GlobalResearch
Center for Research on Globalization

Global Cyber-Warfare Tactics: New Flame-linked Malware used in “Cyber-Espionage”

By RT
Global Research, October 19, 2012
Russia Today

Theme: Intelligence

A new cyber espionage program linked to the notorious Flame and Gauss malware has been detected by Russia’s Kaspersky Lab. The anti-virus giant’s chief warns that global cyber warfare is in “full swing” and will probably escalate in 2013.

The virus, dubbed miniFlame, and also known as SPE, has already infected computers in Iran, Lebanon, France, the United States and Lithuania. It was discovered in July 2012 and is described as “*a small and highly flexible malicious program designed to steal data and control infected systems during targeted cyber espionage operations*,” Kaspersky Lab said in a statement posted on its website.

The malware was originally identified as an appendage of Flame – the program used for targeted cyber espionage in the Middle East and acknowledged to be part of joint US-Israeli efforts to undermine Iran’s nuclear program.

But later, Kaspersky Lab analysts discovered that miniFlame is an “*interoperable tool that could be used as an independent malicious program, or concurrently as a plug-in for both the Flame and Gauss malware.”*

The analysis also showed new evidence of cooperation between the creators of Flame and Gauss, as both viruses can use miniFlame for their operations.

“MiniFlame’s ability to be used as a plug-in by either Flame or Gauss clearly connects the collaboration between the development teams of both Flame and Gauss. Since the connection between Flame and Stuxnet/Duqu has already been revealed, it can be concluded that all these advanced threats come from the same ‘cyber warfare’ factory,” Kaspersky Lab said.

High-precision attack tool

So far just 50 to 60 cases of infection have been detected worldwide, according to Kaspersky Lab. But unlike Flame and Gauss, miniFlame in meant for installation on machines already infected by those viruses.

“*MiniFlame is a high-precision attack tool. Most likely it is a targeted cyber weapon used in what can be defined as the second wave of a cyber attack*,” Kaspersky’s Chief Security Expert Alexander Gostev explained.

“*First, Flame or Gauss are used to infect as many victims as possible to collect large quantities of information. After data is collected and reviewed, a potentially interesting*

victim is defined and identified, and miniFlame is installed in order to conduct more in-depth surveillance and cyber-espionage."

The newly-discovered malware can also take screenshots of an infected computer while it is running a specific program or application in such as a web browser, Microsoft Office program, Adobe Reader, instant messenger service or FTP client.

Kaspersky Lab believes miniFlame's developers have probably created dozens of different modifications of the program. "*At this time, we have only found six of these, dated 2010-2011,"* the firm said.

'Cyber warfare in full swing'

Meanwhile, Kaspersky Lab's co-founder and CEO Eugene Kaspersky warned that global cyber warfare tactics are becoming more sophisticated while also becoming more threatening. He urged governments to work together to fight cyber warfare and cyber-terrorism, Xinhua news agency reports.

Speaking at an International Telecommunication Union Telecom World conference in Dubai, the anti-virus tycoon said, "cyber warfare is in full swing and we expect it to escalate in 2013."

"*The latest malicious virus attack on the world's largest oil and gas company, Saudi Aramco, last August shows how dependent we are today on the Internet and information technology in general, and how vulnerable we are*," Kaspersky said.

He stopped short of blaming any particular player behind the massive cyber attacks across the Middle East, pointing out that "*our job is not to identity hackers or cyber-terrorists. Our firm is like an X-ray machine, meaning we can scan and identify a problem, but we cannot say who or what is behind it."*

Iran, who confirmed that it suffered an attack by Flame malware that caused severe data loss, blames the United States and Israel for unleashing the cyber attacks.
