



**TOOLS**

- [Home](#)
- [Brochure Request](#)
- [Links Directory](#)
- [Newsletters](#)
- [RSS Feeds](#)
- [Advertise](#)
- [Digital Edition](#)
- [Help](#)
- [About Us](#)
- [Contact Us](#)

**TECHNOLOGY CHANNELS**

- [Channel News](#)
- [Channel Talk](#)
- [Data Capture](#)
- [Mobile Computing](#)
- [Print & Label](#)
- [Retail Technology](#)
- [Document Mgmt](#)
- [Networking](#)
- [Internet Security](#)
- [Data Storage](#)
- [Power/UPS](#)
- [Audio/Visual](#)
- [Events](#)
- [Personal Dev.](#)
- [Video](#)
- [Recruitment](#)

## Internet Security

Internet control, email and network protection

### Weekly report on viruses and intruders

14 August 2006 MicroWorld

EMAIL ARTICLE PRINT ARTICLE

#### 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!"

**Advertisements**

#### Related Articles

None

**VERTICAL CHANNELS**

- [POS/hospitality](#)
- [Logistics](#)
- [Field Service](#)
- [Education](#)
- [Healthcare](#)
- [Manufacturing](#)
- [Office Automation](#)

**MAGAZINE**

- Editor**
- Subscribe**
- Media Kit**
- Feedback**
- Digital Edition**

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.

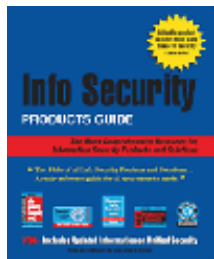
"Worms like these can seriously handicap enterprises by spreading like crazy via their internal mailing systems," points out Sunil Kripalani, Vice President, Global Sales and Marketing, MicroWorld Technologies. "That's precisely why we have been strongly recommending the eScan Enterprise solution in 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.

**Other Internet Security News**

**Internet Security Systems Appoints Two New Members to its Northern Europe Management Team**

Internet Security Systems (ISS), the worldwide leader in pre-emptive, enterprise security, today announced the appointment of Andrew Lawton and Bridget Charles as part its Northern European Management Team.



**Netintelligence Gains the Highest Trust of Customers Worldwide**

Info Security Products Guide names Netintelligence Enterprise Manager Winner of the 2006 Global Excellence in End Point Security Award

**Security White Papers**

**CONTENT FILTERING SOLUTIONS TECHNOLOGY REPORT APRIL 2006**

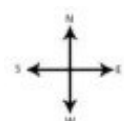
Source: West Coast Labs/Netintelligence



**The Trend of Threats Today: 2005 Annual Roundup and 2006 Forecast**

*Trend Micro*

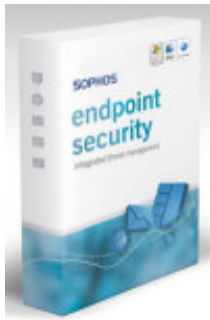
The report that follows is not only an account and analysis of 2005 threat incidents. It also serves as a forecast of what the future holds in 2006 and onwards. Through Trend Micro's extensive research and analysis of the 2005 incidents, this paper documents how threats evolved into the multi-purpose threat regime – thus providing corporate and home users information on what to do to ensure they remain protected against future threats. Download free white paper.



**If you can't beat it, manage it**

Rob Nash, director of eBusiness at Unipalm, looks at the challenges facing IT managers with the growing use of Instant Messaging in the

workplace.



**[CHANNEL WELCOMES  
SOPHOS'S NEW  
INTEGRATED SECURITY  
OFFERING](#)**

Sophos Endpoint Security simplifies management of intrusion, adware, malware and spyware protection from one console



**[Are you becoming a one-stop security shop?](#)**

David Ellis, director of e-security at Unipalm discusses best practice security management and the evolution of protection technology.

**[How to keep spam off your network](#)**

**[The corporate threat posed by email Trojans](#)**

[More >>](#)

**[Secure Computing's Sidewinder G2 Security Appliance Cryptographic Module for SecureOS Achieves FIPS 140-2 Validation](#)**

The Sidewinder G2 Security Appliance is a comprehensive unified threat management (UTM) gateway security appliance. It comprises a wide variety of Internet security functions...

**[Websense Boosts Channel Training Programme](#)**

New accreditation programme builds on current success and creates new revenue opportunities for the channel.

**[Sourcefire to cultivate new channel partnerships](#)**

This drive follows the addition of several new reseller partners in the first quarter of 2006 with the aim to recruit more throughout year.

[More >>](#)