


Entfernung des Bundestrojaners durch Systemwiederherstellung



BUNDESPOLIZEI

Es ist die ungesetzliche Tätigkeit enthüllt!

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 [REDACTED] 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 IP: [REDACTED] Browser: [REDACTED] OS: Windows
Angaben: [REDACTED] Country: [REDACTED] City: - ISP: [REDACTED]

Um die Sperre des Computers aufzuheben, sind Sie dazu verpflichtet eine Strafe von 100 Euro zu zahlen. Sie haben zwei Möglichkeiten die Zahlung von 100 Euro zu leisten.

1) Die Zahlung per Ukash begleichen:
Dazu 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 (enzahlung@landes-kriminal.net) versenden.


2) Die Zahlung per Paysafecard begleichen:
Dazu geben Sie bitte den erworbenen Code (gegebenfalls inkl. Passwort) 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 (enzahlung@landes-kriminal.net) versenden.




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.


Avia


Esso


OMV


Q1


Westfalen

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



wichtige Tasten

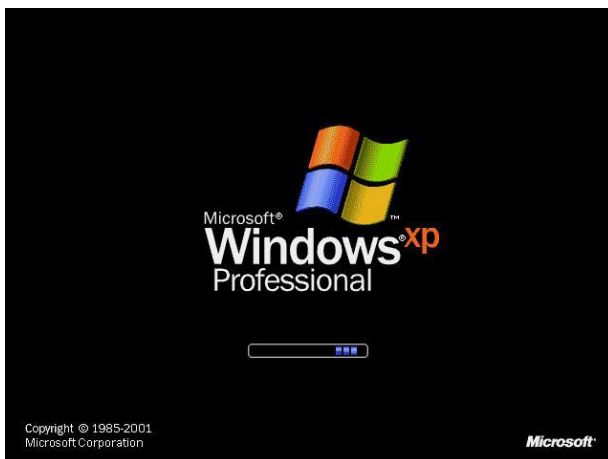
Tastatur und Maus



Schritt 1: Vorbereitungen

Computer ausschalten, oder im ausgeschaltete Zustand beginnen.

Wenn das Windowslogo (nächstes Bild) erscheint, wieder von vorne beginnen, Computer ausschalten.



Schritt 2: Abgesicherter Modus

Computer einschalten und solange **F8** drücken bis folgendes Bild erscheint.

```
Erweiterte Windows-Startoptionen
Wählen Sie eine Option aus:

    Abgesicherter Modus
    Abgesicherter Modus mit Netzwerktreibern
    Abgesicherter Modus mit Eingabeaufforderung
    Startprotokollierung aktivieren
    UGA-Modus aktivieren
    Letzte als funktionierend bekannte Konfiguration
    Verzeichnisdienstwiederherstellung (Windows-Domänencontroller)
    Debugmodus

    Windows normal starten
    Neustarten

Verwenden Sie Pfeil nach oben bzw. unten, um einen Eintrag zu markieren.
```

Den Punkt „Abgesicherter Modus“ mit den **Pfeiltasten** (oben/unten) auswählen, sodass es weiß unterlegt ist und mit der Taste **ENTER** bestätigen.

Schritt 3: Betriebssystem auswählen

Mit der Taste **ENTER** bestätigen.

```
Wählen Sie das zu startende Betriebssystem:

    Microsoft Windows XP Professional

Verwenden Sie Pfeil nach oben bzw. unten, um einen Eintrag zu markieren.
Drücken Sie anschließend die EINGABETASTE.

Problembehebung und erweiterte Windows-Startoptionen: F8-TASTE drücken

Abgesicherter Modus
```

Der Computer lädt nun automatisch alle notwendigen Dateien und Einstellungen.

