

enterpriser.in

India's Small And Medium Business Network

Newsletter

Search

[Tech 4 You](#)

TrendsMore

- [Open XML Going Strong](#)
- [Be IT Savvy: Nasscom to Auto Component SMBs](#)
- [Digital Gear Causing Deadly Pollution](#)

Tech 4 YouMore

- [Unite Your Diverse Storage Platforms Are you grappling with the issue of storage complexity? Are you scouting for a solution that would unite your diverse storage platform? Symantec's Storage United can help you simplify the management of the complex, heterogeneous data center environment](#)

AdvisorMore





[Is keeping an eye on latest technologies a problem for you? Well, to ease your problem, Suresh A. Shan, national head \(Information Systems & Technology\) of Mahindra Finance discusses about some emerging technologies and their implementation](#)

[Home](#) > [Know It](#) > [Online](#)



Look Before You Leap

By [enterpriser staff](#) | Jan 3, 2008

This Article:  

Storm Worm has blown in with new year wishes. 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.

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!"

Once you click the link, a file named happynewyear2008.exe or happy2008.exe, which carries the worm Zhelatin.pt', is downloaded into the computer. And then if you click 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) of 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.

"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 doesn't 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," said Mansukhani. It's also equally important to keep their antivirus and spam control systems up-to-date, he adds.

Post your comment on "Malicious websites."

Articles

Popular

- [Digital Transformation for SMEs](#)
- [The Way the Indian Economy is Growing is Exciting](#)
- [On-demand Enterprise Resource Planning for SMBs](#)
- [Now Office on the Line](#)
- [Good News for Software Pirates](#)

Discussed

- [Digitalize Your Company for Better Business](#)
- [Now Office on the Line](#)
- [The Way the Indian Economy is Growing is Exciting](#)
- [Saving Energy Costs with New Digital Gear](#)
- [Raman FibreScience Opts for Microsoft Dynamics](#)

Comment :

Name :

Company :

City :

E-mail :

Word verification : Type the characters you see in the picture below.

b f e f t



Characters are not case-sensitive

[Comments More](#)

- [From Dry MIS reporting to spicy slice & Dice reports are the order of ..](#)
- **Kannan.M.S., Lason India Pvt**
- [Five more Tips The Patch Management The Content Filter The Intrusion ..](#)
- **Kannan.M.S., Lason India Pvt**
- [Integrating Gateway controls into the datacenter by incorporating an appliance ..](#)
- **Kannan.M.S., Lason India Pvt**
- [Mr. Sekar?s way is the only method to start on your own. What contributes ..](#)
- **Vishwas Londhe, Rashtriya Chemi**
- [Seems to be very attractive !! GREAT keep going](#)
- **Kumaran, MEL Systems and**

ITNation Network: Channeltimes.com – CXOtoday.com – Techtree.com



[About the Network](#) – [Chapters](#) – [Feedback](#) – [Site Map](#) – [Contact Us](#)

Copyright (C) 2007 ITNation India Pvt. Ltd. All Rights Reserved.