Bundespolizei Trojaner entfernen

Wie man den Ukash-BKA-Virus unter Windows unschädlich macht

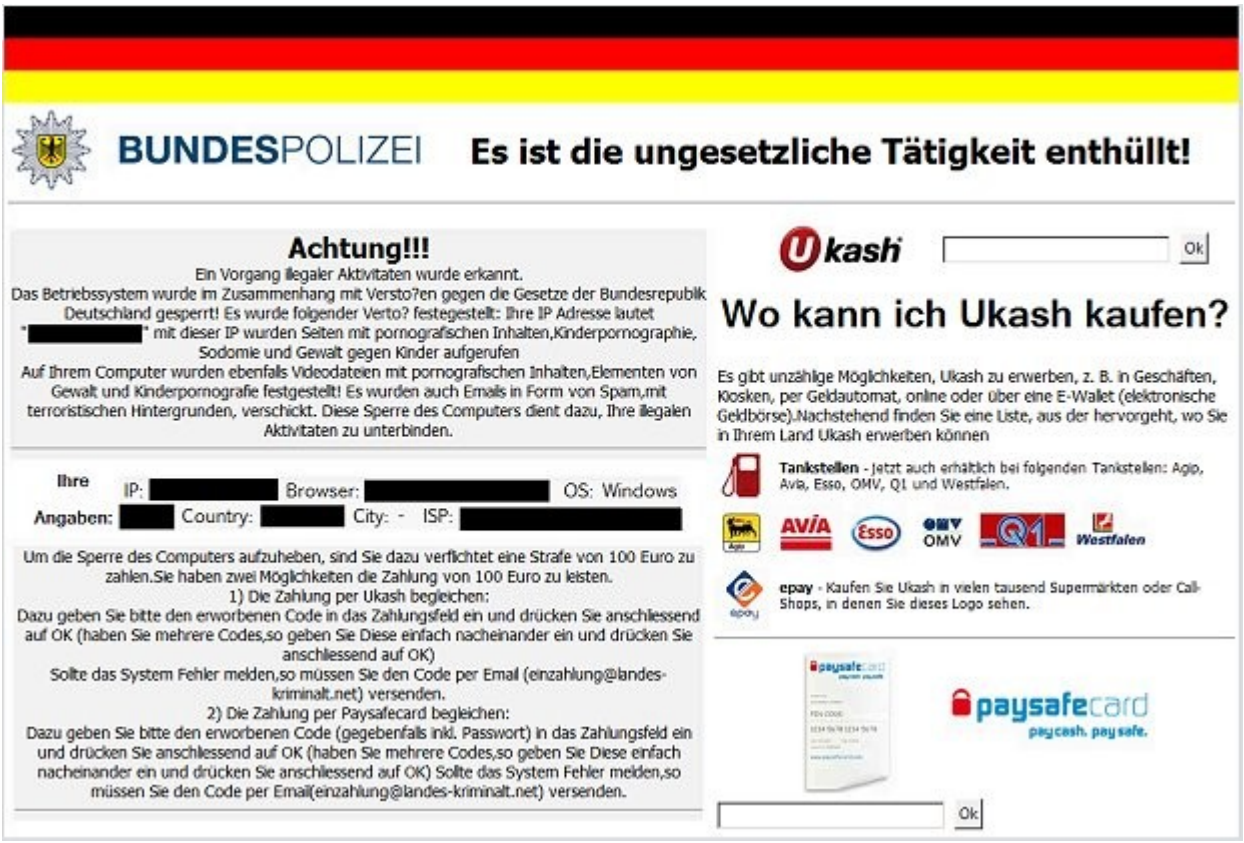
“Notfalleinsatz in der Nachbarschaft wegen einem Windows-Trojaner!” – so der erste Hilfeschrei direkt am Gartenzaun. Der Tatort: Ein infizierter Windows XP Rechner, der zwar noch startet, dann aber nur noch eine vermeintliche **Meldung von der Bundespolizei** zeigt. Bundespolizei?! Was für ein Quatsch. Ich traue den Beamten des BKA ein besseres deutsch als “**Es ist die ungesetzliche Tätigkeit enthüllt**” zu! Und ein Freikauf in Höhe von **100 €** via **Ukash** ist auch nicht so ganz die deutsche Gesetzeslage.

