

Client: Sophos

Publication: TechCentral

Date: 14 October 2010

URL:

http://techcentral.my/news/story.aspx?file=/2010/10/14/it_news/20101014144457&sec=it_news

Thursday October 14, 2010

We must fight malware together

PETALING JAYA: The number of global malware attacks have gone up by more than tenfold to 60,000 a day this year, compared to 5,000 a day 12 months ago.

Security expert Sophos Plc said the alarming figure is based on data it collected from antivirus labs, spam traps, Internet service providers, search engines and security vendors all over the world.

Its chief technologist, Dr James Lyne, warned that the number of malware attacks is expected to rise in the months to come. "It is not stopping anytime soon and we could be seeing more than 100,000 a day," he said.

Also, according to Sophos, more malware attacks are being mounted against the users of social networking sites, such as Twitter and Facebook, in the form of "clickjacking" and "cross scriptings."

Clickjacking is a phishing spam which activates when users try to decline an unwanted application, while cross scripting exploits a vulnerability that injects code into valid Facebook pages or tricks the Facebook site to perform a password reset which will allow the hackers to log in and steal user information.

Users cannot rely on a simple antivirus solution to protect themselves anymore, Lyne said. "This is not enough and doesn't really work nowadays."

To keep up, security vendors like Sophos have had to "reinvent" their products, moving towards multilayered and integrated solutions that are armed with more powerful security features, including reputation and behaviour analysis, intrusion prevention, URL filtering systems, and encryption.

The vendor's latest addition to its arsenal is "cloud lookup," which will use the database in a cloud-computing environment as a second line of defence.

If a suspicious file is detected, that cannot be exonerated by the database, that file will be quarantined until cleared, Lyne said.

He said integrated security solutions must also be easy to install, otherwise most users may not even bother with them. "You cannot expect users to be willing to install seven or eight components separately," he added.

Lyne does not see an end to the malware problem, "but the battle has yet to be lost," he said.

He believes that everyone - vendors, channel partners, government, industry players and users - must collaborate against the threat.

End-users, especially, must regularly update their security system with the newest software patches and the latest technologies. They should also have strong passwords.

And when thinking up answers to security questions, "always lie," he suggested. "That makes it harder for hackers to guess the answers."

He said many celebrities got their accounts hacked because they gave truthful answers to the security questions - information that was public knowledge in view of their status.

Also, it is very tempting for social-media users to be connected to as many people as possible, but that only increases the risk that you may be targeted by a hacker. As in real life, choose your friends carefully, said Lyne.