Bank account-draining Zeus gets lots of action in 2013

June 5 2013, by Nancy Owano

(Phys.org) —A Trojan program designed to steal money from people's bank accounts has not only been around for years but is now on the rise. A *New York Times* Bits blog report said it is enjoying a good life on Facebook. If you click on the wrong link on Facebook, the virus gets access to your bank account and can steal your money, according to the report. Called Zeus, the malicious program dates back to around 2007, but security experts say it rose steadily this year. According to Cupertino, California-based Trend Micro, incidents of Zeus gained momentum, and the firm's Zeus watchers pointed to a steady rise in the first five months of 2013. Actually, what has been seen are what Trend Micro refers to as Zeus/ZBOT variants, the same old type of threat resurfacing but now with refinements and new features.

According to Trend Micro, "ZBOT variants surged in the beginning of February and continued to be active up to this month. It even peaked during the middle of May 2013. These malware are designed to steal online credentials from users, which can be banking credentials/information or other personally identifiable information."

The nasty part about Zeus is that it does not make itself immediately known. No crashes or signs of chaos leave no cause for suspicion that anything has gone wrong and the user takes no immediate action. Zeus lurks silently but if a user logs into a bank site the program does its work, stealing log-in information and passwords and draining accounts, as well as further exercising its resources to peddle stolen personal information. (The compromised websites may not look strange; the user may easily assume at first glance that the page looks "legitimate," but there may be additional blanks in the signup invites, beckoning to be filled in that ask for the kind of information the thieves need.)

According to Trend Micro, "ZBOT malware of this generation are found to be mostly either Citadel or GameOver variants. Unlike earlier version, the mutex name is randomly generated."

Though both variants send DNS queries to randomized domain names, the GameOver variant does something extra; it also opens a random UDP port and sends encrypted packets before sending DNS queries to randomized domain names, according to Trend Micro.

One year ago a warning appeared about Zeus using Facebook login pages posing as friendly looking invites to click on compromised log in pages. Also last year, Boston-based Trusteer said it had spotted attacks from a P2P variant of the Zeus platform targeting users of Facebook, Google Mail, Hotmail and Yahoo, in which the thieves pretended to offer rebates and new security measures.

The question is often raised, why has Zeus been around for so long when it causes so much damage? One reason given is that Zeus is difficult to detect with antivirus software.

More information: blog.trendmicro.com/trendlabs- … e-shapes-up-in-2013/
bits.blogs.nytimes.com/2013/06 … hriving-on-facebook/