



# Storm Worm blows in with New Year wishes

## News Release

Return to: [Computer Security News](#)

Or: [Recent Computer Security News](#)

## Storm Worm blows in with New Year wishes

<http://www.msspl.co.in>

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

MicroWorld Technologies ([www.msspl.co.in](http://www.msspl.co.in)) is the developer of highly advanced AntiVirus, Content Security and Firewall software solutions eScan, MailScan, and eConceal. MicroWorld Winsock Layer (MWL) is the revolutionary technology that powers most of MicroWorld products enabling them to achieve 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.

For more information, please visit [www.msspl.co.in](http://www.msspl.co.in)

Submitter: [Shardul](#)

MicroWorld Software Services Pvt Ltd.  
January 03, 2008 11:27:55 AM

## NewsWire

[Find articles](#) with the ArticleOn.com [article directory](#) or [submit articles](#) for publication. We are listed at the World Online Index of [top websites](#) and at Finest4 [free directory](#).

---

ExactRelease.com [News Release](#), [newswire](#) gives you "Tomorrow's news released today™" by listing the latest press releases from thousands of sources around the globe sorted according to popular news

releases and [recent news](#) and categorized into the appropriate industry press release categories for easy browsing. Try the ExactRelease.com [submit press release](#) service for free online [press release](#) distribution and get your news noticed. ExactRelease.com - The news as it is released™.

Copyright ©2008 [www.exactrelease.com](http://www.exactrelease.com)