Ich will hier gar nicht viel herum labern, denn wer nach einer Problemlösung sucht, will nicht viel lesen, sondern eine **Schritt-für-Schritt-Anleitung**. Hier ist sie!

Die ersten Maßnahmen

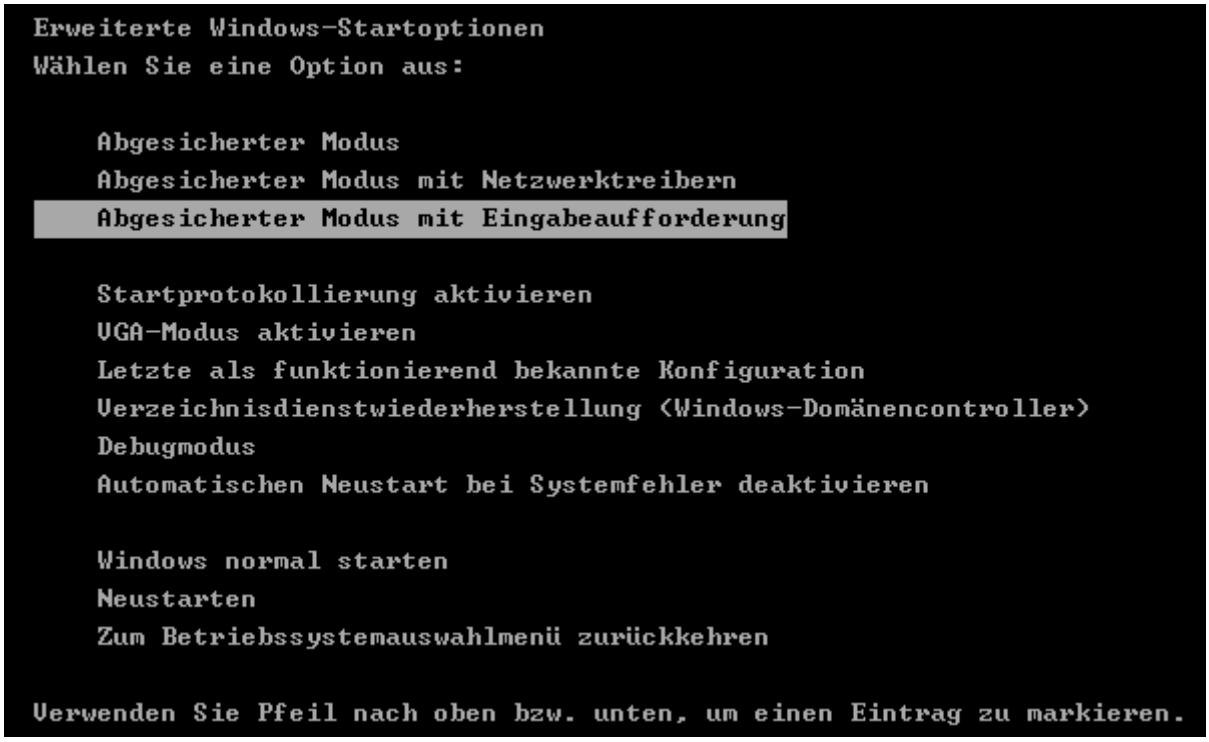
1. **Ruhe bewahren!** Es ist nicht die Bundespolizei die hier einen Virus auf den Rechner installiert hat, sondern “nur” eine kriminelle Vereinigung, die versucht, an schnelles Geld heran zu kommen.
2. Beweise sichern! Am besten ein Foto von der Meldung anfertigen. Bitte nicht direkt auf den Monitor das Blitzlicht halten, das wird so nichts. (Optional, dem Virus ist diese Aktion egal)
3. Bei der örtlichen Polizeidienststelle anrufen und Anzeige erstatten. (ebenfalls Optional, dem Virus ist auch diese Aktion egal)
4. Der Rechner muss **nicht** platt gemacht werden und es gehen auch keine Daten verloren.
5. **Internetverbindung trennen** (Netzwerkkabel heraus ziehen, DSL-Verbindung trennen)
6. Etwas Zeit nehmen und diese Anleitung zum Entfernen des Bundespolizei Trojaners beachten. Ich versuche die Schritte ganz einfach zu beschreiben; das bekommt man auch als Leihe wieder hin.

