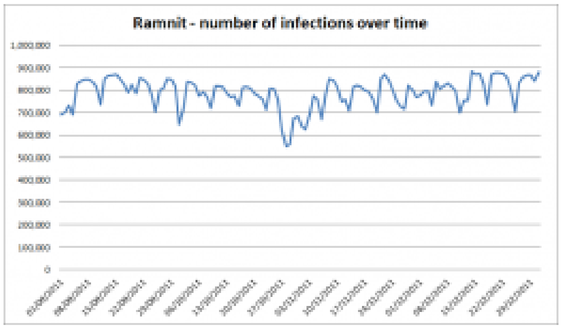
Ramnit's heist bags 45,000 Facebook passwords

January 6 2012, by Nancy Owano



Number of Ramnit Infected Machines Between September 2011 and December 2011. Image: Seculert.

(PhysOrg.com) -- Ramnit, the bank-thieving worm, is at it again, this time scoffing up Facebook accounts. The latest oh-look-another-threat is one that security watchers say could get ugly. Ramnit has grown up since it was first discovered as a virus in the wild in 2010. Security company Seculert has posted a January 5 blog saying that Ramnit has stolen 45,000 Facebook login credentials. The accounts are mostly in the UK and France. The security firm, which has been tracking Ramnit, discovered the stolen Facebook cache in its Seculert labs. Seculert in turn passed on to Facebook the stolen credentials that it found on Ramnit servers.

Ramnit’s command and control center is visible and accessible, and the security experts were able to determine the precise number of Facebook victims, which consisted of 69 percent from the UK, 27 percent from France and 4 percent from other countries.

When Ramnit first started causing mischief in 2010 it was considered as a low-level threat, comments SearchSecurity.com.

That assessment has changed. Ramnit's operators were able to graduate from an older generation of techniques to infect files to morph it into something more powerful, adding Zeus source code to the mix. Trusteer, another security company, warned that the worm had acquired the ability to inject HTML code into a web browser.

A worm is a type of malware that secretly integrates itself into program or data files, and infects more files each time the host program is run. Ramnit can infect Windows executable files, HTML files and other file types.

Ramnit's subsequent target was finance, bypassing two-factor authentication and transaction signing systems. In gaining remote access to financial institutions, Ramnit was able to compromise online banking sessions and was able to penetrate corporate networks.

Even before the latest Facebook heist, Seculert, using a sinkhole security tool, counted 800,000 machines as infected with Ramnit from September to the end of December 2011.

Ramnit's presence is not immediately obvious. The worrisome nature of Ramnit is compounded by the fact, say experts, that users tend to use the same password for a number of web-based services, which may include not only Facebook but their mail, a VPN, and others..

Blogger reactions to the news have ranged from “Change your passwords, and often!” to “Don't click any links, never, no matter from who or how interesting!”

Considering the very definition of social networks and why they are used, that kind of advice may be timely but curiously counter to the whole point. Suspecting friends and relatives of having virus-choked messages and afraid to share links for fear of infection run counter to the reason why users sign on to social networks. Behavioral trends and countertrends will get interesting too.

Another troubling sign of the times is what cybercriminals now see as choice game. E-mail worms are so Yesterday, say computer security experts.

Malware writers are replacing old-school worms transmitted via email with their malware now targeted for social-networks.

More information: blog.seculert.com/2012/01/ramnit-goes-social.html

Citation: Ramnit's heist bags 45,000 Facebook passwords (2012, January 6) retrieved 19 April 2024 from https://phys.org/news/2012-01-ramnits-heist-bags-facebook-passwords.html