

▼ advertisement

[email to friend](#) [print-friendly version](#) [feedback](#) [bookmark](#)



- [NEWS](#)
- [PRODUCTS](#)
- [HOW TO](#)
- [FEATURES](#)
- [WHITE PAPERS](#)
- [CONTEST ZONE](#)
- [RESOURCE CENTER](#)
- [ISP SPEEDOMETER](#)

Which section you like to visit the most at ZDNet India?

- PRODUCT
- BIZ TECH / NEWS
- DEVELOPER
- DOWNLOADS

Total Clicks : 20181

A	8.46%
B	1.79%
C	86.74%
D	3.01%

NEWSLETTERS

- Biz Tech
- Personal Tech
- Tech Roundup

SUBSCRIBE

▼ advertisement

Storm Worm blows in with New Year wishes

By **ZDNet India Staff**, **January 4, 2008** Apply caution when you get New Year messages in your mailbox. 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," Mansukhani 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. It is also equally important to keep their AntiVirus and Spam Control systems up-to-date, he adds.

Web

zdnnetindia.com

▼ advertisement

▼ advertisement

Specials

[Click here to find out your ISP speed.](#)

SPONSORED LINKS

Type i: [Content Services for Business](#)

[Your Privacy](#) | [Contact Us](#)



The Indian edition of 'ZDNET' is published under license from CNET Networks, San Francisco, CA, USA. Editorial items appearing in 'ZDNET India' that were originally published in the U.S. Edition of 'ZDNET' are the copyright property of CNET Networks or its suppliers. Copyright © 2007 CNET Networks. All Rights Reserved. 'ZDNET' is a registered trademark of CNET Networks. Jasubhai Interactive Pvt. Ltd. owns the compilation copyright in the Localized Edition and all materials thereon not obtained under license from CNET Networks or other third parties.