



- 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 | ARTICLES | SOFTWARE | VULNERABILITIES | EVENTS | NEWSLETTER | | | |
| HOME | Security | Latest Articles | Windows Linux | Vendor Advisories | Webcasts | Subscribe Current | E-MAIL ALERTS | SEARCH | RSS |
| | World | Interviews | Mac OS X | Vulnerability Database | Conferences | Issue Archive | | | |
| | Virus Center | Book Chapters | Pocket PC | | | | | | |

OFF THE WIRE **SECURITY WORLD**

- [How Microsoft fights off 100,000 attacks per month](#)
- [Winkler: Nike + iPod 'vulnerability' blown out of proportion](#)
- [HP pays \\$14.5m to end 'spy' probe](#)
- [Microsoft readies Windows, Visual Studio security fixes](#)
- [Incident response tools](#)
- [The truth about patching](#)
- [Making a distribution secure](#)
- [Florida man pleads guilty to a Distributed Denial of Service Attack](#)
- [Beta version of BitDefender 10 Internet Security for Microsoft Windows Vista](#)
- [SquirrelMail 1.4.9a update fixes multiple vulnerabilities](#)
- [X-Force predicts security trends for 2007](#)
- [New wave of FBI spam](#)

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?](#)
- [Don't open that Word file; it may be carrying a trojan](#)
- [Trojan spreading and confidential information stealing malware](#)
- [A new worm creeps all over Myspace](#)
- [Warezov worm tops latest Kaspersky charts](#)
- [Bank web site monitoring trojan and a couple of other pests](#)

SECURITY SOFTWARE

- [++ GFI LANguard Network Security Scanner 7](#)
- [++ Acunetix Web Vulnerability Scanner 4](#)
- [SSL-Explorer 0.2.9.03](#)
- [Outpost Firewall Pro 4.0](#)
- [Password Safe](#)

[3.05](#) • [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](#)
• [Nmap 4.20](#) • [GnuPG 2.0.1](#) • [Aide 0.13](#) • [Firewall Builder 2.1.8](#) • [Distributed Access Control System 1.4.16](#) • [Sussen 0.33](#) • [MailScanner 4.57.6-1](#) • [Stunnel 4.20](#) • [Dazuko 2.3.2](#) • [NuFw 2.0.11](#) • [Nagios 2.6](#) • [MaraDNS 1.2.12.04](#)
• [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](#) • [Radmind 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**

• [Debian Security Advisory - clamav \(DSA 1232-1\)](#) • [Debian Security Advisory - gnupg \(DSA 1231-1\)](#) • [OpenPKG Security Advisory - GNU tar \(OpenPKG-SA-2006.038\)](#) • [SUSE Security Announcement - SUSE Security Summary Report \(SUSE-SR:2006:028\)](#) • [Debian Security Advisory - I2tpns \(2.0.14-1sarge1\) \(DSA-1230-1\)](#) • [Trustix Secure Linux Security Advisory - gnupg, proftpd \(2006-0070\)](#)
• [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!](#)

Don't open that Word file; it may be carrying a trojan

Posted on 08.12.2006

A new vulnerability has been identified in Microsoft Word. Security Analysts at MicroWorld Technologies inform that exploits for the vulnerability are out already, which can successfully thrust Trojan Downloaders into user computers.

Microsoft Corporation said they are investigating the vulnerability that exists in Microsoft Word 2000, 2002 and 2003, Word Viewer 2003, Word 2004 for Mac, and Word v. X for Mac, as well as Microsoft Works 2004, 2005, and 2006.

According to [MicroWorld Experts](#), a specially crafted Word file carrying a Trojan Dropper named 'MSWord.Agent' can push Trojan downloaders into victim's computers. The Trojans deposited this way can log on to predefined websites and bring in dangerous malwares like Backdoors and Rootkits into a victim's computer.

"One stream of malware writers are quiet enthusiastic about exploring application software vulnerabilities as they think that's a lot more easier and rewarding than getting into the OS level intricacies," commented Sulabh Mahant, a Security Expert at MicroWorld Technologies. "And incidentally, that's a fast growing tribe which is quiet apparent in the present tide of exploits targeting various vulnerabilities in a range of applications, including some of the AntiVirus products."

In the last one year, MicroWorld Technologies have detected many vulnerability exploits aimed at MS Word files. While 'Win32.Mdropper' and 'MSWord.1Table.bd' were Trojan Droppers that transported Backdoors into targeted computers, a recent Macro Virus detected in the month of November was primarily acting as a vehicle for Password Stealing Trojans.

To combat masqueraded threats like these, one's best bet would be to rely on an Intelligent and fast updating Antivirus software, that can catch Viruses and Worms at the Socket Level, which is the entry point for an external file to come into a computer. eScan from MicroWorld Technologies scans incoming data for Viruses right there at the Winsock layer with the help of its MWL technology, to provide the most advanced protection for Information Systems.



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.

