

<i>IT Management Begins With Security</i>		<b>WebProWorld Security Forum</b>	<b>RSS Feeds</b>	Subscribe to our <a href="#">RSS feed</a> . Stay current with our latest!		
	<b>SecurityProNews</b>	<b>Breaking Security Related News</b> Your Source for investigative security related reporting and breaking news		SPONSORED BY: 		
HOME	IT ARTICLES	NEWS	NEWSLETTER ARCHIVES	ABOUT US	ADVERTISE	SUBMIT AN ARTICLE

SecurityProNews > News > Security News > **Trojan Downloader Circulates Among Orkut Users**

[ [news\\_security\\_news](#) ]

## Trojan Downloader Circulates Among Orkut Users

**Btv Raj** | Contributing Writer  
2006-07-17

 [PRINT VERSION](#)  [EMAIL](#)  [BOOKMARK](#)

**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, credit card companies and orkut itself. This information is sent to the remote attacker who uses it for online financial crimes.

Last month, a password stealing Trojan named 'Infostealer.Orcu', was

Search:



SecurityProNews

NetworkingFiles



ITManagementNews



FENTRY  
Help Center

**McAfee TOTAL PROTECTION for Small Business No Payment Until August - [Click Here](#)**

 [Top Stories](#)

### VIRUS WARNINGS

Newsletter Signup

**Subscribe to SecurityProNews FREE!**

[ [more newsletters](#) ]

Featured On:

AS FEATURED ON  
**NEWS NOW**

article resources

**Search Articles:**

[ [advanced search](#) ]

WebProWorld.com

- **Get in-touch** with industry experts and leaders
- **Post** your site for review by expert and peers
- **Ask** Security, IT, Development and Design questions

Free Membership: **Join Now!**

Visit [WebProWorld.com](#)

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 about 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."

Tags: [Orkut](#), [Trojan](#)

Add to [Del.icio.us](#) | [DiggThis](#) | [Yahoo! My Web](#) | [Furl](#)

[View All Articles by Btv Raj](#)

---

#### **About the Author:**

To learn more, kindly visit <http://www.mwti.net>.

Btv Raj is the Content Writer and Creative Visualizer, MicroWorld Technologies.

[More news security news Articles](#)



**iEntry Featured Services:** [Jayde Member Services](#) | [Forums](#) | [Freeware](#) | [Advertise with Us](#)

[Contact Us](#) | [Advertise](#) | [Newsletter Archive](#) | [Sitemap](#) | [Submit an Article](#) | [News Feeds](#)

SecurityProNews is an [iEntry, Inc.](#)® publication - 1998-2006 All Rights Reserved | [Privacy Policy](#) and [Legal](#)

Join the WebProWorld Forums: [Click Here](#)