

BKA-Trojaner (Ransomware)

evild3ad.com/405/bka-trojaner-ransomware/

evild3ad

Seit dem 24.03.2011 wird im Internet vor einer neuen Betrugs- bzw. Erpressungsvariante von Cyberkriminellen mittels Schadsoftware gewarnt (Ransomware). Die Schadsoftware soll auf den infizierten PC's sämtliche Zugriffe auf das System blockieren und eine angeblich offizielle Mitteilung der Polizei einblenden, in der der Nutzer zur Zahlung einer vermeintlichen Strafe via Ukash in Höhe von 100 Euro aufgefordert wird. Andernfalls werde seine Festplatte gelöscht.

Die offizielle Mitteilung des Bundeskriminalamtes

BUNDESPOLIZEI Bundeskriminalamt

Ukash

Wo kann ich Ukash kaufen?

Es gibt unzählige Möglichkeiten, Ukash zu erwerben, z. B. in Geschäften, Kiosken, per Geldautomat, online oder über eine E-Wallet (elektronische Geldbörse).

Nachstehend finden Sie eine Liste, aus der hervorgeht, wo Sie in Ihrem Land Ukash erwerben können.

Tankstellen - jetzt auch erhältlich bei folgenden Tankstellen: Agip, Avia, Esso, OMV, Q1 und Westfalen.

epay - Kaufen Sie Ukash in vielen tausend Supermärkten oder Call-Shops, in denen Sie dieses Logo sehen.

Achtung!

Ein Vorgang illegaler Aktivitäten wurde erkannt. Das Betriebssystem wurde im Zusammenhang mit Verstößen gegen die Gesetze der Bundesrepublik Deutschland gesperrt! Es wurde folgender Verstoß festgestellt: Ihre IP Adresse lautet mit dieser IP wurden Seiten mit pornografischen Inhalten, Kinderpornografie, Sodomie und Gewalt gegen Kinder aufgerufen.

Auf Ihrem Computer wurden ebenfalls Videodateien mit pornografischen Inhalten, Elementen von Gewalt und Kinderpornografie festgestellt!

Es wurden auch Emails in Form von Spam, mit terroristischen Hintergründen, verschickt. Diese Sperre des Computers dient dazu, Ihre illegalen Aktivitäten zu unterbinden.

Ihre Daten:

IP: [REDACTED]
Browser: Internet Explorer 7.0
OS: Windows XP
Das Land: GERMANY
City: BERLIN
ISP: DEUTSCHE TELEKOM AG

Um die Sperre des Computers aufzuheben, sind Sie dazu verpflichtet eine Strafe von 100 Euro zu zahlen. Die Zahlung ist innerhalb von 24 Stunden zu leisten. Sollte der Eingang der Zahlung in der vorgegebenen Zeit nicht erfolgen, so wird Ihre Festplatte unwiderruflich formatiert/gelöscht.

Die Bezahlung erfolgt durch einen Ukash Coupon-Code in Höhe von 100 Euro.

Um die Bezahlung durchzuführen, geben Sie bitte den erworbenen Code in das Zahlungsfeld ein und drücken Sie anschließend auf OK (haben Sie mehrere Codes, so geben Sie diese einfach nacheinander ein und drücken Sie anschließend auf OK)

Sollte das System Fehler melden, so müssen Sie den Code per Email (ukash@bundeskriminalamt.org) versenden.

Nach Eingang der Zahlung wird Ihr Computer innerhalb von 24 Stunden wieder freigestellt.

Copyright 2011 Dieser Dienst des Internet Services wurde mit der Unterstützung folgender Firmen entwickelt: McAfee, symantec, KASPERSKY, Microsoft

Nach der Eingabe des Ukash Voucher Codes bzw. nach der Eingabe eines Phantasiewertes erscheint folgendes Fenster...eine "Freischaltung" erfolgt jedoch nicht!

Die offizielle Mitteilung des Bundeskriminalamtes

Ukash BKA-Trojaner

Wo kann ich Ukash kaufen?

Es gibt unzählige Möglichkeiten, Ukash zu erwerben, z. B. in Geschäften, Kiosken, per Geldautomat, online oder über eine E-Wallet (elektronische Geldbörse).

Nachstehend finden Sie eine Liste, aus der hervorgeht, wo Sie in Ihrem Land Ukash erwerben können.

Tankstellen - jetzt auch erhältlich bei folgenden Tankstellen: Agip, Avia, Esso, OMV, Westfalen.

e-pay - Kaufen Sie Ukash in vielen Supermärkten oder Call-Shops, dieses Logo sehen.

