

Cyberspying tool could have US, British origins (Update)

November 24 2014, by Rob Lever



Symantec said the malware shares some characteristics with the Stuxnet worm—a tool believed to have been used by the US and Israeli governments to attack computer networks involved in Iran's nuclear program

A sophisticated cybersespionage tool has been stealing information from governments and businesses since 2008, researchers said Monday, and one report linked it to US and British intelligence.

The security firm Symantec identified the malware, known as Regin, and

said it was used "in systematic spying campaigns against a range of international targets," including governments, businesses, researchers and private individuals.

The news website The Intercept reported later Monday that the malware appeared to be linked to US and British intelligence, and that it was used in attacks on EU government networks and Belgium's telecom network.

The report, citing industry sources and a technical analysis of the malware, said Regin appears to be referenced in documents leaked by former National Security Agency contractor Edward Snowden about broad surveillance programs.

Asked about the report, an NSA spokeswoman said: "We are not going to comment on speculation."

Symantec's report said the malware shares some characteristics with the Stuxnet worm— a tool believed to have been used by the US and Israeli governments to attack computer networks involved in Iran's nuclear program.

Because of its complexity, the Symantec researchers said in a blog post that the malware "would have required a significant investment of time and resources, indicating that a nation state is responsible."

The researchers added that "it is likely that its development took months, if not years, to complete and its authors have gone to great lengths to cover its tracks."

Lurking in shadows

"Regin's developers put considerable effort into making it highly inconspicuous," Symantec said.

"Its low key nature means it can potentially be used in espionage campaigns lasting several years. Even when its presence is detected, it is very difficult to ascertain what it is doing. Symantec was only able to analyze the payloads after it decrypted sample files."

The researchers also said many components of Regin are still probably undiscovered and that there could be new versions of this tool which have not yet been detected.

The infections occurred between 2008 and 2011, after which the malware disappeared before a new version surfaced in 2013.

The largest number of infections discovered—28 percent—was in Russia, and Saudi Arabia was second with 24 percent. Other countries where the malware was found included Mexico, Ireland, India, Afghanistan, Iran, Belgium, Austria and Pakistan. There were no reported infections in the United States.

Around half of all infections occurred at addresses belonging to Internet service providers, but Symantec said it believes the targets of these infections were customers of these companies rather than the companies themselves.

Telecom companies were also infected, apparently to gain access to calls being routed through their infrastructure, the report noted.

Regin appeared to allow the attackers to capture screenshots, take control of the mouse's point-and-click functions, steal passwords, monitor traffic and recover deleted files.

Symantec said some targets may have been tricked into visiting spoofed versions of well-known websites to allow the malware to be installed, and in one case it originated from Yahoo Instant Messenger.

Other security experts agreed this was a dangerous tool likely sponsored by a government.

"Regin is a cyberattack platform, which the attackers deploy in victim networks for total remote control at all levels," said a research report from Kaspersky Lab.

Kaspersky added that Regin also appears to have infiltrated mobile communications through GSM networks, exposing "ancient" communication protocols used by cellphone networks.

Antti Tikkanen at Finland-based F-Secure called it "one of the more complex pieces of malware around," and added that "our belief is that this malware, for a change, isn't coming from Russia or China."

The news comes amid heightened concerns on cyberespionage.

Last month, separate teams of security researchers said the Russian and Chinese governments are likely behind widespread cyberespionage that has hit targets in the US and elsewhere.

© 2014 AFP

Citation: Cyberspying tool could have US, British origins (Update) (2014, November 24)
retrieved 10 April 2024 from
<https://phys.org/news/2014-11-advanced-cyberspying-tool-dates.html>

<p>This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.</p>
--