GlobalResearch
Center for Research on Globalization

“Stuxnet” and “Flame”: With New Malware Virus, Israel Fans A Virtual Flame Against Iran

By Pierre Klochendler
Global Research, June 28, 2013
Inter Press Service 31 May 2012

Region: Middle East & North Africa
Theme: Intelligence, US NATO War Agenda
In-depth Report: IRAN: THE NEXT WAR?

The IPS article below originally posted by Global Research on May 31, 2012 sheds light on what is now “official” following the alleged leak of classified information about a covert cyberattack on Iran’s nuclear facilities.

> Retired Marine Gen. James “Hoss” Cartwright has been told he is a target of the probe, NBC News and The Washington Post reported Thursday. A “target” is someone a prosecutor or grand jury has substantial evidence linking to a crime and who is likely to be charged.
>
> The Justice Department referred questions to the U.S. attorney’s office in Baltimore, where a spokeswoman, Marcia Murphy, declined to comment.

With New Malware Virus, Israel Fans A Virtual Flame Against Iran

Pierre Klochender

IPS, May 31, 2012

A new super-weapon has entered the Mideast cyber arena. First detected on Monday by a Moscow-based security company, ‘Worm.Win32.Flame’ – just call it ‘Flame’ – might be “the most sophisticated cyber weapon yet unleashed” on Iran’s secret nuclear networks.

“Flame can easily be described as one of the most complex threats ever discovered. Big and incredibly sophisticated, it redefines the notion of cyber-war and cyber-espionage,” Alexander Gostev posted on the ‘Securelist’ blog of Kaspersky Labs, the company that uncovered the worm. Gostev is head of the firm’s Global Research and Analysis Team.

The newly-discovered multi-task device sniffs network traffic, takes screenshots when certain applications of interest are run, records audio conversations, intercepts keyboards – the web seems to be the limit.

From an initial analysis performed by Kaspersky Labs, the ‘Flame’ creators gather highly sensitive intelligence on highly sensitive operations of states, principally in the Middle East – e-mails, documents, messages, or discussions inside sensitive locations – and can “target SCADA (supervisory control and data acquisition) devices, ICS (industrial control systems), critical infrastructure and so on.”

The hijacked data is then retrieved by operators through links to command-and-control (C&C) servers. “Key here is Flame’s completeness – the ability to steal data in so many different ways,” Gostev notes.

Kaspersky Labs discovered ‘Flame’ following a request from the United Nations. The world body’s International Telecommunication Union suspected the existence of an unknown malware – codenamed ‘Wiper’ – whose task would be to delete sensitive information across the Middle East.

Iran is the top target, with the worm ‘crawling’ in at least 189 of its computers. The West Bank comes second with 89 infected computers.

Sudan comes third with 32 damaged computers. Then almost in a tie, stands Syria with the worm identified in 30 computers. Eighteen computers were targeted in Lebanon; ten in Saudi Arabia. Next but not last is Egypt, with five contaminated computers. All, except the latter, are considered enemy states of Israel.

In its blog, the security software maker Symantec said ‘Flame’ was also uncovered in computers in Hungary, Austria, Russia, Hong Kong and the United Arab Emirates.

Though no trace in the code ties the latest malware to any specific copyrighter, author or state, Iran indirectly blamed Israel for ‘Flame’.

“Some countries and illegitimate regimes are used to producing viruses,” Foreign Ministry Spokesman Ramin Mehman-Parast was quoted on Tuesday in the semi-official Iranian news agency Fars.

Tehran often refers to Israel as “the illegitimate Zionist regime”. The allegation was based on an interview given on Monday by Israeli Vice Prime Minister Moshe Ya’alon to Israel Army Radio.

“Anyone who sees the Iranian (nuclear) threat as a significant threat – it’s reasonable (to assume) that he’ll take various steps, including these, to harm it,” Ya’alon declared. He said “Israel is blessed as a country rich with high-tech; these tools that we take pride in open up all kinds of opportunities for us.”

According to a New York Times investigation published in January, ‘Stuxnet’, the cyber villain discovered in 2010 which attacked Iranian centrifuges, specifically in the Natanz uranium enrichment facility, was tested within the premises of the Dimona nuclear complex located in southern Israel.

According to Gostev, links could indicate that the ‘Flame’ wizards accessed technology used in ‘Stuxnet’. Indeed, the worm seems to have run in parallel to the ‘Stuxnet’ project as preliminary analyses show it’s been disseminated since February 2010.

Kaspersky Labs points at certain characteristics shared by ‘Flame’ and ‘Stuxnet’, but unlike ‘Stuxnet’ which damages computerized equipment, ‘Flame’ is meant to collect information.

‘Duqu’, another information-gathering malware useful in targeting ICS systems and attached to ‘Stuxnet’ was first uncovered in 2011 by the Laboratory of Cryptography and System Security (CrySyS) of the Budapest University of Technology and Economics.

In April, news came out from Iran that Tehran disconnected servers from the Internet as a cyber outbreak stroke at the Kharg island oil terminal (from which Iran exports some 80 percent of its crude oil). The attack is now thought to have been provoked by 'Flame'.

The major difference between 'Flame' and the 'Stuxnet/Duqu' project lies in the fact that the 'Flame' code is 20 times larger, and targets thousands of systems worldwide, including computers in academia, private companies and of specific individuals.

What's more, operators "can conduct analysis of the data of the victim systems and uninstall 'Flame' from systems that aren't interesting, leaving the most important ones in place. After which they start a new series of infections," Gostev emphasized.

Ilan Proimovich, Kaspersky's representative in Israel, told Army Radio that the worm "is operated by remote control. It's not always active, thus it's so difficult to detect."

Though the common assumption is that a small code like the one of 'Stuxnet' is easier to hide, the large size of the 'Flame' code (over 20MB) is precisely why it wasn't discovered for so long, notes Gostev.

While the analysis of the 'Stuxnet' code (500K) took months, it's estimated that deciphering the more complex 'Flame' code will last at least a year.

Israeli Information Security analysts say the worm highlights the Iranian nuclear program's Achilles heel – its inability to ward off cyber attacks.

Assaf Turner, CEO of the Israeli-based Maya Security company, believes that "'Flame' likely penetrated highly secure computer systems" in Iran.

"Iran's brush with 'Duqu' and disastrous encounter with 'Stuxnet' prove that the Islamic Republic is, indeed, lacking in the field of cyber security," he asserted on the Israeli news site YNet.

One could entertain the euphoric dream that the current cyber-espionage war would provide an elegant, virtual, way to put an end to the alarming suspicion that Iran is developing the capability to master the doomsday weapon. This, before other far more mortal means are employed to try to destroy the nuclear threat once and for all.

The original source of this article is Inter Press Service

Articles by: **Pierre Klochendler**

Disclaimer: The contents of this article are of sole responsibility of the author(s). The Centre for Research on Globalization will not be responsible for any inaccurate or incorrect statement in this article. The Centre of Research on Globalization grants permission to cross-post Global Research articles on community internet sites as long the source and copyright are acknowledged together with a hyperlink to the original Global Research article. For publication of Global Research articles in print or other forms including commercial internet sites, contact: publications@globalresearch.ca

For media inquiries: publications@globalresearch.ca