

Tuesday, 15 January 2008

You are not logged in: [Log In](#) | [Register Now](#) | [Bookmark this page](#) | ●●●●●●

# ArabianBusiness.com

**SITE SEARCH:**

home of:



YOUR DIRECTORY /

[Print this page](#) | [Email this to a friend](#) | [Discuss this article \(0 Comments\)](#) |

## New year storm worm rolls in

by [Matthew Wade](#) on Sunday, 06 January 2008

Users are being advised to exercise inbox caution this month, as a large-scale attack of the Storm Worm variant 'Zhelatin.pt' takes place under the cover of New Year greetings e-mails.

The process of PC infection begins, according to the expert team at MicroWorld Technologies, when an e-mail arrives with the subject line 'Happy New Year' or 'Message for new year'.

The body text of such mails features a web address along the lines of [newyearcards2008.com](#), [newyearwithlove.com](#), [hohoho2008.com](#), [hellosanta2008.com](#), [happy2008toyou.com](#) and [uhavepostcard.com](#). Should a user click through to such websites, a message then appears that reads: "Your download should begin shortly..... [Click here](#) to launch the download and press Run. Enjoy!"

[Story continues below](#) ↓

advertisement

Clicking this link leads to a file named [happynewyear2008.exe](#) or [happy2008.exe](#) being opened, which in turn carries the worm 'Zhelatin.pt'. This installs its own files, designed to

wrestle control of the host computer and to use it as 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," commented Manoj Mansukhani, MicroWorld Technologies' head of global marketing. "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, when it was spread with the help of mails with the subject line '230 dead as storm batters Europe' and other socio political events - thereby deriving its popular 'Storm Worm' name.

"Storm Worm is the most successful malware of its kind with an established botnet of around three million compromised computers worldwide, according to some estimates," Mansukhani added. This network of zombie PCs relays a significant portion of the spam mail traffic on the internet today."

 [Print](#) |  [Email](#) |  [Discuss this article](#) |

#### **TOP IN MIDDLE EAST TECHNOLOGY**

1. [Motorola wins \\$150mn Saudi deal](#)
2. [Kuwait slashes international call charges](#)
3. [Raya studying bid for Egypt fixed-line licence](#)
4. [Abraaj sells stake in Maktoob.com](#)
5. [Qtel joins sharks circling Lebanese telcos](#)

#### **TOP MIDDLE EAST BUSINESS STORIES**

1. [Kuwait vows war on property costs](#)
2. [France, Qatar ink energy deals](#)
3. [Saudi dengue fever fears persist](#)
4. [Gulf bows to US pressure on Iran](#)