



GFILANguard
Network Security Scanner

Download Your
FREE Trial Today!



- ABOUT US
- CONTACT
- ADVERTISE

>>> [Get the latest issue of \(IN\)SECURE Magazine, your FREE way to quality security knowledge!](#) <<<

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 Issue](#)
- [Archive](#)

HOME

E-MAIL ALERTS

SEARCH

RSS



OFF THE WIRE **SECURITY WORLD**

- [Apple patches two critical QuickTime for Java flaws](#)
- [Security professionals allege RDP vulnerability](#)
- [ID cards off to slow start](#)
- [Terrorism not focus of Homeland Security](#)
- [Survey reveals scandal of snooping IT staff](#)
- [A tale of dueling anti-spyware bills](#)
- [The image spammer's new bag of tricks](#)
- [The whole security suite on a USB stick](#)
- [New version of DeviceWall endpoint security product](#)
- [PC Tools acquires world-class behavioral malware technology](#)
- [Is your company PCI DSS compliant?](#)
- [Internet Spyware Prevention Act a leap forward in protecting online consumers](#)

LATEST ARTICLES **VIRUS CENTER**

- [Survey Reveals Scandal of Snooping IT Staff](#)
- [Lessons From a Honeynet That Attracted 700,000 Attacks](#)
- [How To Prepare For a Security Information and Event Management Deployment](#)
- [Stephen Northcutt on Security Certification and the SANS Top 20](#)
- [Today's Biggest IT Security Menace and 6 Ways to Fight It](#)
- [New worm spreads via email, web and network shares](#)
- [A look at the MSN photo worm and a trojan with 9 different malware inside](#)
- [Pirates of the Caribbean trojan](#)
- [The Briz.X Trojan has already stolen the confidential details of 14,000 users](#)
- [OpenOffice worm witnessed in the wild](#)

SECURITY SOFTWARE



• [++ GFI LANguard Network Security Scanner 8](#) • [J2SSH 0.2.9](#) • [JSch 0.1.33](#) • [TightVNC 1.3.9](#) • [WebScarab 20070504-1631](#) • [SSL-Explorer 0.2.13](#) • [Tor, Privoxy and Vidalia bundle 0.1.2.13](#) • [Ad-aware SE Personal Edition 1.06](#) • [Secrets Protector Pro 2006](#) • [Tracks Eraser Pro 6.1](#) • [Generic Security Service 0.0.19](#)
• [FireHOL R5 1.256](#) • [SILC Client 1.1 beta 5](#) • [Logwatch 7.3.6](#) • [Another File Integrity Checker 2.10.1](#) • [Tinc 1.0.8](#) • [GnuPG 2.0.4](#) • [Nagios 3.0a4](#) • [Prelude Manager 0.9.8](#) • [Firewall Builder 2.1.11](#) • [Samhain 2.3.4](#) • [MailScanner 4.58.9-2](#) • [strongSwan 4.1.2](#)
• [Random Password Generator 1.6.1](#) • [Radmind Assistant 1.0.0](#) • [PDFKey Pro 3.4.1](#) • [MultiAlarm 3.4.2](#) • [Mac GPG 1.4.7](#) • [Little Snitch 1.2.4](#) • [iStumbler 98](#)
• [IPSecuritas 3.0rc3](#) • [GlowWorm FW Lite 1.5.3](#) • [FrameSeer 1.7.2](#) • [iProtector 1.3](#) • [Data Guardian 1.1](#)
• [SecuBox for Pocket PC 1.2](#) • [Crippin 2.12](#) • [Aircanner Mobile Encrypter 2.9](#) • [Sentry 2020 2.9](#) • [WiFiFoFum 2.1.1](#) • [AirFix 1.0b](#) • [Confidential Notes 1.1](#) • [Aircanner Mobile Firewall 2.4](#) • [WiFi Graph 0.3 RC3](#) • [SignWise Pro 2.52](#) • [eWallet 4.0](#) • [Pocket Warrior 15022003-B](#)

 **ADVISORIES**  **VULNERABILITIES**

• [Apple Security Update - Security Update \(QuickTime 7.1.6\) \(APPLE-SA-2007-05-29\)](#) • [Debian Security Advisory - otrs2 \(DSA 1298-1\)](#) • [Gentoo Linux Security Advisory - Blackdown Java: Applet privilege escalation \(GLSA 200705-20\)](#) • [Gentoo Linux Security Advisory - PHP: Multiple vulnerabilities \(GLSA 200705-19\)](#) • [Ubuntu Security Notice - pulseaudio vulnerability \(USN-465-1\)](#) • [OpenPKG Security Advisory - php \(OpenPKG-SA-2007.019\)](#)
• [Pie Cart Pro affiliates.php Inc_Dir Variable Remote File Inclusion](#) • [Pie Cart Pro orders.php Inc_Dir Variable Remote File Inclusion](#) • [Pie Cart Pro events.php Inc_Dir Variable Remote File Inclusion](#) • [Pie Cart Pro index.php Inc_Dir Variable Remote File Inclusion](#) • [Pie Cart Pro articles.php Inc_Dir Variable Remote File Inclusion](#) • [Pie Cart Pro faqs.php Inc_Dir Variable Remote File Inclusion](#)



New worm spreads via email, web and network shares

Posted on 29.05.2007

'Here is your documents', 'Mail Delivery System', 'Mail Transaction Failed' or 'Re: Thank you for delivery'. If you chance upon a new mail in your mailbox with any of these lines in its subject field, carrying an attachment, apply caution! It's a new Worm named Cheburgen.a and the email mode of proliferation is just one of many ways in which it can wriggle into computers, say experts at MicroWorld Technologies.

The Worm is written in VC++ language. The name of the attachment is randomly picked from a list that contains words like Data, Body, Doc and Text. The file extension again is a random choice from bat, cmd, exe, scr, pif and zip. The malware comes with its own SMTP engine and sends copies to email addresses harvested from the Windows Address Book of the compromised computer. It modifies the Windows HOSTS files to stop computers from accessing websites of some security companies.

"Cheburgen is also distributed by other Trojans as well as using Drive-by-Download route when someone visits a malicious website," says Manoj Mansukhani, Head – Technology and Marketing, MicroWorld Technologies. "As if that's not trouble enough, it scans other PCs in the network and drops the malware in shared folders. And finally, the Worm is also found to be spreading by exploiting the 'LSASS vulnerability' in Windows."

The Malware displays its Backdoor capabilities when it opens certain ports, connects to IRC channels and takes orders from the remote attacker. The attacker can direct the malware to download and execute files from the Internet by working through this Backdoor component.

"This one has taken the term 'Blended Threat' real far that it adopts something or the other from a variety of malware breeds," points out Govind Rammurthy,

CEO of MicroWorld Technologies.

“People behind this malicious program simply believe that the more is merrier and tries to fire on as many cylinders as possible in their attempt to proliferate it. If you want to protect your computers against a threat like this, it is imperative that you rely on a Security Software that checks all the modes of its spreading routine,” he adds.

[[Virus Center main page](#)]



[Home Security](#)

[Security software Australia](#)

[Security Cameras](#)

[Computer Security Audit](#)

[Asset Tracking](#)

[Keylogger](#)

[Sunex](#)

[Security systems](#)

[Security camera systems](#)

Kaspersky **Antivirus** Software

[GFI EndPoint Security](#)

[POS Software & Systems](#)

//COPYRIGHT 1998-2007 BY HNS CONSULTING LTD. // [READ OUR PRIVACY POLICY](#) //