



anz

- [Start](#)
- [News](#)
- [Tests](#)
- [Praxis](#)
- [Downloads](#)
- [Preisvergleich](#)
- [Specials](#)
- [Forum](#)
- [ePaper](#)
- [Premium](#)
- [PC-WELT-Abo](#)

[News](#) » [Sicherheit](#)

PC-WELT Suche

in

markt.pcwelt.de

[Sicherheit](#)

Von Frank Ziemann
11.08.2006 14:02

- [Verschicken](#)
- [Newsletter](#)
- [Trackback](#)
- [Drucken](#)
- [Forum](#)

[Aktuelle Ausgabe](#)



Wurmstichiges Foto aus Paris

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



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.

[...zum Inhalt...](#)[zum Abo](#)
[Umfrage](#)



Welche Windows-Vista-Variante interessiert Sie am meisten?

[JETZT HIER ABSTIMMEN](#)

[eBook des Tages](#)

eBOOK DES TAGES

Täglich neu

Punkt 00:00 Uhr

eBook des Tages!

[Windows XP Professional](#)

Nur €2.49!

Nur heute so günstig!

[Hier geht's direkt zum Download](#)

[...mehr eBooks](#)

[PDF des Tages](#)

Nur heute so günstig!:

[PC-WELT Extra \(10/05\)](#)

[Digital fotografieren](#)

Nur 1,99 Euro!

[Hier geht's direkt zum Download](#)

[... Download](#)

Anzeige

PC-Welt - [Jetzt testen!](#)

Forumsbeiträge: 0

[Alle Beiträge anzeigen](#) [Beitrag schreiben](#)

[Alle Beiträge anzeigen](#) [Beitrag schreiben](#)

Trackback

[Trackback setzen](#)



Ja, bitte senden Sie mir die nächsten 3 Ausgaben der PC-WELT und den MP3-Player+Card-Reader 2in1 zum Vorteilspreis von nur 8,99 Euro.

Vorname Nachname

Straße/Nr.

PLZ Ort

E-Mail (optional)

Ich will die PC-WELT mit Heft-DVD für nur 50,90 €Jahr weiterbeziehen, wenn ich mich nicht innerhalb von 2 Wochen nach Erhalt der 3. Ausgabe melde.

Preise inkl. Porto & Versand. Prämienvsrand (MP3-Player+Card-Reader 2in1) nur in die EU. Kündigung jederzeit nach dem Test-Abo möglich: PC-WELT-Abo-Betreuung, Konrad-Zuse-Str. 16, 74172 Neckarsulm.

Visortech Fingerprint Reader USB

statt ~~EUR 69,90~~
Jetzt **EUR 29,90**
Sie sparen **EUR 40,00**

Datenschutz mit der Fingerspitze. Für Windows, Internet & Co.

Shopping: [Tipp 1](#) [Tipp 2](#)
· Sudoku · kostenlos · Tintenpatronen

Whitepapers:

Security

- [HOB Enterprise Access - erweitert Server Based Computing auf Unternehmensserver](#)
- [Dark Traffic E-Mail-Report Q1/2005](#)
- [Federated Identity – Erschließen Sie mit Trusted-Identities und SSO neue Märkte](#)
- [HOB-Konzept zum Virenschutz auf dem Windows Terminal Server](#)
- [Sentinel 5 Overview: Navigating The Waves of Compliance](#)

[...weitere Downloads](#)

Sponsored Links

[MIS](#)

DSL Informationen: [WLAN Router](#) auf DSLWEB

Der große DSL-Vergleich: [Arcor](#), [1&1](#), [freenet](#) etc.
auf top-dsl.com

[Ratenkredite](#) von Direktbanken über modern-
banking vergleichen

[Produktsuche](#)

[Preissuchmaschine](#)

Telefonieren zum Festpreis: [Arcor-ISDN Telefon](#)

[Flatrate](#)

[Shopping-Tipps](#)

[Computer & Zubehör](#)

[Neckermann.de](#)

[EP Netshop](#)

[Schwab.de](#)

[Conrad Electronic](#)

[Computer & Hardware](#)

[Preisvergleich für Österreich](#)

[Marktplatz Österreich](#)

[Hotels](#)

IDG-Publikationen im Internet: