SpyEye Trojan defeating online banking defenses

computerworld.com/article/2509482/spyeye-trojan-defeating-online-banking-defenses.html

Banks are facing more trouble from SpyEye, a piece of malicious software that steals money from people's online bank accounts, according to new research from security vendor Trusteer.

SpyEye is a particularly nasty piece of malicious software: it can harvest credentials for online accounts and also initiate transactions as a person is logged into their account, literally making it possible to watch their bank balance drop by the second.

In its latest versions, SpyEye has been modified with new code designed to evade advanced systems banks have put in place to try and block fraudulent transactions, said Mickey Boodai, Trusteer's CEO.

Banks are now analyzing how a person uses their site, looking at parameters such as how many pages a person looks at on the site, the amount of time a person spends on a page and the time it takes a person to execute a transaction. Other indicators include IP address, such as if a person who normally logs in from the Miami area suddenly logs in from St. Petersburg, Russia.

SpyEye works fast, and can automatically and quickly initiate a transaction much faster than an average person manually on the website. That's a key trigger for banks to block a transaction. So SpyEye's authors are now trying to mimic -- albeit in an automated way -- how a real person would navigate a website.

"They used to pay less attention to the way they execute transactions on the bank's website and now they are really trying to show normal user patterns," Boodai said. "

Boodai said he has little idea of how successful SpyEye's new evasion code is, although Trusteer does collect intelligence from banks that have distributed its browser security tool, Rapport, to their customers. Trusteer has also noticed that SpyEye in recent months has expanded the number of financial institutions it is able to target in an increasing number of countries.

New target countries include Russia, Saudi Arabia, Bahrain, Oman, Venezuela, Belarus, Ukraine, Moldova, Estonia, Latvia, Finland, Japan, Hong Kong and Peru. What that means is that more criminal groups around the world are purchasing the SpyEye toolkit, Boodai said.

Financial institutions continue to increase their security spending to protect online transactions, said Avivah Litan, an analyst at Gartner who regularly consults banks on security issues.

Even to her, financial institutions are coy about revealing how hard they've been hit, but "everyone refers to Zeus or SpyEye -- some as common as the word 'teller'" Litan said.

Police have had some limited successes. In April, a 26-year-old Lithuanian and a 45-year-old Latvian were charged with conspiracy to cause unauthorized modifications to computers, conspiracy to defraud and concealing proceeds from crime for allegedly using SpyEye. A third, 26-year-old man whose nationality was not revealed was bailed pending further questioning.

SpyEye is actually a botnet with a network of command-and-control servers hosted around the world. As of Tuesday, some 46 command-and-control servers were online, according to the SpyEye Tracker, a website dedicated to gathering statistics about the malicious software.

That is sharply up. In May, there were just 20 or so active servers responding to computers that were infected with SpyEye, said Roman Hüssy, who runs the site.

"SpyEye is growing quite well," he said.

Send news tips and comments to jeremy_kirk@idg.com