



**STOP 98%** of spam and phishing emails whilst minimizing false positives!

with **GFI MailEssentials** for Exchange/SMTP

**DOWNLOAD YOUR FREE TRIAL!**

- 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>
	<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</a> <a href="#">Archive</a>		<b>RSS</b>
	<a href="#">Virus Center</a>	<a href="#">Book Chapters</a>	<a href="#">Pocket PC</a>					

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

- [Security expert recommends 'Net diversity](#)
- [Microsoft officially launches paid security product](#)
- [Card fraudsters: a world unto themselves](#)
- [Hostage threat to home PCs](#)
- [The importance of the limited user, revisited](#)
- [Arizona leads U.S. in identity theft](#)
- [First StarOffice virus detected](#)
- [DigiKeyGen, a new spyware program that blackmails users](#)
- [Bogus Microsoft Security Warning Leads To Thieving Malware](#)
- [MicroWorld to Launch Futuristic Network Firewall](#)
- [OpenService Launches Guaranteed Security Analysis Programme](#)
- [MSN Phisher Jailed For 21 Months](#)

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

- [Understanding Technical vs. Logical Vulnerabilities](#)
- [Help Net Security Podcast: Episode 1 - Nortel's Approach To Security](#)
- [How Companies Can Manage Strong Authentication Intelligently](#)
- [Cross-Site Scripting Worms and Viruses: The Impending Threat and the Best Defense](#)
- [Identity Theft - Should You Be Worried?](#)
- [Mail Written in Russian Spreads Scano Worm](#)
- [Weekly Report on Viruses and Intruders - Gusi.A and Gusi.B Trojans](#)
- [1Table.A - trojan that uses a Microsoft Word vulnerability](#)
- [Weekly Report on Viruses and Intruders - Clickbot.A and Kitty.Kat Trojans and the Hoots.A worm](#)
- [Virus Leaks Power Plant Secrets Twice](#)

[In Four Months](#)**SECURITY SOFTWARE**

• [++ GFI LANguard Network Security Scanner 7](#) • [++ Acunetix Web Vulnerability Scanner 3.0](#) • [WinSCP 3.8.1](#) • [JSch 0.1.28](#) • [GFI Endpoint Security 3](#) • [WinDeveloper IMF Tune 2.8](#) • [VisualRoute 2006 10.0i](#) • [Password Safe 3.0 beta 1](#) • [SSL-Explorer 0.1.16](#) • [Reason 0.5.1](#) • [Tor 0.1.0.17](#) • [Digital Invisible Ink Toolkit 1.4](#)

• [John the Ripper 1.7.2](#) • [MailScanner 4.54.6-1](#) • [TinyCA 0.7.3](#) • [MaraDNS 1.2.07.4](#) • [Nagios 2.3](#) • [The Sleuth Kit 2.04](#) • [Autopsy Forensic Browser 2.07](#) • [Sussen 0.21](#) • [KisKis 0.19](#) • [yaSSL 1.3.0](#) • [Distributed Access Control System 1.4.12](#) • [Vuurmuur 0.5.71](#)

• [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](#) • [Aircanner Mobile Encrypter 2.5](#) • [Confidential Notes 1.1](#) • [Aircanner 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**

• [Mandriva Linux Security Update Advisory - dia \(MDKSA-2006:093\)](#) • [SUSE Security Announcement - fomatic-filters \(SUSE-SA:2006:026\)](#) • [Debian Security Advisory - New Linux kernel 2.4.17 packages fix several vulnerabilities \(DSA 1082-1\)](#) • [Ubuntu Security Notice - nagios vulnerability \(USN-287-1\)](#) • [Ubuntu Security Notice - postgresql-7.4/-8.0, postgresql, psycopg, python-pgsql vulnerabilities \(USN-288-1\)](#) • [Debian Security Advisory - libextractor \(DSA 1081-1\)](#)

• [Basic Analysis and Security Engine \(BASE\) BASE\\_path Variable Remote File Inclusion](#) • [Realty Pro One listings/index.php listingid Variable SQL Injection](#) • [Realty Pro One listings/index\\_other.php listingid Variable XSS](#) • [Realty Pro One search/searchlookup.php propertyid Variable XSS](#) • [Realty Pro One images.php id Variable XSS](#) • [Realty Pro One listings/request\\_info.php agentid Variable XSS](#)

**Mail Written in Russian Spreads Scano Worm**

Posted on 30.05.2006

Security experts at [MicroWorld Technologies](#) inform that a worm named 'Worm.Win32.Scano.e' spreads via emails written in Russian carrying an attachment in 'HTA' format.

The malicious component of this Worm is a Windows PE EXE file. Once inside the victim's computer, it goes about stealing the email addresses from user's address book and starts sending itself as attachments to the email-ids found. The subject and body of the mail vary as it is chosen randomly from a list.

"The earlier versions of Scano and similar types, used to spread via injecting script worms through Internet Explorer vulnerabilities," says Arti Taru, Assistant Manager, R&D, MicroWorld Technologies. "But this one takes the email route and can claim large number of victims as it nicks email addresses from the victim's computer. Well, if a normal user receives an email from his friend, carrying a rather harmless looking 'HTA' attachment, I don't see a reason why he should be apprehensive about opening it!"

At the next level, Scano.e logs on to various pre-decided websites and downloads more dangerous Trojans and Backdoors without the knowledge of the user. Such backdoors can even turn your computer to a remote-controlled bot, via IRC channels.

“The modus operandi of many new breeds of malware, is to find a foothold in your computer in the first place, using a small piece of malware code. Then it moves on to downloading more harmful stuff from specific websites. Some of them can upgrade to a higher degree of threat while some others can mutate to become different breed altogether with the newly acquired components,” explains Govind Rammurthy, CEO, MicroWorld Technologies.

With the nature of online threats changing so rapidly, it’s becoming increasingly difficult to assign a specific threat level for a particular Virus or worm. An otherwise low-threat worm can become lethal, if used in a targeted attack, in a coordinated fashion.

Security Solutions from MicroWorld Technologies are designed and developed, keeping the fast transforming nature of present-day malwares in mind. The security firm believes that even a miniscule crack in your defense system won’t take long before it becomes a gaping hole, leaving open your system for more attacks. Hence, their software eScan and MailScan are empowered with a combination of signature based and proactive technologies, to make sure that all kinds of malware are detected and prevented.

[ [Virus Center main page](#) ]

 <p><b>ActiveWorx</b> SECURITY CENTER</p> <p>Click For <b>FREE</b> Trial</p> <p><b>Offers Out-of-the-Box Compliance Reports to Help Meet SOX and HIPAA requirements</b></p>  <p><b>CrossTec</b> Corporation</p>	 <p><b>GFI LANguard</b> Network Security Scanner</p> <p><b>DOWNLOAD FREE VERSION TODAY!</b></p>	 <p><b>Secure Your Business.</b></p>  <p><b>infosecurity</b> CANADA</p> <p><b>June 19-21, 2006</b> Metro Toronto Convention Centre Toronto, Ontario</p>
---	--	--