



PRIVACY AND SECURITY FANATIC

By Ms. Smith

About |

Ms. Smith (not her real name) is a freelance writer and programmer with a special and somewhat personal interest in IT privacy and security issues.

Reformatting won't remove invisible and persistent malware infecting hard drive firmware

Kaspersky Lab discovered stealthy, sophisticated and scary Equation group cyber-espionage attacks such as infecting hard drive firmware with "invisible and persistent" malware that cannot be disinfected by reformatting the drive or by reinstalling the operating system.

Network World | Feb 17, 2015 8:25 AM PT

Kaspersky Lab dropped a bombshell by revealing the most badass attack group that has ever been known. It smells like the NSA, although that is not certain; it has developed and deployed "invisible and persistent" Trojans to infect possibly "tens of thousands of victims" since at least 2001 and perhaps since 1996 when its command and control (C&Cs) were registered. A wise person would read GReAT's write-up on Securelist and Kaspersky Lab's news release about the Equation Group. The information from this article is primarily from Kaspersky's Equation Group questions and answers (pdf) report.

The scariest aspect – or what Kaspersky Lab researchers call the "most sophisticated" thing about the Equation group, is its "**the ability to infect the hard drive firmware.**" That attack technology exceeds anything Kaspersky has ever seen. By reprogramming the HDD (hard drive) firmware, it is an extremely persistent infection that cannot be wiped by formatting the drive or by reinstalling the operating system. It acts as "an invisible, persistent storage hidden inside the hard drive."

It is extraordinarily beyond normal for attackers to even know the unique ATA commands which hard drive vendors use to format their products, nevertheless to utilize infection capabilities of that when developing malware.

According to the Equation Group questions and answers ([pdf](#)), the group's EquationDrug and GrayFish have the ability to reprogram hard drives; Kaspersky lists the classes supported as: drives from Western Digital's WDC WD, HGST – a Western Digital company – IC, IBM, Hitachi, HTS, HTE, HDS, HDT and ExcelStor. Seagate's Maxtor, Maxtor STM, Max, ST, and Seagate ST. Samsung; Micron Technology's C300 and M4; Toshiba and Toshiba M; OCZ, OWC, Corsair and Mushkin.

If it makes you feel any better, Kaspersky said the Equation group's HDD reprogramming module is extremely rare and only the most valuable victims are targeted. Kaspersky called the Equation group "unique in almost every aspect of their activities."

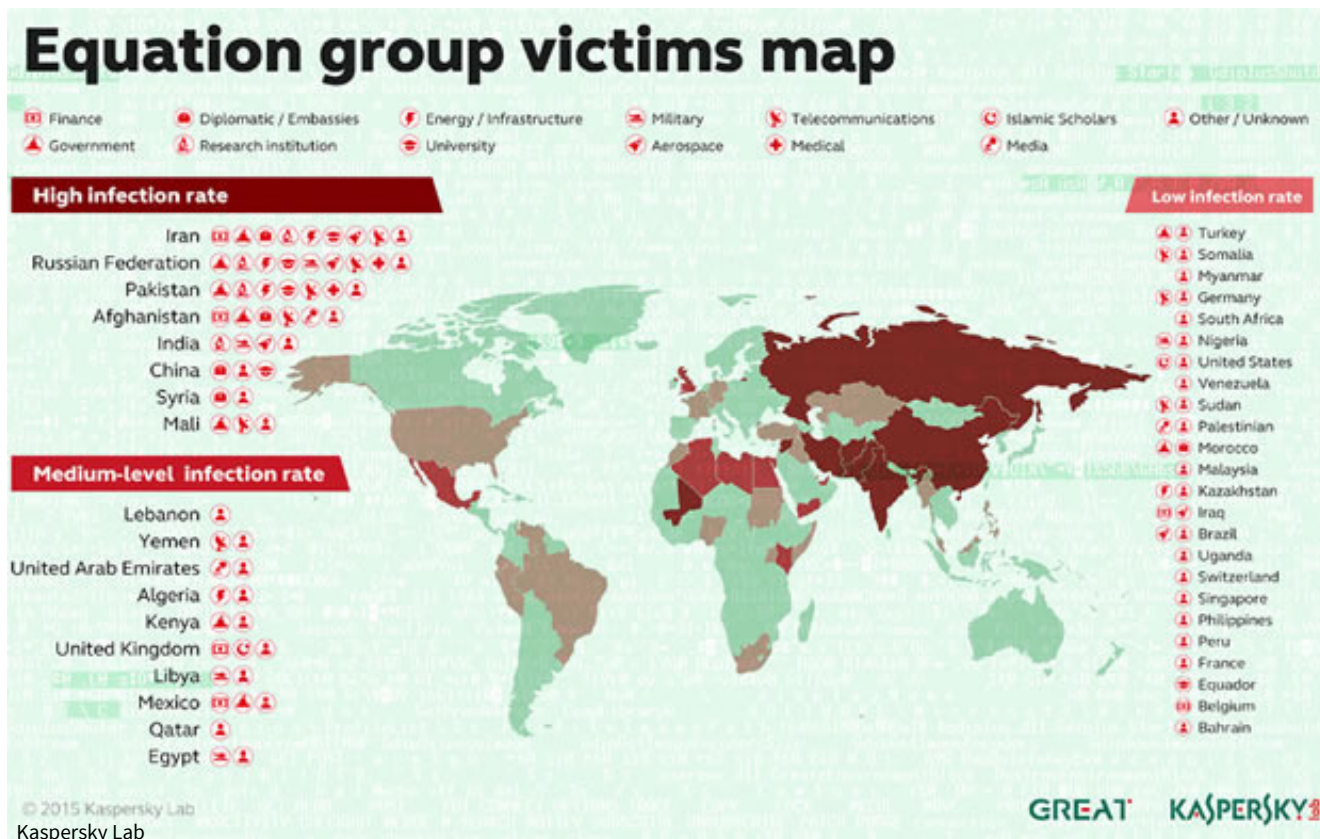
They use tools that are very complicated and expensive to develop, in order to infect victims, retrieve data and hide activity in an outstandingly professional way, and utilize classic spying techniques to deliver malicious payloads to the victims.

