation-the-death-star-of-malware-galaxy/68750/ [Last accessed: 14.11.2022]

[16] Kaspersky (2012), *Kaspersky Lab Experts Provide In-Depth Analysis of Flame's C&C Infrastructur*e. Available at: https://www.kaspersky.com/about/press-releases/2012_kaspersky-lab-experts-provide-in-depth-analysis-of-flame-s-c-c-infrastructure [Last accessed: 14.11.2022]

[17] Goodin, D. (2012), *Crypto breakthrough shows Flame was designed by world-class scientists*, ARS Technica. Available at: https://arstechnica.com/information-technology/2012/06/flame-crypto-breakthrough/ [Last accessed: 14.11.2021]

[18] Nakashima, E., Miller, G. (2012), *U.S., Israel developed Flame computer virus to slow Iranian nuclear efforts, officials say*, The Washington Post. Available at: https://www.washingtonpost.com/world/national-security/us-israel-developed-computer-virus-to-slow-iranian-nuclear-efforts-officials-say/2012/06/19/gJQA6xBPoV_story.html [Last accessed: 14.11.2022]

[19] Heise (2012), *Bericht: Israel und USA entwickelten Flame*. Available at: https://www.heise.de/security/meldung/Bericht-Israel-und-USA-entwickelten-Flame-1621770.html [Last accessed: 14.11.2022]

[20] Spiegel (2012), *Virenforscher halten Flame für Stuxnet-Cousin*. Available at: https://www.spiegel.de/netzwelt/netzpolitik/kaspersky-flame-und-stuxnet-sind-verwandt-a-838249.html [Last accessed: 14.11.2022]

[21] Johnson, A. L. (2012), *Flamer: Urgent Suicide, Broadcom*. Available at: https://community.broadcom.com/symantecenterprise/communities/community-home/librarydocuments/viewdocument?DocumentKey=b17110bd-8387-4c38-b27e-7c875ca98021&CommunityKey=1ecf5f55-9545-44d6-b0f4-4e4a7f5f5e68&tab=librarydocuments [Last accessed: 14.11.2022]

[22] Spiegel (2012), *Flame-Virus erhält Selbstmordbefehl.* Available at: https://www.spiegel.de/netzwelt/web/flame-virus-soll-sich-selbst-loeschen-a-838081.html [Last accessed: 14.11.2022]

[23] Heise (2012), *Obama ordnete angeblich Stuxnet-Einsatz an*. Available at: https://www.heise.de/newsticker/meldung/Obama-ordnete-angeblich-Stuxnet-Einsatz-an-1588466.html

[24] Rosenbach, M., Hilmar, S., Stöcker, C. (2015), *Experts Unmask 'Regin" Trojan as NSA Tool*, Spiegel. Available at: https://www.spiegel.de/international/world/regin-malware-unmasked-as-nsa-tool-after-spiegel-publishes-source-code-a-1015255.html [Last accessed: 14.11.2022]

[25] Council on Foreign Relations (CFR), *Regin*. Available at: https://www.cfr.org/cyber-operations/regin [Last accessed: 14.11.2022]

[26] Perlroth, N. (2021), *This is how they tell me the world ends, The Cyberweapons Arms Race*. Available at: https://www.bloomsbury.com/us/this-is-how-they-tell-me-the-world-ends-9781635576061/ [Last accessed: 14.11.2022]

[27] BBC (2013), *US bugged Merkel's phone from 2002 until 2013, report claims*. Available at: https://www.bbc.com/news/world-europe-24690055 [Last accessed: 14.11.2022]

[28] Siwei, Z. (2022), *Exclusive: Report reveals how US spy agencies stole 97b global internet data, 124b phone records in just 30 days, Global Times*. Available at: https://www.globaltimes.cn/page/202206/1268024.shtml [Last accessed: 14.11.2022]

[29] Zetter, K., Modderkolk, H. (2019), *Revealed: How a secret Dutch mole aided the U.S.-Israeli Stuxnet cyberattack on Iran*. Available at: https://news.yahoo.com/revealed-how-a-secret-dutch-mole-aided-the-us-israeli-stuxnet-cyber-attack-on-iran-160026018.html [Last accessed: 14.11.2022]

[30] Langner, R. (2013), *To kill a centrifuge: A technical analysis of what Stuxnet's creators tried to achieve*. Available at: https://www.langner.com/to-kill-a-centrifuge/ [Last accessed: 14.11.2022]

[31] Council on Foreign Relations (CFR), *Equation Group*. Available at: https://www.cfr.org/cyber-operations/equation-group [Last accessed: 14.11.2022]

[32] Bing, C. (2017), *Meet the man responsible for teaching some of the NSA's best young hackers*, FedScoop. Available at: https://www.fedscoop.com/meet-the-man-responsible-for-teaching-some-of-the-nsas-best-young-hackers/ [Last accessed: 14.11.2022]

[33] NSA (2021), Rob Joyce begins as NSA's Director of Cybersecurity. Available at: https://www.nsa.gov/Press-Room/News-Highlights/Article/Article/2567021/rob-joyce-begins-as-nsas-director-of-cybersecurity/ [Last accessed: 14.11.2022]

Calculations for the Threat Level Index Indicator are based on version 1.0 of the EuRepoC Database downloadable here: https://strapi.eurepoc.eu/uploads/Eu_Repo_C_Global_Database_1_0_22d4a4aee7.xlsx

Last updated: 05.12.2022