

IT BackbonesTM

Security News



Give your mouse a heart!

search

The IT Shield - Dedicated To IT Security Issues, Featuring News, Press Releases, IT Directory & Links

- [Home](#)
- [About](#)
- [Contact](#)
- [Submit PR](#)
- [Search News](#)
- [What We Can Offer You](#)
- [IT Events](#)
- [Time & Money](#)

New Worm Claims To Show You Pictures Of Paris!

Published 10th August 2006



If you get an email from one of your friends, with a subject line-‘My Photo on Paris’, do not click and download the zipped attachment. The poor fellow has definitely not been to the fashion capital of the world on a pleasure trip! And instead of showing you the picturesque Paris and its great Eiffel Tower, the email will pave way for a worm to rear its ugly head inside your computer the moment you open the attachment.

Security Analysts at MicroWorld Technologies inform that the attached file ‘Picture.zip’ bundles two ‘.bat’ files and a file named ‘picture.bmp’. This bmp is a Trojan Downloader code that goes on to connect to predefined websites and

bring in ‘Worm.Win32.Brontok.o’

‘Brontok.o’ is a mass mailing worm with its own emailing engine. After harvesting mail addresses from the victim’s computer, it forges the email identity of the victim and sends ‘picture.bmp’ to all the contacts found in the address book. The mail could be either in Indonesian or English.

“Offering to show personal photographs has been a regular mode of proliferation for most Brontok varieties,” says Sulabh Mahant, Security Analyst, MicroWorld

Technologies. “The fact they are continuing the same method with slight modifications in the vector and code, goes to prove that the attackers are still managing to hit large number of unsuspecting users and plant this worm successfully. May be one should blame it on most people’s curiosity to view some wonderful candid frames from the lives of their friends and relatives!”

Inside the computer, Brontok moves on to shut down many popular AntiVirus software and overwrites the HOSTS file to stop their regular process of signature updating. The worm installs itself in the registry and replaces infected files with clean copies to evade detection by AntiVirus software. Brontok has the capability to log on to specific websites and download more malware, and with the AntiVirus out of action, it could potentially bring in deadly Trojans.

“Worms like these can seriously handicap enterprises by spreading like crazy via their internal mailing systems,” points out Sunil Kripalani, Vice President, Global Sales and Marketing, MicroWorld Technologies. “That’s precisely why we have been strongly recommending the eScan Enterprise solution in providing a multi-layered protection for the mailing systems in organizations and business houses.”

In eScan Enterprise, you have ‘MailScan’ to protect the Mail Server and ‘eScan’ that protects the Server and each Workstation across the board. Both our solutions are powered by Unique MWL technology and the world’s best AntiVirus engine with the fastest detection rate, to make sure that we leave nothing to chance in consistently and steadfastly protecting information Integrity and Business Continuity, explains Sunil Kripalani.

Company Profiles powered by ITReseller.com

- MicroWorld - [View profile](#)