



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
Testers swoop on McAfee Falcon beta
Mine data not details
How to build a low-cost, extended-range RFID skimmer
Fail-Safe Techniques Erase Magnetic Storage media
Linksys introduces wireless security webcam
Server monitoring with BixData
Security for websites - breaking sessions to hack into a machine
New Incident Database Tracks Web Application-Related Security Breaches
PayPal identity theft; Microsoft France hacked - can you afford to be next?
Global Protection for Companies of All Sizes
Survey on inadequate storage of administrative passwords
New FISMA Security Policy Framework for Federal Government Organizations

LATEST ARTICLES VIRUS CENTER
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
How To Win Friends And Influence People With IT Security Certifications
Understanding Technical vs. Logical Vulnerabilities

• [Nude World Cup worm spreads via email](#) • [Doombot worm spreads via phishing model attack](#) • [Weekly Report on Viruses and Intruders - BlackAngel.B worm, Trojans Banker.DJH and Xorpix.O, the Detnat.A virus](#) • [Beware of PornMagPass, another attempt to blackmail users](#) • [PandaLabs warns of the spread of the BlackAngel.B worm](#)

## 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](#)

• [MaraDNS 1.2.07.6](#) • [Nmap 4.10](#) • [XML Security Library 1.2.10](#) • [NuFw 1.0.25](#) • [Sussen 0.23](#) • [Dazuko 2.2.1](#) • [Distributed Access Control System 1.4.13a](#) • [WebJob 1.6.0](#) • [Nagios 2.4](#) • [strongSwan 2.7.1](#) • [Open1x 1.2.5](#) • [John the Ripper 1.7.2](#)

• [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](#) • [Aircscanner Mobile Encrypter 2.5](#) • [Confidential Notes 1.1](#) • [Aircscanner 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

• [SUSE Security Announcement - awstats remote code execution \(SUSE-SA:2006:033\)](#) • [US-CERT Technical Cyber Security Alert - Microsoft Excel Vulnerability \(TA06-167A\)](#) • [Ubuntu Security Notice - mysql-dfsg-4.1, mysql-dfsg-5.0 vulnerability \(USN-303-1\)](#) • [Trustix Secure Linux Security Advisory - 2006-06-16 \(fcron, libtiff\)](#) • [Mandriva Linux Security Update Advisory - mdkkdm \(MDKSA-2006:106\)](#) • [Mandriva Linux Security Update Advisory - kdebbase vulnerability \(MDKSA-2006:105\)](#)

• [APBoard board.php PHPSESSID Variable SQL Injection](#) • [APBoard main.php viewcatmod Variable SQL Injection](#) • [Calendarix Basic cal\\_event.php id Variable SQL Injection](#) • [Calendarix Basic cal\\_popup.php id Variable SQL Injection](#) • [35mm Slide Gallery index.php imgdir Variable XSS](#) • [35mm Slide Gallery popup.php Multiple Variable XSS](#)

### Doombot worm spreads via phishing model attack

Posted on 16.06.2006

Security experts at [MicroWorld Technologies](#) inform that a Backdoor Worm named 'Doombot.k', is spreading fast via 'abuse warning' emails, spoofing domain names of security software companies and leading business houses. The modus operandi of proliferation is strikingly similar to many phishing attacks in recent times.

Doombot.k comes with IRC bot capabilities and spreads via mass mailing. Once inside the computer, the worm runs in the background, acting as a Backdoor Server that provides access to the victim's PC via IRC channels, for the remote attacker. The smart worm also lowers the security level of the computer, and changes entries in the Windows HOSTS files in order to block websites of AntiVirus companies.

For its spreading routine, the worm steals email IDs from the victim's address book and starts sending itself as .pif, .scr, .exe, .cmd and bat attachments. The most interesting aspect noted here is that it spoofs the domain name of the sender to the same domain of the harvested email address. For example, if the worm steals an email address 'john@xyz.com', it will fake the sender's id as 'abuse@xyz.com', or 'security@xyz.com' and will send it to John's mail address. In the

internal email system of enterprises, this can wreck havoc by spreading fast to infect the entire network.

The subject line of the email is picked from a list that includes various titles like-‘Account Alert’, ‘Important Notification’, ‘Members Support’, ‘Notice of account limitation’, and ‘Security measures’.

The body of the message too is chosen from a list of five options. One of them threatens the user that if the user doesn’t follow the link and confirm the authenticity of the account, it will be terminated. It directs you to two links, one of which throws up an error page and the other, the Doombot Worm in ‘Pif’ format.

In the last few months, MicroWorld has detected a large number of Trojans and Worms that can create bots out of user PCs. Botnets are formed by a network of such computers taken over by hackers, to launch, direct and manage fraudulent activities, online crimes and malicious attacks. The security firm that produces the world’s most advanced security software solutions, reported a three fold increase in the number of bots across the globe in the year 2005, compared to 2004.

“This is a fine instance of what we call as the Convergence of Online Crimes,” says Govind Rammurthy, CEO, MicroWorld Technologies. “You’ve got an attack that resembles phishing, which spreads an email worm that eventually creates large botnets, to be used as hotbeds of online crimes. It clearly indicates that in the dark under-belly of Internet, criminals are connecting, grouping and organizing all sorts of malicious activities with clear financial and informational motives.”

[ [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](#)