New version of Flame virus uncovered: researchers

October 15 2012

A new cyberespionage tool linked to the Flame virus has been infecting computers in Lebanon, Iran and elsewhere, security researchers said.

A new cyberespionage tool linked to the Flame virus has been infecting computers in Lebanon, Iran and elsewhere, security researchers said Monday.

Kaspersky Lab, which was credited with revealing the Flame virus earlier this year, dubbed the new malware "miniFlame," and said it was "a small and highly flexible malicious program designed to steal data and control infected systems during targeted cyber espionage operations."

Russian-based Kaspersky said miniFlame "is based on the same architectural platform as Flame," widely reported to be part of a US-Israeli effort to slow Iran's suspected nuclear weapons drive.

The smaller version "can function as its own independent cyber espionage program or as a component" inside Flame and related malware.

Unlike Flame, which is designed for "massive spy operations," miniFlame is "a high precision, surgical attack tool," according to Alexander Gostev at Kaspersky Lab.

"Most likely it is a targeted cyberweapon used in what can be defined as the second wave of a cyberattack."

Kaspersky Lab data indicates the total number of infections worldwide is just 50 to 60, including computers in Lebanon, France, the United States, Iran and Lithuania.

MiniFlame operates "as a backdoor designed for data theft and direct access to infected systems," according to Kaspersky, which said development of the malware might have started as early as 2007 and continued until the end of 2011, with several variations.

"We believe that the developers of miniFlame created dozens of different modifications of the program," Kaspersky said. "At this time, we have only found six of these, dated 2010-2011."

Flame previously has been linked to Stuxnet, which attacked computer control systems made by German industrial giant Siemens used to manage water supplies, oil rigs, power plants and other critical infrastructure.

Most Stuxnet infections have been discovered in Iran, giving rise to speculation it was intended to sabotage nuclear facilities there. The worm was crafted to recognize the system it was to attack.

Some reports say US and Israeli intelligence services collaborated to develop the computer worm to sabotage Iran's efforts to make a nuclear bomb.

(c) 2012 AFP

Citation: New version of Flame virus uncovered: researchers (2012, October 15) retrieved 26 April 2024 from https://phys.org/news/2012-10-version-flame-virus-uncovered.html