Anleitung zum Löschen des Bundespolizei Virus



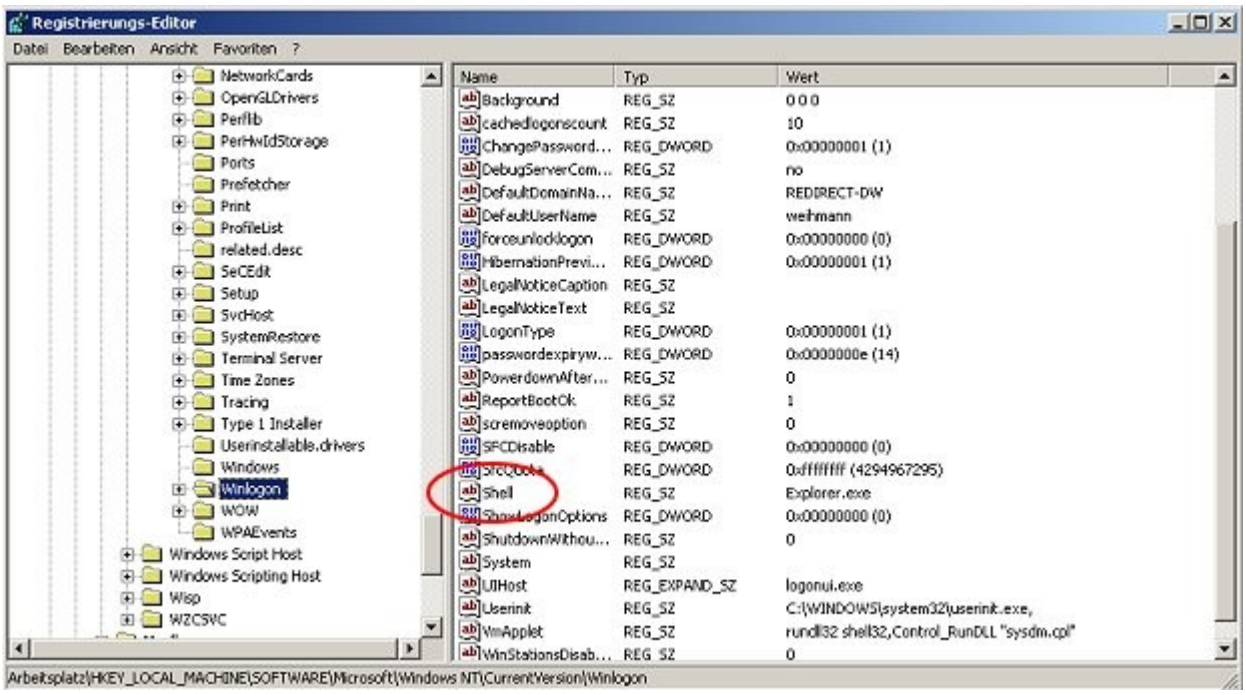
Bundespolizei Virus - Bildschirm eines infizierten Windows PCs

1. Rechner einschalten und immer wieder im Sekundentakt (noch vor dem Windows-Logo) die Taste [F8] drücken bis eine Auswahlliste verschiedener Startvarianten erscheint.
2. Mit den Pfeiltasten die Option “Abgesicherter Modus Eingabeaufforderung” wählen und mit [Enter] bestätigen.



