GlobalResearch
Center for Research on Globalization

Moscow-Based Security Firm Reveals What May Be the Biggest NSA "Backdoor Exploit" Ever

By Zero Hedge

Theme: Intelligence

Global Research, February 17, 2015
Zero Hedge 16 February 2015

Since 2001, a group of hackers – dubbed the "Equation Group" by researchers from Moscow-based Kaspersky Lab – have infected computers in at least 42 countries (with Iran, Russia, Pakistan, Afghanistan, India, and Syria most infected) with what Ars Technica calls ***"superhuman technical feats" indicating "extraordinary skill and unlimited resources."***

The exploits – including the **'prized technique' of the creation of a secret storage vault that survives military-grade disk wiping and reformatting – cover every hard-drive manufacturer** and have many similar characteristics to the infamous NSA-led Stuxnet virus.

> According to Kaspersky, **the spies made a technological breakthrough by figuring out how to lodge malicious software in the obscure code called firmware that launches every time a computer is turned on.**
>
> Disk drive firmware is viewed by spies and cybersecurity experts as the second-most valuable real estate on a PC for a hacker, second only to the BIOS code invoked automatically as a computer boots up.
>
> "The hardware will be able to infect the computer over and over," lead Kaspersky researcher Costin Raiu said in an interview.
>
> …
>
> **Kaspersky's reconstructions of the spying programs show that they could work in disk drives sold by more than a dozen companies, comprising essentially the entire market.** They include Western Digital Corp, Seagate Technology Plc, Toshiba Corp, IBM, Micron Technology Inc and Samsung Electronics Co Ltd.

The group used a variety of means to spread other spying programs, such as by compromising jihadist websites, infecting USB sticks and CDs, and**developing a self-spreading computer worm called Fanny**, Kasperky said.

Fanny was like Stuxnet in that it exploited two of the same undisclosed software flaws, known as "zero days," which strongly suggested collaboration by the authors, Raiu said. He added that it was "quite possible" that the **Equation group used Fanny to scout out targets for Stuxnet in Iran and spread the virus.**

Which, *as Reuters reports,* strongly suggests the "extraordinary skills and unlimited

resources" were funded by the NSA…

> **The U.S. National Security Agency has figured out how to hide spying software deep within hard drives made by Western Digital, Seagate, Toshiba and other top manufacturers, giving the agency the means to eavesdrop on the majority of the world's computers,** according to cyber researchers and former operatives.
>
> **That long-sought and closely guarded ability was part of a cluster of spying programs discovered by Kaspersky Lab,** the Moscow-based security software maker that has exposed a series of Western cyberespionage operations.
>
> Kaspersky said it found personal computers in 30 countries infected with one or more of the spying programs, **with the most infections seen in Iran, followed by Russia, Pakistan, Afghanistan, China, Mali, Syria, Yemen and Algeria.** The targets included government and military institutions, telecommunication companies, banks, energy companies, nuclear researchers, media, and Islamic activists, Kaspersky said.
>
> **The firm declined to publicly name the country behind the spying campaign, but said it was closely linked to Stuxnet, the NSA-led cyberweapon** that was used to attack Iran's uranium enrichment facility. The NSA is the agency responsible for gathering electronic intelligence on behalf of the United States.
>
> **A former NSA employee told Reuters that Kaspersky's analysis was correct,** and that people still in the intelligence agency valued these spying programs as highly as Stuxnet. Another former intelligence operative **confirmed that the NSA had developed the prized technique of concealing spyware in hard drives, but said he did not know which spy efforts relied on it.**

The global coverage is clearly focused in a particular region (and not in the US)…

As Kasperskey exposes, victims generally fall into the following categories:

- 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

As an interesting note, some of the “patients zero” of Stuxnet seem to have been infected by the EQUATION group. **It is quite possible that the EQUATION group malware was used to deliver the STUXNET payload.**

So far, Kaspersky have identi?ed several malware platforms used exclusively by the Equation group. They are:

EQUATIONDRUG – A very complex attack platform used by the group on its victims. It supports a module plugin system, which can be dynamically uploaded and unloaded by the attackers.

DOUBLEFANTASY – A validator-style Trojan, designed to con?rm the target is the intended one. If the target is con?rmed, they get upgraded to a more sophisticated platform such as EQUATIONDRUG or GRAYFISH.

EQUESTRE – Same as EQUATIONDRUG.

TRIPLEFANTASY – Full-featured backdoor sometimes used in tandem with GRAYFISH. Looks like an upgrade of DOUBLEFANTASY, and is possibly a more recent validator-style plugin.

GRAYFISH – The most sophisticated attack platform from the EQUATION group. It resides completely in the registry, relying on a bootkit to gain execution at OS startup.

FANNY – A computer worm created in 2008 and used to gather information about targets in the Middle East and Asia. Some victims appear to have been upgraded ?rst to DoubleFantasy, and then to the EQUATIONDRUG system. Fanny used exploits for two zero-day vulnerabilities which were later discovered with Stuxnet.

EQUATIONLASER – An early implant from the EQUATION group, used around 2001-2004. Compatible with Windows 95/98, and created sometime between DOUBLEFANTASY and EQUATIONDRUG.

Although the implementation of their malware systems is incredibly complex, surpassing even Regin in sophistication, **there is one aspect of the EQUATION group’s attack technologies that exceeds anything Kaspersky has ever seen before.**

This is the ability to infect the hard drive ?rmware.

The plugin version 4 is more complex and can reprogram 12 drive “categories”

* * *

So to summarize:

> 1) **US sanctions Russia**
>
> 2) **a Russian-based research group** (Kaspersky Lab is an international group operating in almost 200 countries and territories worldwide. The company is headquartered in Moscow, Russia, with its holding company registered in the United Kingdom. Kaspersky Lab currently employs over 2,850 qualified specialists) **reveals** that through Equation group’s code, **there is NSA presence across the supply chain of the highest margin US products** .
>
> 3) As Reuters notes, **the exposure of these new spying tools could lead to greater backlash against Western technology,**particularly in countries such as China, which is already drafting regulations that would require most bank technology suppliers to proffer copies of their software code for inspection.
>
> 4) And **Peter Swire, one of five members of U.S. President Barack Obama’s Review Group on Intelligence and Communications Technology**, said the Kaspersky report showed that it is essential for the country to **consider the possible impact on trade and diplomatic relations** before deciding to use its knowledge of software flaws for intelligence gathering. **“There can be serious negative effects on other U.S. interests,”** Swire said.

It appears the ‘boomerang’ is boomerang-ing…

* * *

Full Kaspersky Labs report below:

Equation Group Questions and Answers

Equation Group Questions and Answers

Articles by: **Zero Hedge**