

[News](#)[Articles](#)[Press](#)[Releases](#)[Downloads](#)[Privacy](#)[Policy](#)[RSS Feeds](#)**Channels**[IT Security](#)[Insight](#)[Storage](#)[Reviews](#)[Editorials](#)[Wireless](#)[About ITO](#)[Advertise](#)[Whitepapers](#) [RSS Feed](#)**Trojan Exploits MS06-040 Windows Vulnerability, Drops Rootkit**

Friday, 15 September 2006 11:28 EST

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.!' 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.

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."

Acunetix Web Security Scanner

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**

GFI LANguard Security Scanner

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.**

**Downloads**

- » [BeEF - Browser Exploitation Framework 0.2.1](#)
- » [TrackMeNot - Firefox extension to protect against data-profiling 0.3.0a](#)
- » [fwknop - Single Packet Authorization 0.9.7](#)
- » [Wapiti - Web application vulnerability scanner 1.1.3](#)
- » [SSH Tunnel Manager 1.2](#)

Press Releases

- » [CODA manages risk worldwide with Vistorm's Information Assurance approach](#)
- » [Risto Siilasmaa becomes Chairman of the Board at F-Secure effective November 6th 2006 – Kimmo Alkio from Nokia appointed as new CEO](#)
- » [LogLogic and Opsware Partner for New Automation Features for the Data Center](#)
- » [Managed IT Service Saves Nichols Plc £80K per Year and Supports Proactive, Intelligence-Led Business Strategy](#)
- » [Touchpaper IT Service Management Suite Verified by](#)

Consortium for Service Innovation

Reviews

- » [Safend Auditor - Review](#)
- » [Web Application Code Auditing with SWAAT](#)
- » [Review: Acunetix Web Vulnerability Scanner](#)
- » [iSafe: Store Personal Data Securely on Your Mac](#)
- » [NetInfo: Diagnostic and Network Information Utility](#)

Copyright © IT-Observer.com 2000 - 2006