



SA Computer MAGAZINE

Age is coming... 29 Sep - 1 Oct 2006
The Dome, Northgate



Latest News

Trojan Bot Exploits Windows Vulnerability, Drops Rootkit

A network creeping Trojan itself is insidious in nature and what if it uses a Rootkit to evade detection as well? Security Experts at MicroWorld Technologies inform that a Trojan Bot is exploiting multiple Windows vulnerabilities to spread in networks, whilst using a Rootkit component to hide its files and processes.

'Backdoor.Rbot.ayg' spreads via AOL Instant Messenger at its first level of proliferation. Once it is installed in the system registry, the Bot can move to other computers in the network by exploiting the recently found and patched Server Service Vulnerability-MS06-040 and earlier flaws like MS03-049 in Microsoft Windows.

Last month, MicroWorld Technologies had reported about 'IRCBot.st', which exploited MS06-040, to launch a zero-day attack on targeted computers. It had an identical spreading routine using AOL Messenger and was also capable of exploiting earlier flaws in Windows.

Backdoor.Rbot.ayg uses 'Win32.Rootkit.l' to hide its files and processes. It communicates to the remote attacker via IRC channels and accepts and executes commands. The Bot can shutdown and restart the computer, log on to websites and download malicious code, log off current user, send files to the intruder, capture network user information and search disks for files.

"What's worrying with these sorts of malware samples is that they show increased hybridization in code and Multiple Layering in mode of attack," observes Manoj Mansukhani, Head-Technology and Marketing, MicroWorld Technologies.

"As you see, this is a Backdoor Trojan with network creeping abilities, which uses a Rootkit component to hide itself. For spreading, it employs dual channels of Instant Messenger and Vulnerability Exploitation while the Rootkit deposited in the computer can even be used by a future Trojan. All this points towards a lot of planning, improvisation and innovation that goes into creating and proliferating malware today"

MicroWorld Labs closely studies the evolution of various malware breeds, to develop and implement dynamic technologies that combat today's

About Us

Latest Issue



SEPTEMBER 2006
HIGH-DEFINITION TV AND THE XBOX 360: The Biggest Revolution in Home Entertainment. Includes new Cover CD!

On shelf 24 August
[\[Subscribe \]](#)

Contact Details

[tel] +27 11 704 2679
[fax] +27 11 704 4120

[Subscriptions](#)
[Advertising](#)
[Webmaster](#)



emerging threats in a comprehensive manner.

Sunil Kripalani, Vice President, Global Sales and Marketing, MicroWorld Technologies, observes "If you are serious about security, you just can't be complacent in patching vulnerabilities in Operating Systems or other applications. However, regardless of security flaws in OS or elsewhere, you must be able to rely on your AntiVirus software to protect your system from all kinds of malware types. And that will be possible only when the security software combines multiple technologies that are proactive and reactive in nature and always keeps a few steps ahead of Virus writers."

MicroWorld

MicroWorld is the developer of the world's first Real-Time Anti-Virus and Content Security software eScan for desktops and servers. Its communication security software, MailScan is the first comprehensive e-mail scanner for your SMTP/POP3 Mail Server. MicroWorld Winsock Layer (MWL) is the revolutionary technology underlying these products, powering them to several certifications and awards by some of the most prestigious testing bodies, notable among them being Virus Bulletin, Checkmark, TUCOWS, Red Hat Ready, and Novell Ready. Combining their powerful scanner with MWL technology, MicroWorld solutions provide a Real-Time Proactive security for your systems. For network security of enterprises, eConceal Firewall is the latest powerful offering from MicroWorld.

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

Press Release / *Posted on 16 Sep 2006*

Content Management Powered by [CuteNews](#)

[archives](#) / 

All content (c) SA Computer Magazine, All Rights Reserved.