

- **Interne Weisungen der Bundesagentur für Arbeit jetzt im Internet zugänglich**
- **Panda Soft: Erster Wurm entdeckt, der die Microsoft-Schwachstelle MS06-040 ausnutzt**
- **Vermeintliches Urlaubsfoto des Pariser Eiffelturms enthält Computer-Wurm**
- **Bitkom: Wett-Monopol ein Anachronismus im Internetzeitalter**
- **Neun neue kritische Sicherheitslücken in Microsoft-Anwendungen**

[Startseite](#) [Security Blog](#) Vermeintliches Urlaubsfoto des Pariser Eiffelturms enthält Computer-Wurm

Weitere Links zum Thema:

Vermeintliches Urlaubsfoto des Pariser Eiffelturms enthält Computer-Wurm

Benutzer Bewertung: / 0

Schlecht Sehr gut

[Security - Viren, Würmer & Trojaner](#)

Montag, 14. August 2006

(box) München, 14.08.2006 - Wieder einmal zur Hauptreisezeit nutzt ein Computer-Wurm die Neugier der Menschen nach vermeintlichen Urlaubsfotos aus. In fast allen Fällen erhält der Computer-Benutzer die initial seinen Computer infizierende eMail aus seinem privaten Bekanntenkreis oder geschäftlichen Umfeld, da sich der schädigende Wurm per eMail an sämtliche Kontakte des eMail-Adressbuchs eines befallenen Computers versendet, wobei der arme Kerl, der Absender, in den meisten Fällen nicht in Paris gewesen ist. Anti-Virus-Spezialisten des Security-Unternehmens MicroWorld warnen davor eintreffende eMails, selbst von sehr gut bekannten Absendern mit der Betreff-Zeile "My Photo on Paris" zu ignorieren und möglichst gleich zu löschen. So hat der Empfänger, auch später unbeabsichtigt, keine Möglichkeit den Dateianhang 'picture.zip' durch einen Doppelklick zu öffnen, der zwei ausführbare Stapeldateien (.bat) und das Bild 'picture.bmp' enthält.

http://prolog.biz/presse/microworld/img/brontok_worm.jpg ((diese Ansichtsdateri enthält natürlich keinen Wurm))
Die Datei enthält einen Code, der über bestimmte Web Sites den Trojaner 'Worm.Win32.Brontok.o' herunter lädt.

"Bereits mehrere frühere Varianten aus der Brontok-Serie haben sich die Neugier der eMail-Adressaten zu Nutze gemacht und damit ihre weitere Verbreitung gesichert", so Mario Gunsch, Country Manager der Münchner MicroWorld Technologies GmbH. "Dass in Abständen immer wieder leicht modifizierte neue Varianten des Brontok-Wurms auftreten zeigt, wie erfolgreich die Programmierer solcher Schädlinge mit jeder neuen Variante sind."

Wie verhält sich die Malware auf dem befallenen Computer?

Nachdem der Computer-Benutzer durch Doppelklick auf die Datei-Anhänge eine Kopie des Wurms aus dem Internet geladen hat durchsucht dieser Adressbücher nach eMail-Adressen und versendet sich selbst mithilfe einer eigenen eMail-Engine an diese gefundenen Opfer, natürlich mit dem Absender-Namen des befallenen Rechners damit der sorglose Empfänger keinen Grund sieht, die Dateien eines Bekannten nicht zu öffnen.

Der Schädling kopiert sich selbst unter zufälligen Dateinamen in einige Verzeichnisse auf der lokalen Festplatte und legt mehrere Registry-Einträge an, die teilweise beim Start von Windows automatisch ausgeführt werden. Mit verschiedenen Methoden versucht der neue Brontok-Ableger Antivirus-Software auszuschalten um so ungehindert langfristig seinem Werk nachgehen zu können.

Mit dem kostenlosen Anti-Virus Toolkit von MicroWorld steht unter

<ftp://ftp.microworldsystems.com/download/tools/mwav.exe>

jedermann ein kostenloses Identifizierungs-Tool (ca. 10 MByte) zur Verfügung, das alle drei Tage von MicroWorld aktualisiert wird. Das Security-Unternehmen rät generell die Signaturen der Antivirus-Systeme stets auf dem

Drucken

E-Mail

A+ | A- | Reset

News Blogs

[News Blog](#)

[Security Blog](#)



[Viren, Würmer und Trojaner](#)



[Information](#)



[Publikationen](#)



[MS Bulletin](#)



[Das Buch der Computerviren](#)

[ABC Blog](#)

[Archiv Blog](#)

[Artikel per E-Mail](#)

Themen

[Startseite](#)

[Downloads](#)

[Forum](#)

[Google Maps](#)

[Google Search](#)

[Kleinanzeigen](#)

[Lexikon \(Wiki\)](#)

[Sitemap](#)

[Suche](#)

[Viren Top 10](#)

[Web Links \(Bookmarks\)](#)

[Wetterdaten](#)

Community

neuesten Stand zu halten.

[Diesen Beitrag im Forum diskutieren. \(0 Beiträge\)](#)

[\[Zurück \]](#)

Benutzername

Passwort

Angemeldet bleiben

[Passwort vergessen?](#)

Noch kein Benutzerkonto?

[Registrieren](#)

Empfehlung

[Photo Gallery](#)

[Unser Provider](#)

Wetterdaten

Kufstein, Austria

<input type="checkbox"/>	Temp:	18°C
	Gefühlt:	18°C
	Feucht:	73%
Gesch.:	8 km/h	
Richt.:	120°	
Barom.:	1007.1 mb	ESE

[Mehr Details zeigen](#)

Aktuelle Umfrage

Aus welchen Bereichen hätten Sie gern mehr Informationen?

Sicherheit (Viren, Würmer und Trojaner)

DSL

Internet

Recht & Gesetz

Software (Freeware, Open Source)

Telekommunikation

Österreich

Web Links

Downloads

Betriebssystem Linux

Who's Online

Site Info

[Impressum](#)

[Media Daten](#)

[Datenschutz](#)

[Nutzungsbedingungen](#)

[Suche](#)

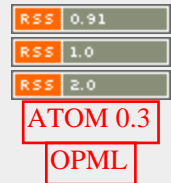
[Empfehlung](#)

[FAQ](#)
[Sitemap](#)
[Stats](#)

Kontakt

[E-Mail](#)
[Rückruf](#)
[Ticket senden](#)

RSS-Feeds



© 2006 news-select.de

[Joomla!](#) is Free Software released under the GNU/GPL License.

[Template Design by funky-visions.de](#)