



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](#)

'I love You' Mail Carries Bagle Worm in Zip File

Posted on 23.06.2006

When you get an email from Anna, Alice or Ellyn saying that she loves you and offers you a password to open her heart, don't get carried away. The encrypted zipped file is a Bagle worm.

Security Analysts at [MicroWorld Technologies](#) inform that "Win32.Bagle.fy" comes via password protected ZIP archives attached to spammed emails with a variety of sender names and subject lines.

The subject of the mail is the name of a person chosen from a list that carries common ones like Alice, Andrew, Androw, Annes, Christean, Dorothy, Edmond and many more. The mail body reads 'I love you' and shows an image of the randomly generated numeric password next to it. The worm employs its own SMTP engine to proliferate, spreading fast in US, Europe and South Asia when reports last came in.

"It's always a tendency of the human psyche to open up a protected secret and nobody knows it better than the Virus writer," said Govind Rammurthy, CEO, MicroWorld Technologies. "Now when you club that penchant with a message that says 'I love you', coming from a rather common name, the whole thing adds up to the temptation and smoothly gets you into its vicious design. This is smart Social Engineering with a heady mix of emotional plays."

With its password protected encryption, 'Bagle.fy' evades detection by security solutions at the Gateway provided by some popular AntiVirus firms. After finding an entry into the computer, the worm connects to many websites and downloads much more malicious stuff in the true tradition of Bagle family.

The Bagle family known for its innovation, fast mutation and adaptability has been hugely menacing and dangerous for enterprise security over last few years. These mass mailing worms coming in a wide variety of size, spite and modes of proliferation, have been advancing really fast into deadly Trojans that are even equipped with Rootkit capabilities. An earlier variant named Bagle.GE, carried a Rootkit component which hid the registry keys of another member, Bagle.GF.

"MicroWorld has always advocated for integrated security for enterprises with multi-tiered protection. Viruses and other malware need to be defeated at some point or the other before it sneaks into the user data. With our proactive technologies, gateway level protection and MWL technology, we leave nothing to chance in providing that layer after layer of protection," reflected Govind Rammurthy.

[[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!**

(IN)SECURE
OPEN, INFORMATIVE, TO THE POINT

FREE SECURITY MAGAZINE
DOWNLOAD HERE!

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