

A Storm Worm variant is using the 2008 theme for a large-scale attack. 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.

"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.

#### More from **Digital Security**

- [Worm keeps spam volumes high](#)
- [AVG forecasts security threats](#)
- [Facebook gets invaded](#)
- [Virtual PCs enhance security](#)
- [New laws to affect ICT industry](#)