The New York Times

August 10, 2012

BITS; Computer Virus Is Aimed at Banks in Lebanon, Security Firm Says

By NICOLE PERLROTH

A security firm said Thursday that it had discovered what it believed was the fourth state-sponsored computer virus to surface in the Middle East in the last three years, apparently aimed at computers in Lebanon.The firm, Kaspersky Lab, said that the virus appeared to have been written by the same programmers who created Flame, the data-mining computer virus that was found to be spying on computers in Iran in May, and that it might be linked to Stuxnet, the virus that disrupted uranium enrichment work in Iran in 2010.

The latest virus, nicknamed Gauss after a name found in its code, has been detected on 2,500 computers, most in Lebanon, the firm said. Its purpose appeared to be to acquire logins for e-mail and instant messaging accounts, social networks and, notably, accounts at certain banks - a function more typically found in malicious programs used by profit-seeking cybercriminals.

The researchers said the target banks included several of Lebanon's largest - the Bank of Beirut, Blom Bank, Byblos Bank and Credit Libanais - along with Citibank and the online payment system PayPal.

"We have never seen any malware target such a specific range of banks," Costin Raiu, Kaspersky's director of global research and analysis, said in an interview. "Generally, cybercriminals target as many banks as possible to maximize financial profit, but this is a very focused cyberespionage campaign targeting certain users of online banking systems."

Lebanon experts said that an American cyber espionage campaign directed at Lebanon's banking system would seem to be a plausible possibility, given Washington's concerns that the country's banks are being used as a financial conduit for the Syrian government and for Hezbollah, the Lebanese militant group and political party.

"The United States has had a number of Lebanese banks under the microscope for a while," said Bilal Y. Saab, a Lebanon expert at the Monterey Institute of International Studies, who said the banks "operate much like Swiss banks" in terms of secrecy. "A computer virus could completely undermine that," he said.

Researchers at Kaspersky Lab, based in Moscow, said they found the Gauss virus while analyzing the Flame virus in June. Flame is a reconnaissance tool that can capture images of a user's computer screen, record e-mail and chat sessions, turn on microphones remotely and monitor keystrokes and network traffic. It can infect an offline computer through a USB stick or a Bluetooth connection.

Kaspersky's researchers said they were confident that Gauss was the work of the same hands as Flame, because the two viruses were written in the same language (known as C++) on the same platform and shared some code and features. Different people probably wrote Doqu and Stuxnet, the first two state-sponsored viruses to surface in recent years, they said, but all four were probably commissioned by the same state-sponsored entity.

"There is absolutely no doubt that Gauss and Flame were printed by the same factories," Mr. Raiu said. "An early version of Stuxnet used a module from Flame, which shows they are connected. Stuxnet was created by a nation-state - it simply could not have been designed without nation-state support - which means Flame and Gauss were created with nation-state support as well."

Kaspersky Lab has declined to speculate on which nation-states were responsible. The New York Times reported in June, based on interviews with officials in several countries, that Stuxnet was jointly developed by the United States and Israel.

Security experts not connected with the lab were less sure that a government was behind Gauss. "It's a fairly large leap, in terms of deductive reasoning, to assume that because they share a common architectural platform, this variant is also state-sponsored," said Will Gragido of RSA, a security firm, who has studied Flame but has not yet analyzed Gauss. "It's possible the code was made available underground and repurposed or reused by cybercriminals."

Kaspersky researchers said Gauss contained a "warhead" that seeks a very specific computer system with no Internet connection and installs itself only if it finds one. "It's done in such a clever way that security researchers cannot analyze it, because they don't know the decryption key that unlocks the true purpose of that program," Mr. Raiu said.

http://query.nytimes.com/gst/fullpage.html?res=9C02E5DA1438F933A2575BC0A9649D8B63&ref=lebanon&pagewanted=print