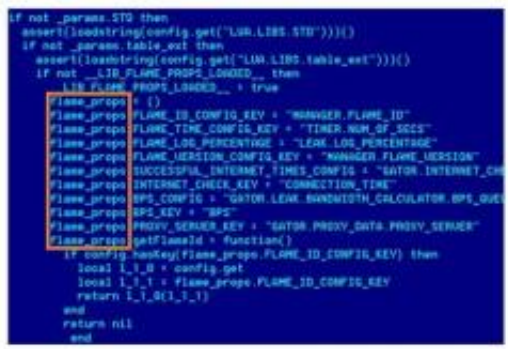
Flame spy virus gets order to vanish: experts

June 10 2012, by Glenn Chapman



This undated screen grab taken released by the Kaspersky Lab site shows a program of the computer virus known as Flame. US computer security researchers said Sunday that the Flame computer virus that smoldered undetected for years in Middle Eastern energy facilities has gotten orders to vanish, leaving no trace.

US computer security researchers said Sunday that the Flame computer virus that smoldered undetected for years in Middle Eastern energy facilities has gotten orders to vanish, leaving no trace.

Anti-virus company Symantec said in a blog post that late last week, some Flame "command-and-control servers sent an updated command to several compromised computers."

"This command was designed to completely remove (Flame) from the compromised computers."

Flame malicious software (malware) 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, especially in Iran.

The discovery of Flame immediately sparked speculation that it had been created by US and Israeli security services to steal information about Iran's controversial nuclear drive.

Kaspersky Lab, 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.

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.

Computers infected with malware are typically programmed to reach out on the Internet to get updated orders from command servers controlled by hackers.

In this case, it appeared that Flame masters gave an order for the malware to vanish, leaving behind no trail that investigators might be

able to follow or clues to its origin.

The self-destruct command was evidently sent after Flame was exposed and investigations commenced.

Infected computers that got the command went on to delete an array of files and then cram disks with random characters to thwart recovery of original code, according to security researchers.

It was unknown how many infected computers received the self-destruct command.

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