Dieser Service wird Ihnen bereitgestellt durch:

http://www.trojaner-info.de

HijackThis Anleitung - Deutsche Übersetzung

Hinweis: Diese deutsche Übersetzung erfolgte nach besten Wissen und Gewissen auf dem Stand der englischsprachigen Originalseite **HijackthisTutorial** vom 28. Januar 2004, ergänzt um die erweiterten Angaben mit Stand vom 30. Juni 2004 und 13. Januar 2005. Dennoch können etwaige Übersetzungsfehler nicht ausgeschlossen werden. Bitte außerdem beachten, dass aufgrund des Zeitbedarfs für die Übersetzung ins Deutsche das englische Originaldokument in der Zwischenzeit möglicherweise aktualisiert wurde, wodurch diese Übersetzung inhaltlich abweichen kann.

In diversen Foren zum Thema Internetsicherheit, häufen sich die Bitten verunsicherter Anwender nach Hilfe bei der Analyse der Logdatei von **HijackThis**, weil sie nicht wissen, welche Einträge 'gut' und welche 'schlecht' sind. Ohne dieses Wissen ist es kaum möglich, 'schlechte' Einträge herauszufinden und mit HijackThis zu reparieren (zu fixen). Dies ist eine einführende Erläuterung, der einzelnen Angaben (und ihrer Bedeutungen) eines HijackThis-Log. Bleiben Fragen offen oder bei Zweifeln kann eine erstellte Log-Datei natürlich auch weiterhin mit der Bitte um Hilfe in einen **neuen Beitrag** in **unserem Forum** kopiert werden.

Übersicht

Jeder Bereich in einem HijackThis-Log beginnt mit einem Bereichstitel. Für technische Informationen über die einzelnen Bereiche, kann im Hauptfenster von HijackThis auf 'Info' geklickt und dann nach unten gescrollt werden. Mit Markieren des gewünschten Bereichs und einem weiteren Klick auf 'More info on this item' erhält man innerhalb des Programms HijackThis Hinweise zum ausgewählten Bereich (*Anmerkung:* Die Erläuterungen sind in englischer Sprache).

In der hier vorliegenden deutschsprachigen Anleitung einfach den Link zu dem Abschnitt anklicken, für den Erläuterungen gewünscht sind:

- O17 - Lop.com-Domain Veränderungen
- O18 - Zusätzliche bzw. veränderte Protokolle
- O19 - Veränderungen des 'User Style Sheet' (CSS)

Neu hinzugekommene Einträge ab der Version HijackThis 1.98:

- O20 - AppInit_DLLs - Autostarteinträge in der Registry
- O21 - ShellServiceObjectDelayLoad (SSODL) - Autostarteinträge in der Registry
- O22 - SharedTaskScheduler - Autostarteinträge in der Registry

Neu hinzugekommene Einträge ab der Version HijackThis 1.99:

- O23 - Windows NT Services - Dienste unter Windows NT

R0, R1, R2, R3 - Internet Explorer Start- /Suchseiten

Beispieleinträge:

R0 - HKCU\Software\Microsoft\Internet Explorer\Main,Start Page = **http://www.google.de/**
R1 - HKLM\Software\Microsoft\Internet Explorer\Main,Default_Page_URL = **http://www.google.de/**
R2 - (this type is not used by HijackThis yet)
R3 - **Default URLSearchHook is missing**

Was zu unternehmen ist:

Handelt es sich bei der URL am Ende des Eintrags um eine bekannte, bzw. selbst ausgewählte Seite oder Suchmaschine ist der Eintrag OK. Handelt es sich um einen unbekannten Eintrag, sollte dieser mit HijackThis gefixt werden.
Einträge unter 'R3' sollten immer gefixt werden, es sei denn, es wird ein bekanntes Programm erwähnt (z.B. Copernic).

F0, F1, F2, F3 - Autostart-Programmeinträge in INI-Dateien

Beispieleinträge:

F0 - system.ini: Shell=Explorer.exe **Openme.exe**
F1 - win.ini: run=**hpfsched**

Was zu unternehmen ist:

Einträge unter 'F0' sind **immer** 'schlecht' und sollten gefixt werden.
Bei Einträgen unter 'F1' handelt es sich in der Regeln um sehr alte Programme, welche normalerweise 'gut' sind. Bei Unklarheiten sollte mittels Google versucht werden, weitere Informationen zum erwähnten Dateinamen zu finden, um so herauszufinden, ob es sich um ein 'gutes' oder 'schlechtes' Programm handelt.
Pacman's Startup List kann bei der Identifizierung solcher Einträge ebenfalls hilfreich sein.

