



- ABOUT US
- CONTACT
- ADVERTISE

// [Learn about the current state of e-mail security in the latest HNS Podcast](#) //

	NEWS								
	Off The Wire	ARTICLES	SOFTWARE	VULNERABILITIES	EVENTS	NEWSLETTER			
HOME	Security	Latest Articles	Windows Linux	Vendor Advisories	Webcasts	Subscribe Current	E-MAIL ALERTS	SEARCH	RSS
	World	Interviews	Mac OS X	Vulnerability Database	Conferences	Issue Archive			
	Virus Center	Book Chapters	Pocket PC						


OFF THE WIRE **SECURITY WORLD**

- [The secrets of laptop encryption](#) • [Six tips for a painless Patch Tuesday](#) • [Thailand intensifies Web crackdown](#) • [Mozilla seeks security researchers to look at alpha code](#) • [Step cautiously into an online bank](#) • [DVD security group fixes piracy hack](#) • [Hack exposes AACS 'hole'](#)
- [ESET Smart Security Public beta program](#) • [First secure SMS-based mobile payment service deployed](#) • [Enhancements in Deep Six DS200 anti-spam appliance](#) • [\(ISC\)2 launches next phase of NSA training and certification testing programs](#) • [New book release: "Endpoint Security"](#)

LATEST ARTICLES **VIRUS CENTER**

- [Hacking the Cisco NAC - NACATTACK](#) • [HNS Podcast: The Present State of E-mail Security](#) • [The Rise of SSL VPNs](#) • [JavaScript Malware for a Gray Goo Tomorrow!](#) • [Hackers convened in Amsterdam for Black Hat Europe](#)
- [Worm spreads in the guise of a Security Update](#) • [Two worm "families" make up most botnets](#) • [Combined Spamtta and Spamtload attack and the look at Grum.A worm](#) • [Peed trojan family tops Bitdefender's March malware chart](#) • [Combined attack caused by the Spamtta.VK worm and the Spamtload.DT trojan](#)

SECURITY SOFTWARE



- [++ GFI LANguard Network Security Scanner 8](#) • [GFI LANguard Network Security Scanner 8](#) • [WinSCP 4.0.0](#) • [ZoneAlarm 7.0.0337](#) • [Outpost Firewall Pro](#)

[4.0.1007.7323](#) • [PortsLock 2.0](#) • [AxCrypt 1.6.3](#) • [BestCrypt 8.01 beta](#) • [Cryptainer LE 7.0.3.0](#) • [Password Door 8.3.2](#) • [Privatefirewall 5.0](#)
• [Scapy 1.1.1](#) • [Shorewall 3.4.2](#) • [Linux-VServer 2.6.20.4](#) • [SnortALog 2.4.2](#) • [Distributed Access Control System 1.4.18](#) • [The Sleuth Kit 2.08](#) • [Foremost 1.4](#)
• [Metalog 0.8 RC4](#) • [sconly 4.6](#) • [Hardening Patch for PHP 4.4.4 0.4.15](#) • [FreeRADIUS 1.1.5](#) • [OS-SIM 0.9.0 rc4](#)
• [Random Password Generator 1.6.1](#) • [Radmin Assistant 1.0.0](#) • [PDFKey Pro 3.4.1](#) • [MultiAlarm 3.4.2](#) • [Mac GPG 1.4.7](#) • [Little Snitch 1.2.4](#) • [iStumbler 98](#)
• [IPSecuritas 3.0rc3](#) • [GlowWorm FW Lite 1.5.3](#) • [FrameSeer 1.7.2](#) • [iProtector 1.3](#) • [Data Guardian 1.1](#)
• [Crippin 2.12](#) • [Aircscanner Mobile Encrypter 2.9](#) • [Sentry 2020 2.9](#) • [WiFiFoFum 2.1.1](#) • [AirFix 1.0b](#) • [Confidential Notes 1.1](#) • [Aircscanner Mobile Firewall 2.4](#)
• [WiFi Graph 0.3 RC3](#) • [SignWise Pro 2.52](#) • [eWallet 4.0](#) • [Pocket Warrior 15022003-B](#) • [Touch Password Protection 2.3](#)

