the Availability Digest

www.availabilitydigest.com

First Stuxnet – Now the Flame Virus

June 2012

It was just two years ago, in June, 2010, that the Stuxnet virus was found.[1] At the time, it was termed "the most refined piece of malware ever discovered." The worm was significant because mischief or financial reward wasn't its purpose. It was aimed right at the heart of a critical infrastructure. Stuxnet was specifically designed to cause Iran's centrifuges used in its nuclear program to spin out of control and to destroy themselves. It was the first known virus that could damage critical infrastructure.

The international alarm created by Stuxnet has now been superseded by a newly discovered virus, Flame (also known as Flamer or sKyWIper). The UN's International Telecommunications Union (ITU) has issued a Flame warning to its member nations that it says is the most serious cyber warning it has ever put out. In its present form, Flame is not designed to do physical damage. Rather. it is an extraordinarily sophisticated surveillance tool that appears to be used for dangerous espionage of targeted systems. However, its architecture lends itself to be easily extended to Stuxnet-like destructive capabilities.

The Discovery of Flame

Flame was discovered quite by accident by the large Russian anti-virus firm, Kaspersky Labs, the same company that first identified Stuxnet. The Iranians had notified the ITU about a virus that was wiping out disk files. The ITU asked Kaspersky Labs, which provides virus protection for Iran, to try to find the virus. Kaspersky was unable to do so, but instead found Flame in April, 2012. It determined that Flame had infected almost 200 Iranian computers and was targeting Iran's Oil Ministry, its oil rigs, and its major oil export hub. In response, Iranian computer technicians took drastic actions, cutting off all Internet links to its computers.

Kaspersky announced Flame to the international community just recently, on May 28, 2012. However, it estimated that Flame has been around, undetected, since 2010.

When Stuxnet was discovered, its size was surprising. It measured a half-megabyte in size, which was considered quite large for malware. In comparison, Flame is massive. It comprises about 20 megabytes of code! It is deemed to be the most complex malware ever found.

Interestingly, its very size may be what allowed it to go undetected for two years. Evidently, malware-detection facilities assume that viruses are small so as to go undetected. The massive size of Flame made it appear not to be malware at all.

Further, as we will describe, Flame has infected only a very small number of targeted computers. It operates in such a way that a user never notices its actions; and when it has finished its job, it deletes itself and moves on to other computers.

[1] Stuxnet – The World's First Cyber Weapon, *Availability Digest*; March 2011. http://www.availabilitydigest.com/public_articles/0603/stuxnet.pdf

What Does Flame Do?

In its present form, Flame is an exceptionally powerful piece of spyware. It can:

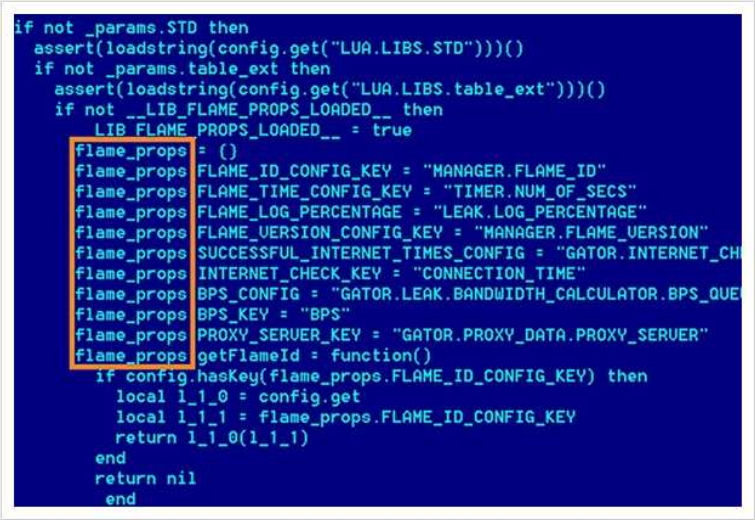
- copy data found on the computer's disks.
- activate the computer's microphone so that it can eavesdrop on office conversations.
- eavesdrop on Skype calls.
- log keystrokes.
- take screen shots.
- steal data from Bluetooth-enabled devices connected to the computer.
- steal data from USB devices connected to the computer.
- infect USB flash drives and re-infect any computer into which the drive is inserted.
- copy itself to other computers on the network.

In short, it can control every aspect of a computer. It organizes the data it collects and communicates that data back to one of many command and control servers for further analysis via an encrypted link. When it has finished with a computer, it deletes itself without a trace.

How Is Flame Built?

Kaspersky Labs, Symantic, and others have called Flame the most powerful, ingenious, and stealthy malware ever written.

Surprisingly, the Flame core is programmed in Lua, a video-gaming language used for such popular games as Angry Bird. The Flame core comprises twenty modules, each with a different purpose. It can deploy any of its modules to a targeted computer. The module subroutines and libraries are generally written in C++, and the total package comprises about 650,000 lines of code and consumes twenty megabytes of storage. It currently infects only Windows systems – Windows 7, Windows XP, and Vista.



