



Offers Out-Of-The-Box Compliance Reports to Help Meet SOX and HIPAA Requirements



Activeworks SECURITY CENTER Click For FREE Trial



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

NEWSLETTER

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

HOME

E-MAIL ALERTS

SEARCH

RSS

OFF THE WIRE SECURITY WORLD

- [Federated identity: scenarios, architecture, and implementation](#)
- [Consultant breached FBI's computers](#)
- [Researcher vows to publish a browser bug a day for July](#)
- [McAfee sees 400,000 virus definitions by 2008](#)
- [The hidden dangers of instant messaging](#)
- [Skype steps up security spin](#)
- [A day in the life of a security professional](#)
- [Double Password security manager announced](#)
- [ICICI Bank phishing scam targets customers in india](#)
- [Survey reveals end point security loophole 49% fail to lock down devices](#)
- [DNSChanger redirects users to fake bank websites](#)
- [The largest network security event in Asia](#)

LATEST ARTICLES VIRUS CENTER

- [Limiting Vulnerability Exposure Through Effective Patch Management](#)
- [Securing Wireless, Remote and Mobile Computing - Quick Fixes](#)
- [The Ten Most Critical Wireless and Mobile Security Vulnerabilities](#)
- [Striking the Balance Between Storage Security and Availability](#)
- [Security for Websites - Breaking Sessions to Hack Into a Machine](#)
- [Chronicle of malware detected in the first half of 2006](#)
- [Sophos: because of malware home users should switch to Macs](#)
- [New worm holds no genuine](#)

[advantage for Windows users](#) • [Weekly Report on Viruses and Intruders - Kelvir.EO worm, Kukudro.A virus and Downloader.JIH trojan](#) • [Sophos warns of mass-spammed trojan](#)

## SECURITY SOFTWARE



• [++ GFI LANguard Network Security Scanner 7](#) • [++ Acunetix Web Vulnerability Scanner 3.0](#) • [Password Gorilla 1.4](#) • [SSL-Explorer 0.2.3](#) • [VisualRoute 2006 10.0j](#) • [Password Safe 3.01](#) • [WinSCP 3.8.1](#) • [JSch 0.1.28](#) • [GFI Endpoint Security 3](#) • [WinDeveloper IMF Tune 2.8](#) • [Reason 0.5.1](#) • [Tor 0.1.0.17](#) • [NuFw 1.0.27](#) • [OS-SIM 0.9.0 rc2](#) • [TinyCA 2.0.7.4](#) • [Prelude Manager 0.9.5](#) • [Samhain 2.2.1](#) • [yaSSL 1.3.5](#) • [MIMEDefang 2.57](#) • [MaraDNS 1.2.10](#) • [ProShield 3.7.47](#) • [Sussen 0.24](#) • [GnuPG 1.4.4](#) • [strongSwan 2.7.2](#) • [KisMAC 0.21a](#) • [iStumbler 96](#) • [Fugu 1.2.0](#) • [Little Snitch 1.2.2](#) • [Victor 2.0](#) • [Net Tool Box 3.1](#) • [PDFKey Pro 1.0](#) • [HenWen 2.1.2](#) • [Mac GPG 1.4.1](#) • [IPSecuritas 2.1](#) • [Pastor 1.7](#) • [JellyfiSSH 4.2](#) • [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

• [Ubuntu Security Notice - libmms vulnerability \(USN-309-1\)](#) • [Ubuntu Security Notice - shadow vulnerability \(USN-308-1\)](#) • [Ubuntu Security Notice - ppp vulnerability \(USN-310-1\)](#) • [Mandriva Linux Security Update Advisory - kernel \(MDKSA-2006:116\)](#) • [SUSE Security Announcement - acroread \(SUSE-SA:2006:041\)](#) • [SUSE Security Announcement - OpenOffice\\_org \(SUSE-SA:2006:040\)](#) • [Some Chess board.php gameId Variable SQL Injection](#) • [Webmin / Usermin simplify\\_path\(\) Failure Arbitrary File Disclosure](#) • [MyBulletinBoard \(MyBB\) editpost.php Cross-Site Request Forgery](#) • [MyBulletinBoard \(MyBB\) Unspecified SQL Injection](#) • [BLOG:CMS index.php id Variable SQL Injection](#) • [Gracnote CDDbControl ActiveX Control Option String Overflow](#)

**GFI:** [Catch hackers red-handed with LANguard Security Event Log Monitor. Download free trial!](#)

**DNSChanger redirects users to fake bank websites** Posted on 03 July 2006.

You want to pay up your credit card account immediately, as you just remembered that today is the due date. After getting on to your bank's website by carefully typing in the URL, you put in your account number and password, go to the credit card payment section and perform the transaction. Satisfied with completing a task in time, you move onto other chores, till you find out that the website you visited and punched in confidential financial information was in fact a fake one!

Security experts at [MicroWorld Technologies](#) inform that 'DNSChanger.eg' is a high risk potential Trojan that can redirect users to spoofed websites of leading banks, credit card firms and online shops.

DNSChanger.eg works by corrupting the process of translating a domain name to the actual website. When a user types in the web address 'jpmorgan.com', made up of text-strings, it needs to be translated to an IP address like '192.220.34.11', as the Internet understands only numerical info.

Now, the smart Trojan is designed to change the 'NameServer' Registry key value to a fraudulent IP address. So, even if the victim types in the right URL, he will be taken to a scam website that robs him of his identity and finances in broad day light.

"Newer Methods of 'Pharming' are getting truly sophisticated, threatening the very fundamentals on which the world does business online," observes Govind

Rammurthy, CEO, MicroWorld Technologies. "If Phishing requires you to be lured through emails that lead you to imposter websites, this one needs none of that sort. While the unsuspecting user continues an online transaction in good faith, he could be playing directly into the hands of a remote fraudster. It's like creating a make-believe world to fine perfection and then looting everything that a victim has."

In yet another mode of Pharming, attackers work by manipulating and corrupting a DNS Server itself. In here they poison the DNS cache, so that regular website requests are answered with fraudulent ones, affecting a large number of computers in a particular geographical area.

"While coordinated efforts are required among Banks, Other Financial Companies, ISPs, Security Firms and governmental authorities to curb these criminal networks, users can do their best by safeguarding their personal computers with up-to-date protection from Viruses and other intruders. As for enterprises, we know that more and more business critical operations are moving to the Internet and protecting office workstations has long become a basic necessity in Information Integrity and Security," points out Govind Rammurthy.

MicroWorld produces the world's most advanced AntiVirus and Content Security Solutions, growing at the fastest rate in the world today. 'eScan' from MicroWorld offers comprehensive Virus Protection and Content Security, working on its Unique MWL Technology. The other product from MicroWorld, 'MailScan', is a Mail Gateway solution that protects corporate mail systems by enforcing an integrated Security Policy across the enterprise.

[ [Security World main page](#) ]

**Activeworkx**  
SECURITY CENTER

Click For  
**FREE** Trial

Offers Out-of-the-Box  
Compliance Reports  
to Help Meet SOX and  
HIPAA requirements

**CrossTec**  
Corporation

**GFiLANguard**  
Network Security Scanner

**DOWNLOAD FREE  
VERSION TODAY!**

**Black Hat USA 2006**  
Briefings & Training  
July 29-August 3  
Caesars Palace Las Vegas