



only with

GFI MailSecurity

Download your FREE trial today!

- ABOUT US
- CONTACT
- ADVERTISE

Welcome to a new version of Help Net Security. Much has improved and more is on the way. Subscribe to our RSS feeds and stay updated!

NEWS

[Off The Wire](#)
[Security World](#)
[Virus Center](#)

ARTICLES

[Latest Articles](#)
[Reviews](#)
[Interviews](#)
[Book Chapters](#)

SOFTWARE

[Windows Linux](#)
[Mac OS X](#)
[Pocket PC](#)

VULNERABILITIES

[Vendor Advisories](#)
[Vulnerability Database](#)

EVENTS

[Webcasts](#)
[Conferences](#)

NEWSLETTER

[Subscribe](#) [Current](#)

E-MAIL ALERTS

SEARCH

RSS




HOME

OFF THE WIRE **SECURITY WORLD**



- [Zombies and botnets - detecting "crowd surges" in logs and network traffic](#)
- [Cybercrooks add Ajax coding to bag of hacking tricks](#)
- [Security guru leaves Microsoft](#)
- [RSS for hackers?](#)
- [Microsoft invites hackers to test Vista](#)
- [Management apps could pose security risk](#)
- [Hackers clone e-passports](#)
- [Panda Antivirus 2007 launched](#)
- [Centrino wireless flaw leaves laptops vulnerable](#)
- [Security vulnerability in Sun N1 Grid Engine daemons](#)
- [Apple security update 2006-004 is now available](#)
- [Secure-It introduces iPod security cases](#)

LATEST ARTICLES **VIRUS CENTER**

- [Nine Ways to Stop Industrial Espionage](#)
- [Removable Storage: The New Breed](#)
- [Malware Evolution: Mac OS X Vulnerabilities 2005 - 2006](#)
- [Continuous Data Protection](#)
- [Essential Security Software for Mac OS X Users](#)
- [Backdoor Trojan threatens to take over user computers](#)
- [Panda ActiveScan Top Viruses for July 2006](#)
- [Kaspersky Lab Virus Top 20 for July 2006](#)
- [July 2006 top 10 malware threats and hoaxes](#)
- [Victoria's Secret spyware attack steals usernames and passwords](#)


SECURITY SOFTWARE


[++ GFI LANguard Network Security Scanner 7](#) • [++ Acunetix Web Vulnerability Scanner 3.0](#) • [Password Safe 3.02](#) • [CommView 5.3](#) • [Acunetix Web Vulnerability Scanner 4.01](#) • [Tor 0.1.1.22](#) • [Password Gorilla 1.4](#) • [SSL-Explorer 0.2.3](#) • [VisualRoute 2006 10.0j](#) • [WinSCP 3.8.1](#) • [JSch 0.1.28](#) • [GFI Endpoint Security 3](#)
[The Sleuth Kit 2.05](#) • [Snort SMS 1.4.4](#) • [TinyCA 2.0.7.5](#) • [MaraDNS 1.2.07.8](#) • [Sussen 0.26](#) • [FTimes 3.7.0](#) • [yaSSL 1.3.7](#) • [Samhain 2.2.2](#) • [Easy Integrity Check System 3.1c](#) • [TrouSerS 0.2.7](#) • [KisKis 0.19.1](#) • [Aide 0.12 rc1](#)
[Crypt 3](#) • [Web Confidential 3.7.6](#) • [Pastor 1.7.3](#) • [Little Snitch 1.2.3](#) • [KisMAC 0.21a](#) • [iStumbler 96](#) • [Fugu 1.2.0](#) • [Victor 2.0](#) • [Net Tool Box 3.1](#) • [PDFKey Pro 1.0](#) • [HenWen 2.1.2](#) • [Mac GPG 1.4.1](#)
[WiFiFoFum 2.1.1](#) • [Crippin 2.8](#) • [AirFix 1.0b](#) • [Aircanner Mobile Encrypter 2.5](#) • [Confidential Notes 1.1](#) • [Aircanner Mobile Firewall 2.4](#) • [WiFi Graph 0.3 RC3](#) • [SignWise Pro 2.52](#) • [Sentry 2020 2.8](#) • [eWallet 4.0](#) • [Pocket Warrior 15022003-B](#) • [Touch Password Protection 2.3](#)


ADVISORIES

VULNERABILITIES

[Debian Security Advisory - gnupg vulnerability \(DSA 1140-1\)](#) • [Debian Security Advisory - ruby1.6 \(DSA 1139-1\)](#) • [Ubuntu Security Notice - gnupg vulnerability \(USN-332-1\)](#) • [Slackware Security Advisory - gnupg \(SSA:2006-215-01\)](#) • [Debian Security Advisory - cfs \(DSA 1138-1\)](#) • [Ubuntu Security Notice - tiff vulnerabilities \(USN-330-1\)](#)
[OpenForum openforum.asp Multiple Variable XSS](#) • [Dokeos Multiple Unspecified XSS](#) • [Codewalkers PHP Event Calendar calendar.php id Variable SQL Injection](#) • [QaTraq top.inc Multiple Variable XSS](#) • [QaTraq components_copy_content.php Multiple Variable XSS](#) • [QaTraq components_modify_content.php Multiple Variable XSS](#)

Backdoor Trojan threatens to take over user computers

Posted on 03.08.2006

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.”

[[Virus Center main page](#)]



GFI EndPoint Security

**DOWNLOAD YOUR
FREE EVAL TODAY!**



(IN) SECURE
OPEN, INFORMATIVE, TO THE POINT

**FREE SECURITY MAGAZINE
DOWNLOAD HERE!**

//COPYRIGHT 1998-2006 BY HNS CONSULTING LTD. // [READ OUR PRIVACY POLICY](#) // [HOSTED BY ARUBA.IT](#)