Landeskriminalamt Niedersachsen
-Zentralstelle Internetkriminalität-

Alternativen zur Löschung
des so genannten
BKA- oder auch Bundespolizei bzw. Ukash-Trojaners

Achtung: Die nachstehenden Handlungsempfehlungen sind nicht abschließend, da der Trojaner in der Vergangenheit mehrfach verändert wurde, so dass dieses auch in der Zukunft zu erwarten sein dürfte. Mittlerweile beschäftigen sich im Internet eine Vielzahl von verschiedenen Foren, Malwareboards etc. mit dem Trojaner und seiner Bekämpfung.

Von den bisher im Internet recherchierten Empfehlungen zu Entfernungsmethoden der Malware, erscheint den Fachleuten des LKA Niedersachsen die Handlungsempfehlungen des Projektes **„Anti-Botnet Beratungszentrums“** (http://blog.botfrei.de) in besonderem Maße hilfreich. Das Beratungszentrum verfolgt das Ziel, Informationen und Hilfe zum Entfernen von Schadsoftware auf infizierten PC`s einer breiten Öffentlichkeit zugänglich zu machen, um dadurch die Größe von Botnetzen zu verringern. Getragen wird das Onlineportal vom Branchenverband **eco**, vom **BSI** (Bundesamt für Sicherheit in der Informationstechnik), vom **BMI** (Bundesministerium des Innern) sowie von verschiedenen Internetprovidern und Sicherheitsunternehmen.

Neben Informationen zum Entfernen von Schadsoftware wird auf dem Portal auch Hilfe von Experten **(rund um die Uhr über** technik@botfrei.de **oder im Live-Support, Montags bis Freitags zw. 9 und 21 Uhr)** und darüber hinaus auch kostenlose Software von namhaften Herstellern zum Erkennen und Entfernen von Schadsoftware angeboten.

Hinweis:
Seitens des LKA Niedersachsen wird keine Gewährleistung bzw. Haftung für die Bereinigung des Rechners und dem Entfernen der Schadsoftware übernommen. Größtmögliche Sicherheit bietet in letzter Konsequenz immer nur ein Neuaufsetzen des Betriebssystems und eine regelmäßige Datensicherung.

BKA-Trojaner manuell über die Registry entfernen:

Quellen:
http://blog.botfrei.de/2011/07/anleitung-bka-trojaner-manuell-uber-die-registry-entfernen/

Voraussetzungen:

Bitte beachten Sie, dass diese Anleitung **nur für computererfahrene Benutzer empfohlen wird**. Halten Sie sich bitte an die Anweisungen dieser Anleitung.

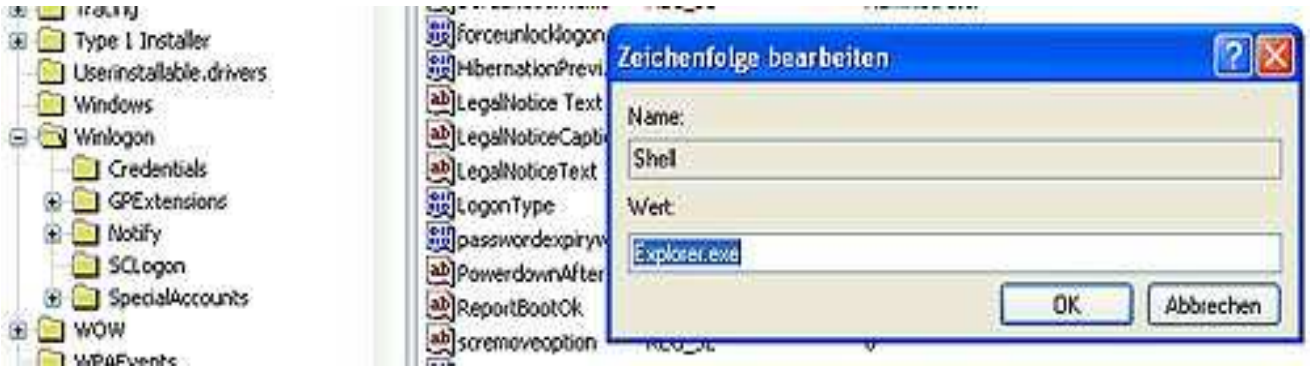
Vorteile:

Diese Entfernungsmethode hat den Vorteil, dass Sie keine zusätzliche Software herunterladen müssen.

1. Starte Sie ihren Rechner im „**Abgesicherten Modus mit Eingabeaufforderung“**.
   - Beim Hochfahren mehrmals **F8** drücken. (Kann bei manchen Systemen auch eine andere F Taste sein)
   - Navigieren Sie mit den Pfeiltasten zu **Abgesicherter Modus mit Eingabeaufforderung** und drücken Enter.
   - Loggen Sie sich in ein **Konto** ein, welches über **Administrationsrechte** verfügt.