Achtung!

Ein Vorgang illegaler Aktivitäten wurde erkannt. Das Betriebssystem wurde im Zusammenhang mit Verstößen gegen die Gesetze der Bundesrepublik Deutschland gesperrt! Es wurde folgender Verstoß festgestellt: Ihre IP Adresse lautet ... mit dieser IP wurden Seiten mit pornografischen Inhalten, Kinderpornographie, Sodomie und Gewalt gegen Kinder aufgerufen.

Auf Ihrem Computer wurden ebenfalls Videodateien mit pornografischen Inhalten, Elementen von Gewalt und Kinderpornografie festgestellt!

Es wurden auch Emails in Form von Spam, mit terroristischen Hintergründen, verschickt. Diese Sperre des Computers dient dazu, Ihre illegalen Aktivitäten zu unterbinden.

Ihre Daten:

IP: ...

Meldung von Webseite

Ihre Anfrage haben wir erhalten, diese wird innerhalb von 72 Stunden bearbeitet.

... verpflichtet eine Strafe von 100 Euro zu zahlen. ... Eingang der Zahlung in der vorgegebenen ... Zeit nicht erfolgen, so wird Ihre Festplatte unwiderruflich formatiert/ gelöscht). Die Bezahlung erfolgt durch einen Ukash Coupon-Code in Höhe von 100 Euro. Um die Bezahlung durchzuführen, geben Sie bitte den erworbenen Code in das Zahlungsfeld ein und drücken Sie anschließend auf OK (haben Sie mehrere Codes, so geben Sie diese einfach nacheinander ein und drücken Sie anschließend auf OK) Sollte das System Fehler melden, so müssen Sie den Code per Email (ukash@bundeskriminalamt.de) versenden. Nach Eingang der Zahlung wird Ihr Computer innerhalb von 24 Stunden wieder freigestellt.

Copyright 2011 Dieser Dienst des Internet Services wurde mit der Unterstützung folgender Firmen mitanbietet: McAfee, symantec, KASPERSKY, Microsoft

Dateisystem:

Im Rahmen einer Infektion werden unter C:\Dokumente und Einstellungen\Benutzerkonto\Lokale Einstellungen\Temporary Internet Files\Content.IE5\ mehrere Unterverzeichnisse mit zufälligen Namen (8 Zeichen) angelegt (z.B. "SRKBUTOP", "S6JZACFV", "DNYHQU88").

C:\Dokumente und Einstellungen\Benutzerkonto\Lokale Einstellungen\Temporary Internet Files\Content.IE5\SRKBUTOP\QQkFBwQEBwECAQMGEkcJBQcEBgUDDQ0HAW==[1].htm
C:\Dokumente und Einstellungen\Benutzerkonto\Lokale Einstellungen\Temporary Internet Files\Content.IE5\SRKBUTOP\setup[1].exe (MD5: ba9a4732e63ed72d1c77d4a2828f777e)

Registry:

Damit der BKA-Trojaner bei jedem Neustart eines infizierten PC's automatisch wieder aufgerufen wird, legt er eine Kopie der EXE und folgenden Registry-Key an:
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon
->C:\Programme\T-Online\T-Online_Software_6\Browser\test.exe (MD5: ba9a4732e63ed72d1c77d4a2828f777e)

Connections:

IP: 70.86.96.219:80
Host: http://tools.ip2location.com
IP: 78.26.187.235:80 (Ukraine)

Infektionsweg:

Der BKA-Trojaner wird primär über Webseiten mit pornografischem Inhalt verbreitet. Die Infektion erfolgt dabei, ohne Interaktion des Nutzers, über eine ungepatchte Betriebssystem-, Browser- oder Anwendungsschwachstelle beim Zugriff auf den präparierten bzw. manipulierten Web-Server (Drive-By-Infektion).

