Flame pieces found in Stuxnet virus: Expert

Jim Finkle

(Reuters) - A leading computer security firm has linked some of the software code in the powerful Flame virus to the Stuxnet cyber weapon, which reportedly was used by the United States and Israel to attack Iran's nuclear program.

Eugene Kaspersky, chief executive of Moscow-based Kaspersky Lab, which uncovered Flame last month, said at the Reuters Global Media and Technology Summit on Monday his researchers have since found that part of the Flame program code is nearly identical to code found in a 2009 version of Stuxnet.

The new research could bolster the belief of many security experts that Stuxnet was part of a massive U.S.-led cyber program still active in the Middle East and perhaps other parts of the world.

Although Kaspersky did not say who he thought built Flame, news organizations, including Reuters and The New York Times, have reported the U.S. and Israel were behind Stuxnet -- which was uncovered in 2010 after it damaged centrifuges used to enrich uranium at a facility in Natanz, Iran.

Instead of issuing denials, authorities in Washington recently launched investigations into leaks about the highly classified project.

On Stuxnet and Flame, "there were two different teams working in collaboration," Kaspersky told the Reuters Summit in London.

Flame is a highly sophisticated computer virus that disguises itself as common business software. It was deployed at least five years ago and can eavesdrop on conversations on the computers it infects and steal data.

Security experts have suspected a link between Flame, Stuxnet and Duqu -- another piece of malicious software that was discovered last year -- but Kaspersky Lab is the first to say it found hard evidence.

Other private security companies were also racing to uncover the secrets of Flame and will soon weigh in on Kaspersky Lab's latest findings.

If the U.S. is proven to be a force behind Flame, it would confirm the country that invented the Internet is involved in cyber espionage -- something for which it has criticized China, Russia and other nations.

A Pentagon report last year that outlined the still-evolving U.S. cyber strategy said economic espionage could prove the greatest threat to long-term U.S. interests, pointing to thefts of industrial and defense secrets via Internet spyware.

SIMILAR TRAITS

Kaspersky Lab had said Flame was developed with a different set of tools than Stuxnet, though it said its analysis was just beginning and would take many months.

After digging deeper, Kaspersky Lab said Monday its researchers identified segments of Flame and a version of Stuxnet released in 2009 that were nearly identical -- suggesting the engineers who built the two viruses had access to the same set of source code.

That suggested tight collaboration between the teams behind the two viruses. Eugene Kaspersky said it was clear there were two or more teams with differing styles, and that Flame as a whole might have employed 100 people.

Researchers have been looking for a connection between Stuxnet and Flame because both viruses infected machines by taking advantage of a Windows flaw to launch the "autorun" feature, and infected personal computers from a small drive inserted via USB slot.

The section of code now cited as connecting the two pieces of malicious software not only concerns that flaw but does so in the same style.

The Windows flaw was unknown before Stuxnet's discovery in 2010, according to Roel Schouwenberg, one of the Kaspersky Lab researchers who helped discover the Flame virus.

Kaspersky Lab researchers did not find the Flame components in more advanced versions of Stuxnet, added Schouwenberg.

"Flame was used as some sort of a kick-starter to get the Stuxnet project going," Schouwenberg theorized. "As soon as the Stuxnet team had their code ready, they went their way."

He suspected the creators of Stuxnet removed the borrowed components from later versions so the Flame program would not be compromised if the attack on the Iranian nuclear program was discovered.

Stuxnet was discovered in 2010 and has been closely scrutinized by the world's smartest cyber sleuths. Yet Flame remained hidden until last month, when a United Nations agency asked Kaspersky Lab to look for a virus that Iran said had sabotaged its computers, deleting valuable data.

When Kaspersky's team started looking for suspicious files in the Middle East, they found Flame.

Schouwenberg said he suspected Flame may be capable of deleting data and attacking industrial control systems that run plants like the uranium enrichment facility at Natanz, but he has yet to find the evidence to prove it.

Kaspersky Lab researchers are still trying to understand the function of more than 100 mysterious files built into the Flame samples that they have discovered, he said.

Analysts already widely regard Flame as one of the most sophisticated pieces of malicious software ever detected, along with Stuxnet and its data-stealing cousin, Duqu.