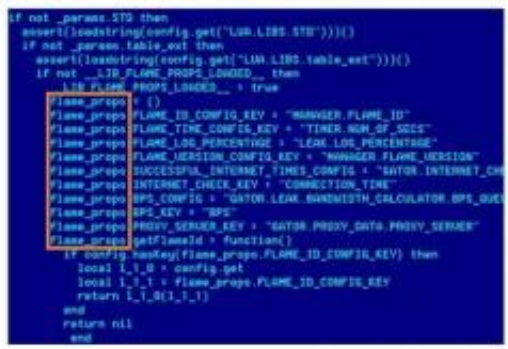
Flame virus a new age cyber spy tool

May 31 2012, by Glenn Chapman



Code from the computer virus known as Flame. The virus that smoldered undetected for years in Middle Eastern energy facilities has confirmed fears that the world has entered a new age of cyber espionage and sabotage, experts say.

The Flame computer virus that smoldered undetected for years in Middle Eastern energy facilities confirmed fears that the world has entered a new age of cyber espionage and sabotage.

Internet defenders on Wednesday were tearing into freshly exposed Flame malware (malicious software) that could be adapted to spread to critical infrastructures in countries around the world.

While the components and tactics of Flame were considered old school, the gigantic virus's interchangeable software modules and targeted nature were evidence that malware is a potent weapon in the Internet era.

"We are seeing much more specific types of malware and attacks," said

McAfee Labs director of security research David Marcus.

"When you talk about a situation where the attacker knows the victim and tailors the malware for the environment it jumps out," he said. "That speaks to good reconnaissance and an attacker who knows what they are doing."

Gathering intelligence on targets and then crafting viruses to exploit specific networks as well as the habits of people using them is "certainly in vogue" and is an attack style heralded by the Stuxnet malware, Marcus said.

Stuxnet, which was detected in July 2010, targeted 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 were discovered in Iran, giving rise to speculation it was intended to sabotage nuclear facilities there, especially the Russian-built atomic power plant in the southern city of Bushehr.

Suspicion fell on Israel and the United States, which have accused Iran of seeking to develop a weapons capability under the cover of a civilian nuclear drive. Tehran denies the charges.

"Stuxnet and Duqu belonged to a single chain of attacks, which raised cyberwar-related concerns worldwide," said Eugene Kaspersky, founder of Kaspersky Lab, which uncovered Flame.

"The Flame malware looks to be another phase in this war, and it's important to understand that such cyber weapons can easily be used against any country."

Flame malware was larger than Stuxnet and protected by multiple layers of encryption.

It appears to have been "in the wild" for two years or longer and prime targets so far have been energy facilities in the Middle East.

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

File photo shows Kaspersky Lab employees in Moscow. Kaspersky Lab, one of the world's biggest producers of anti-virus software, said its experts discovered a new computer virus with unprecedented destructive potential that chiefly targets Iran and could be used as a "cyberweapon" by the West and Israel.

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.

While Stuxnet was crafted to do real-world damage to machinery, Flame

was designed to suck information from computer networks and relay what it learned back to those controlling the virus.

Flame can record keystrokes, capture screen images, and eavesdrop using microphones built into computers.

In an intriguing twist, the malware can also use Bluetooth capabilities in machines to connect with smartphones or tablets, mining contact lists or other information, according to security researchers.

"There is lot of intelligence gathering and espionage-like behavior from the malware," Marcus said. "You can turn that to target any industry you want.

"It looks like the infection spread is specific to Middle East, but malware is indiscriminate in a lot of things so it can jump," he continued.

Marcus advised companies to not only keep network software up to date but to ratchet up security settings because threats such as Flame are carefully crafted to "fly under the radar."

For example, Flame reportedly sneaked back out to the Internet by activating a seemingly innocuous Internet Explorer online browsing session.

Geographically targeted cyber espionage and even modular components in viruses have been around for years, Rik Ferguson of security firm Trend Micro said in his blog at countermeasures.trendmicro.eu.

Flame stands out for being a malware behemoth of nearly 20 megabytes and for its use of Bluetooth capabilities, according to Ferguson, who branded the malware a tool, not a weapon.

"You can't get around the fact that the thing is gigantic," Marcus said. "Someone went to a lot of trouble to really confound researchers. We are going to be ripping this sucker apart for a long time to figure everything it was doing."

(c) 2012 AFP