

BLACKNET NEWS


[Articles Index](#)
[Article Search](#)
[Newsletter Signup](#)
[Refer a Friend](#)
[Navy SEAL Recruiting](#)

MEMBERS AREA
[Log In](#)



NOT A MEMBER?
[Join Now](#)

Media Center [ARTICLE INDEX](#) [ARTICLE SEARCH](#)

 **Global News** [Article Index](#) » [Global News](#) » [General](#)

 Search

- Paris Photo Virus Advertisement
- Source: marketing@mwti.net
- Thursday August 10, 2006

 EMAIL TO A FRIEND  PRINT ARTICLE Page: | 1 |

[ed.note: Oops. You opened it.]

Hello (%Name%),

[New Worm Claims to Show You Pictures of Paris!](#)

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.

CUSTOM SUGGESTIONS



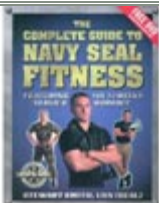
[Rocket Fin Dive Kit](#)



[Garmont T6 Tactical Boot - Tan](#)



[Luminox Original Navy SEAL Dive Watch](#)



[The Complete Guide to Navy SEAL Fitness - Book and DVD Combo](#)

“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.

MicroWorld

MicroWorld (www.mwti.net) is the developer of the world's first Real-Time Anti-Virus and Content Security software eScan for desktops and servers. Its communication security software, MailScan is the first comprehensive e-mail scanner for your SMTP/POP3 Mail Server. MicroWorld Winsock Layer (MWL) is the revolutionary technology underlying these products, powering them to several certifications and awards by some of the most prestigious testing bodies, notable among them being Virus Bulletin, Checkmark, TUCOWS, Red Hat Ready, and Novell Ready. Combining their powerful scanner with MWL technology, MicroWorld solutions provide a Real-Time Proactive security for your systems. For network security of enterprises, eConceal Firewall is the latest powerful offering from MicroWorld.

To learn more, kindly visit <http://www.mwti.net>.

Regards,
MicroWorld
Marketing Department
Email: marketing@mwti.net

Page: | 1 |

This article is copyrighted material, the use of which has not been specifically authorized by the copyright owner. We are making such material available in our efforts to advance understanding of environmental, political, human rights, economic, democracy, scientific, and social justice issues, etc. We believe this constitutes a 'fair use' of any such copyrighted material as provided for in section 107 of the US Copyright Law. In accordance with Title 17 U.S.C. Section 107, the material on this site is distributed without profit to those who have expressed a prior interest in receiving the included information for research and educational purposes. For more information go to: <http://www.law.cornell.edu/uscode/17/107.shtml>. If you wish to use copyrighted material from this site for purposes of your own that go beyond fair use, you must obtain permission from the copyright owner.

© 1996-2006 NavySEALs.com | [About Us](#) | [Privacy Policy](#) | [Terms of Use](#) | [Contact Us](#) | [Log In](#) | [Site Map](#)

[Navy SEAL Museum](#) | [SEAL Archives](#) | [NavySEALs.com STORE](#) | [SEAL Fitness and Health Center](#)
[Com Shack Community](#) | [Resources and Links](#) | [Recruit Depot](#) | [Media Center](#)