

Register

Newsletter

Search

- » Home
- » Products
- » Brands
- » Reviews
- » Games
- » News
- » User Reviews **New!**
- » Downloads
- » Guides
- » Price Search (beta)
- » eClassifieds
- » Forum
- » Ask Techtree
- » User Comments
- » Contests
- » Columns
- » Updates **XML**

Make TechTree your Homepage 

Latest News 

- + Windows Vista SP1 RC Downloadable
- + Macworld 2008 to Begin Jan 15
- + RCom Alloted GSM Spectrum
- + Logitech Labtec Peripherals in India
- + BSNL to Offer CDMA Services

Latest Reviews 



- + The Rise of the Sliders - I
- + MSN Live Suite
- + Techtree Game Awards
- + Samsung G600
- + SanDisk Sansa Shaker (1GB)

User Reviews 

News > Security

Storm Worm Blows New Year Wishes

Techtree News Staff

 Email  Print
 Jan 3, 2008



Handle with care -- security experts at MicroWorld Technologies are warning about new year emails.

They've discovered that a massive attack by the Storm Worm variant, "Zhelatin.pt" is currently underway, and that the modus operandi is deceptively simple.

First, you get an email with a subject line that says, "Happy New Year" or "Message for New Year". The body of the email contains any of the following URLs: newyearcards2008.com, newyearwithlove.com, hohoho2008.com, hellosanta2008.com, happy2008toyou.com, or uhavepostcard.com.

By visiting any of these URLs, you get a message that reads: "Your download should begin shortly. Click here to launch the download." In the event you click, a file, "happynewyear2008.exe" or "happy2008.exe" that carries the Storm Worm variant, "Zhelatin.pt" is downloaded on to your computer.

If you happen to click on the exe, the worm drops some files and runs certain services to stealthily make your computer part of a large spam relaying network or Botnet.

According to Manoj Mansukhani, head (Global Marketing) of MicroWorld Technologies, most of the Web sites used in this Worm attack are hosted using a technique called Fast-Flux DNS.

Fast-Fluxing is the method wherein virus authors use a continuously changing network of botnet computers to act as proxy for hosting harmful Web sites.

Meanwhile, the first of the "Zhelatin" variants appeared in January last year -- also as email, but with subject line, "230 dead as storm batters Europe".

Storm Worm is perhaps the most successful malware of its kind, with an established botnet of around 3 million compromised computers worldwide. Unlike other botnets, it does not have a central command; rather, operates using peer-to-peer networks.

To protect against Storm Worm and its variants, users are advised to resist the temptation of clicking on season's

For Members

email

password

- sign up for a newuser
- forgot password

Most Popular

News

[+Tata's 1 Lakh Car Unveiled](#)

[+Sony Ericsson Unveils the W960i](#)

[+Sony Ericsson W200i Gets Colorful](#)

[+Motorola Acquiring Soundbuzz](#)

[+Facebook, Google, Plaxo Join Group](#)

[+Study Abroad Website for Indians](#)

Reviews

[+PS3 Home \(Preview\)](#)

[+Samsung G600](#)

[+SanDisk Sansa Shaker \(1GB\)](#)

[+Genius SW-N2.1 1100](#)

[+Techtree Game Awards](#)

[+Tishlish Phones](#)

Forum

- + Nokia - 5610
- + Transcend - T.sonic 610 (1GB)
- + Sony Ericsson - W910
- + Nokia - 6500 slide
- + Nokia - 5610

Latest Classifieds

- + Ducat IT Training...
- + Jobs in Manual & ...
- + Placement/Job in ...
- + .Net Corporate Tr...
- + Fresher Jobs in J...

Latest Downloads

ZoneAlarm

Internet Tools

Engine001 Game Maker

Developer Tools

PhotoRazor

Multimedia Tools

Vista Codec Package

Plugins and Add-ons

GoneIn60s

System Tools

Latest Forum Posts

- + Then the best option is to contact I...
- + Share : how to rip D VD and convert V...
- + hey !!!! N o one know the ...
- + n73 music edition in pune is availab...
- + Try to reduce reso a nd details to mi...

Latest AskTT Posts

- + I would call it a pe ssimistic approa...
- + hi, i bought a t mob ile nokia 6300 a...
- + Hi, Can you suggest me the best lap...
- + try ACER ASPIRE 4700 seies Laptop....
- + check PG signal f S. M.P.S. OR call h...

greetings. They also need to keep their anti-virus and spam control systems up-to-date.

More:

[Small.DAM Poses as News on Storm](#)

[Home](#) | [News](#) | [Security](#)

Express Your Opinion!

Comment :

Name :

City :

E-mail :

(We email you a copy of your comment)

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



Characters are not case-sensitive

(All fields essential)

Your Comments

[Report as offensive](#)

> [how do I get rid of it if my server has it?](#)

by **K Bay** from Austin, TX on 04/01/08 01:45 AM

[Reply](#)

[+Pls help me in selecting a new graphic card](#)

[+SUPER PI](#)

["CHALLENGE" ATTN:- OVERCLOCKERS](#)

[+My Complete Rig](#)

[+help on buying graphics cards - < Rs 9000](#)

[+PC in 25k](#)

[+Need configuration for best performance pc in 40K](#)

Security News

- + New Trojan Uses Rootkit Techniques
- + Watch your Printer for Spam!
- + Trend Micro Intros Security Suite '08
- + F-Secure Gives PCs a Health Check
- + Trojans took Center Stage in 2007

Most Wanted Downloads

RAMBooster

System Tools

Best CashBook

Productivity Tools

IE7Pro

Internet Tools

Foxit PDF Reader

Productivity Tools

Tab Mix Plus

Plugins and Add-ons