



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



ActiveWorx SECURITY CENTER Click For FREE Trial CrossTec Corporation

- 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!

Navigation menu with categories: NEWS, ARTICLES, SOFTWARE, VULNERABILITIES, EVENTS, NEWSLETTER, HOME, SECURITY, WORLD, VIRUS CENTER, E-MAIL ALERTS, SEARCH, RSS

OFF THE WIRE SECURITY WORLD


- The ten most critical wireless and mobile security vulnerabilities • Studies question e-voting security • Ajax security basics • Security software slaps IE in "Sandbox" • MySpace case opens security can of worms • Security needs vary for each industry vertical • Windows Genuine program revised following uproar • Apple releases security update for Mac OS X • Kaspersky Lab releases an analytical paper on proactive protection • Comodo expands their Mutual Authentication initiative • Survey reveals NHS failing to secure data on mobile devices • Data security six-month summary


LATEST ARTICLES VIRUS CENTER

- 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 • Microsoft Patch Tuesday Brings Eight Critical Vulnerabilities • Interview with Kenny Paterson, Professor of Information Security at Royal Holloway, University of London • Sophos warns of mass-spammed trojan • Backdoor trojan unleashes dual-media attack • Trojan attacks antivirus software • M00P virus-writing gang busted • Weekly Report on Viruses and Intruders - Bagle.JP, Bagle.JQ and Sixem.A worms, Downloader.JFN Trojan

 SECURITY SOFTWARE


[++ GFI LANguard Network Security Scanner 7](#) • [++ Acunetix Web Vulnerability Scanner 3.0](#) • [Password Safe 3.01](#) • [WinSCP 3.8.1](#) • [JSch 0.1.28](#) • [GFI Endpoint Security 3](#) • [WinDeveloper IMF Tune 2.8](#) • [VisualRoute 2006 10.0i](#) • [SSL-Explorer 0.1.16](#) • [Reason 0.5.1](#) • [Tor 0.1.0.17](#) • [Digital Invisible Ink Toolkit 1.4](#)
[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](#) • [NuFw 1.0.26](#) • [Nmap 4.10](#) • [XML Security Library 1.2.10](#) • [Dazuko 2.2.1](#) • [Distributed Access Control System 1.4.13a](#)
[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

[Cisco Security Advisory - Access Point Web-Browser Interface Vulnerability \(cisco-sa-20062806-ap\)](#) • [Cisco Security Advisory - Cisco Security Advisory: Multiple Vulnerabilities in Wireless Control System \(cisco-sa-20060628-wcs\)](#) • [Ubuntu Security Notice - mutt vulnerability \(USN-307-1\)](#) • [Turbolinux Security Announcement - sendmail denial of service attack](#) • [OpenPKG Security Advisory - curl \(OpenPKG-SA-2006.012\)](#) • [OpenPKG Security Advisory - png \(OpenPKG-SA-2006.011\)](#)
[Ad Manager Pro ad.php ipath Variable Remote File Inclusion](#) • [Ad Manager Pro common.php ipath Variable Remote File Inclusion](#) • [BtitTracker torrents.php Multiple Variable SQL Injection](#) • [Cisco CallManager Web Interface ccmadmin/phonelist.asp pattern Variable XSS](#) • [Cisco CallManager Web Interface ccmuser/logon.asp XSS](#) • [Particle Gallery viewimage.php imageid Variable XSS](#)

Backdoor trojan unleashes dual-media attack

Posted on 28.06.2006

Security experts at [MicroWorld Technologies](#) have received reports about a text message being spammed to mobile phone users in US and parts of Canada, thanking them for subscribing to a nonexistent dating website that would charge them \$2 per day. To unsubscribe the service you are told to visit a URL and follow the instructions.

The professionally designed website directs you to click on a button that says 'unregister your mobile'. You are instructed to type in the mobile number in a textbox and click 'confirm' and subsequently a new window opens up telling you to run a program. The program is nothing but a deadly Backdoor Trojan named as Dumador.bc!

Dumador.bc is a Bot Trojan with keylogging capabilities. To connect to the remote attacker, it opens up dual TCP ports, communicating via 'GET' requests to multiple URLs. The Trojan also blocks websites of several AntiVirus firms by modifying the Windows 'HOSTS' file. The Keylogger component captures personal financial information pertaining to several leading banks and credit card companies, which are passed over to the malware author. Through the port, the attacker controls and manipulates the victim's computer to eventually turn it into a zombie.

"Our users updating their software have no reason to worry as we've been providing protection for this Trojan ever since Apr 11, 2005," informs Sulabh Mahant, Security analyst, MicroWorld Technologies. "What's intriguing here is the bi-layered mode of proliferation with truly sophisticated Social Engineering. The thought

of draining two dollars per day is good enough to make one panic. And the trick is all about inducing that state of mind where you lose senses and readily follow what the fraudster tells you to do”

Backdoor Trojans work surreptitiously in the background, while the infected user remains unaware of the hacker's activities. Many a times they come bundled with popular games and utilities so as to arouse no suspicion what so ever. The person controlling the program can capture keystrokes, view files, steal screen shots and even work the mouse.

Botnets are created by grouping such infected computers, taken over by hackers using Backdoors and Trojans. These networks are employed in a plethora of illegal activities like Denial-of-Service attacks, hijacking SMTP Mail Servers to launch Spam campaigns, wrongfully increasing hit count of specific websites and proliferating deadly viruses.

[[Virus Center main page](#)]

Activeworx
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

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