

7 May 2008



Inside orkut

By: Bogdan Popa, Security and Search Engines Editor

Social Networks - Tomorrow's Hackers' Favorite Targets

Kaspersky predicts a tough future for social networks

The social networks out there, no matter if we're talking about Facebook, Bebo, Orkut, MySpace or others, recorded hack/spyware/spam attacks every once in a while, especially due to their increasing popularity. And like this wouldn't be enough, Kaspersky Lab predicts a tough fight for these social networks because attackers may attempt to spread their infections using social networking websites and even user profiles created on these pages. "We forecast that in 2008 users of social networking sites will become the main targets for phishing attacks. There will start to be increased demand among malicious users for account data to services such as Facebook, MySpace, LiveJournal, Blogger and others. This will become a dangerous alternative to placing malicious programs on hacked sites. In 2008, many Trojan programs will spread via user accounts on social networking sites, on their blogs and on their profiles," Kaspersky Lab wrote in a recently published paper. And the attacks which occurred in the past come to support these predictions: Google's social network Orkut was hit by a serious attack in February 2008. "On-line banking is very popular in Brazil. Orkut is very popular in Brazil. There are lots of virus writers in Brazil. These three factors combine to result in one thing: the appearance of a worm which spreads via Orkut and steals account data to online banking systems," Kaspersky Lab explained the way the attackers planned to assault Orkut. Social networks are incredibly popular these days and their number of users will be probably increase in the near future because more and more consumers from all over the world are lured to register new accounts. Facebook and MySpace, which are said to be the kings of the social networks, bring thousands of new users every day, which does nothing than to underline the need for better security measures.