Equation Group - Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 13:07:03 UTC

APT group: Equation Group

Names	Equation Group *(real name)* Tilded Team *(CrySys)* Platinum Colony *(SecureWorks)* APT-C-40 *(Qihoo 360)* G0020 *(MITRE)*
Country	USA
Sponsor	State-sponsored, believed to be tied to the NSA's Tailored Access Operations unit
Motivation	Information theft and espionage, Sabotage and destruction
First seen	2001
Description	(Ars Technica) Kaspersky researchers have documented 500 infections by Equation Group in at least 42 countries, with Iran, Russia, Pakistan, Afghanistan, India, Syria, and Mali topping the list. Because of a self-destruct mechanism built into the malware, the researchers suspect that this is just a tiny percentage of the total; the actual number of victims likely reaches into the tens of thousands. A long list of almost superhuman technical feats illustrate Equation Group's extraordinary skill, painstaking work, and unlimited resources. They include: • The use of virtual file systems, a feature also found in the highly sophisticated Regin malware. Recently published documents provided by Ed Snowden indicate that the NSA used Regin to infect the partly state-owned Belgian firm Belgacom. • The stashing of malicious files in multiple branches of an infected computer's registry. By encrypting all malicious files and storing them in multiple branches of a computer's Windows registry, the infection was impossible to detect using antivirus software. • Redirects that sent iPhone users to unique exploit Web pages. In addition, infected machines reporting to Equation Group command servers identified themselves as Macs, an indication that the group successfully compromised both iOS and OS X devices. • The use of more than 300 Internet domains and 100 servers to host a sprawling command and control infrastructure.

	• USB stick-based reconnaissance malware to map air-gapped networks, which are so sensitive that they aren't connected to the Internet. Both Stuxnet and the related Flame malware platform also had the ability to bridge airgaps. • An unusual if not truly novel way of bypassing code-signing restrictions in modern versions of Windows, which require that all third-party software interfacing with the operating system kernel be digitally signed by a recognized certificate authority. To circumvent this restriction, Equation Group malware exploited a known vulnerability in an already signed driver for CloneCD to achieve kernel-level code execution. Taken together, the accomplishments led Kaspersky researchers to conclude that Equation Group is probably the most sophisticated computer attack group in the world, with technical skill and resources that rival the groups that developed Stuxnet and the Flame espionage malware in Operation Olympic Games. Other publicly exposed major APT activities from the NSA involve the wholesale worldwide spying from programs such as PRISM and, together with GCHQ, INCENSER, where various international Internet trunks were tapped. China's Ministry of State Security (MSS) has accused the U.S. of breaking into Huawei's servers, stealing critical data, and implanting backdoors since 2009, amid mounting geopolitical tensions between the two countries.	
Observed	Sectors: Aerospace, Defense, Education, Energy, Government, Media, Oil and gas, Telecommunications, Transportation and Nanotechnology, Nuclear research, Islamic activists and scholars, and companies developing cryptographic technologies. Countries: Afghanistan, Algeria, Austria, Bangladesh, Belgium, Bolivia, Bosnia and Herzegovina, Botswana, Brazil, Chile, China, Cyprus, Ecuador, Egypt, Finland, France, Gabon, Germany, Greece, Hong Kong, Hungary, India, Iran, Iraq, Israel, Italy, Japan, Jordan, Kazakhstan, Kenya, Lebanon, Libya, Malaysia, Mali, Mexico, Netherlands, Nicaragua, Nigeria, Norway, Pakistan, Palestine, Philippines, Poland, Qatar, Romania, Russia, Saudi Arabia, Singapore, Somalia, South Africa, South Korea, Spain, Sudan, Sweden, Switzerland, Syria, Thailand, Turkey, UAE, UK, USA, Venezuela, Yemen.	
Tools used	Bvp47, DanderSpritz, DarkPulsar, DOUBLEFANTASY, DoubleFeature, DoublePulsar, Duqu, EQUATIONDRUG, EQUATIONLASER, FANNY, Flame, GRAYFISH, GROK, Lambert, OddJob, Regin, TRIPLEFANTASY, UNITEDRAKE and many others.	
Counter operations	Aug 2016	Their arsenal of 0-day cyber weapons was stolen by an actor Shadow Brokers, who leaked a large section on the internet and tried to sell the rest afterward. Most notable among the dumps were 0-days such as ETERNALBLUE and ETERNALROMANCE that were used by other groups for the creation of infamous ransomware explosions such as WannaCry and NotPetya.

Information	<https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/08064459/Equation_group_questions_and_answers.pdf> <https://arstechnica.com/information-technology/2015/02/how-omnipotent-hackers-tied-to-the-nsa-hid-for-14-years-and-were-found-at-last/> <https://en.wikipedia.org/wiki/Equation_Group> <https://en.wikipedia.org/wiki/PRISM_(surveillance_program)> <https://www.electrospaces.net/2014/11/incenser-or-how-nsa-and-gchq-are.html> <https://www.inversecos.com/2025/02/an-inside-look-at-nsa-equation-group.html>
MITRE ATT&CK	<https://attack.mitre.org/groups/G0020/>

Last change to this card: 16 August 2025

Download this actor card in PDF or JSON format
