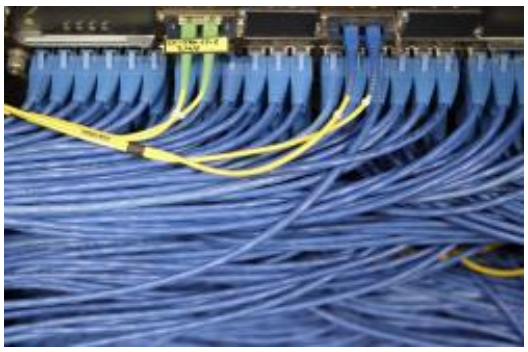
Suspected Russian spyware Turla targets Europe, United States

2:45pm EST



By Peter Apps and Jim Finkle

LONDON/BOSTON (Reuters) - A sophisticated piece of spyware has been quietly infecting hundreds of government computers across Europe and the United States in one of the most complex cyber espionage programs uncovered to date.

Several security researchers and Western intelligence officers say they believe the malware, widely known as Turla, is the work of the Russian government and linked to the same software used to launch a massive breach on the U.S. military uncovered in 2008.

It was also linked to a previously known, massive global cyber spying operation dubbed Red October targeting diplomatic, military and nuclear research networks.

Those assessments were based on analysis of tactics employed by hackers, along with technical indicators and the victims they targeted.

"It is sophisticated malware that's linked to other Russian exploits, uses encryption and targets western governments. It has Russian paw prints all over it," said Jim Lewis, a former U.S. foreign service officer, now senior fellow at the Center for Strategic and International Studies in Washington.

However, security experts caution that while the case for saying Turla looks Russian may be strong, it is impossible to confirm those suspicions unless Moscow claims responsibility. Developers often use techniques to cloud their identity.

The threat surfaced this week after a little known German anti-virus firm, G Data, published a report on the virus, which it called Uroburos, the name text in the code that may be a reference to the Greek symbol of a serpent eating its own tail.

Experts in state-sponsored cyber attacks say that Russian government-backed hackers are known for being highly disciplined, adept at hiding their tracks, extremely effective at maintaining control of infected networks and more selective in choosing targets than their Chinese counterparts.

"They know that most people don't have either the technical knowledge or the fortitude to win a battle with them. When they recognize that someone is onto them, they just go dormant," said one expert who helps victims of state-sponsored hacking.

A former Western intelligence official commented: "They can draw on some very high grade programmers and engineers, including the many who work for organized criminal groups, but also function as privateers."

Russia's Federal Security Bureau declined comment as did Pentagon and U.S. Department of Homeland Security officials.

On Friday, Britain's BAE Systems Applied Intelligence - the cyber arm of Britain's premier defense contractor - published its own research on the spyware, which it called "snake."

The sheer sophistication of the software, it said, went well beyond that previously encountered - although it did not attribute blame for the attack.

"The threat... really does raise the bar in terms of what potential targets, and the security community in general, have to do to keep ahead of cyber attacks," said Martin Sutherland, managing director of BAE Systems Applied Intelligence.

NATO NATIONS TARGETED

Security firms have been monitoring Turla for several years.

Symantec Corp estimates up to 1,000 networks have been infected by Turla and a related virus, Agent.BTZ. It named no victims, saying only that most were government computers.

BAE said it has collected over 100 unique samples of Turla since 2010, including 32 from Ukraine, 11 from Lithuania and 4 from Great Britain. It obtained smaller numbers from other countries.

Hackers use Turla to establish a hidden foothold in infected networks from which they can search other computers, store stolen information, then transmit data back to their servers.

"While it seems to be Russian, there is no way to know for sure," said Mikko Hypponen, chief research officer with Helsinki-based F-Secure, which encountered Turla last year.

Security firms that are monitoring the threat have said the operation's sophistication suggests it was likely backed by a nation state and that technical indicators make them believe it is the work of Russian developers.

European governments have long welcomed U.S. help against Kremlin spying, but were infuriated last year to discover the scale of surveillance by America's National Security Agency that stretched also to their own territory.

AGENT.BTZ, RED OCTOBER

Security experts say stealthy Turla belongs to the same family as one of the most notorious pieces of spyware uncovered to date: Agent.BTZ. It was used in a massive cyber espionage operation on U.S. Central Command that surfaced in 2008 and is one of the most serious U.S. breaches to date. While Washington never formally attributed blame, several U.S. officials have told Reuters they believed it was the work of Russia.

Hypponen said Agent.BTZ was initially found in a military network of a European NATO state in 2008, but gave no details. F-Secure is credited with naming that piece of malware in 2008, though researchers believe it was created already in 2006.

Kaspersky Lab researcher Kurt Baumgartner said he believes Turla and Agent.BTZ are related to Red October, which suddenly shut down after his firm reported on it in January 2013.

"Unusually unique artifacts link Red October, Agent.BTZ and Turla," he said, referring to strings of text contained in the code and functionality of the malware.

Eric Chien, technical director with Symantec Security Response, described Turla as "the evolution" of Agent.BTZ. "They are a very active development group," Chien said.

Finland said its Foreign Ministry computer systems had been penetrated by an attack last year but would not elaborate.

Sweden's National Defence Radio Establishment said cyber espionage was "more common than people think", adding that it had discovered multiple attacks against authorities, governments and universities, some only detected after several years.

Government sources in the Czech Republic, Estonia, Poland and Romania said Turla had not affected them directly. Other European governments contacted by Reuters declined comment.

CHASING TURLA

Although computer security researchers have been quietly studying Turla for more than two years, public discussions of the threat only began after G Data published its report.

G Data spokesman Eddy Willems declined to name any victims or identify the author of the report, saying the firm was concerned the group behind Turla might attempt to harm him.

Jaime Blasco, director of AlienVault Labs, said that Turla was more of a "framework" for espionage than simply malware.

The malware is a "root kit" that hides the presence of the spying operation and also creates a hidden, encrypted file system to store stolen data and tools used by the attackers, he said. Those tools include password stealers, tiny programs for gathering information about the system and document stealers.

The operators can download specialized tools onto an infected system, adding any functionality they want by including it in the encrypted file system, Blasco said.

They have used dozens of different "command and control" servers located in countries around the world to control infected systems, according to Symantec, whose researchers have helped identify and shut down some of those systems.

Researchers say Turla's code is regularly updated, including changes to avoid detection as anti-virus companies detect new strains. BAE said it had two samples created in January 2014.

Chien said that in some cases when a command and control server was taken offline, Turla's operators have quickly pushed out new versions of the malware that directed infected computers to new command and control servers.

"They have a super active development team," he said.

(Additional reporting by Jan Strouhal in Prague, Marcin Goeetig in Warsaw, Guy Faulconbridge in London, Zoran Radosavljevic in Zagreb, Gwladys Fouche in Oslo, Matthias Williams in Bucharest, Gabriela Baczynska in Moscow, Alexandra Hudson in Berlin, Johan Sennero in Stockholm, Phil Stewart in Washington; Editing by Richard Valdmanis and Ralph Boulton)
