Equation Group

Equation Group

Type	Advanced persistent threat
Location	United States
Products	Stuxnet, Flame, EternalBlue
Parent organization	National Security Agency Signals Intelligence Directorate Tailored Access Operations

The **Equation Group**, classified as an advanced persistent threat, 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).[1][2][3] Kaspersky Labs describes them as one of the most sophisticated cyber attack groups in the world and "the most advanced ... we have seen", operating alongside the creators of Stuxnet and Flame.[4][5] Most of their targets have been in Iran, Russia, Pakistan, Afghanistan, India, Syria, and Mali.[5]

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.[5][6]

In 2017, WikiLeaks published a discussion held within the CIA on how it had been possible to identify the group.[7] 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.[8]

Discovery

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.[9] The malware used in their operations, dubbed EquationDrug and GrayFish, is found to be capable of reprogramming hard disk drive firmware.[4] 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

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".[10]:13

Firmware

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),[10]: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,[10]: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.[10]:23–26

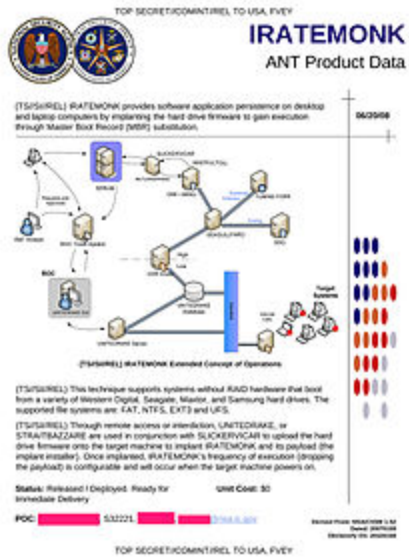
Codewords and timestamps

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 a 08:00–17:00 (8:00 AM - 5:00 PM) workday in an Eastern United States time zone.[11]

The LNK exploit

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.[12] 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.[4]

Link to IRATEMONK



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",[13] one of the items from the NSA ANT catalog exposed in a 2013 *Der Spiegel* article. IRATEMONK provides the attacker with an 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.[14] It is capable of infecting certain hard drives from Seagate, Maxtor, Western Digital, Samsung,[14] IBM, Micron Technology and Toshiba.[4]

2016 breach of the Equation Group

In August 2016, a hacking group calling itself "The Shadow Brokers" announced that it had stolen malware code from the Equation Group.[15] 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.[16] 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.[17] EXTRABACON, a Simple Network Management Protocol exploit against Cisco's ASA software, was a zero-day exploit as of the time of the announcement.[17] Juniper also confirmed that its NetScreen firewalls were affected.[18] The EternalBlue exploit was used to conduct the damaging worldwide WannaCry ransomware attack.

See also

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

References

1. ^ *Fox-Brewster, Thomas (February 16, 2015). "Equation = NSA? Researchers Uncloak Huge 'American Cyber Arsenal'". Forbes. Retrieved November 24, 2015.*
2. ^ *Menn, Joseph (February 17, 2015). "Russian researchers expose breakthrough U.S. spying program". Reuters. Retrieved November 24, 2015.*
3. ^
4. ^ 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."*
5. ^ 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.*
6. ^ *Kirk, Jeremy (17 February 2015). "Destroying your hard drive is the only way to stop this super-advanced malware". PCWorld. Retrieved November 24, 2015.*
7. ^ *Goodin, Dan (7 March 2017). "After NSA hacking exposé, CIA staffers asked where Equation Group went wrong". Ars Technica. Retrieved 21 March 2017.*
8. ^ *"What did Equation do wrong, and how can we avoid doing the same?". Vault 7. WikiLeaks. Retrieved 21 March 2017.*
9. ^ *"Equation Group: The Crown Creator of Cyber-Espionage". Kaspersky Lab. February 16, 2015. Retrieved November 24, 2015.*
10. ^ 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.*
11. ^ *Goodin, Dan (March 11, 2015). "New smoking gun further ties NSA to omnipotent "Equation Group" hackers". Ars Technica. Retrieved November 24, 2015.*
12. ^ *"A Fanny Equation: "I am your father, Stuxnet"". Kaspersky Lab. February 17, 2015. Retrieved November 24, 2015.*
13. ^ *"The Equation Group Equals NSA / IRATEMONK". F-Secure Weblog : News from the Lab. February 17, 2015. Retrieved November 24, 2015.*
14. ^ a b *Schneier, Bruce (January 31, 2014). "IRATEMONK: NSA Exploit of the Day". Schneier on Security. Retrieved November 24, 2015.*
15. ^ *Goodin, Dan (August 15, 2016). "Group claims to hack NSA-tied hackers, posts exploits as proof". Ars Technica. Retrieved August 19, 2016.*

16. ^ *Goodin, Dan (August 16, 2016). "Confirmed: hacking tool leak came from "omnipotent" NSA-tied group". Ars Technica. Retrieved August 19, 2016.*
17. ^ a b *Thomson, Iain (August 17, 2016). "Cisco confirms two of the Shadow Brokers' 'NSA' vulns are real". The Register. Retrieved August 19, 2016.*
18. ^ *Pauli, Darren (August 24, 2016). "Equation Group exploit hits newer Cisco ASA, Juniper Netscreen". The Register. Retrieved August 30, 2016.*

External links

Wikimedia Commons has media related to Equation Group.

- *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

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

- Grum
- Joanap
- NetTraveler
- R2D2
- Tinba
- Titanium
- Vault 7
- ZeroAccess botnet

2019