Flame virus linked to Stuxnet: researchers (Update 2)

June 11 2012

The Flame computer virus which has been raging in the Middle East has strong links to Stuxnet, a malware program widely believed to have been developed by the United States or Israel, a security firm said Monday.

Kaspersky, the Russian computer security firm credited with discovering Flame last month, said its research shows the two programs share certain portions of code, suggesting some ties between two separate groups of programmers.

Kaspersky researcher Alexander Gostev said in a blog post that a first examination made it appear the two programs were unrelated.

"But it turns out we were wrong," he wrote. "Our research unearthed some previously unknown facts that completely transform the current view of how Stuxnet was created and its link with Flame."

Gostev said Flame, even though it was discovered just recently, appears to predate Stuxnet, which was created in 2009.

"By the time Stuxnet was created (in January-June 2009), the Flame platform was already in existence (we currently date its creation to no later than summer 2008) and already had modular structure," he said.

"The Stuxnet code of 2009 used a module built on the Flame platform, probably created specifically to operate as part of Stuxnet."

This, he said, points to the existence of "two independent developer teams... (each) developing its own platform since 2007-2008 at the latest."

Kaspersky, one of the world's biggest producers of anti-virus software, said the Flame virus was "about 20 times larger than Stuxnet," the worm which was discovered in June 2010 and used against the Iranian nuclear program.

High concentrations of computers compromised by Flame were also found in Lebanon, the West Bank and Hungary. Additional infections have been reported in Austria, Russia, Hong Kong and the United Arab Emirates.

Compromised computers included many being used from home connections, according to security researchers who were looking into whether reports of infections in some places resulted from workers using laptops while traveling.

Stuxnet was designed to attack computer control systems made by German industrial giant Siemens and commonly used to manage water supplies, oil rigs, power plants and other critical infrastructure.

Most Stuxnet infections have been discovered in Iran, giving rise to speculation it was intended to sabotage nuclear facilities there. The worm was crafted to recognize the system it was to attack.

Some reports say US and Israeli intelligence services collaborated to develop the computer worm to sabotage Iran's efforts to make a nuclear bomb.

Johannes Ullrich, a researcher at the Washington-based SANS Technology Institute, said the relationship between the two viruses

remains unclear.

"Flame did initially appear very different, and I still think it wasn't written by the same group or individual that wrote Stuxnet," Ullrich told AFP.

"However, this doesn't mean that the two groups didn't coordinate or share code with each other. I do think this may have been the case with Stuxnet and Flame... the code could have been written by two different contractors who worked for the same government and as a result had access to each other's resources."

(c) 2012 AFP