Cyber-crooks targeting social-networking websites

March 3 2009, by Glenn Chapman

Computer security specialists warn that Facebook users have been hit with a series of data-stealing attacks in the past week as cyber crooks increasingly stalk social-networking websites. Facebook has become prime hunting ground for tricksters and malicious software spreaders because it is the leading social-networking community, with more than 175 million people sharing personal information.

Computer security specialists warn that Facebook users have been hit with a series of data-stealing attacks in the past week as cyber crooks increasingly stalk social-networking websites.

Facebook has become prime hunting ground for tricksters and malicious software spreaders because it is the leading social-networking community, with more than 175 million people sharing personal information.

"There are so many people on social-networking sites it is becoming profitable for bad guys to go there," said David Perry, global director of education at software security firm Trend Micro.

"Bad guys can see all the things you post. You may be revealing personal information that is extremely valuable."

Even seemingly innocent information posted on profile pages can sometimes provide opportunities for criminals.

For example, names of grandparents or pets in posted pictures can tip hackers off to answers for typical challenge questions asked before providing information about "forgotten passwords" to online accounts.

Hackers can try to infect software used at social-networking websites with malicious code as well as dupe people in the trust-based communities with fake messages and rigged mini-applications.

Facebook soared in popularity after it began letting outside developers craft mini-applications that people customize profile pages with hip, fun or functional features.

Facebook only vets mini-applications after they are released and someone complains.

"We have a rogue application that happened this weekend," said Trend Micro research manager Jamz Yaneza on Monday. "It was an application that got through security at Facebook. Kudos to Facebook for shutting it down real quick."

The application seemed to be a variation of one unleashed on Facebook users last week, according to Trend Micro.

Applications installed by Facebook users sent messages to their friends warning that the website was shutting down or that they had been reported for violating terms of service.

If people followed instructions in the bogus messages, software was installed on their computers that stole information and sent similar bogus messages to their friends on the site.

The most recent Facebook attack came in the form of messages claiming to be from friends that wanted to share digital video of the receivers.

Clicking on the link results in a prompt to download viewing software that is actually a computer worm called Koobface, a variation on the spelling of Facebook.

"It steals your cookie on your desktop; not just for Facebook but for a half-dozen social networking websites including MySpace," Yaneza said.

"Your account is compromised at that point. Using the hijacked cookie it tries to log in as you, goes through your address book and starts posting messages and comments."

Internet services routinely install small bits of software, called "cookies," on users' computers to store identifying information that can include user names and passwords.

Facebook and other social-networking websites that let outside developers customize Web-2.0 style widgets for users need to beef-up vetting processes to guard against "rogue developers," according to Yaneza.

He cited the stringent vetting process that Apple puts developers through before making third-party applications available at iTunes for iPhones

and iPod Touch devices.

People can reduce the odds of becoming victims by being selective about friends at social networking websites and not clicking on links that take them outside the walls of their online communities.

Computer users are also wise to use unique complex passwords for each online account so if hackers get hold of one virtual key it won't open other locks, according to Yaneza.

(c) 2009 AFP