



COMPUTERWORLD

THE VOICE OF ICT MANAGEMENT



PHILIPPINES

MEDIA G8WAY > COMPUTERWORLD

Computerworld

[Home](#)
[CWP Exclusives](#)
[Dossier](#)
[CIO Roundtables](#)
[In The Magazine](#)
[This Month's News](#)
[CWP Events](#)
[Archive](#)
[Advertise](#)
[Industry Bulletin](#)
[Contact Us](#)
[About Us](#)

February 2008
Print Edition



Stay up to date with the latest news, features and industry events. Subscribe now and get a 10% discount!!!

Industry Bulletin

Don't fall for this gentle kiss! It's the Storm Worm in a new form

January 23, 2008

A new wave of attack has begun from the Storm Worm. This time the theme is love. Emails with links to a bait website hosting the malware are sent out in bulk numbers for the last three days, says AntiVirus, AntiSpam and Content Security firm MicroWorld Technologies.

Virus writers do have a heart, or at least they are faking one! The subject lines of this Worm spreading mail are as mushy as they can get. They go like: 'Eternity of Your Love', 'I Love You Soo Much', 'falling in love with you', 'For You My Love', 'our journey', 'our love nest', 'Memories of You' and 'A Kiss So Gentle'.

The mail shows a nice pink heart and a message that reads as, "Your download should begin shortly. If your download does not start in 10-20 seconds, you can click here to launch the download and then press run. Enjoy!". What's downloaded on clicking this message is a file named withlove.exe or with_love.exe, which carries a not-a-bit lovable malware named 'Zhelatin.sg'.

"This is a new rollout from the ill famed storm factory with some changes in code and a new spreading theme. And if one has to go by the initial volumes, the attack seems fairly large," says Govind Rammurthy, CEO of MicroWorld Technologies. "The two important factors that enable this malware to give a hard time for many security solutions are the speed at which new variants are dished out and countless places where they can host these threats".

The activities of Zhelatin.sg inside the compromised computer are pretty much the same as its predecessors. The Worm drops a file named 'burito.ini', stops Antivirus running on the computer and activates a range of ports to connect to peer-to-peer networks before making the computer a part of the mammoth sized storm botnet. From that point on, the computer would send out spam or do many other things that the remote attacker would want it to do.

"So far the primary duty of a computer in this network is only to relay spam. However one would shudder to think what happens when the controllers behind this network having such massive computing power move on to spread more harmful Viruses or start widespread Denial-of-Services attacks? I believe it's high time law enforcement agencies work with security companies to initiate a global crackdown on this criminal gang," says Govind Rammurthy.

Govind's firm MicroWorld offers multilevel protection against all

Spotlight:



[Articles on Technologies for Small and Medium Enterprises](#)



[Articles on Open Source](#)



[Articles on IT Disaster Recovery](#)



[Articles on Outsourcing](#)



[Articles on Vista](#)

variants of this malware. Its AntiVirus and AntiSpam solution at mail server, MailScan, tackles all sorts of spam and threat laden mails by employing a range of technologies including MicroWorld's recent invention called 'Non Intrusive Learning Patterns'. eScan, the Enterprise security solution, combines fast updating signature based detection with proactive technologies to keep the Worm at bay all time .

Home



Read sector reviews [here](#).



Zune hits the streets
Track the story [here](#).



Google bets big on Internet Video
Track the story [here](#).

[Home](#) [CWP Exclusives](#) [CIO Roundtables](#) [This Month's News](#) [Archive](#) [Industry Bulletin](#) [About Us](#)

Media G8way News Network

[Computerworld Philippines](#) [PC World Philippines](#) [Enterprise](#) [Stuff Philippines](#) [IT Resource](#)

2005 Media G8way Corp. All rights reserved. Reproduction in whole or in part in any form or medium without express written permission of Media G8way Corp. is prohibited.

Powered by [Philippine Web Hosting Provider](#).