



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

- Security in Windows Communication Foundation Seven keys for complete message security IBM seeks dismissal of claims it hacked into law firm's e-mail Copyright watchdog steps up the fight against film pirates New virus pretends to be WGA Energy Review looks to generate security Hacking Xandros Desktop Home 4.0 Global threat report on Web filtering, spyware and viruses Widespread Gmail phishing email lures users with cash prize World's smallest secure USB flash disk introduced Aurora Password Manager 1.5 released Secure Computing to acquire CipherTrust

Latest Articles

VIRUS CENTER

- Successful Backups Are Not Enough 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 Vladimir Putin death spam spreads a trojan horse Insidious network worm threatens enterprise security Weekly Report on Viruses and Intruders - Oscarbot.IV, Peerbot.B and Netsad.B worms Chronicle of malware detected in the first half of 2006 Sophos: because of malware home users should switch

[to Macs](#)

++ GFI LANguard Network Security Scanner 7 ++ Acunetix Web Vulnerability Scanner 3.0 Tor 0.1.1.22 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 Sussen 0.25 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 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 Airscanner Mobile Encrypter 2.5 Confidential Notes 1.1 Airscanner 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

Mandriva Linux Security Update Advisory - xine-lib vulnerability (MDKSA-2006:121) Mandriva Linux Security Update Advisory - libmms (MDKSA-2006:117-1) Cisco Security Advisory - Cisco Intrusion Prevention System Malformed Packet Denial of Service (cisco-sa-20060712-ips) Cisco Security Advisory - Multiple Cisco Unified CallManager Vulnerabilities (cisco-sa-20060712-cucm) Cisco Security Advisory - Cisco Router Web Setup Ships with Insecure Default IOS Configuration (cisco-sa-20060712-crws) Ubuntu Security Notice - libmms, xine-lib vulnerabilities (USN-315-1) WinRAR Self-extracting Archive Comment Processing Overflow Mico set_answer_invoke() Function DoS Linux Kernel prctl Core Dumps Handling Local Privilege Escalation Gimp XCF Parsing xcf_load_vector() Function Overflow TTCalc loan.php Multiple Variable XSS TTCalc mortgage.php Multiple Variable XSS

Insidious network worm threatens enterprise security

Posted on 11.07.2006

If you are used to sharing data over the Internet or your enterprise's intranet, apply caution. A network worm that will eventually bring in dangerous Trojans to your computer, is on the prowl.

Security Analysts at [MicroWorld Technologies](#) inform that 'Win32.Detnat.a' is a Network worm that infects uncompressed PE (Portable Executable) files. With its unique algorithm and polymorphic nature, the worm employs a different mode of encryption each time it infects a file, while keeping the file size unchanged, making it hard to detect.

Detnat.a spreads on shared network resources and file sharing programs. At the second level of attack, the worm goes ahead and downloads 'Infostealer.Lineage', a Trojan that steals usernames and passwords of popular online game 'Lineage' and passes it on to the remote attacker. With its dynamic nature, Detnat can invite any other Trojan as well, if the writer of the worm decides so.

Individual Users and subgroups can freely exchange files in the internal networks of most organizations. This makes it easier for the spreading routine of a worm like Detnat. If the worm stations itself in the startup folder of the workstation connected to a network, then it will come back every time when that computer reboots, even if one cleans up the entire network. In a more targeted operation, an attacker hitting the Server can ensure that every user logging on to that

Server gets infected.

In March, MicroWorld had reported about the Antinny worm which infects the Japanese file sharing program Winny. Top-secret military information, business documents of hundreds of corporate firms, confidential data of 'Liberal Democratic Party' and a thousand others were all floating over the Internet, creating an enormous flood of information leakage in Japan, thanks to Antinny.

[[Virus Center 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!**

Secure
Your
Business.



infosecurity
CANADA

June 19-21, 2006
Metro Toronto Convention Centre
Toronto, Ontario

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