

## Storm Worm returns as a Mushy Valentine's Day Greeting

1 2 3 4 5 0 Votes - Rate It

Saturday, January 19th, 2008 | Related entries: [Internet](#), [Security](#)



**Not matter what the season or occasion, the Storm Worm somehow rears its ugly head! The New Year 2008 saw the return of the Storm Worm posing as a fake greeting and more recently, the botnet was targeting Barclay's customers. Now, a new wave of attack has begun and this time in keeping with the upcoming celebration of love more commonly known as Valentine's Day, the Storm Worm has popped up once again.**

AntiVirus, AntiSpam and Content Security firm MicroWorld Technologies has said that emails with links to a bait web site hosting the Storm Worm malware are being sent out in bulk over the last three days.

The subject lines of this email containing the Storm Worm are very mushy, making you feel that the sender is totally in love with you. So beware, because the virus writers are indeed faking that they have a heart! Subject lines of these emails include 'Eternity of your Love', 'I Love You So Much', 'Falling in Love with You', 'For You My Love', 'Our Journey', 'Our Love Nest', 'Memories of You' and 'A Kiss So Gentle.'

The virus writers are very smart as the mail shows a pink heart and a message that read, "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!"

A file named withlove.exe or with\_love.exe is then downloaded on clicking the message. This file carries a not so lovable malware named 'Zhelatin.sg'.

According to **Govind Rammurthy, CEO of MicroWorld Technologies**, "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. 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 once inside the compromised computer are similar to the worm's predecessors. The Storm Worm drops a file names '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 botnet. From this point beyond, the computer will send out spam or do many other things that the remote attackers 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," continued Govind Rammurthy.

MicroWorld offers multilevel protection against all variants of this malware. The company's 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'. Also, eScan, the Enterprise security solution, combines fast updating signature based detection with proactive technologies to keep the Worm at bay all time.