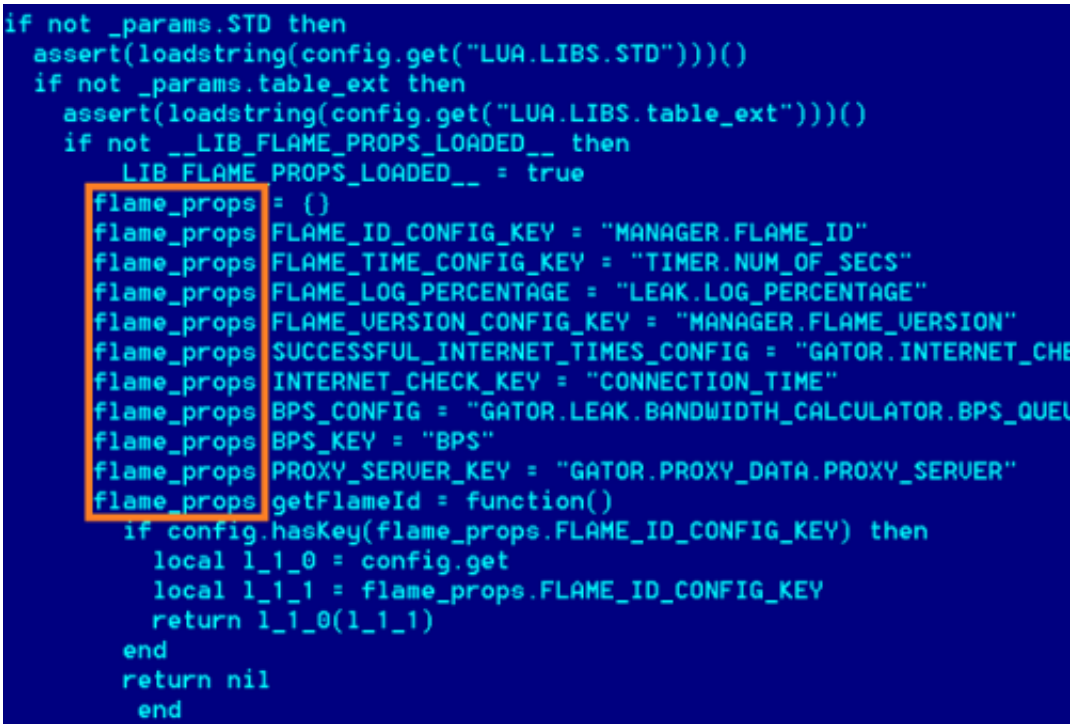
Global wave of Flame cyber attacks called staggering

May 28 2012, by Nancy Owano



(Phys.org) -- Kaspersky Lab has discovered complex malware that has been in operation for at least five years, collecting data from countries including both Israel and Iran. Kaspersky experts think the masterminds are state-sponsored but have come short of short of naming exact origins. The malicious program is detected as Worm.Win32.Flame by Kaspersky Lab's security products. The UN International

Telecommunication Union has worked with Kaspersky Lab in the investigation, which finds that individuals, businesses, academic institutions and government systems have been hit. The total number of targets is an estimated 600.

Iran has acknowledged Flame as a source of malware incidents. Iran's National Computer Emergency Response Team has posted a security alert stating Flame behind recent incidents of data loss. Other countries affected by the attack are Israel, Sudan, Syria, Lebanon, Saudi Arabia and Egypt.

Flame is considered extraordinary. Move over Stuxnet, which struck Iran . Step aside Wiper, deleting information in Western Asia. Later for Duqu, infiltrating networks to steal data. This is called “one of the most complex threats ever discovered,” according to Kaspersky. Flame is a backdoor, a Trojan, and it has worm-like features. It can replicate in a local network and on removable media on command. The chief malware expert Vitaly Kamluk at Kaspersky explains that Flame goes to work to siphon off sensitive information, by first sniffing network traffic, taking screenshots, recording audio conversations via microphone, compressing it and sending it back to the attacker, and intercepting the keyboard. Once the initial Flame malware has infected a machine, more modules can be added to perform specific tasks, as if adding apps to a smartphone. Kamluk says he is convinced that this is sophisticated work enabled by “nation-state” sponsorship.

The Malware code is 20 times larger than Stuxnet. The Flame package of modules is reported as huge, at 20MB when fully deployed. Flame is huge because of what it includes--libraries, such as for compression (zlib, libbz2, ppmd) and database manipulation (sqlite3), together with a Lua (a scripting language) virtual machine. Many parts of Flame have high order logic written in Lua with effective attack subroutines and libraries compiled from C++, according to Kaspersky Lab.

One computing professor from University of Surrey sees no reason not to agree with Kaspersky that Flame is massive, complex, and unusual. Prof. Alan Woodward said, like Stuxnet, Flame can be spread by USB stick but has “very unusual” data-stealing features. He likens the Flame malware to an industrial vacuum cleaner. Flame reaches out to any Bluetooth-enabled device nearby, for example. Flame is an extremely advanced attack, he said, and “is more like a toolkit for compiling different code-based weapons than a single tool.”

Kaspersky’s Aleks Gostev, chief security expert, said that Flame ”redefines the notion of cyberwar and cyberespionage.” He said that the malware was still stealing data. "One of the most alarming facts is that the Flame cyber attack campaign is currently in its active phase, and its operator is consistently surveying infected systems.”

More information: www.securelist.com/en/blog/208 … uestions_and_Answers

Citation: Global wave of Flame cyber attacks called staggering (2012, May 28) retrieved 24 April 2024 from https://phys.org/news/2012-05-global-flame-cyber-staggering.html