2. Geben Sie in der Eingabeaufforderung(Dosbox)
   - **regedit.exe** ein und drücken Enter

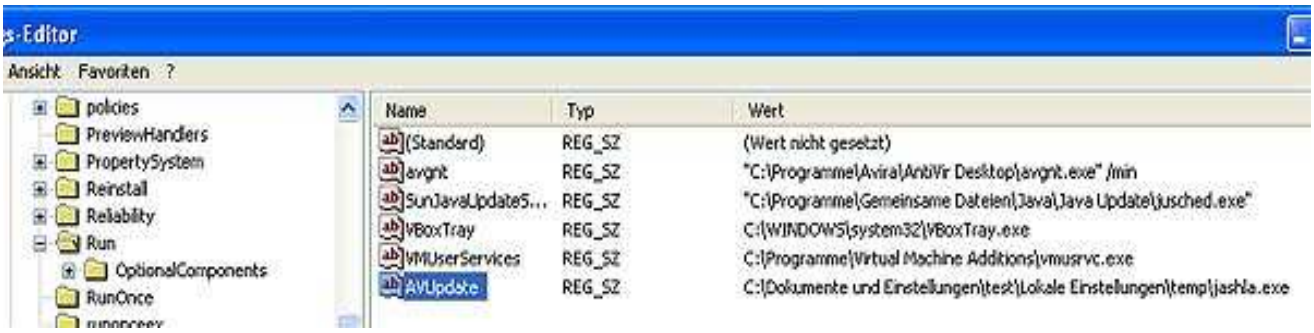
3. Überprüfen Sie als erstes diese Einträge:
   - **Für XP User:**
     [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon] “Shell”=”**explorer.exe**“
   - **Für Vista/ W7 User**:
     [HKEY_Current_User\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon] “Shell”=”**explorer.exe**“



Im **Winlogon** steht der Schlüssel **shell**. Wenn Sie diesen mit Doppelklick öffnen, sollte dort als Wert: **explorer.exe** stehen. Wenn das nicht der Fall ist, löschen Sie den Eintrag und schreiben dort den Wert **explorer.exe** hinein und bestätigen mit **OK**.

Wenn diese Pfade keine Auffälligkeiten hatten, schauen Sie bitte in folgenden Pfaden nach auffälligen **Exe-Dateien (*.exe)**

[HKEY_LOCAL_MACHINE\SOFTWARE\ Microsoft\ Windows CurrentVersion\ Run]
[HKEY_CURRENT_USER\ Software\ Microsoft\ Windows\ CurrentVersion\ Run]



Alles was in diesem **Run** Verzeichnis steht hier, wird für **alle Benutzer des Rechners** automatisch beim **Windowsstart** mit gestartet. Wenn hier als Eintrag ein ziemlich langer nichts sagender und keinen Sinn ergebender Name dabei ist z.B. **AVUpdate mit dem verdächtigen Wert: ../jashla.exe**, dann überprüfen Sie, wo diese Datei liegt und entfernen Sie anschließend den betroffenen Eintrag und auch die Datei.
Es bietet sich in diesem Schritt an, alle unnötigen Einträge zu entfernen um den Autostart etwas aufzuräumen. Aber Vorsicht: Wichtige Einträge (Virenscanner etc.) sollten nicht entfernt werden.

<u>Für Experten:</u>

Sie haben in den verschieden Pfaden der Registrierung nicht die Einträge vorgefunden (z.B. **explorer.exe**), sondern nichtssagende und keinen Sinn ergebende Namen, so löschen Sie nicht gleich den Eintrag. Schreiben Sie sich den **Namen und den Pfad der Datei** auf. Das sind wertvolle Informationen, um evtl. die bösartige Datei manuell zu untersuchen und zu löschen. Wenn Sie den Rechner wieder im normalen Modus starten, können Sie diese **Datei zur Überprüfung** im Internet zu **Virustotal** (http://www.virustotal.com) oder zu **Jottis Malwarescan** (http://virusscan.jotti.org/de) laden, dort wird diese Datei mit bis zu **40 Virenscannern** auf Viren und Malware überprüft. Wenn die Datei als Schadsoftware erkannt ist, können Sie die Datei löschen.

Eine weitere Möglichkeit wäre die Systemwiederherstellung, das heißt, das System auf ein Datum vor der Infizierung zurück zu setzen. Dazu geben Sie in der Eingabeaufforderung (Dosbox) den Befehl ein:

Abhängig vom Betriebssystem entweder: **rstrui.exe** oder den kompletten Pfad **\windows\system32\restore\rstrui.exe** und bestätigen mit der **Entertaste**, nach wenigen Sekunden öffnet sich der **Systemwiederherstellungsassistent**.

Dort klicken Sie auf "**Computer zu einem früheren Zeitpunkt wiederherstellen**" und bestätigen mit "**weiter**". Nun suchen Sie einen **Wiederherstellungspunkt vor der Infizierung** und bestätigen mit "**weiter**". Der Computer wird nun zurückgesetzt.

Grundsätzlich werden **keine persönlichen Dateien oder E-Mails und ähnliche Dateien bei diesem Verfahren überschrieben bzw. gelöscht**. Aber Sie sind immer gut beraten, vorher eine Datensicherung Ihres Systems zu erstellen.

Wenn die Wiederherstellung funktioniert hat und die Vorschaltseite des UKASH nicht mehr erscheint, wird die eigentliche **Malware noch auf dem System** sein. Sie sollten den Rechner gründlich mit **verschiedenen Scannern überprüfen** lassen.

Um 100% sicher zu gehen, dass der Computer "sauber" ist, empfehlen wir immer eine Neuinstallation.

BKA-Trojaner mit Hilfe einer Live-CD entfernen:

Quelle:
http://blog.botfrei.de/2011/07/anleitung-bka-trojaner-mit-hilfe-des-avira-de-cleaner-automatisch-entfernen/