Windows im abgesicherten Modus starten

3. Windows startet nun in einer Art Minimal-Konfiguration.
4. Der Bildschirm sieht nun nicht wie gewohnt aus. Es öffnet sich möglicherweise nur die DOS-Eingabeaufforderung (schwarzes Fenster mit Texteingabemöglichkeit).
5. Den Befehl *regedit* eingeben und [Enter] drücken
6. Es öffnet sich die Windows-Registry, wo eine Änderung vorzunehmen ist.
7. Hier muss man sich durch das Verzeichnis klicken. Ziel der “Reise” ist*HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon* (immer auf das [+]-Symbol klicken und am Ende *Winlogon* direkt auswählen).
8. Hier gibt es einen Schlüssel (auf der rechten Fensterseite) namens *Shell*. Der Wert dieses Schlüssels ist der Pfad zum Trojaner *C:\verzeichnis\zur\jashla.exe*. Dieses Pfad unbedingt notieren, hier muss später die Datei noch gelöscht werden.
9. Ein Doppelklick auf *Shell*, den kompletten Pfad zum Virus löschen und durch *Explorer.exe* ersetzen.
10. [OK] klicken und das Registry-Fenster schließen [x].



Windows-Registry - Pfad zur jashla.exe

Der Start des **BKA-Trojaners** wird somit schon mal verhindert. Jetzt muss dieser aber auch noch von der Festplatte gelöscht werden.
Wenn das DOS-Eingabefenster noch geöffnet ist, dann *Explorer.exe* eingeben. Windows sieht jetzt fast schon wieder wie gewohnt aus, oder!? Nun entweder zur *jashla.exe* navigieren oder die Windows-Suche nutzen, um die *jashla.exe* auf der Festplatte zu finden. Die Datei nun löschen.
Ansonsten kann man auch die Tasten [STRG] + [ALT] + [ENTF] einmal drücken und im sich öffnenden Fenster unter Anwendungen auf Neuer Task klicken. Jetzt sich zum zuvor notierten Pfad durch klicken und die *jashla.exe* löschen.
Die Datei hatte in meinem Fall noch ein paar Zeichen mehr im Dateinamen:*jashla.exe.1234567.pd* (oder so ähnlich).

« Den Rechner jetzt ganz normal neu starten »

Hat alles geklappt? Sehr schön, dann ist der Spuk (**erst mal**) vorbei! Falls nicht, dann bitte nochmals prüfen, ob die **Anleitung zum Entfernen des Bundespolizei Trojaners** genau beachtet wurde. Ansonsten hier die Kommentarfunktion nutzen, vielleicht kann ich oder ein anderer Leser weiter helfen.

Rechner auf Schadsoftware prüfen

Mit einem Antivirus-Programm sofort die Festplatte(n) prüfen. Zum Beispiel mit einer aktuellen Version von **Avia AntiVir** (kostenlos).
Empfehlen kann ich an dieser Stelle sich eine professionelle Sicherheitssoftware zuzulegen. Die abgespeckten kostenlosen Softwarelösungen sind oft besser als gar nichts, jedoch fehlt es hier oft an zusätzlichen Schutzmechanismen.
Das Geld sollten jedem die eigenen Daten wert sein. Ein anderer Virus hätte vielleicht alle Fotos

von der Festplatte gelöscht, Zugangsdaten an Dritte versandt, einen Keylocker heimlich installiert oder private Daten aus “Scherz” im Internet veröffentlicht.

Was heißt, der Spuk ist “erst mal” vorbei?

Nun ja. Der Trojaner kam nicht ganz von allein auf die Festplatte. Möglicherweise eine E-Mail mit einer vermeintlichen PDF, die versucht wurde zu öffnen? Oder eine andere Datei – eine Powerpoint vielleicht … Nach einem Neustart des Rechners ging dann nichts mehr.

Die bekannten “Floskeln”: Keine Anhänge von unbekannten Absendern öffnen. Software (Betriebssystem, Anwendungen, Anti-Viren-Programm) aktuell halten. Die Updates haben einen Sinn!

Sich davon lösen, dass Sicherheits-Software kostenlos ist. Am besten jetzt sofort 30, 50 oder 100 € investieren und den Rechner schützen. Was hätte die Entfernung dieses Trojaners gekostet, wenn man von einem IT-Dienstleister das Problem hätte beheben lassen? Welche Folgekosten kommen auf einen zu, wenn solch eine Schadsoftware noch ganz andere Probleme verursacht. Einfach mal der eigenen kriminellen Phantasie freien Lauf lassen …