

11.08.2006 14:02 Uhr

Drucken | Versenden | Kontakt

## Vorsicht Urlaubsfoto

### Wurmstichiges Foto aus Paris

**Ein Wurm verbreitet ein angebliches Urlaubsfoto, in der vermeintlichen Bilddatei steckt jedoch Malware.**

Von *Markus Pilzweger*

Das Versenden vorgeblicher Fotos als Anhang einer Mail gehört seit Jahren zum Standardrepertoire von Malware. Diese Methode ist typisch für den Wurm "c" (oder auch "Rontokbro"). Wie Micro World Technologies, Hersteller von "Escan" meldet, versendet die neueste Variante Brontok.o ein angebliches Urlaubsfoto aus Paris, das jedoch eine ausführbare Datei ist.

Die Mails kommen mit einem Betreff wie "My photo on Paris" und einem Dateianhang namens "picture.zip". Diese ZIP-Datei enthält eine Batch-Datei "View-Picture.bat" sowie das vermeintliche Bild "Picture.bmp". Wird die BMP-Datei durch Doppelklick geöffnet, lädt sie eine Kopie des Wurms aus dem Internet herunter und führt sie aus.

Der Schädling ist mutmasslich indonesischer Herkunft, denn er versendet seine Mails sowohl in englischer als auch in indonesischer Sprache, abhängig von der Mail-Adresse. Der indonesische Betreff lautet "Foto

## Süddeutsche Zeitung



**Abo-/Leserservice**   
**Gratis SZ-Probeabo**   
**SZ-E-Paper**   
**SZ-Archiv**   
**Anzeige buchen**

## Surftipp des Tages



**Service**  
 Mobil in der Ausbildung

**weitere Surftipps**

## Spezial



**Windows-Tuning bis zum Anschlag**  
 Wie lahme Rechner wieder flott werden

**Das war die Cebit 2006**  
 Themen und Trends von der weltgrößten Computermesse

Liburanku di Bali". Brontok durchsucht die Festplatte nach Mail-Adressen und versendet sich mit der Adresse des Opfers als Absenderangabe.

Der Wurm verstreut etliche Kopien seiner selbst über mehrere Verzeichnisse und verwendet dabei Datei- und Verzeichnisnamen mit zufälligen Ziffernfolgen. So landen einige Kopien im Profil des angemeldeten Benutzers und im Windows-Verzeichnis, andere in einem neu angelegten Unterverzeichnis von C:\Windows\System32. Ferner erstellt Brontok JOB-Dateien für den Windows-Taskplaner, zum Beispiel "at1.job", die diesen anweisen den Wurm einmal täglich auszuführen.

Außerdem legt der Wurm eine Reihe von Registry-Einträgen an, die zum Teil der automatischen Ausführung beim Start von Windows dienen. Andere Einträge deaktivieren den Registry-Editor sowie die Eingabeaufforderung und schalten die Anzeige von Dateierweiterungen und versteckten sowie System-Dateien im Windows Explorer aus. Brontok versucht Antivirus-Software zu beenden und überschreibt die HOSTS-Datei, um zu verhindern, dass Antivirus-Programme aktualisiert werden können. Dazu leitet er diverse Web-Adressen auf den lokalen Rechner um, zum Beispiel:

127.0.0.19 www.mcafee.com  
127.0.0.19 www.grisoft.com  
127.0.0.19 www.kaspersky.com  
127.0.0.19 www.symantec.com

Die HOSTS-Datei befindet sich in C:\Windows\System32\drivers\etc\ und enthält laut der Beschreibung von Sophos mehr als 300 derartige Einträge, wenn der PC mit diesem Wurm verseucht ist. Es sind bereits mehr als 100 Brontok-Varianten bekannt, die Verbreitung dieser Wurm-Variante ist eher gering.

PC-Welt Online

## Spiele

Find Bill

### Find Bill

Zusammen- klicken was zusammen- gehört



### Plankengott

Das etwas andere Online-Quiz

## Internetwörterbuch

Geben Sie hier einen Suchbegriff ein:

## Leser empfehlen

1. Computerkriminalität  
**"Datendiebstahl? Schicken Sie doch ein E-Mail"**
2. Porträt des älteren Lebens-Surfer Allan Weisbecker  
**"Sie hat mich verlassen, obwohl ich ein guter Surfer bin"**
3. Grass zu den Reaktionen auf seine SS-Beichte  
**"Man will mich zur Unperson zu machen"**
4. Günter Grass' SS-Beichte  
**Und nun zurück zu den Fakten**
5. PC-Hersteller  
**Dell ruft Millionen Akkus zurück**

## Infothek

**Telefontarife**

**Internettarife**

**Internetwörterbuch**

**Virenwarnungen**

**Top 10 Viren**

**Top 10 Hoaxes**

**Digicam-Datenbank**

**Bildschirmschoner**

## Ihre Meinung ist gefragt



**Ist Linux eine echte Alternative zu Windows?**  
Jahrelang war Linux eine Sache für Spezialisten, die mit Mainstream-Programmen aus der Windows-Welt nichts am Hut hatten. Doch nun gibt es auch für Linux viele gute Programme.

### Welchen Browser verwenden Sie?

Firefox nimmt dem Internet Explorer Marktanteile ab, weil er als sicherer gilt.

Artikel drucken ::  
Artikel empfehlen ::  
Kontakt zur Redaktion ::

Websuche

powered by **YAHOO!** Suche

 top

Mediadaten :: Newsletter :: Datenschutz :: AGBs :: Impressum :: Kontakt

Copyright © sueddeutsche.de GmbH/Süddeutsche Zeitung GmbH

Artikel der Süddeutschen Zeitung lizenziert durch DIZ München GmbH. Weitere Lizenzierungen  
exklusiv über [www.diz-muenchen.de](http://www.diz-muenchen.de).

Nachrichten :: Politik :: Wirtschaft :: Finanzen :: Sport :: Kultur :: Panorama  
München :: Job :: Immobilienmarkt :: Auto :: Reise :: Computer :: Wissen :: Wetter  
Stellenangebote :: Immobilien :: Automarkt :: Kino :: SZ-Mediathek

#### Verwandte Artikel

##### Raumfahrt

Nasa kann Mondlandungs-  
Video nicht mehr finden ::

##### Störche

Adebars Rückkehr ::

