Virus found in Middle East that can spy on finance transactions

Jim Finkle, Rueters

(Reuters) - A new cyber surveillance virus has been found in the Middle East that can spy on financial transactions, email and social networking activity, according to a leading computer security firm, Kaspersky Lab.

Dubbed Gauss, the virus may also be capable of attacking critical infrastructure and was built in the same laboratories as Stuxnet, the computer worm widely believed to have been used by the United States and Israel to attack Iran's nuclear program, Kaspersky Lab said on Thursday.

The Moscow-based firm said it found Gauss had infected personal computers in Lebanon, Israel and the Palestinian Territories. It declined to speculate on who was behind the virus but said it was related to Stuxnet and two other cyber espionage tools, Flame and Duqu.

"After looking at Stuxnet, Duqu and Flame, we can say with a high degree of certainty that Gauss comes from the same 'factory' or 'factories,'" Kaspersky Lab said in a posting on its website. "All these attack toolkits represent the high end of nation-state-sponsored cyber-espionage and cyber war operations."

Kaspersky Lab's findings are likely to fuel a growing international debate over the development and use of cyber weapons. Those discussions were stirred up by the discovery of Flame in May by Kaspersky and others. Washington has declined comment on whether it was behind Stuxnet.

According to Kaspersky Lab, Gauss can steal Internet browser passwords and other data, send information about system configurations, steal credentials for accessing banking systems in the Middle East, and hijack login information for social networking sites, email and instant messaging accounts.

Modules in the Gauss virus have internal names that Kaspersky Lab researchers believe were chosen to pay homage to famous mathematicians and philosophers, including Johann Carl Friedrich Gauss, Kurt Godel and Joseph-Louis Lagrange.

Kaspersky Lab said it called the virus Gauss because that is the name of the most important module, which implements its data-stealing capabilities.

One of the firm's top researchers said Gauss also contains a module known as "Godel" that may include a Stuxnet-like weapon for attacking industrial control systems.

Stuxnet, discovered in 2010, spread via USB drives and was designed to attack

computers that controlled the centrifuges at a uranium enrichment facility in Natanz, Iran [1].

(Jim Finkle in Boston, editing by Tiffany Wu and John Wallace)

Source URL (retrieved on *03/08/2014 - 8:15pm*):
http://www.ecnmag.com/news/2012/08/virus-found-middle-east-can-spy-finance-transactions

Links:
[1] http://www.reuters.com/places/iran