 **ADVISORIES**  **VULNERABILITIES**

• [Mandriva Linux Security Update Advisory - freetype2 \(MDKSA-2007:081-1\)](#) • [Mandriva Linux Security Update Advisory - krb5, netkit-combo \(MDKSA-2007:077-1\)](#) • [Ubuntu Security Notice - ipsec-tools vulnerability \(USN-450-1\)](#) • [Apple Security Update - Firmware version 7.1 for AirPort Extreme Base Station with 802.11n* \(APPLE-SA-2007-04-09\)](#) • [Gentoo Linux Security Advisory - zziplib: Buffer Overflow \(GLSA 200704-05\)](#) • [Gentoo Linux Security Advisory - libwpd: Multiple vulnerabilities \(GLSA 200704-07\)](#)
• [Pie Cart Pro affiliates.php Inc Dir Variable Remote File Inclusion](#) • [Pie Cart Pro orders.php Inc Dir Variable Remote File Inclusion](#) • [Pie Cart Pro events.php Inc Dir Variable Remote File Inclusion](#) • [Pie Cart Pro index.php Inc Dir Variable Remote File Inclusion](#) • [Pie Cart Pro articles.php Inc Dir Variable Remote File Inclusion](#) • [Pie Cart Pro faqs.php Inc Dir Variable Remote File Inclusion](#)



Worm spreads in the guise of a Security Update

Posted on 10.04.2007

Security experts at [MicroWorld Technologies](#) warn that a worm named 'Win32.Warezov.ms' is spreading via spammed emails, disguised as system generated security warnings from the email service provider.

The smartly crafted mail is a good specimen of clever Social Engineering adopted by present day malware authors. It goes as follows;

Dear Customer,

Our robot has fixed an abnormal activity from your IP address on sending e-mails. Probably it is connected with the last epidemic of a Worm which does not have patches at the moment. We recommend you to install a firewall module and it will stop e-mail sending. Otherwise your account will be blocked until you do not eliminate malfunction.

Customer support center robot.

"Some recipients will definitely be stupefied by the 'System Generated' appearance of the mail," says Govind Rammurthy, CEO of MicroWorld Technologies. "Their deluded reflex would tell them that it's originating from a machine and not created by a human being, which would benumb their ability to smell the rat. That is the very moment the malware writer was hoping for, to slip his malicious file into the victim's computer".

The Warazov worm - also known as Stration - is an exe file that appears as a legitimate Windows patch. This variant is a Trojan downloader which brings in

malicious files into the compromised computer by contacting various websites via HTTP. Coming with its own SMTP engine, it harvests email addresses from the victim's address book and sends its copy to all those user ids.

"The Warezov family has been a permanent fixture at most Top Ten Virus charts for six months in a row now. The malware creator's strategy is to release countless variants of the worm with slight modifications in code to confuse AntiVirus engines. We combat this menace by incorporating an advanced Intentional and Behavioral analysis that nails down the worm, what ever may its attire be," says Govind Rammurthy.

[[Virus Center main page](#)]





7EC50B88386FB0370DA637BCDEB6EA
8DC1951ADE1B8793CD9DE6AD6A56AIC2E
C32FI **INFORMATION IS EVERYTHING** 793C
5E6F6AC5D3B3DA3C32F13E87896A00
37BCDEB6EAD0CEF36AIC2B6A5D8E96F
896A00A **REGISTER FREE TODAY!** A0CEF3
IF **The Premier IT Security Event in Canada** 5
2F13E87896A00A156A10AC32F13E87896
D9DE6AD6A56AIC2B6A5D8E96F6D5E6
3CD9DE6AD6A56A18793C3CD9DE6AD
AIC2B886F **infosecurity** 8386FB8E
F35F0FDA **CANADA** DC1951ADE

Infosecurity Canada | June 13-14, 2007
Metro Toronto Convention Centre | Toronto, Canada

[Home Security](#)
[Security software Australia](#)
[security cameras](#)
[Security Cameras](#)
[Computer Security Audit](#)

[Kaspersky **Antivirus** Software](#)
[GFI EndPoint Security](#)
[POS Software & Systems](#)