# CS 5343 Secure Systems and Software Spring 2015


**A Report on "The Equation Group"**

**Submitted by:** **Viswanath Nuggu (tef771)**

**Submitted to:** **Dr. Gregory B. White**

## Introduction

This article is about malicious activities being performed by an attacker group named“The Equation Group”, which were identified byKaspersky Lab. This article was published with the title “Newly Discovered 'Master' Cyber Espionage Group Trumps Stuxnet” in the website “darkreading.com” onFeb 16, 2015.

### Synopsis

The Equation Group is a highly advanced secretive computer espionage group, suspected by security expert Claudio Guarnieriand unnamed former intelligence operativesof being tied to the United States National Security Agency (NSA), because of the group's predilection for strong encryption methods in their operations, the name Equation Group was chosen by Kaspersky Lab, which discovered this operation and also documented 500 malware infections by the group's tools in at least 42 countries [1].

According to Kaspersky Lab's the group has been active since at least 2001, armed with sophisticated tools and techniques which are capable of reprogramming hard disk drive firmware by using their sophisticated encryption algorithms, the malware has prompted fears of widespread computer eavesdropping.It also allows them to reprogram the hard drive firmware of over a dozen different hard drive brands, including Seagate, Western Digital, Toshiba, Maxtor and IBM.

Their targets are in government and diplomacy, telecommunications, aerospace, energy, nuclear- research, oil and gas, military, nanotechnology, mass media, transportation, financial institutions, cryptographic development, as well as Islamic activists and scholars based in the US and UK.The malware used in this attack is targeting windows systems and was infecting around 2000 machines per month.

Kaspersky Lab has claimed that equation group has ties with stuxnet, flame teams. The malware used in their operations, dubbed EquationDrug and GrayFish, is found to be capable of reprogramming hard disk drive firmware [1]. Because of such advanced techniques involved and high degree of covertness, there has been a speculation that NSA could be the equation group since the evidence shows that it has US connections, code written in English and capability to have expensive servers. In future, we might see more attacks of the same kind as stuxnet, like apple malware,mac malware related to APT.

This group has got unique and complex capabilities to reprogram the hard drives; they have been one of the most powerful groups in hacking.This capability allows them attack with (advanced persistent threat), by allowing the malware to go undetected by antivirus and to remain alive even if the drive is reformatted or the operating system gets reinstalled, this is what it makes this group more powerful and tells the complexity of attack they are using.

Kaspersky has also named specialist tools used by the group EquationLaser, EquationDrug, DoubleFantasy, TripleFantasy, Fanny and GrayFish, but the list is far from complete and each tool is sophisticated and professionally used.

Fanny named due to fanny.bmp file found on compromised systems is a computer worm created in 2008 which targets victims in the Middle East and Asia. The worm, which infects USB hard drives, has also been found on thousands of USBs, and are still there. The purpose of Fanny appears to be the mapping of air-gapped networks. In order to do so, the malware uses a "unique" USB-based command and control mechanism carving out a hidden storage space on the USB to store stolen data and carry out commands.

Kaspersky also mentions they are sure that there might be malwares related to Linux and Mac from Equation group.

**Advanced Persistent Threat (APT)**

An advanced persistent threat is an attack in which an unauthorized person gains access to a network and stays there undetected for a long period of time. The purpose of an APT attack is to steal data rather than to cause damage. The goal in APT is to achieve ongoing access. To maintain access without discovery, the intruder must continuously rewrite code and employ sophisticated evasion techniques [2].

APT attacks organizations in sectors with high-value information, such as national defense, manufacturing and the financial industry.

**APT Process:**

An APT attacker often uses spear fishing, a type of social engineering, to gain access to the network through legitimate means. Once access has been achieved, the attacker establishes a back door.

The next step is to gather valid user credentials (especially administrative ones) and move laterally across the network, installing more back doors. The back doors allow the attacker to install bogus utilities and create a "ghost infrastructure" for distributing malware that remains hidden in plain sight.

Although APT attacks are difficult to identify, the theft of data can never be completely invisible. Detecting anomalies in outbound data is perhaps the best way for an administrator to discover that his/her network has been the target of an APT attack.

Identifying an APT may be difficult but the theft of data is not difficult to identify. By checking the outbound data a system administrator can be able to find anomalies.

**Legal/Political Issues surrounding the Equation Group**

The researchers from Kaspersky lab think that NSA is behind the Equation Group, but they don’t have any evidence about this. . The equation group was using the same exploits that stuxnet has

used. Stuxnet was led by NSA,so some people are guessing NSA might be supporting and leading equation group too. The legal issue comes from modifying or reprogramming the legal or original code.

**Conclusion**

The researchers of the Kaspersky lab discovered the equation group which is a highly sophisticated group that attacks the high-end systems with advanced persistent threats in order to gain access to information and to stay active on the victim machines for a long period of time.This group has not performed any activities from 2014 but researchers are sure this group is doing their activities secretly and Kaspersky lab researchers are expecting some serious threats from this group in near future.

References:

[1] http://en.wikipedia.org/wiki/Equation_Group

[2] http://searchsecurity.techtarget.com/definition/advanced-persistent-threat-APT

[3] http://www.cnbc.com/id/47962225

[4] https://securelist.com/files/2015/02/Equation_group_questions_and_answers.pdf