



- 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!

NEWS

- [Off The Wire](#)
- [Security](#)
- [World](#)
- [Virus](#)
- [Center](#)

ARTICLES

- [Latest Articles](#)
- [Reviews](#)
- [Interviews](#)
- [Book Chapters](#)

SOFTWARE

- [Windows Linux](#)
- [Mac OS X](#)
- [Pocket PC](#)

VULNERABILITIES

- [Vendor Advisories](#)
- [Vulnerability Database](#)

EVENTS

- [Webcasts](#)
- [Conferences](#)

NEWSLETTER

- [Subscribe](#)
- [Current](#)
- [Issue](#)
- [Archive](#)

HOME

E-MAIL ALERTS

SEARCH

RSS

OFF THE WIRE SECURITY WORLD

- [Sailor sentenced to 12 years for espionage](#)
- [Copyright pirates face crackdown](#)
- [Yahoo Music continues DRM-free download experiment](#)
- [Test reveals that free firewalls outclass paid-for ones](#)
- [Introduction to the Windows Management Instrumentation Command-line \(WMIC\)](#)
- [Researchers spot first mobile spyware](#)
- [Microsoft: attacks targeting unpatched Word flaw](#)
- [X-Force predicts security trends for 2007](#)
- [New wave of FBI spam](#)
- [First comprehensive tracking and analysis website for zero-day vulnerabilities](#)
- [Tips: Don't give an identity thief the gift of your personal information](#)
- [Senforce introduces SDK for endpoint security management](#)

LATEST ARTICLES VIRUS CENTER

- [The Truth About Patching](#)
- [Introduction to the Windows Management Instrumentation Command-line \(WMIC\)](#)
- [E-Mail Content Security: Filtering Out the Hype](#)
- [Introducing Stealth Malware Taxonomy](#)
- [What Are The Most Common Causes Of Security Breaches?](#)
- [A new worm creeps all over Myspace](#)
- [Warezov worm tops latest Kaspersky charts](#)
- [Bank web site monitoring trojan and a couple of other pests](#)
- [Sdbot.ftp worm once again rules the malware charts](#)
- [Scoop on the latest trojans and worms](#)

SECURITY SOFTWARE



[++ GFI LANguard Network Security Scanner 7](#) • [++ Acunetix Web Vulnerability Scanner 4](#) • [Outpost Firewall Pro 4.0](#) • [Password Safe 3.05](#) • [SSL-Explorer 0.2.9.02](#) • [Cain & Abel 4.0](#) • [Tor 0.1.1.25](#) • [JSch 0.1.30](#) • [Le Putty 2006-10-03](#) • [Data Guardian 1.0](#) • [Kaspersky Security for MS Exchange Server 2003 5.5](#) • [Kaspersky Anti-Virus 6.0](#)
• [Dazuko 2.3.2](#) • [GnuPG 2.0.1](#) • [NuFw 2.0.11](#) • [Nagios 2.6](#) • [Aide 0.13 rc1](#) • [MaraDNS 1.2.12.04](#) • [ArpAlert 1.1.3](#) • [yaSSL 1.5.0](#) • [suPHP 0.6.2](#) • [Tinc 1.0.5](#)
• [Stunnel 4.19](#) • [MIMEDefang 2.58](#)
• [Data Guardian 1.0](#) • [iProtector 1.0](#) • [MultiAlarm 3.4](#) • [OS X Rootkit Hunter 0.1](#) • [Password Gorilla 1.4](#) • [Pict Encrypt 2.0](#) • [Safer Workstation 1.0.1](#) • [FrameSeer](#) • [XNmap 3.0](#) • [NetShred X 3.1.7](#) • [Radmin 1.7.0](#) • [JellyfiSSH 4.4](#)
• [Aircanner Mobile Encrypter 2.9](#) • [Crippin 2.9](#) • [Sentry 2020 2.9](#) • [WiFiFoFum 2.1.1](#) • [AirFix 1.0b](#) • [Confidential Notes 1.1](#) • [Aircanner Mobile Firewall 2.4](#) • [WiFi Graph 0.3 RC3](#) • [SignWise Pro 2.52](#) • [eWallet 4.0](#) • [Pocket Warrior 15022003-B](#) • [Touch Password Protection 2.3](#)

