



TOOLS

- [Home](#)
- [Brochure Request](#)
- [Links Directory](#)
- [Newsletters](#)
- [RSS Feeds](#)
- [Advertise](#)
- [Digital Edition](#)
- [Help](#)
- [About Us](#)
- [Contact Us](#)

TECHNOLOGY CHANNELS

- [Channel News](#)
- [Channel Talk](#)
- [Data Capture](#)
- [Mobile Computing](#)
- [Print & Label](#)
- [Retail Technology](#)
- [Document Mgmt](#)
- [Networking](#)
- [Internet Security](#)
- [Data Storage](#)
- [Power/UPS](#)
- [Audio/Visual](#)
- [Events](#)
- [Personal Dev.](#)
- [Video](#)
- [Recruitment](#)

Internet Security

Internet control, email and network protection

Weekly report on viruses and intruders

07 August 2006 MicroWorld

 EMAIL ARTICLE  PRINT ARTICLE

Backdoor Trojan Threatens to Take Over User Computers

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

Advertisements

Related Articles

None

VERTICAL CHANNELS

- [POS/hospitality](#)
- [Logistics](#)
- [Field Service](#)
- [Education](#)
- [Healthcare](#)
- [Manufacturing](#)
- [Office Automation](#)

MAGAZINE

- [Editor](#)
- [Subscribe](#)
- [Media Kit](#)
- [Feedback](#)
- [Digital Edition](#)

victim machine."

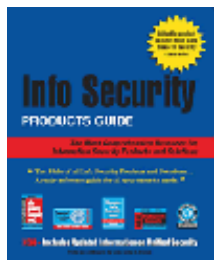
"Though many of these Backdoor Trojans are detected by some of the AntiVirus programs, they are not removed from the Windows registry. Hence when the computer reboots, this malware finds its way back from nowhere. That's why our proactive Security solution, eScan, removes registry entries too so that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

Other Internet Security News

[Internet Security Systems Appoints Two New Members to its Northern Europe Management Team](#)

Internet Security Systems (ISS), the worldwide leader in pre-emptive, enterprise security, today announced the appointment of Andrew Lawton and Bridget Charles as part its Northern European Management Team.



[Netintelligence Gains the Highest Trust of Customers Worldwide](#)

Info Security Products Guide names Netintelligence Enterprise Manager Winner of the 2006 Global Excellence in End Point Security Award

Security White Papers

[CONTENT FILTERING SOLUTIONS TECHNOLOGY REPORT APRIL 2006](#)

Source: West Coast Labs/Netintelligence

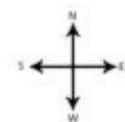


[The Trend of Threats Today: 2005 Annual Roundup and 2006 Forecast](#)

Trend Micro

The report that follows is not only an account and analysis of 2005 threat incidents. It also serves as a forecast

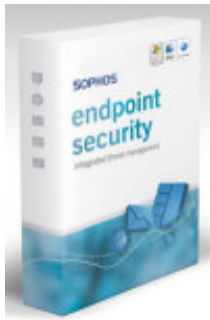
of what the future holds in 2006 and onwards. Through Trend Micro's extensive research and analysis of the 2005 incidents, this paper documents how threats evolved into the multi-purpose threat regime – thus providing corporate and home users information on what to do to ensure they remain protected against future threats. Download free white paper.



[If you can't beat it, manage it](#)

Rob Nash, director of eBusiness at Unipalm, looks at the challenges facing IT managers with the growing use of Instant Messaging in the

workplace.



**[CHANNEL WELCOMES
SOPHOS'S NEW
INTEGRATED SECURITY
OFFERING](#)**

Sophos Endpoint Security simplifies management of intrusion, adware, malware and spyware protection from one console



[Are you becoming a one-stop security shop?](#)

David Ellis, director of e-security at Unipalm discusses best practice security management and the evolution of protection technology.

[How to keep spam off your network](#)

[The corporate threat posed by email Trojans](#)

[More >>](#)

[Secure Computing's Sidewinder G2 Security Appliance Cryptographic Module for SecureOS Achieves FIPS 140-2 Validation](#)

The Sidewinder G2 Security Appliance is a comprehensive unified threat management (UTM) gateway security appliance. It comprises a wide variety of Internet security functions...

[Websense Boosts Channel Training Programme](#)

New accreditation programme builds on current success and creates new revenue opportunities for the channel.

[Sourcefire to cultivate new channel partnerships](#)

This drive follows the addition of several new reseller partners in the first quarter of 2006 with the aim to recruit more throughout year.

[More >>](#)