

Stealthy spy software snooping for years: Symantec

November 25 2014

Computer security firm Symantec on Monday [said it uncovered stealthy software](#) wielded as part of a years-long spying campaign, most likely by a nation state.

The [malicious software](#), dubbed [Regin](#), has a rare level of sophistication and has been targeting government agencies, telecoms, utilities, airlines, research facilities, private individuals and others since at least 2008, according to Symantec Corporation.

Attacks on telecom firms appeared aimed at getting access to calls being routed through networks.

"Regin is a highly complex threat which has been used in systematic data collection or intelligence gathering campaigns," the Silicon Valley-based computer security firm said in a paper detailing the threat.

"The development and operation of this malware would have required a significant investment of time and resources, indicating that a nation state is responsible."

Regin was found mainly in 10 countries, but more than half of infections discovered were in Russia and Saudi Arabia, according to Symantec researchers.

Regin's capabilities include letting hackers snap screen-shots, steal passwords, monitor network traffic, take files or tap into mobile

telephone calls, researchers said.

The "backdoor-type Trojan" takes great measures to hide its presence as well as any data it is stealing, according to Symantec.

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

"Its low key nature means it can potentially be used in espionage campaigns lasting several years."

Regin may have taken years to make, according to Symantec, which said the tool could be used for mass surveillance.

Nearly half the infections discovered targeted small businesses and [private individuals](#).

Researchers found Regin infected a variety of organizations from 2008 to 2011, only to be withdrawn, though a new version of the malicious software appeared last year.

Symantec did not indicate who it thought might be behind the cyber-espionage tool.

© 2014 AFP

Citation: Stealthy spy software snooping for years: Symantec (2014, November 25) retrieved 3 June 2024 from <https://phys.org/news/2014-11-stealthy-spy-software-snooping-years.html>

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.