

IT Backbones™

Security News



Give your mouse a heart!

search

The IT Shield - Dedicated To IT Security Issues, Featuring News, Press Releases, IT Directory & Links

- [Home](#)
- [About](#)
- [Contact](#)
- [Submit PR](#)
- [Search News](#)
- [What We Can Offer You](#)
- [IT Events](#)
- [Time & Money](#)

Trojan Downloader Circulates Among Orkut Users

Published 17th July 2006

Security experts at MicroWorld Technologies inform that members of Orkut Online Community Service powered by Google may receive a message from their contacts urging them to click on a link. Once the link is clicked, a Trojan downloader named 'Win32.Banload.aoo' will find its way to user computers.

In an attack that's very similar in nature to the last month's password stealing Trojan in Orkut, this one too comes from infected contacts, thereby evoking no suspicion in recipient's mind. The message written in Brazilian Portuguese asks users to download a file named 'fotovideo.exe', where it's important to note that 67% of Orkut users are Brazilians.

"Orkut is a network of trusted contacts and it's the very 'trust' that this worm exploits in tricking unsuspecting users," observes Aneesh Paliwal, Security analyst, MicroWorld Technologies. "Checking the authenticity of every material posted on online networks, by contacting the sender before you act upon them, is impractical to say the least!"

After getting into the victim's computer, 'Win32.Banload.aoo' logs on to malicious websites to download dangerous password stealing Trojans and keyloggers without the knowledge or consent of the user.

At the first stage of its infection routine, Banload.aoo installs itself in the system registry, lowers the security levels of the computer and tries to turn off AntiVirus

software installed in the PC. Then it goes ahead and downloads members of Trojan-PSW family that captures usernames, passwords and other confidential data while the victim logs on to the websites of leading banks and credit card companies. This information is sent to the remote attacker who uses it for multiple online financial crimes.

Last month, a password stealing Trojan named 'Infostealer.Orcu', was directly spread via orkut as an 'exe' posting, without the help of any conduit like Banload.aoo. Reacting to the malice, Google then cautioned users saying, "Orkut.com users and users of all online services and applications should always be careful when opening or clicking on anything suspicious."

"Orkut is growing very fast among online community enthusiasts across the world and it's quite natural that malware writers are increasingly targeting it," says Govind Rammurthy, CEO, MicroWorld Technologies. "Though Orkut has a definite advantage in having a by and large enlightened user base that's cautious while dealing with suspicious files, the guard slips off for some of them at times. That's when your proactive Security Software should defend you even from a new threat by applying Futuristic Security Intelligence."

Company Profiles powered by ITReseller.com

- MicroWorld - [View profile](#)

[Links](#) | [About Us](#) | [Privacy Policy](#) | [Contact Us](#) | © 2004-2006 IT Backbones Limited

Site developed and hosted by [Design Solution](#) Ltd.