Facebook, Twitter to face more sophisticated attacks: McAfee

December 30 2009

The logo of social networking website 'Facebook' is displayed on a computer screen. "The explosion of applications on Facebook and other services will be an ideal vector for cybercriminals," McAfee said.

Social networks will face increasingly sophisticated hacker attacks in 2010 but law enforcement is expected to make strides in fighting cybercrime, according to Web security firm McAfee Labs.

"The explosion of applications on Facebook and other services will be an ideal vector for cybercriminals, who will take advantage of friends trusting friends to click links they might otherwise treat cautiously," McAfee said.

In its 2010 Threat Predictions report, McAfee also said it expected to see increased threats to banking security and a rise in the use of "botnets," armies of infected computers used to spread malicious software or malware.

"However, in 2010 we expect to see an increase in the effectiveness of law enforcement to fight back against cybercrime," the Santa Clara, California, computer security firm said in the report released on Tuesday.

McAfee said Adobe products were likely to come under increasing threat next year and the release by Google of its Chrome computer operating system would "create another opportunity for malware writers to prey on users."

"Cybercriminals have long picked on Microsoft products due to their popularity," the report said. "In 2010, we anticipate Adobe software, especially Acrobat Reader and Flash, will take the top spot."

"Based on the current trends, we expect that in 2010 Adobe product exploitation is likely to surpass that of Microsoft Office applications in the number of desktop PCs being attacked," it said.

McAfee said hackers were expected to try to take advantage of the proliferation of URL shortening services such as bit.ly and tinyurl.com.

"These services now appear in all sorts of communications -- making it easier than ever to mask the URLs that users are asked to click," it said.

"This trick will play a more predominant role in 2010; it's the perfect avenue to direct users to websites that they would normally be wary about visiting.

"As users' expectations of their Web 2.0 services evolve, we expect to see many rogue services set up with the hidden purpose of capturing credentials and data," McAfee said.

McAfee also said email remained vulnerable.

"Email is increasing in popularity as the preferred method for targeting attacks against individual users, corporations, and government institutions," it said.

"Although such attacks were rare some years ago, we now see many reports of successful assaults, both by criminals and for espionage, in which an email with an attachment or a link to a website is the attack vector," it said.

"During the last six years, botnets have become the biggest thorn in the side of cybersecurity professionals," McAfee added.

"Botnets have become the essential infrastructure used by cybercriminals and nation states for launching nearly every type of cyberattack," it said.

Law enforcement has made some progress in battling botnets.

"As a result of aggressive efforts to take offline these service providers that cater predominantly to the cybercriminal element, as well as of direct targeting of specific botnet control channels, numerous botnet operations have been severely disrupted in recent years," McAfee said.

(c) 2009 AFP