



[SmallBusiness](#) [WebKnowHow](#) [HostReview](#) [CGIDir](#) [JavascriptSearch](#) [PromotionWorld](#) [HTMLPrimer](#) [DomainInformer](#)

Sections

- [Home](#)
- [News](#)
- [Articles](#)
- [Domain Tools](#)
- [Best Registrars](#)
- [FAQ](#)
- [Editorials](#)
- [Domain Name Forum](#)
- [Submit Article / News](#)

Search

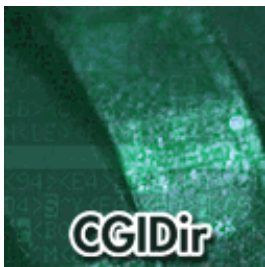
[Search by Category](#)

Advertisement

Domain Tools

- [Domain Suggestions](#)
- [Deleted/On Hold Domains](#)
- [Newly Registered](#)
- [Advanced "who is"](#)
- [Domain Name Statistics](#)
- [Scheduled for Deletion](#)

NEW CGI Directory



Domain Newsletter



[Domain Newsletter](#)

[Home](#) ▶ [Press Releases](#) ▶ Storm Worm blows in with New Y ...

Press Releases by DomainInformer.com

• PRESS BY MONTH	
• EDITOR'S DESK	
• SUBMIT PRESS	
• add to	
• XML	

Storm Worm blows in with New Year wishes

January 3, 2008; 06:02 AM

Apply caution when you get New Year messages in your mail box! A massive attack of the Storm Worm variant called 'Zhelatin.pt' is underway with a rather simpler modus operandi, say Security Experts at MicroWorld Technologies.

It begins with emails arriving with subject line 'Happy New Year' or 'Message for new year'. The mail body has a web address chosen from a random list that contains URLs like newyearcards2008.com, newyearwithlove.com, hohoho2008.com, hellosanta2008.com, happy2008toyou.com and uhavepostcard.com.(Please don't try to access any of these websites on your computer!)

On these websites, a message is displayed which reads as, "Your download should begin shortly..... Click here to launch the download and press Run. Enjoy!". Clicking the link, a file named happynewyear2008.exe or happy2008.exe, which carries the worm Zhelatin.pt', is downloaded into the computer. Once a victim clicks on the downloaded exe, the Worm drops some files and runs certain services to quickly and silently to make the computer a part of a large spam relaying network or Botnet.

"Taking down the websites used in this Worm attack is quite a challenge as all of them are hosted using a technique called Fast-Flux DNS," says Manoj Mansukhani, Head - Global Marketing, MicroWorld Technologies. "Fast-Fluxing is a method where Virus authors deploy a continuously changing network of botnet computers to act as proxies for hosting harmful websites. To add to it, the Russian domain name provider where these sites are registered to is closed for the first week of January, which gives ample time for the criminals behind the worm to make merry!"

The first Zhelatin variant appeared in January 2007 which spread with the help of mails with a subject line '230 dead as storm batters Europe' and other socio political events, thereby deriving its popular name - Storm Worm. All mails carried exe attachments with randomly chosen names that invariably lured recipients into downloading them.

"Storm Worm is the most successful malware of its kind with an established botnet of around 3 million compromised computers worldwide according to some estimates. This network of zombie PCs relays a significant portion of the spam mail traffic on the Internet today. Unlike most other botnets, this one does not have a central command but operates using peer-to-peer networks which makes it practically impossible to dismantle it," Manoj points out.

Users can protect their computers from Storm Worm by resisting the temptation of clicking on season's greetings or other messages that require them to visit unknown websites and to download files, Manoj says. It is also equally important to keep their AntiVirus and Spam Control systems up-to-date, he adds.

MicroWorld

for desktops and servers. Its gateway-level email security software, MicroWorld Technologies (www.mwti.net) is the developer of the world's most advanced AntiVirus and Content Security software eScanMailScan, is a comprehensive mail scanner for your SMTP/POP3 Mail Servers. MicroWorld Winsock Layer (MWL) is the revolutionary technology underlying these products, powering them to several certifications and awards by some of the most prestigious testing bodies, notable among them being Virus Bulletin, Checkmark, TUCOWS, Red Hat Ready and Novell Ready. On the Network Security side, MicroWorld offers a powerful, futuristic network firewall branded as eConceal.

To learn more, kindly visit <http://www.mwti.net>

[Contact Us](#) | [Sitemap](#) | [Corporate](#) | [Advertise](#) | [Privacy policy](#) | [User Agreement](#)

Copyright © 1998 - 2007 [DevStart, Inc.](#) All Rights Reserved

Advertisement

DevStart Network

- [DevStart](#)
- [HostReview](#)
- [Business Owners Idea Cafe](#)
- [Dedicated Servers Seek](#)
- [PromotionWorld](#)
- [DomainInformer](#)
- [Small Business Informer](#)
- [CGI Dir](#)
- [Javascript Search](#)
- [WebKnowHow.Net](#)
- [HTML Primer](#)

Partners

- [Dotster domain names](#)
- [Free & Premium Web Tools](#)
- [Web Design](#)

- [Message Boards](#)
- [PHP Code Examples](#)

Related Resources

- [Business Hosting](#)
- [affordable web hosting](#)
- [web templates](#)
- [cheap hosting](#)
- [Business Opportunity](#)
- [Search Engine Marketing](#)
- [Dedicated Servers from \\$ 79/mo.](#)
- [Website templates](#)
- [Scripts](#)
- [Website Builder](#)
- [Web Design and Web Marketing](#)

Other Resources

