



only with

GFI MailSecurity

Download your FREE trial today!

- ABOUT US
- CONTACT
- ADVERTISE

Welcome to a new version of Help Net Security. Much has improved and more is on the way. [Subscribe to our RSS feeds and stay updated!](#)

NEWS

- [Off The Wire](#)
- [Security World](#)
- [Virus Center](#)

ARTICLES

- [Latest Articles](#)
- [Reviews](#)
- [Interviews](#)
- [Book Chapters](#)

SOFTWARE

- [Windows Linux](#)
- [Mac OS X](#)
- [Pocket PC](#)

VULNERABILITIES

- [Vendor Advisories](#)
- [Vulnerability Database](#)

EVENTS

- [Webcasts](#)
- [Conferences](#)

NEWSLETTER

- [Subscribe](#)
- [Current](#)
- [Issue Archive](#)

HOME

E-MAIL ALERTS

SEARCH

RSS



OFF THE WIRE SECURITY WORLD

- [Symantec cries foul over Vista's bolted down kernel](#)
- [Hacker sophistication outpacing forensics](#)
- [Gartner's top 5 tips to boost data security](#)
- [Security tech firms may benefit from foiled plot](#)
- [Worm fears raised after release of Windows malware](#)
- [Technology for rescuing stolen laptops](#)
- [FISMA could solve data security issues](#)
- [First portable anti-spyware product for U3 smart drive platform](#)
- [Info on HITBSecConf2006 Capture The Flag contest](#)
- [Up to one in 600 social-networking pages host malware](#)
- [Warning of a serious BlackBerry security threat](#)
- [DesktopSecure for Linux for Ubuntu 6.06 LTS available](#)

LATEST ARTICLES VIRUS CENTER

- [How to Start Up a Mobile Security Project](#)
- [10 Tips for Reducing Storage TCO](#)
- [Nine Ways to Stop Industrial Espionage](#)
- [Removable Storage: The New Breed](#)
- [Malware Evolution: Mac OS X Vulnerabilities 2005 - 2006](#)
- [New worm claims to show you pictures of Paris](#)
- [Weekly Report on Viruses and Intruders - spying, hijacking computers and stealing bank details](#)
- [Backdoor Trojan threatens to take over user computers](#)
- [Panda ActiveScan Top Viruses for July 2006](#)
- [Kaspersky Lab Virus Top 20 for July 2006](#)

SECURITY SOFTWARE



- [++ GFI LANguard Network Security Scanner 7](#) • [++ Acunetix Web Vulnerability Scanner 3.0](#) • [Kaspersky Internet Security 6.0](#) • [Kaspersky Anti-Virus 6.0](#) • [Tor 0.1.1.23](#) • [Password Safe 3.02](#) • [CommView 5.3](#) • [Acunetix Web Vulnerability Scanner 4.01](#) • [Password Gorilla 1.4](#) • [SSL-Explorer 0.2.3](#) • [VisualRoute 2006 10.0j](#) • [WinSCP 3.8.1](#)
- [Distributed Access Control System 1.4.14](#) • [NuFw 1.0.27](#) • [MailScanner 4.55.9-1](#) • [GnuPG 1.4.5](#) • [The Sleuth Kit 2.05](#) • [Snort SMS 1.4.4](#) • [TinyCA 2.0.7.5](#)
- [MaraDNS 1.2.07.8](#) • [Sussen 0.26](#) • [FTimes 3.7.0](#) • [yaSSL 1.3.7](#) • [Samhain 2.2.2](#)
- [Crypt 3](#) • [Web Confidential 3.7.6](#) • [Pastor 1.7.3](#) • [Little Snitch 1.2.3](#) • [KisMAC 0.21a](#) • [iStumbler 96](#) • [Fugu 1.2.0](#) • [Victor 2.0](#) • [Net Tool Box 3.1](#) • [PDFKey Pro 1.0](#) • [HenWen 2.1.2](#) • [Mac GPG 1.4.1](#)
- [WiFiFoFum 2.1.1](#) • [Crippin 2.8](#) • [AirFix 1.0b](#) • [Aircanner Mobile Encrypter 2.5](#) • [Confidential Notes 1.1](#) • [Aircanner Mobile Firewall 2.4](#) • [WiFi Graph 0.3 RC3](#) • [SignWise Pro 2.52](#) • [Sentry 2020 2.8](#) • [eWallet 4.0](#) • [Pocket Warrior 15022003-B](#) • [Touch Password Protection 2.3](#)

ADVISORIES

VULNERABILITIES

- [Microsoft Security Bulletin - Summary for August, 2006](#) • [Debian Security Advisory - ncompress \(DSA 1149-1\)](#) • [Debian Security Advisory - gallery \(DSA 1148-1\)](#) • [Mandriva Linux Security Update Advisory - ncompress \(MDKSA-2006:140\)](#) • [Mandriva Linux Security Update Advisory - krb5 \(MDKSA-2006:139\)](#) • [Apple Security Update - Security Update 2006-004 for Mac Pro \(APPLE-SA-2006-08-09\)](#)
- [aWebNews login.php page Variable Arbitrary File Access](#) • [Lhaplus LZH Archive Extended Header Processing Overflow](#) • [MyNewsGroups layersmenu.inc.php myng_root Variable Remote File Inclusion](#) • [IBM Informix Dynamic Server DBINFO\(\) Function Overflow](#) • [IBM Informix Dynamic Server LOTOFILE\(\) Function Overflow](#) • [IBM Informix Dynamic Server C Code UDR Unspecified Privilege Upgrade](#)

New worm claims to show you pictures of Paris

Posted on 10.08.2006

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.

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.

[[Virus Center main page](#)]

Gfi EndPointSecurity

**DOWNLOAD YOUR
FREE EVAL TODAY!**

Gartner
IT Security Summit 2006

18-19 September 2006
Royal Lancaster Hotel, London
europe.gartner.com/security

//COPYRIGHT 1998-2006 BY HNS CONSULTING LTD. // [READ OUR PRIVACY POLICY](#) // [HOSTED BY ARUBA.IT](#)