Beware of Emails from Google, Hallmark, Twitter

Techtree News Staff, Mar 29, 2010 1302 hrs IST

New wave of spam attacks spreading variants of Vundo and Buzus trojan

Be careful before opening emails from suspicious or unknown senders, as online security firm eScan has warned of malicious malware that are more potent that earlier variants. Security experts have said that the new variants are network aware and pose a great danger to corporate networks, as a single infection can lead to a network outbreak within an hour.

eScan has warned against opening emails or attachments with subject lines such as, "You have received A Hallmark E-Card!", "Your friend invited you to twitter!", "Thank you from Google!", "Jessica would like to be your friend on hi5!" and "Shipping update for your Amazon.com order 254-71546325-658732". These emails also carry zipped attachments that have been found to contain new variants of the malware.

The "You have received A Hallmark E-Card!", spam email comes with postcard.zip or a similarly named attachment. The payload in the zip file contains malware that has the capability to mass mail message(s) with the built-in SMTP client engine to the email addresses harvested from the local computer. The payload also contains a malware with the characteristics of Vundo (a.k.a VirtuMonde/VirtuMundo), a trojan horse that cause popups and advertises rogue antispyware programs. Vundo can infect a system when a browser just visits a website link contained in a spammed email. It is known to add itself to the startup registry, create a DLL file in the Windows system32 directory and inject it into system processes winlogon.exe and explorer.exe. The malware can also send downloads/requests to get other files from Internet and spread quickly by itself in a network.

Another email doing the rounds is taking advantage of the popularity of social networking sites such as "Twitter" and "Hi5" to spread. These spam emails carry a deadly payload of a variant of the Buzus worm that is a network aware bot creating trojan. On infection, it creates a startup registry entry and modifies the host files to prevent access to security websites.

To avoid such catastrophic scenarios, use reputed and genuine security software and have the latest security updates installed in your system.

Related Links

Google Launches Mobile Help Forum

Now, Sync Google Contacts With BlackBerry

Google Search Juggernaut Rolls on

Tag keywords

Spam Vundo Buzus trojan malware Google Hallmark Twitter