EquationDrug utilizes virtual file systems, but GrayFish is even more extreme and stealthy because it "exclusively uses the registry to store all malware-related modules and data in encrypted format." The report states, "GrayFish bootkit starts from the VBR [variable bitrate], loads the operating system and hijacks the loading of the first driver in the kernel. Next, it loads all the other malware stages from the registry, making it almost completely invisible in terms of footprint."

In terms of advanced features, GrayFish and EquationDrug include perhaps the most sophisticated persistence mechanism we've ever seen: re-flashing the HDD firmware. Due to the complexity of this process and the knowledge and resources required to implement something like it, the mechanism appears to be out of the reach of most advanced threat groups in the world except the Equation group.

Stuxnet was radically ambitious and sophisticated, capable of penetrating air-gapped networks, but Kaspersky Lab said the Equation group had access to those zero-days even *before* they were used in Stuxnet and Flame. The Equation Group's Fanny can map air-gapped networks and allow "attackers to pass data back and forth from air-gapped networks." That implies the Equation group is the "crown creator of cyber-espionage;" Kaspersky did not go so far to name-blame the NSA, but it did reference documents published by Der Spiegel about the NSA's Office of Tailored Access Operations (TAO).

So far, Kaspersky identified more than 500 victims from 30 countries.



Equation group “sometimes selects its victims with surgical precision. When precision is not possible, the victims are targeted by a validator (DoubleFantasy) implant and subsequently disinfected if they do not appear to be ‘interesting’ to attackers.”

The researchers added that attackers infect their victims by methods such as physical media like CD-ROMs, USB sticks and exploits, web-based exploits, and Fanny self-replicating worm code.

Regarding the codename GROK that came to light via Der Spiegel publishing Snowden-leaked documents, Kaspersky said, “Our analysis indicates Equation group’s GROK plugin is indeed a keylogger on steroids that can perform many other functions.”

Another interesting attack targeted Firefox 17 that was being used as a Tor browser; it used an unknown exploit. The researchers first discovered EquationDrug modules on a PC located in the Middle East; they call this computer “The Magnet of Threats” due to advanced malware infecting it.

Kaspersky Lab gave an example of attacks that could be delivered via Java exploits to advertisements on popular Middle East websites as well as by visiting specific Islamic jihadist discussion forums; a PHP script, which was designed to work as part of the commercial forum platform vBulletin, exploited only forum visitors who were logged in; additionally those authenticated users had to come from specific IP address ranges. Attackers took “special care” not to infect users from Jordan, Turkey or Egypt.


The C&C infrastructure includes over 300 domains registered using “Domains By Proxy” and more than 100 servers hosted in the US, UK, Italy, Germany, Netherlands, Panama, Costa Rica, Malaysia, Colombia and the Czech Republic.

Although all of the malware Kaspersky Lab collected targets Microsoft Windows, the researchers sinkholed a C&C domain that receives connections to victims in China running Mac OS X. They believe DoubleFantasy also comes in a Mac OS X flavor; iPhones can be targeted via malicious forum





injection.

Kaspersky Lab chose the name Equation group “because of their preference for sophisticated encryption schemes.” Researchers so far have “identified 20 different compiled versions of the RC5/6 code in the Equation group malware.”

Kaspersky Lab has thus far identified and named the powerful arsenal of implants as “EquationLaser, EquationDrug, DoubleFantasy, TripleFantasy, Fanny and GrayFish.” Expect to hear more about those, but the researchers added that “Without a doubt there will be other ‘implants’ in existence.”



Ms. Smith



 **View 1 Comment**

YOU MIGHT LIKE