



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](#)

NEWSLETTER

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

HOME

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](#)

## Trojan attacks antivirus software

Posted on 27.06.2006

You've seen Hollywood flicks in which the enemy sneaks in through some hatch, kills security guards in dark silence and cold blood, then moves on to open secret doors to bring in more of its fellow folks. Security experts at [MicroWorld Technologies](#) inform that a Trojan-Dropper named 'Win32.Delf.se' works with an uncanny similarity to the sequences of a Beverly Hills potboiler.

Win32.Delf.se's core component is a Windows PE EXE file written in Delphi, wrapped with UPX. Once launched, it goes on to disable popular AntiVirus Applications and paves way for more Adware, Spyware, Trojan and Backdoor.

Often, a Trojan Dropper slips into your computer from malicious websites without showing you any alert or notification. If via emails, they come with hoaxes, jokes, games, graphics and so forth to make the user believe that they are harmless, while discreetly performing deadly operations in the background.

Trojan Droppers contain a few other files than its core component. When executed, they extract these files into a temporary folder and run them all. At times, a Trojan Dropper masquerades its activities by keeping harmless image files like jpegs and gifs along with it. Some breeds of this malware are found to be extracting executable files straight to the memory and launch them, making it all the more difficult for many AntiVirus Solutions to prevent them. Trojan Droppers also tampers with the registry, in order to make the malware start automatically with Windows.

“Malware today, work in a coordinated and incremental fashion with well-defined tasks to be performed at each stage of infection,” viewed Sunil Kripalani, Vice President, Global Sales and Marketing, MicroWorld Technologies. “First you have a small piece of Javascript or VB script sneaking into your computer through a browser vulnerability. It stops security applications, logs on to other malicious websites and brings in all kinds of harmful stuff, compromising your privacy and security in the process.”

To thwart intrusions to information systems, MicroWorld offers the world’s most advanced security solutions, eScan and MailScan to the advantage of security conscious computer users worldwide. eScan provides Real-Time Virus protection and Content Filtering round the clock, powered by proactive methodologies and MWL technology. MailScan on the other hand, protects enterprise communication systems at the gateway level to provide a comprehensive Security Policy Enforcement across the board.

“Hundreds of species of malware are coming out with each passing day. There are mutants, variants, hybrids and brand new creations out there. The best fight-plan in such a scenario would be to have the most updated signature reaction system combined with the most intelligent proactive technology. In eScan and MailScan, we translate that concept into live action!” asserted Sunil Kripalani.

[ [Virus Center main page](#) ]

 <p><b>ActiveWorx</b> SECURITY CENTER</p> <p>Click For <b>FREE</b> Trial</p> <p>Offers Out-of-the-Box Compliance Reports to Help Meet SOX and HIPAA requirements</p>  <p><b>CrossTec</b> Corporation</p>	 <p><b>GFiLANguard</b> Network Security Scanner</p> <p><b>DOWNLOAD FREE VERSION TODAY!</b></p>	 <p>Secure Your Business.</p>  <p><b>infosecurity</b> CANADA</p> <p><b>June 19-21, 2006</b> Metro Toronto Convention Centre Toronto, Ontario</p>
---	---	---

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