GlobalResearch
Center for Research on Globalization

Military-Grade Malware "Regin" Linked to US and British Intelligence Agencies, Targeting Governments, Academics and Telecoms

By Lauren McCauley

Global Research, November 25, 2014
Common Dreams

Theme: Intelligence

Symantec, which published a technical whitepaper on the malware Sunday, says it's likely "one of the main cyberespionage tools used by a nation state." (Photo: Grant Hutchinson/flickr/cc)

Security researchers have recently exposed a sophisticated new "military grade" malware program which is specifically targeting governments, academics and telecoms and, according to new reports, is suspected as being the handiwork of U.S. and British intelligence agencies.

According to security analysts with the Russian security firm Kaspersky Lab, which has been tracking the malware known as "Regin" for two years, the technology has two main objectives: intelligence gathering and facilitating other types of attacks.

Perhaps most notable, security researchers point out, is that none of the targets are based in either the U.S. or U.K. According to the *Guardian*, 28 percent of victims are based in Russia and 24 percent are based in Saudi Arabia. Ireland, with 9 percent of detected infections, has the third highest number of targets.

Since initial signs of the malicious software emerged in 2008, there have only been 100 or so victims uncovered globally. These include telecom operators, government institutions, multi-national political bodies, financial institutions, research institutions, and individuals involved in advanced mathematical/cryptographical research.

Described as highly complex, the malware works by disguising itself as Microsoft software and then stealing data through such channels as "capturing screenshots, taking control of the mouse's point-and-click functions, stealing passwords, monitoring the victim's web activity and retrieving deleted files," according to *Guardian* reporter Tom Fox-Brewster.

Mikko Hypponen, chief research officer at F-Secure, told Fox-Brewster that his firm does not believe Regin was made by Russia or China, "the usual suspects." According to Fox-Brewster, this leaves the U.S., U.K. or Israel as the "most likely candidates," an assumption that Symantec threat researcher Candid Wueest said was "probable."

On Monday, *Intercept* reporters Morgan Marquis-Boire, Claudio Guarnieri, and Ryan Gallagher published the first of an investigative series on Regin. Specifically, they note, Regin is the suspected technology behind both a GCHQ surveillance attack on Belgium telecom operator Belacom as well as an infection of European Union computer systems

carried out by the National Security Agency. Both attacks were revealed last year through documents leaked by NSA whistleblower Edward Snowden.

On Sunday, Symantec was the first to report on the technology, publishing a technical whitepaper which described Regin as "a complex piece of malware whose structure displays a degree of technical competence rarely seen."

"Its capabilities and the level of resources behind Regin indicate that it is one of the main cyberespionage tools used by a nation state," the paper continues.

Articles by: Lauren McCauley