

Sie sind hier: [Startseite](#) > [Computer](#) > [News](#)



Suchen mit

on Computer

onComputer Insider

[:: Startseite](#)

[:: Insider werden](#)

[:: Gutschein einlösen](#)

Computer-Themen

[:: News](#)

[:: Hardware](#)

[:: Software](#)

[:: Mobil & Co](#)

[:: Sicherheit](#)

[:: Audio, Video, Foto](#)

[:: Forum](#)

[:: Newsletter](#)

Download-Center

[:: Download Startseite](#)

[:: Vollversionen](#)

[:: Neue Downloads](#)

[:: Download-Specials](#)

[:: Tipp des Tages](#)

[:: Meine Vollversionen](#)

Specials

[:: Nokia Smartphone](#)

[:: Falk Navigation](#)

[:: MehrwertAuktion](#)

T-Online Partner

Marktplätze

[:: Themen](#)

[Nachrichten](#)

[Wirtschaft](#)

[Sport](#)

[Reisen](#)

[Leben](#)

[Unterhaltung](#)

[Spiele](#)

[Handy](#)

[:: Vollversionen](#)



Festplattenturbo

O&O Defrag v8 sogt für High-Speed. [mehr](#)

[:: onComputer Insider](#)



Animierte Bilder

Fast 8000 "Gifs" für jeden Zweck herunterladen. [mehr](#)

[:: News](#)

Wurmstichiges Foto aus Paris



[Bild großklicken](#)

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 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.

powered by © [www.pcwelt.de](#)

[Zurück zur Übersicht](#)

[:: Vollversionen](#)



Ausweise und Tickets, bitte

Mit der Fälscherwerkstatt 3 zur Spaßidentität [mehr](#)

[:: Vollversionen](#)



VHS auf DVD

So sichern Sie Ihre VHS-Aufnahmen. [mehr](#)

[:: Anzeige](#)



Die Mauer muss weg

"Magic Spinball": Ballern bis die Ziegel bröckeln. [mehr](#)

[:: Shopping](#)



Design USB-Sticks

Auch was für's Auge. [zum Shop](#)

Von eBay

Tolle Shopping-Angebote
[Hier klicken & stöbern](#)



DSL Telefonie

Die T-Online DSL Telefonie

Mehr erfahren über Preise und Verfügbarkeit. [mehr](#)

[Probleme mit der Seite](#)

[Lesezeichen setzen](#)

[Seite drucken](#)

[Seite weiterempfehlen](#)

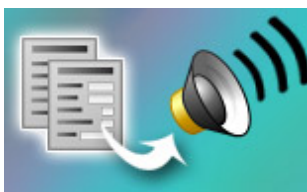
[:: Vollversionen](#)

[on Computer](#)



Gehörsinn trainieren

Musik besser hören lernen mit audite! 6.0. [mehr](#)



Computer liest Ihre Texte vor

Natural Voice Reader lässt Dokumente sprechen. [mehr](#)



Dateien sicherer aufbewahren

Secure Disk verschlüsselt Ihre Festplatte. [mehr](#)



Überflüssiges per Klick löschen

Magical Optimizer reinigt die Festplatte. [mehr](#)

ACDSee 8.0

[Profi-Foto-Manager](#)

Magical Burn

[Leicht CD/DVDs brennen](#)

OnlineTV Global 2

[TV und Radio aus dem Web](#)

Ulead Photo Impact 11

[Fotos schöner machen](#)

Produkte auf einen Blick

[Alle Multimedia-Produkte](#)

Langenscheidt T1

[Übersetzen per Mausclick](#)

PDF Converter Pro 3

[PDF zu Word und zurück](#)

Ahnenforscher 3.0

[Ihre Familiengalerie](#)

Telefonbuch Frühjahr 2006

[Schnelle Nummernsuche](#)

Produkte auf einen Blick

[Alle Office-Inhalte](#)

HDD Life Pro 2.8

[Der Festplattenwächter](#)

DiskRecovery V 4

[Rettung für gelöschte Daten](#)

Pestblock 3.0

[PC-Schädlinge entfernen](#)

Partition Manager 5.5

[Festplatte neu aufteilen](#)

Produkte auf einen Blick

[Alle Sicherheits-Produkte](#)

Registry First Aid 4.3

[Jetzt neu: Platinum-Edition](#)

XP Tools 3.3

[Verbessert die PC-Leistung](#)

XP Master Tuning 2

[Die volle PC-Leistung](#)

Driver Genius 6 Pro

[PC-Treiber aktualisieren](#)

Produkte auf einen Blick

[Alle Tuning-Produkte](#)

Anzeigen

[Ya.com](#) [España](#) [Club](#) [Internet](#) [France](#) [Terravista](#) [Portugal](#) [T-Online](#) [Österreich](#) [T-Online](#) [Schweiz](#)

[Public Relations](#) [Jobs@T-Online](#) [Kontakt](#) [Impressum](#) [Datenschutz](#) [Jugendschutz](#) [Verbraucherinfos](#)

© Deutsche Telekom AG 2006