

[News](#)[Articles](#)[Press](#)[Releases](#)[Downloads](#)[Privacy Policy](#)[RSS Feeds](#)**Channels**[IT Security](#)[Insight](#)[Storage](#)[Reviews](#)[Editorials](#)[Wireless](#)[About ITO](#)[Advertise](#)[Whitepapers](#) [RSS Feed](#)**Backdoor Trojan Threatens To Take Over User Computers**

Friday, 4 August 2006 08:25 EST

What if your computer boots on its own, logs on to websites that it wants, downloads harmful stuff like no one's business, takes commands from someone in hinterland Russia and send mails to anyone and everyone like there's no tomorrow? Scary? Well, infection of a Backdoor Trojan named 'Backdoor.Win32.SdBot.asr' can lead computers into a situation like that.

Security analysts at MicroWorld Technologies inform that 'Win32.SdBot.asr' slips into user computers via Trojan Downloaders or through manual downloads from the Internet. The Trojan Bot is a Windows PE DLL file created in 'C' and packed with WinUpack.

'Win32.SdBot.asr' can execute programs, reboot the system, open files, open webpages in the default browser of the host, download files, launch and manage a Proxy Server on the victim machine, redirect information sent to local port towards a remote port and send out system information to the remote attacker. The backdoor will also log on to specific websites to update, upgrade and mutate towards better capabilities.

"Backdoor Trojans often come bundled with programs, games and utilities that pretend to be safe and legitimate otherwise," says Arti Taru, Assistant Manager R&D, MicroWorld Technologies. "Some of the Backdoors are also distributed via the email route, where a small piece of code gets into user computer and grows on to a full fledged malware by logging on to nefarious websites to upgrade themselves. Threat potential of a Trojan bot is very high as the attacker almost completely takes over a user computer and gains the ability to perform a plethora of illegal activities using the victim machine."

"Though many of these Backdoor Trojans are detected by some of the AntiVirus programs, they are not removed from the Windows registry. Hence when the computer reboots, this malware finds its way back from nowhere. That's why our proactive Security solution, eScan, removes registry entries too so that a resurrection of this Trojan is ruled out," continues Arti Taru.

"The advancements in recent Backdoor Trojans reflect a larger and radical shift in the nature and purpose of today's malware landscape," observes Govind Rammurthy, CEO, MicroWorld Technologies. "Newer threats are getting extremely focused and insidious in nature where the attacker works with clinical precision in organizing and orchestrating a range of online financial crimes. Right from large enterprises to a single PC home user, anything and anyone can be targeted and manipulated while the victim can still remain completely unawares of it, unless fast-updating and proactive defense measures are employed in implementing Real-Time security for information systems."

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

- [IoDine - IP over DNS 0.3.1](#)
- [sshsan 1.2](#)
- [Oedipus - Web Application Security Scanner 1.8.1](#)
- [Centron Firewall Iptables GUI Client 0.6.5](#)
- [Keygloo 1.0.17](#)

Press Releases

- [Debian Linux Adopts OpenVZ Virtualization Software](#)
- [2X Enables Desktop Virtualization with 2X ThinClientServer](#)
- [ZANTAZ Ranked Top-Five Service Provider for Second Year in a Row](#)
- [PlateSpin Assists in Upgrading to VMware Infrastructure 3 with Near-Zero Downtime](#)
- [VoIP Service Efonica Reaches 250,000 Subscribers in Under 45 Days](#)

Reviews

- [The death of email?](#)
- [5 Steps to Choosing The Right BPM Suite](#)
- [What CIOs can learn from Mediaeval Castles](#)
- [Email: a question of content](#)
- [IT Virtualization](#)