



FIND SQL INJECTION, XSS & OTHER WEB VULNERABILITIES

[Articles](#)[News](#)[Reviews](#)[Releases](#)[Downloads](#)[Contact Us](#)[White Papers](#)**Sponsors:**

Is your network open to attack? Find out with the #1 sold network security scanner: GFI LANguard Network Security Scanner! [Download your FREE trial version today.](#)

Check your website security with a FREE [website security audit](#) by [Acunetix](#). Audit your web applications for [SQL injection](#), [cross site scripting](#) & more with [Acunetix Web Vulnerability Scanner](#)

Software security section is sponsored by GFI, a leading developer of network security, content security and messaging software - [Free trial!](#)

Mail Written In Russian Spreads Scano Worm*Tuesday, 30 May 2006 12:21 EST*

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.

[Read Full Story](#)**News**

[Steve Hunt Joins Promisec Advisory Board](#)

May 30, 2006, 14:13 EST

[Where is the security for our personal data?](#)

May 30, 2006, 13:27 EST

[How 802.11w will improve wireless security](#)

May 30, 2006, 13:25 EST

[Next Explorer more secure](#)

May 30, 2006, 13:22 EST

[SMEs are not keeping pace with IT security](#)

May 30, 2006, 13:19 EST

[Mail Written In Russian Spreads Scano Worm](#)

May 30, 2006, 12:21 EST

[Single Sign-On Raise Concern Amongst Security Experts](#)

May 30, 2006, 12:20 EST



