

- [IT Mgt.](#)
- [State & Local](#)
- [Software Apps.](#)
- [Web Strategies](#)
- [Workflow/Collaboration](#)

[GCN Home](#) > [01/03/08 web stories](#)

New year, new Storm Worm variant

By [William Jackson](#)



Story Tools:

- [Print this](#)
- [Email this](#)
- [Purchase a Reprint](#)
- [Link to this page](#)

I really do wish you a happy New Year, but you'll just have to take my word for that. You probably should assume that any e-mail from me or anyone else with holiday wishes is a not-so-sly attempt to get you to download malware.

The folks at MicroWorld Technologies have identified a new variant of the venerable Storm Worm that is being spread through e-mails with the subject line "Happy New Year" or "Message for a new year." The body of the e-mail contains a link to any of a number of .com sites that read as if they should deliver some sort of e-greeting. But the downloaded file contains the Zhelatin.pt worm. When executed, the worm installs files and recruits your computer to a botnet as a spam relay.

The Storm Worm has been around in a variety of forms now for a year, owing its success to frequent morphing of the code and its use of social-engineering techniques to lure unsuspecting recipients. It is responsible for an estimated 3 million compromised computers available for relaying spam, holding files and hosting malicious code.

"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," said Manoj Mansukhani, head of MicroWorld global marketing. "Fast-Fluxing deploys 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 to is closed for the first week of January, which gives ample time for the criminals behind the worm to make

merry!”

You should keep antivirus and spam filters updated, but the best way to protect against this and other variants sure to come is to be suspicious of such greetings, avoid clicking links in any unexpected e-mail and just do not download files from Web sites if you are not absolutely sure what they are.

And happy New Year. No need to click on anything to verify that.

More news on related topics: [IT Security](#), [Web Strategies](#)

Latest News ■ [WashingtonTechnology.com](#) ■ [FCW.com](#)

■ **GCN.com**

The latest technology news from [GCN.com](#)

- [Even more untrustworthy](#)
- [DOD battery contest venue chosen](#)
- [Hill Web sites need work](#)
- [Customs automates workers' comp filing](#)
- [Secure E-mail standard](#)

- [Home](#)
- [About](#)
- [Advertise](#)
- [Contact](#)
- [Custom Media](#)
- [Editorial Calendar](#)
- [Events](#)

- [List Rental](#)
- [Privacy Policy](#)
- [Reprints/Linking Policy](#)
- [Subscribe](#)
- [Site Map](#)

GCN