

4 January 2008

SEARCH


INTERNET | [more..](#)

- [Napster moves to MP3-only](#)
- [TDI hosts e-billing session](#)

Loading...



### Sponsor's Message

Magix empowers clients to fight against fraud with continuous, non-invasive auditing and monitoring solutions designed to take the hard work out of risk management. Visit our website to see the various solutions we specialize in. [www.magix.co.za](http://www.magix.co.za)

### Virtual Press Office™

[Click here](#) for our latest company news.

FINANCIAL | [more..](#)

- [MTN defends position](#)
- [MTN confirms Nigeria deal](#)

COMPUTING | [more..](#)

- [E-governance in Africa goes backwards](#)
- [Intel sticks to its own](#)



Free daily and weekly newsletters.  
Latest IT and telecoms news, information and commentary.

SECURITY

[<< Security](#)

# New year brings worm attack

BY [STAFF WRITER](#), ITWEB[Comment on this](#)[Quick print](#)[Personal archive](#)[Send to a friend](#)[Send a sms](#)

[ Johannesburg, 4 January 2008 ] - A massive attack of the Storm Worm variant called 'Zhelatin.pt' is under way, with a rather simple modus operandi.

This is according to Manoj Mansukhani, head of Global Marketing at MicroWorld Technologies. He says it begins with e-mails 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 Web sites, a message is displayed, which reads: "Your download should begin shortly... Click here to launch the download and press Run. Enjoy!"

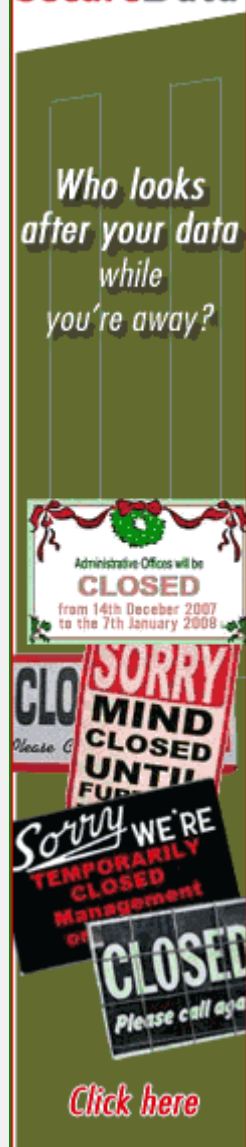
After clicking the link, he explains, Zhelatin.pt is downloaded into the **computer**. "Once a victim clicks on the downloaded exe, the worm drops some files and runs certain services to quickly and silently make the computer a part of a large **spam** relaying network or botnet.

"Taking down the Web sites used in this worm attack is quite a challenge, as all of them are **hosted** using a technique called Fast-Flux DNS," explains Mansukhani.

advertisement

sponsor

SecureData



SecureData

## COMPUTER



[Click here for more on Dell's extensive range of products.](#)

## SPAM

NetXactics

[Sophos ES1000 and ES4000 at the e-mail gateway, integrating anti-virus, anti-spam and policy enforcement capabilities.](#)

## HOSTED



[Want to reduce the complexity of managing your IT environment? Click here for more!](#)

[Click here to subscribe.](#)

**BUSINESS** | [more..](#)

- [Professional brokers vital](#)
- [Sophos placed in Leaders' Quadrant](#)

**ENTERPRISE** | [more..](#)

- [EMC wants Document Sciences](#)
- [Microsoft focuses on EIM](#)

**NETWORKING** | [more..](#)

- [AT&T uses Cisco](#)
- [SMEs to benefit from VPN offering](#)

**TELECOMS** | [more..](#)

- [Government to spend R45bn](#)
- [Kenyan telcos on alert](#)

**CHANNEL** | [more..](#)

- [Comztek resellers compete](#)
- [Pinnacle Micro buys Tri Continental](#)

 [RSS feed](#)

 [News Alerts](#) 

"Fast-Fluxing is a method where virus authors deploy a continuously changing network of botnet computers to act as proxies for hosting harmful Web sites. To add to it, the Russian domain name provider where these sites are registered is closed for the first week of January, which gives ample time for the criminals behind the worm to make merry."

According to Mansukhani, 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," he says.

"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 Web sites, and to avoid downloading files, Manoj says. It is also equally important to keep their anti-virus and spam control systems up-to-date, he adds.

[Comment on this](#)



**ITWeb Business Intelligence 2008**

**Early bird R3 050 + VAT (14%) = R3 477**

26-27 February  
The Forum, Bryanston

Created with the end-user's perspective in mind, the **BI 2008 conference** will focus on working solutions and practical examples of BI in action, presented by a cross-industry mix of IT executives who will share their experiences and lessons learnt.

**Make sure you reserve your seat today!**



**MORE INTERNET NEWS**

- [CA forecasts online threats](#)

[Information Security Leaders](#)

**MOST POPULAR STORIES**

- [MTN defends position](#)
- [SARS warns of tax speed wobble](#)
- [ICASA licenses more USALs](#)

Brought to you by [internet solutions](#)

**Sponsored links**

- [We secure your information while you're away! Click here to find out how.](#)
- [Get back2work with the book Microsoft Office Powerpoint 2007 Plain and Simple.](#)
- [Sophos, a world leader in enterprise IT security and control.](#)

advertisement

**SecureData** LOOKS AFTER YOUR DATA WHILE YOU'RE AWAY?  
**Click here!**

Copyright (c) 1996 - 2008 ITWeb Limited. All rights reserved.

Would you like to see your news here? Contact us for more details at [itnews@itweb.co.za](mailto:itnews@itweb.co.za)

IT DISTRIBUTION DYNAMICS

e-billing  
specialists

verizonbusiness



opa MEMBER OF THE  
ONLINE PUBLISHERS  
ASSOCIATION