Equation APT Group - Brandefense

Published: 2022-09-05 · Archived: 2026-04-05 15:38:05 UTC

Group’s Mission and Vision

Equation Group has been conducting cyber operations since 2001 (perhaps it could even start in 1996), and it is known for its sophisticated methods. The group was discovered in 2014 by Kaspersky Lab. This group uses encryption and obfuscation a lot. That is why they are called “Equation Group.” This group uses zero-days, gains persistence by reprogramming hard drive firmware, and if anything goes wrong, malware destroys itself. This group is linked with Stuxnet and Flame groups since Equation Group had access some zero-days before Stuxnet and Flame used it. Even though the mistakes and fingerprints that reveal the identity of the group are rare, there are some clues. For example, this group is linked with NSA since some NSA keywords are found, and malware (a keylogger named Grok) is also associated with Equation Group and NSA.

Targeted Countries & Industries

Equation Group generally target these sectors:

- Governments and diplomatic institutions
- Telecommunication
- Aerospace
- Energy
- Nuclear research
- Oil and gas
- Military
- Nanotechnology
- Islamic activists and scholars
- Mass media
- Transportation
- Financial institutions
- Companies developing cryptographic technologies.

Countries that are in the target of the Equation Group:

Highly targeted:

- Iran
- Russia
- Pakistan
- Afghanistan
- India

- China
- Syria
- Mali

Not highly as the previous ones but also targeted ones:

- Lebanon
- Yemen
- UAE
- Algeria
- Kenya
- UK
- Libya
- Mexico
- Qatar
- Egypt

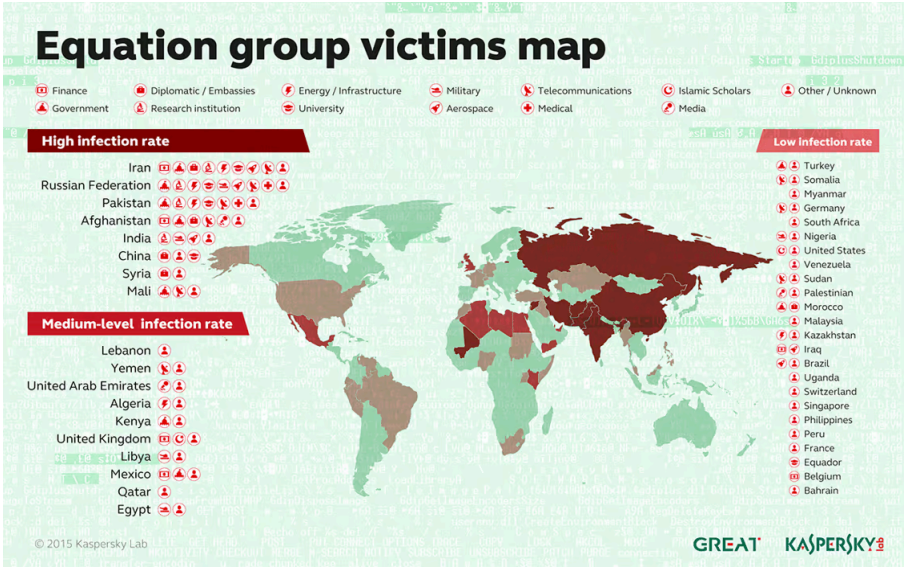

Figure 1: Targeted countries

Cyber Attack Lifecycle and TTPs

Equation Group infects its victims by several ways. These ways include:

- Worm code
- Physical media, CD-ROMs
- USB Sticks
- Web Exploits

Equation Group uses physical media, worm, or web exploits to infect victims. The compromised computer is used to execute an installer to begin to escalate privileges. Then the **DOUBLEFANTASY** malware is installed, and the victim is verified. Verifying process is done in order to figure out if the victim is essential to hack or not. Then

DOUBLEFANTASY malware is upgraded to **GRAYFISH** or **EQUATIONDRUG** malware which is sophisticated espionage malware. GRAYFISH uses a bootkit so that it can gain execution privilege as the OS boots.

Physical devices and USB sticks are used to infect the systems that are not connected to the internet, for example, nuclear power plants.
The reason why this group is considered sophisticated is that they reprogrammed hard drive firmware so that they can gain persistence. After reprogramming the firmware, re-infection begins as needed. This is used for the first time. Therefore, forensics professionals are not looking for there, and this improves persistence.

Tactic	Tactic ID	Technique	Technique ID
Defense Evasion	TA0005	Execution Guardrails: Environmental Keying	T1480.001
		Hide Artifacts: Hidden File System	T1564.005
Discovery	TA0007	Peripheral Device Discovery	T1120
Persistence, Defense Evasion	TA0003TA0005	Pre-OS Boot: Component Firmware	T1542.002

Group's Toolset and Related Malware

- ***EQUATIONDRUG*** – An attack platform which has plugins as modules.
- ***DOUBLEFANTASY*** – This platform decides if the target is the one that the group wants to attack. If it is, then the platform is upgraded to EQUATIONDRUG or GRAYFISH.
- ***EQUESTRE*** – Same as EQUATIONDRUG.
- ***TRIPLEFANTASY*** – A backdoor which is used with GRAYFISH. It is probably a more recent version of DOUBLEFANTASY.
- ***GRAYFISH*** – A sophisticated attack platform which stays in the registry. It gains execution privilege with a bootkit when the OS boots.
- ***FANNY*** – This computer worm created in 2008 and used for getting information.
- ***EQUATIONLASER*** – This is used between 2001 and 2004 and is compatible with Windows 95/98. This is used somewhere between DOUBLEFANTASY and EQUATIONDRUG.
- ***GROK*** — A keylogger to steal victims' credentials.

For detailed information about these, click here.

Recommendations & Mitigations

Kaspersky Lab found 7 exploits are used by Equation Group. At least 4 of these were used as zero-days. You might consider if your computer is vulnerable to these exploits below. Here are the exploits:

- Windows Kernel EoP exploit used in Stuxnet 2009, fixed with MS09-025. (CVE unknown).

- CVE-2012-0159 (fixed with MS12-034)
- CVE-2013-3894 (fixed with MS13-081)
- CVE-2010-2568 (used by Stuxnet)
- CVE-2013-3918
- CVE-2012-1723
- CVE-2012-4681

Of course there are other mitigations you should consider.

- Do not plug a randomly found physical device (USB, CD, …) in your computer since that device might carry a malware and infect your computer.
- Keep your software up-to-date.
- Do not click on every link or download files sent via email. Phishing attacks might be a start of a malware infection. To detect phishing emails click here.
- Be careful when entering and logging in some websites such as Islamic Jihadist discussion forums.

Conclusion

Equation Group is a sophisticated and old group. They exploit websites, distribute malware with worms and physical devices. It is difficult to detect Equation Group's malware for antivirus software and forensics professionals. All malware samples that are found are designed for Windows, but some clues show that macOS and iPhone devices are also not safe. Therefore, this group should not be ignored and underestimated.
