The King of Espionage Malware Revealed: The Equation Group

The Kaspersky Lab left its Moscow headquarters with its wintry grip behind to hold a Security Analyst Summit in sunny Cancun, Mexico. Kaspersky has already made it a torrid conference with disclosures last weekend of an estimated $ 1 billion stolen from 100 banks by a network of hackers. *CNN* reported what was revealed in the Kaspersky report:

> …hackers surreptitiously installed spying software on bank computers, eventually learned how to mimic bank employee workflows and used the knowledge to make transfers into bank accounts they had created for this theft.

Yesterday, at the Summit, they introduced another cyber security bombshell, a super malware, The Crown Creator of Espionage: the Equation Group.

Equation Group Connections to Malware Stuxnet, Flame and Duqu

Source: Kaspersky

Consider it the granddaddy of Zero-days Malware starting earlier than Stuxnet, and its offspring Duqu, and Flame/Gauss. Kaspersky dramatically announced:

> The team has seen nearly everything, with attacks becoming increasingly complex as more nation-states got involved and tried to arm themselves with the most advanced tools. However, only now Kaspersky Lab's experts can confirm they have discovered a threat actor that surpasses anything known in terms of complexity and sophistication of techniques, and that has been active for almost two

decades – The Equation Group

Malware in the Group use tools that are very complicated and expensive to develop, in order to infect victims, retrieve data and hide activity in an outstandingly professional way, and utilize classic spying techniques to deliver malicious payloads to the victims.

To infect their victims, the group uses a powerful arsenal of “implants” (Trojans) including the following that have been named by Kaspersky Lab: Equation Laser, EquationDrug, DoubleFantasy, TripleFantasy, Fanny and GrayFish. Without a doubt there will be other “implants” in existence.

According to Kaspersky what makes the Equation group dangerous is:

Ultimate persistence and invisibility- ability to enter hard drives enabling reprogramming of firmware:

Ability to retrieve data from isolated networks- using the Fanny malware to map networks via USB memory sticks, and;

Classic spying methods to deliver malware – through internet and physical means.

The Equation Group according to Kaspersky has a powerful and geographically distributed network covering more than 300 web domains involving over 100 servers located in the US, UK, Italy, Germany, Netherlands, Panama, Costa Rica, Malaysia, Colombia and the Czech Republic. Since 2001, it has infected tens of thousands of “high profile victims” in over 30 countries. Examples include: “Government and diplomatic institutions, Telecommunications, Aerospace, Energy, Nuclear research, Oil and Gas, Military, Nanotechnology, Islamic activists and scholars, Mass media, Transportation, Financial institutions and companies developing encryption technologies."

Kaspersky has observed the Equation Group malware in a number of zero days exploits against, for example Firefox and the Tor browser. It notes the prowess of its detection with this comment:

> Automatic Exploit Prevention technology which generically detects and blocks exploitation of unknown vulnerabilities. The Fanny worm, presumably compiled in July 2008, was first detected and blacklisted by our automatic systems in December 2008.

A FoxNews report gave further examples of the power of this "sneakiest" of malware:

> Kaspersky's researchers say that the Equation group uses a hacking tool called "GROK." That is a tool exclusively used by the NSA's elite cyber-warfare unit, Tailored Access Operations, according to classified NSA documents released by former contractor Edward Snowden last year.
>
> Kaspersky says the Equation group also appears to have ties to Stuxnet, the computer worm that sabotaged Iran's nuclear enrichment program in 2010 and was later revealed to be a joint U.S.-Israeli project.

The history of the Equation Group malware origins stretches back nearly 20 years:

> Kaspersky research director Costin Raiu said the Equation Group hacked into hospitals in China; banks and aerospace companies in Iran; energy companies and government offices in Pakistan; and universities, military facilities and rocket science research institutions in Russia.
>
> They attacked Iran the most, researchers said.
>
> The Equation group also spied on Muslim scholars in the

> United States and the United Kingdom, Raiu said. It emerged last year that the NSA and FBI have been monitoring the emails of prominent Muslim-American lawyers and activists.
>
> The group monitored keystrokes and stole documents from computers. In one instance in the Middle East, the hackers programmed the malware to specifically look for oil-related shipping contracts and inventory price lists.
>
> Malware attacked Windows computers, Macs and even iPhones.
>
> Unlike other hackers, however, the Equation Group wasn't interested in destroying computers or wiping them clean, the way North Koreans hurt Sony last year.
>
> "They're interested in long-term intelligence gathering," Raiu said.
>
> [How far back does this go?] Kaspersky researchers say the Equation group built some of its earliest malware in 2002, but the computer infrastructure used to spread the group's computer viruses dates back to 1996.
>
> Their ability to stay quiet this long goes to show how talented they are, the Kaspersky report noted.

As the Kaspersky report stated Enterprise Group could be a co-development of state sponsors. Given the connections to Stuxnet, Flame/Duqu Groups, it may be likely that it is a joint project of the US and Israel. For a useful understanding of the development and detection of Malware, read Free eBook: Stopping Zero Day Exploits for Dummies. Also read the fascinating chronicle of discovery of Stuxnet by a researcher at a small Belarus anti-virus firm and by international cyber sleuths from anti-virus firms like Kaspersky and others in, *In Countdown to Zero Day* by Wired cybersecurity writer Kim Zetter.