*** 北米連携センター定期報告***

2014 年 11 月 24 日

●シマンテック、高度な機能を持つマルウェアを発見

【New York Times, 2014/11/24】

シマンテックは、2008 年から研究者や政府、企業、電気通信の重要インフラなどからの情報傍受に使われていたという高度なマルウェア「Regin」を発見し、23 日、その詳細をまとめた白書を発表。

翌 24 日には、グレン・グリーンウォルド氏が創刊したデジタルマガジン、インターセプトがエドワード・スノーデン氏からの情報を基に、「Regin」は国家安全保障局（NSA）と英国情報機関 GCHQ の共同オペレーションの一環で用いられていたものだと伝えた。

シマンテックによると、マルウェアの世界で他に類のない全く新しい種類のものが登場することは稀だが、「Regin」はそれに当たるとのこと。

同社は、このマルウェアが、サウジアラビア、ロシアを中心にパキスタン、アフガニスタン、インド、メキシコ、アイルランド、ベルギー、オーストリアなど 10 か国のターゲットに対して用いられた証拠を発見。

インターセプトは、さらに EU の民間企業もターゲットになっており、ベルギーの電気通信事業者/ISP、ベルガコムも含まれていたとしている。

「Regin」は極めて柔軟にカスタマイズ可能で、ターゲットに応じて機能を変更することが可能。シマンテックは、その開発には数か月、あるいは数年の時間がかけられたと見ている。

同社によると、マルウェアは 2008 年に個人をターゲットとして使用が開始され、2011 年に突然使用が中止された後、昨年新しいバージョンが様々なターゲットに対して再び使われるようになった。

インターセプトは、2010 年にベルガコムのサーバがこのマルウェアに感染したと伝えている。

マルウェアは、感染したコンピュータのスクリーンショット記録、マウスのポイント＆クリック乗っ取り、パスワードやネットワークトラフィックの傍受、メモリ上のデータの収集といった機能を持っており、研究者等は、これがスパイ用のツールであることは間違いないとしている。

（参考）本件報道記事

Symantec Discovers ‘Regin’ Spy Code Lurking on Computer Networks

By Nicole Perlroth

November 24, 2014 12:42 pm

Security researchers say they have discovered a sophisticated piece of malicious code spying on researchers, governments, businesses, and critical telecommunications infrastructure since 2008.

The malware, called Regin, was first discovered by Symantec, the antivirus company, which released a white paper describing its findings on Sunday. On Monday, The Intercept, a digital magazine started by the journalist Glenn Greenwald, reported that the Regin malware is part of a decade-long joint operation by the National Security Agency and its British counterpart, the Government Communications Headquarters, or G.C.H.Q. The Intercept report is based in part on disclosures from former N.S.A. contractor Edward J. Snowden.

"In the world of malware threats, only a few rare examples can truly be considered groundbreaking and almost peerless," Symantec wrote. "What we have seen in Regin is just such a class of malware."

Symantec found evidence that the malware has been used on targets in 10 countries, primarily Saudi Arabia and Russia, as well as Pakistan, Afghanistan, India, Mexico, Ireland, Belgium and Austria. The Intercept reported Monday that the malware had been used to spy on companies in the European Union, notably Belgacom, a partly state-owned Belgian phone and Internet provider.

The Regin malware is highly customizable, researchers said, and can be tweaked to include new features and capabilities, depending on the target. Symantec's researchers estimate that it likely took months "if not years" to develop and said the malware's "authors have gone to great lengths to cover its tracks."

The researchers believe the malware was first used to spy on individuals in 2008, until it was "abruptly withdrawn" in 2011. The Intercept reported that the malware was used to infect a Belgacom server in 2010.

Then, last year, Symantec said the authors started using a new version of the same malware to spy on a variety of victims. Among them: academic researchers, individuals and small businesses, companies in the airline, energy

and hospitality sectors as well as telecom companies, in what researchers believe was an attempt to gain access to telephone calls routed through their call centers.

Regin is undeniably a spy tool, based on its functions, the researchers said. It is configured to grab screenshots and take over a computer mouse's point-and-click function. It can also grab passwords, monitor network traffic and gather information from the computer's memory. It can scan for and retrieve deleted files.

Beyond those basic functions, its capabilities vary from target to target. In one case, Symantec's researcher found that Regin had been tweaked to sniff traffic sent to mobile telephone base station controllers. In another case, it had been customized to parse mail from Microsoft's Exchange email databases.

One of the remaining mysteries, researchers say, is how victims are infected with Regin in the first place. Symantec said the infection method varies from target to target. In one case, it directed victims to spoofed versions of popular websites, then downloaded malware onto their machines. In the case of Belgacom, The Intercept said it found evidence that the attackers sent employees at the company to a fake LinkedIn page that downloaded the malware onto their machines. In another case, Symantec said, it originated from Yahoo's Instant Messenger service, through an "unconfirmed exploit."

The Regin malware attacks its victims in different stages, with each stage hidden and encrypted, except for the initial encounter.

"It goes to extraordinary lengths to conceal itself and its activities on compromised computers," Symantec researchers wrote in their white paper. "Its stealth combines many of the most advanced techniques that we have ever seen in use."

Symantec discovered five stages of the attack, but because each stage was encrypted, they could only parse the attack once they had collected information on all five stages. "Only by acquiring all five stages is it possible to analyze and understand the threat," Symantec noted.

The multi-staged design of the malware is akin to that of other espionage tools that security researchers believe were the work of nation states, notably Flame, Stuxnet and Duqu — three pieces of malware that were used to spy on computers in Iran and were believed to be a joint effort by the United States and Israel.

Like those spy tools, researchers believe Regin's development took years and could only have been developed by "a nation state" with the time and resources. "Its design makes it highly suited for persistent, long-term surveillance operations against targets."

The Intercept reported Monday that the tool was part of a joint N.S.A.- G.C.H.Q. program, codenamed "Operation Socialist."

Vanee Vines, a N.S.A. spokeswoman declined to comment on what the agency called "speculation."

"The discovery of Regin serves to highlight how significant investments continue to be made into the development of tools for use in intelligence gathering," Symantec researchers said.

They added, "Many components of Regin have still gone undiscovered and additional functionality and versions may exist."

Source: http://bits.blogs.nytimes.com/2014/11/24/symantec-discovers-spy-code-lurking-on-computer-networks/

以　上