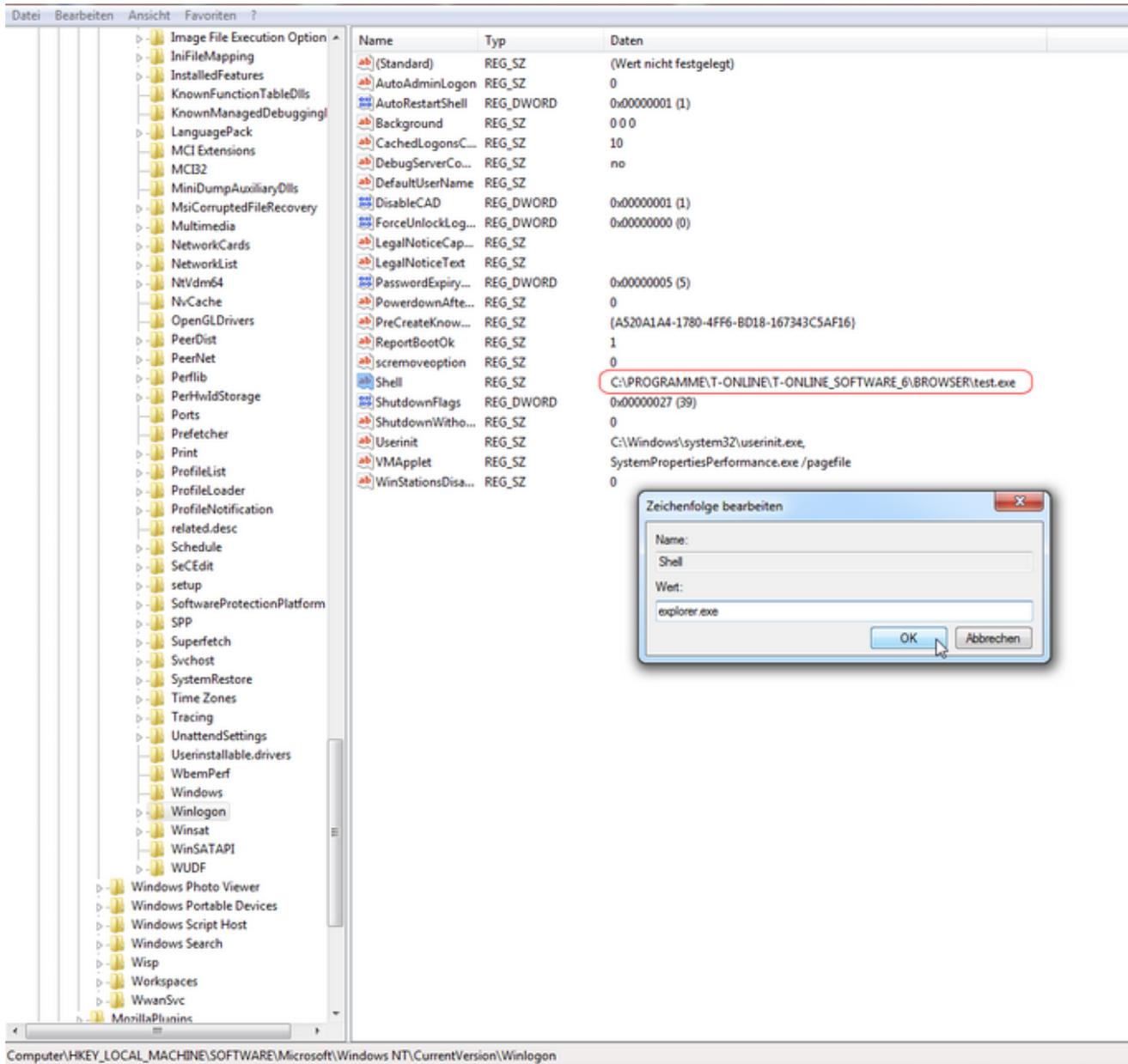
z.B. Exploit.Java.CVE-2010-0840.b

Bereinigung des infizierten Systems:

1. Neustart des Rechners
2. Drückt F8 (ggf. F5) vor Erscheinen des Windows-Start-Bildschirmes, um in das erweiterte Optionsmenü von Windows zu gelangen. Wählt hier den "Abgesicherten Modus mit Eingabeaufforderung" aus.
3. Wählt anschließend das Benutzerkonto "Administrator" und gibt dann in der Konsole "regedit" ein, um den Reg-Editor von Windows zu starten.
4. Navigiert dann zu dem Registry-Schlüssel "Shell" unter folgendem Pfad:

**HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\Winlogon**

5. Doppelklickt auf den Registry-Schlüssel "Shell". Entfernt hier den Dateipfad zu der EXE des BKA-Trojaners (Kopie) und gibt "explorer.exe" ein. Die böartigen Dateien solltet ihr dann nach einem Neustart des Rechners mit einem Virens scanner entfernen (Tipp: [Kaspersky Rescue Disk 10](#)).



Video:

[Download Sample](#)

PW: infected

Copyright by [evild3ad](#) - All Rights Reserved - [keybase.io](#)