N1, N2, N3, N4 - Netscape/Mozilla Start- /Suchseiten

Beispieleinträge:

N1 - Netscape 4: user_pref("browser.startup.homepage", "**www.google.de**"); (C:\Program Files\Netscape\Users\default\prefs.js)

N2 - Netscape 6: user_pref("browser.startup.homepage", "**http://www.google.de**"); (C:\Documents and Settings\User\Application Data\Mozilla\Profiles\defaulto9t1tfl.slt\prefs.js)

N2 - Netscape 6: user_pref("browser.search.defaultengine", "engine://**C%3A%5CProgram%20Files%5CNetscape%206%5Csearchplugins%5CSBWeb_02.src**"); (C:\Documents and Settings\User\Application Data\Mozilla\Profiles\defaulto9t1tfl.slt\prefs.js)

Was zu unternehmen ist:

Normalerweise sind die Start-/Suchseiteneinträge der Netscape- und Mozilla-Browser sicher. Lediglich **Lop.com** ist zur Zeit dafür bekannt, diese Einträge zu verändern. Unbekannte Start-/Suchseiteneinträge in dieser Kategorie sollten von HijackThis gefixt werden.

O1 - Eingetragene Umleitungen in der Datei HOSTS

Beispieleinträge:

O1 - Hosts: 216.177.73.139 **auto.search.msn.com**
O1 - Hosts: 216.177.73.139 **search.netscape.com**
O1 - Hosts: 216.177.73.139 **ieautosearch**
O1 - **Hosts file is located at C:\Windows\Help\hosts**

Die Datei **HOSTS** übernimmt -vereinfacht gesagt- lokal die Aufgabe eines Domain-Name-Servers (DNS) und ordnet einer Webadresse eine IP-Adresse zu. Ein Webbrowser kann -technisch gesehen- keine Webadressen suchen, sondern nur die dazugehörige IP-Adresse.

Was zu unternehmen ist:

Veränderungen an der HOSTS-Datei leiten hinten eingetragene Webadressen (hier fett dargestellt) zu den vorne genannten IP-Adressen um. Gehört die IP-Adresse nicht zu der gewünschten Webadresse, wird der Browser jedesmal zu der falschen Adresse umgeleitet, wenn die Webadresse im Browser eingegeben wird. Unbekannte, bzw. nicht selbst vorgenommene Einträge in der Datei HOSTS sollten mit HijackThis gefixt werden

Der letzte Eintrag tritt manchmal unter Windows 2000/XP bei einer Coolwebsearch-Infektion auf. Diese sollten immer mit HijackThis gefixt, oder mit dem kostenlosen Tool CWShredder automatisch repariert werden. Hinweis: Der CWShredder wird sehr oft aktualisiert. Einmal heruntergeladen empfiehlt sich unbedingt zunächst zu überprüfen ('Check for Update'), ob bereits eine neuere Version dieses Programms vorhanden ist.

O2 - BHO-Programmerweiterungen des IE (Browser Helper Objects)

Beispieleinträge:

O2 - BHO: **Yahoo! Companion BHO** - **{13F537F0-AF09-11d6-9029-0002B31F9E59}** - C:\PROGRAM FILES\YAHOO!\COMPANION\YCOMP5_0_2_4.DLL

O2 - BHO: (no name) - **{1A214F62-47A7-4CA3-9D00-95A3965A8B4A}** - C:\PROGRAM FILES\POPUP ELIMINATOR\AUTODISPLAY401.DLL (file missing)

O2 - BHO: **MediaLoads Enhanced** - **{85A702BA-EA8F-4B83-AA07-07A5186ACD7E}** - C:\PROGRAM FILES\MEDIALOADS ENHANCED\ME1.DLL

Was zu unternehmen ist:
Ist der Name des Browser Helper Objekts (BHO) unbekannt, kann in **TonyK's BHO & Toolbar List** die CLSD ('Class Identifier' -> Zahlen-/Buschstabenkolonnen in geschweiften Klammern {}) gesucht werden In der BHO Liste bedeutet 'X' Spyware und 'L' sicherer Eintrag.

O3 - Internet Explorer Werkzeugleiste (Toolbar)

Beispieleinträge:

O3 - Toolbar: **&Yahoo! Companion** - **{EF99BD32-C1FB-11D2-892F-0090271D4F88}** - C:\PROGRAM FILES\YAHOO!\COMPANION\YCOMP5_0_2_4.DLL

O3 - Toolbar: **Popup Eliminator** - **{86BCA93E-457B-4054-AFB0-E428DA1563E1}** - C:\PROGRAM FILES\POPUP ELIMINATOR\PETOOLBAR401.DLL (file missing)

O3 - Toolbar: **rzillcgthjx** - {5996aaf3-5c08-44a9-ac12-1843fd03df0a} - **C:\WINDOWS\APPLICATION DATA\CKSTPRLLNQUL.DLL**

Was zu unternehmen ist:
Ist der Name der Toolbar unbekannt, kann in **TonyK's BHO & Toolbar List** anhand der Class ID ('Class Identifier' -> Zahlen-/Buschstabenkolonnen in geschweiften Klammern {}) ermittelt werden, ob es sich um einen 'guten' oder 'schlechten' Eintrag handelt. In dieser Toolbar List, bedeutet 'X' Spyware und 'L' sicherer Eintrag.
Wenn sich ein gesuchter Eintrag nicht in der Liste befindet, der Name aus zufälligen Zeichen besteht und sich im Verzeichnis 'Application Data' (Anwendungsdaten) befindet (wie der untere Beispieleintrag), handelt es sich sehr wahrscheinlich um **Lop.com** und sollte zwingend mit HijackThis gefixt werden.