 **ADVISORIES**  **VULNERABILITIES**

• [Slackware Security Advisory - gnupg \(SSA:2006-340-01\)](#) • [Mandriva Linux Security Update Advisory - ruby \(MDKSA-2006:225\)](#) • [Debian Security Advisory - asterisk \(DSA 1229-1\)](#) • [FreeBSD Security Advisory - gtar name mangling symlink vulnerability \(FreeBSD-SA-06:26.gtar\)](#) • [FreeBSD Security Advisory - Kernel memory disclosure in firewire\(4\) \(FreeBSD-SA-06:25.kmem\)](#) • [Mandriva Linux Security Update Advisory - xine-lib \(MDKSA-2006:224\)](#)
• [Pie Cart Pro affiliates.php Inc_Dir Variable Remote File Inclusion](#) • [Pie Cart Pro orders.php Inc_Dir Variable Remote File Inclusion](#) • [Pie Cart Pro events.php Inc_Dir Variable Remote File Inclusion](#) • [Pie Cart Pro index.php Inc_Dir Variable Remote File Inclusion](#) • [Pie Cart Pro articles.php Inc_Dir Variable Remote File Inclusion](#) • [Pie Cart Pro faqs.php Inc_Dir Variable Remote File Inclusion](#)

GFI: [Control entry & exit of data on your network with GFI EndPointSecurity. FREE eval!](#)

A new worm creeps all over Myspace

Posted on 06.12.2006

It's great to meet people online and befriend them, to share your thoughts, photographs, movies and much more. Even better when the community website is easy to login to and manage; until your network intermingles with the criminal gangs of the web underground!

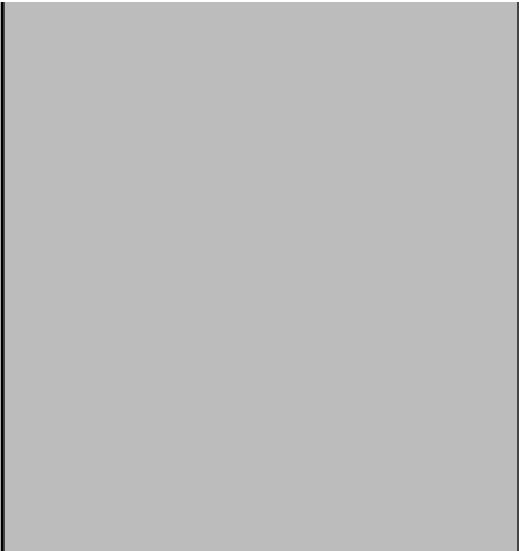
Security Experts at [MicroWorld Technologies](#) inform that a Worm named 'Win32.Ofigel' is spreading in large numbers across the world among a 70 million strong user base of the highly successful community portal, Myspace.com. Security experts had long raised concerns about the vast opportunity that websites like Myspace provide to online thieves and criminals, in exploiting their open nature and easy access.

When a member of the community views an infected profile, a Quicktime movie carrying Ofigel Worm is played, which exploits an XSS vulnerability in the network using a Javascript. The Worm then replaces user's Myspace menu with a fraudulent one and the menu items redirect the user to a Phishing website identical to Myspace, where the Username and Password of the victim are captured.

Then the Worm logs onto certain websites to download the malicious Quicktime movie and adds it to the user's profile. When a new user, mostly the victim's contact, watches the movie, his or her computer gets infected and the chain goes on.

As if that's not enough, Ofigel later harvests the email IDs of victim's contacts and starts sending Spam mails to them with subject lines like: What else is there to do on a Sunday, You better not forget about this, Hehe that was so funny, Better see this one last time lol, Who's coming to the party tonight, etc. All messages quiet in sync with the youth culture of Myspace.

Myspace officials inform that they are acting to minimize the impact of this worm on users, by identifying the URLs attempting to exploit this vulnerability. Those URLs are being blocked, while the infected profiles being removed.



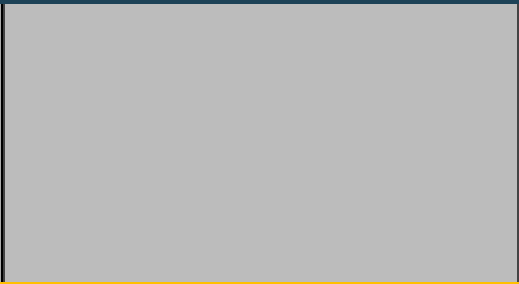
SPI DYNAMICS
Start Secure. Stay Secure.

Free Trial
Download



 **WebInspect**

Protect your web applications from attacks?



HNS Newsletter
Weekly roundup of all security happenings
delivered to your mailbox every Monday.

