



only with

GFI MailSecurity

Download your FREE trial today!

- ABOUT US
- CONTACT
- ADVERTISE

Welcome to a new version of Help Net Security. Much has improved and more is on the way. Subscribe to our RSS feeds and stay updated!

	<b>NEWS</b>								
	<a href="#">Off The Wire</a>	<b>ARTICLES</b>	<b>SOFTWARE</b>	<b>VULNERABILITIES</b>	<b>EVENTS</b>	<b>NEWSLETTER</b>			
<b>HOME</b>	<a href="#">Security</a>	<a href="#">Latest Articles</a>	<a href="#">Windows</a> <a href="#">Linux</a>	<a href="#">Vendor Advisories</a>	<a href="#">Webcasts</a>	<a href="#">Subscribe</a> <a href="#">Current</a>	<b>E-MAIL ALERTS</b>	<b>SEARCH</b>	<b>RSS</b>
	<a href="#">World</a>	<a href="#">Interviews</a>	<a href="#">Mac OS X</a>	<a href="#">Vulnerability Database</a>	<a href="#">Conferences</a>	<a href="#">Issue Archive</a>			
	<a href="#">Virus Center</a>	<a href="#">Book Chapters</a>	<a href="#">Pocket PC</a>						

**OFF THE WIRE** **SECURITY WORLD**

- [Bots, Google hacks: the Internet 'storms'](#) • [Online banks strengthen security](#) • [Oracle owns up to patching problems](#) • [Viruses leap to smart radio tags](#) • [Secure chip program seeks to extend DoD foundry effort](#) • [Are virus writers the new entrepreneurs?](#) • [Juniper shows off its funk\(y\) new security tools](#)
- [Weekly report on the latest vendor security advisories](#) • [Weekly report on the latest Linux security software releases](#) • [Online Banking Security Web Conference](#) • [Acunetix Web Vulnerability Scanner version 4 released](#) • [Global threat report on Web filtering, spyware and viruses](#)

**LATEST ARTICLES** **VIRUS CENTER**

- [Successful Backups Are Not Enough](#) • [Limiting Vulnerability Exposure Through Effective Patch Management](#) • [Securing Wireless, Remote and Mobile Computing - Quick Fixes](#) • [The Ten Most Critical Wireless and Mobile Security Vulnerabilities](#) • [Striking the Balance Between Storage Security and Availability](#)
- [Trojan downloader circulates among Orkut users](#) • [Weekly Report on Viruses and Intruders - Trj/Semys.B, SpyHeal and Microsoft vulnerabilities](#) • [Trojans accounted for 54.4 percent of the new malware detected in Q2 2006](#) • [Vladimir Putin death spam spreads a trojan horse](#) • [Insidious network worm threatens enterprise security](#)

## SECURITY SOFTWARE



• [++ GFI LANguard Network Security Scanner 7](#) • [++ Acunetix Web Vulnerability Scanner 3.0](#) • [Tor 0.1.1.22](#) • [Password Gorilla 1.4](#) • [SSL-Explorer 0.2.3](#) • [VisualRoute 2006 10.0j](#) • [Password Safe 3.01](#) • [WinSCP 3.8.1](#) • [JSch 0.1.28](#) • [GFI Endpoint Security 3](#) • [WinDeveloper IMF Tune 2.8](#) • [Reason 0.5.1](#) • [TrouSerS 0.2.7](#) • [KisKis 0.19.1](#) • [Aide 0.12 rc1](#) • [Nagios 2.5](#) • [Snort SMS 1.3.2](#) • [Sussen 0.25](#) • [NuFw 1.0.27](#) • [OS-SIM 0.9.0 rc2](#) • [TinyCA 2.0.7.4](#) • [Prelude Manager 0.9.5](#) • [Samhain 2.2.1](#) • [yaSSL 1.3.5](#) • [KisMAC 0.21a](#) • [iStumbler 96](#) • [Fugu 1.2.0](#) • [Little Snitch 1.2.2](#) • [Victor 2.0](#) • [Net Tool Box 3.1](#) • [PDFKey Pro 1.0](#) • [HenWen 2.1.2](#) • [Mac GPG 1.4.1](#) • [IPSecuritas 2.1](#) • [Pastor 1.7](#) • [JellyfiSSH 4.2](#) • [WiFiFoFum 2.1.1](#) • [Crippin 2.8](#) • [AirFix 1.0b](#) • [Aircscanner Mobile Encrypter 2.5](#) • [Confidential Notes 1.1](#) • [Aircscanner Mobile Firewall 2.4](#) • [WiFi Graph 0.3 RC3](#) • [SignWise Pro 2.52](#) • [Sentry 2020 2.8](#) • [eWallet 4.0](#) • [Pocket Warrior 15022003-B](#) • [Touch Password Protection 2.3](#)

## ADVISORIES VULNERABILITIES

• [Debian Security Advisory - kernel-source-2.6.8 et. al. \(DSA 1111-1\)](#) • [Debian Security Advisory - samba \(DSA 1110-1\)](#) • [Debian Security Advisory - rssh \(DSA 1109-1\)](#) • [OpenPKG Security Advisory - mutt \(OpenPKG-SA-2006.013\)](#) • [Slackware Security Advisory - Samba DoS \(SSA:2006-195-01\)](#) • [SUSE Security Announcement - SUSE Security Summary Report \(SUSE-SR:2006:016\)](#) • [Multiple Vendor nn nn\\_exitmsg Function Remote Format String](#) • [AjaxPortal Login Routine Username Field SQL Injection](#) • [AjaxPortal Search Field SQL Injection](#) • [Sport Slo Advanced Guestbook guestbook.php Multiple Field XSS](#) • [Microsoft IE TriEditDocument URL Property NULL Dereference](#) • [Microsoft IE DXImageTransform.Microsoft.RevealTrans Transition Property NULL Dereference](#)

### Trojan downloader circulates among Orkut users

Posted on 17.07.2006

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.

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."

[ [Virus Center main page](#) ]



**GFI EndPoint Security**

**DOWNLOAD YOUR  
FREE EVAL TODAY!**





**Black Hat USA 2006**  
**Briefings & Training**  
**July 29-August 3**  
**Caesars Palace Las Vegas**

