# Cyber crooks tarketing banks-social networks: Cisco

December 8 2009, by Glenn Chapman

An annual security report being released Tuesday by technology titan Cisco warns that banks and online social networks are prime targets for increasingly sophisticated cyber crooks.

"Criminals have been taking note of the large crowds in social-networking sites," said Cisco security researcher Scott Olechowski. "They steal them with various techniques."

Tactics used to get into social-networking profiles include hacking password databases at vulnerable online services and then exploiting the fact that many people use one password for multiple accounts.

Cisco estimates that a Koobface computer worm, named as a play on social networking hot spot "Facebook," has infected more than three million computers since it first appeared in 2008.

Koobface is malicious code that steals social networking account credentials, logs into profiles and sends "friends" messages along the lines of wanting to share scintillating online videos.

Links enclosed in the messages lead to bobby-trapped Web pages that trick visitors into infecting their machines with copies of the worm.

Crooks sometimes set up fake profiles and then finagle their ways into people's online social circles and entice them to opening computer files tainted with malicious code.

Money-making tricks can be as simple as hackers using social-networking profiles to pretend to be friends in desperate straits that ask to be wired money to get out of trouble in a far-away places.

Social networks are also targeted by hackers out to control or disrupt political discourse.

Business computers can wind up infected because one of every 50 "clicks" in the workplace is to social-networking websites, according to Cisco.

"The blending of social media for business and pleasure increases the potential for network security troubles, and people, not technology, can often be the source," said Cisco fellow Patrick Peterson.

"Without proper cognizance of security threats, our natural inclination to trust our 'friends' can result in exposing ourselves, home computers and corporate networks to malware."

Cyber criminals can mine profiles for names and email addresses of business executives or accounting department members to "spear phish," target strategically placed workers with scams.

The potential for workplace computers to be infected through a social-networking attack is all the more disturbing given the rise of a computer Trojan named Zeus crafted to digitally loot money from banks.

Once in computers, Zeus can swipe information and alter what is seen in Web browsers so that people tending to online banking see correct balances on screen while accounts are actually being emptied by cyber thieves.

"Zeus is sold on a retail basis by criminals to criminals," Olechowski

said, putting the price at 700 dollars.

Gangs have used Zeus to steal "400,000 to 1.5 million dollars a shot," he added. Cisco predicts Zeus will be a growing bane in 2010.

Spam remains a tried-and-true method for tricking people into downloading malware or buying specious products, such as fake medicine.

Cisco's report estimates that the amount of spam worldwide next year will rise 30 to 40 percent above 2009 levels.

While US and European countries shut down spam-spewing networks of "zombie" computers infected with malicious code and commandeered by criminals, more are being created in developing countries, according to the California-based firm.

Brazil this year dethroned the United States as the country producing the most spam, according to Cisco. The amount of spam coming from Vietnam and India has also soared.

"In the World Cup of spam, Brazil beat the US for the first time," Olechowski said. "We are starting to see emerging economies represent the bulk of spam globally."

Cyber criminals are taking advantage of improved broadband Internet and computer access in developing countries where people may still have lessons to learn about Internet security.

Increasing spam in developing countries is a symptom of a greater problem, acccording to Cisco senior security researcher Henry Stern.

"This means that there is a greater rate of compromised machines, which

means there will be more banking Trojans and other malware," Stern said.

Cisco created a Global Adversary Resource Market Share (ARMS) Race index, which estimates that between five and 10 percent of the world's personal computers are "compromised" by malicious software.

*(c) 2009 AFP*