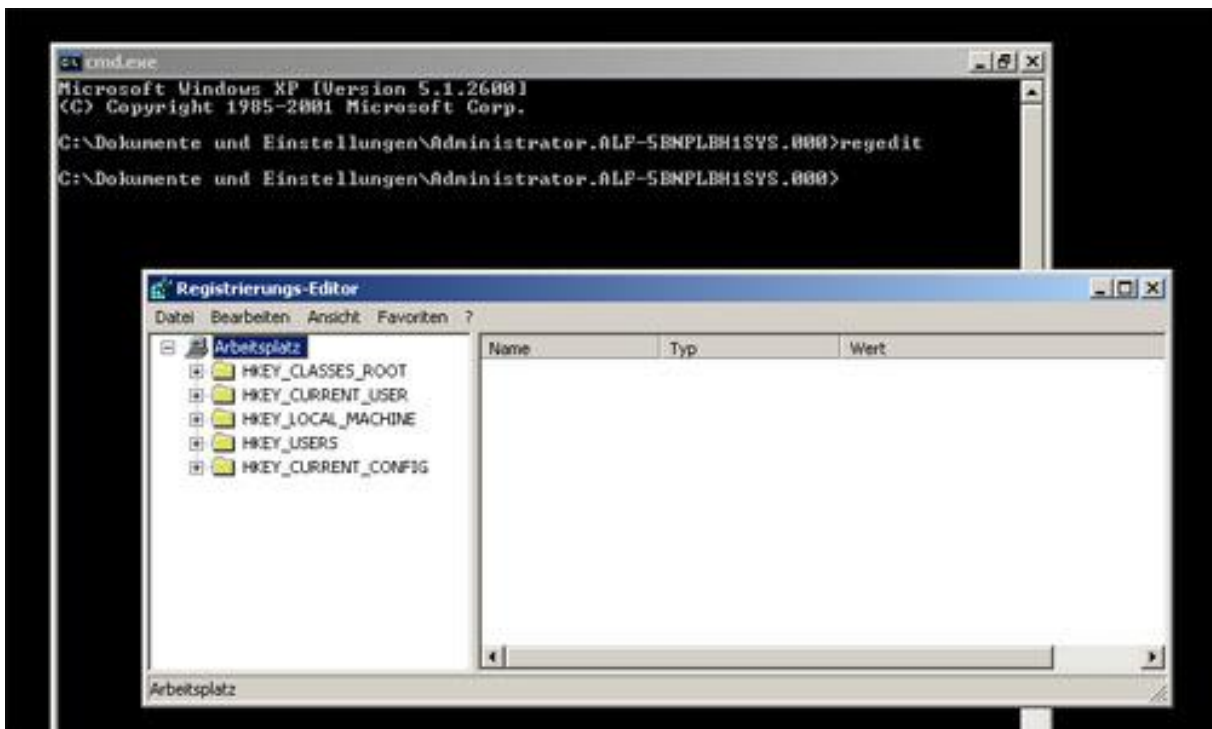
Schritt 4: Benutzer auswählen

Nach dem Laden, muss der Benutzer ausgewählt werden.

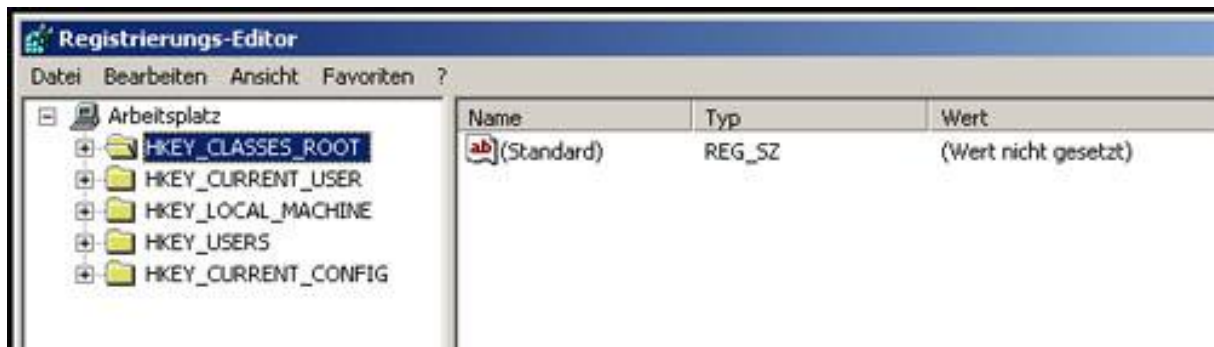


Klick mit der linken Maustaste auf das Bild des Benutzers **1**, gestrichelte Umrandung oder Administrator.

Nun erscheint eine Konsole, in die Konsole **regedit** eingeben, sodass ein anderes Fenster aufgeht



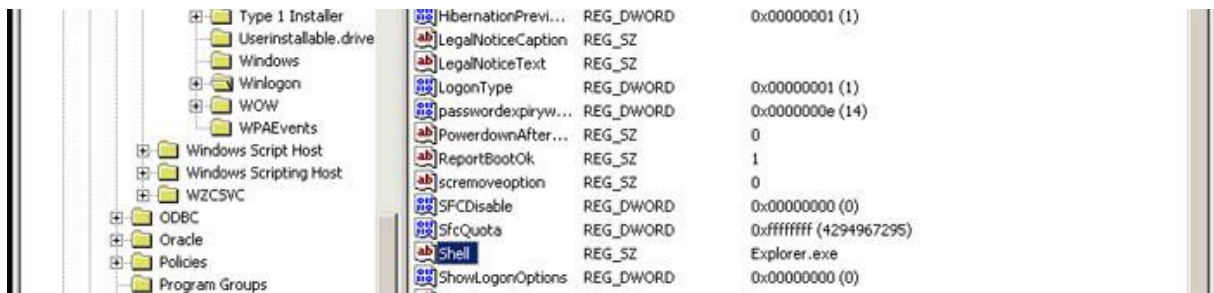
Schritt 5: Ausführen



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

Jetzt durch die Ordnerstruktur durchklicken [+] bis man zum Ordner **Winlogon** kommt diesen dann anklicken

Hat man den Punkt erreicht sollte man auf der rechten Seite den Eintrag **Shell** suchen und diesen doppelt mit der **linken Maustaste** anklicken



folgendes erscheint



Der Wert der da aufgeführt ist, sollte der Pfad zum Trojaner sein, diesen also vollständig löschen und durch **Explorer.exe** ersetzen, mit OK bestätigen und den PC neustarten. Wie gewohnt neustarten **NICHT** den Strom entziehen.