AFP - Getty Images

Each of Flame's surveillance capabilities is represented by a separate module. It appears that a computer is infected initially with only a basic set of modules. Stolen data is organized into a local SQL database and periodically sent over an SSL link to a network of eighty command and control computers located in Asia, Europe, and North America for further analysis by the Flame operators. It they determine that a specific computer is of interest, the operators can deploy additional modules for further surveillance.

It appears that the network of command and control computers represents a limited resource. Only a small number of computers are infected at any one time. When Flame has finished with a computer, it deletes itself without a trace and moves on to another computer.

It is not known how Flame is spread. Common conjecture is that it initially spreads through email phishing, and then spreads itself further over networks and via removable media.

So far, there has been no evidence of malicious, damaging actions by Flame, such as disk wiping or attacking critical infrastructure. However, with its modular architecture, there is not much to prevent such attack modules from being developed and deployed in the future.

How Far Has Flame Spread?

Because Flame infects only a few computers at a time and departs a computer when it has finished without a trace, it cannot be determined how many computers Flame has infected. The rough estimates are that it has infected between 1,000 and 5,000 computers so far.

It appears that most of the infected computers are in Middle Eastern countries. Of roughly 400 confirmed infections, almost half are in Iran. Israel and the Palestine territories account for 25% of the infections. A few infections have been discovered in Sudan, Syria, Lebanon, Saudi Arabia, and Egypt.

Who Dunnit?

Because of the size and complexity of Flame, it is generally thought that it could only have been produced and propagated via a nation-state. As with Stuxnet, the leading suspects are Israel and the United States. Neither country has confirmed that it is party to the Flame attacks. It has been noted that only traces of good English have been found in the code

However, Israel has not gone so far as to deny complicity. An Israel leading politician, Vice Premier Moshe Yaalon, made the following statement:

> "Whoever sees the Iranian threat as a significant threat is likely to take various steps, including these, to hobble it. Israel is blessed with high technology, and we boast tools that open all sorts of opportunities for us."

The Defenses Against Flame

Running and debugging Flame is not trivial. It comprises several DLL libraries that are loaded at system boot time. It includes SQL databases with nested queries and uses several encryption methods and compression algorithms. It is purposefully written to be confusing to thwart security experts from easily deciphering it. Kaspersky Labs estimates that it may take years to fully understand Flame.

However, Kaspersky Labs and other antivirus organizations, as well as Iran, have released detection and removal kits for Flame.

Summary

What might the future bring? Stuxnet and Flame have demonstrated troubling capabilities for nation-states to wage cyber war on each other. Maliciousness can range from sophisticated surveillance to attacks against critical infrastructure. This malware is becoming increasingly difficult to detect and impossible to track to its source.

It seems that cyber warfare has arrived, and it is incumbent upon every organization and every nation to take steps to protect its confidential data and its critical infrastructure.

Postscript

According to a June 6th Symantic report, the controllers of Flame have ordered it to self-destruct and to erase all traces of itself in order to impede the forensic analysis of its code. A suicide module is trying to locate every infected computer to remove Flame's files and to overwrite the disk areas that it used with

random data. It is thought that this is an attempt to hide the authors' identities and to prevent analysis that would allow the development of effective countermeasures.

Will Flame reappear at some time in the future with even more devastating capabilities? Stay tuned.

References

Fox News; May 31, 2012
Iran: 'Flame' virus fight began with oil attack, *Associated Press*; May 30, 2012.
Was Flame virus written by cyberwarriors or gamers?, *MSNBC*; undated.
'Flame' Virus explained: How it works and who's behind it, *RT*; May 29, 2012.
The Flame: Questions and Answers, *Securelist*; May 28, 2012. (Kaspersky Labs blog)
Was Flame virus that invaded Iran's computer networks made in USA?, *MSNBC*; undated.
Stuxnet x20: Massive cyber spy virus 'Flame' hits Iran, Israel, *RT*; May 29, 2012.
Flame virus could attack other nations, *CNET News*; May 30, 2012.
The Flame Virus: Spyware on an Unprecedented Basis, *ReadWriteWeb*; May 30, 2012.
Iran confirms flame virus attacked computers of high-ranking officials, *The Telegraph*; May 30, 2012.
Iran acknowledges that Flame virus has infected computers nationwide, *Washington Post*; undated.
Israel Gets the Blame for Flame Virus, *IHT Rendezvous*; May 29, 2012.
Iran: Powerful "Flame" computer virus briefly hit oil industry but was defeated with data recovered, *PC World*; May 30, 2012.
Iran admits 'Flame' virus caused substantial damage, *The Hindu*; undated.
Flame virus had massive impact on Iran, says Israeli security firm, *Haaretz*; undated.
Iran says Flame virus could be cause behind "mass data loss," UN to send out warning, *Venture Beat*; May 29, 2012.
Flame virus most powerful espionage tool ever, UN warns, *The Telegraph*; May 29, 2012.
World Powers Play Games With Flame Virus, *US News and World Reports*; May 30, 2012.
UN agency plans major warning on Flame virus risk, *Reuters*; May29, 2012.