O4 - Autostartaufrufe aus der Registry

Beispieleinträge:

O4 - HKLM\..\Run: [**ScanRegistry**] C:\WINDOWS\scanregw.exe /autorun
O4 - HKLM\..\Run: [**SystemTray**] SysTray.Exe
O4 - HKLM\..\Run: [**ccApp**] "C:\Program Files\Common Files\Symantec Shared\ccApp.exe"
O4 - Startup: **Microsoft Office**.lnk = C:\Program Files\Microsoft Office\Office\OSA9.EXE
O4 - Global Startup: **winlogon.exe**

Was zu unternehmen ist:

In **PacMan's Startup List** den Eintrag suchen und feststellen, ob dieser als 'gut' oder 'schlecht' gekennzeichnet ist.
Befindet sich der Eintrag in einer 'Startup-Gruppe' (wie der untere Beispieleintrag), kann HijackThis diesen Eintrag nicht fixen, solange sich dieser im Speicher befindet. Mit dem 'Windows Task Manager' (TASKMGR.EXE) muss ein solcher Prozess zunächst beendet werden, bevor er gefixt werden kann.

O5 - IE Optionen werden unter 'Extras' nicht angezeigt

Beispieleinträge:

O5 - control.ini: **inetcpl.cpl=no**

Was zu unternehmen ist:

Insofern die IE-Optionen nicht bewusst ausgeblendet wurden, ist dieser Eintrag mit HijackThis zu fixen.

O6 - Zugriff auf IE Optionen durch Administrator verhindert

Beispieleinträge:

O6 - HKCU\Software\Policies\Microsoft\Internet Explorer**Restrictions present**

Was zu unternehmen ist:

Insofern nicht in dem kostenlosen Anti-Spyware-Tool **Spybot S&D** die Option 'Lock homepage from changes' aktiviert wurde, ist dieser Eintrag mit HijackThis zu fixen.

O7 - Zugang auf Regedit durch Administrator verhindert

Beispieleinträge:

O7 - HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\System, **DisableRegedit=1**

Was zu unternehmen ist:

Diese Einträge **immer** durch HijackThis fixen.

O8 - Extra Einträge im 'Rechts-Klick-Menü' des IE

Beispieleinträge:

O8 - Extra context menu item: **&Google Search** - res://C:\WINDOWS\DOWNLOADED PROGRAM FILES\GOOGLETOOLBAR_EN_1.1.68-DELEON.DLL/cmsearch.html
O8 - Extra context menu item: **Yahoo! Search** - file:///C:\Program Files\Yahoo!\Common/ycsrch.htm
O8 - Extra context menu item: **Zoom &In** - C:\WINDOWS\WEB\zoomin.htm
O8 - Extra context menu item: **Zoom O&ut** - C:\WINDOWS\WEB\zoomout.htm

Was zu unternehmen ist:

Unbekannte Einträge im 'Rechts-Klick-Menü' des IE **immer** mit HijackThis fixen.

O9 - Extra Buttons in der IE-Toolbar, oder zusätzliche Einträge im IE-Menü 'Extras'

Beispieleinträge:

O9 - Extra button: **Messenger** (HKLM)
O9 - Extra 'Tools' menuitem: **Messenger** (HKLM)
O9 - Extra button: **AIM** (HKLM)

Was zu unternehmen ist:

Unbekannte Button oder Einträge im Menü 'Extras' **immer** mit HijackThis fixen.

O10 - Winsock Veränderungen

Beispieleinträge:

O10 - Hijacked Internet access by **New.Net**
O10 - Broken Internet access because of LSP provider **'c:\progra~1\common~2\toolbar\cnmib.dll**' missing
O10 - Unknown file in Winsock LSP: **c:\program files\newtonknows\vmain.dll**

Was zu unternehmen ist:

Diese Einträge sollten nicht manuell gelöscht werden!
Beste Möglichkeiten zur Reparatur bieten **LSPFix** von **Cexx.org**, oder **Spybot S&D** von Kolla.de.
Hinweis: Aus Gründen der Systemsicherheit können unbekannte Dateien im 'LSP stack' nicht durch HijackThis gefixt werden.

O11 - Zusätzliche Gruppe im IE-Fenster 'Erweiterte Optionen'

Beispieleinträge:

O11 - Options group: [CommonName] **CommonName**

Was zu unternehmen ist:

Es ist bisher nur ein Hijacker (**CommonName**) bekannt, der eine zusätzliche Gruppe im IE-Fenster 'Erweiterte Optionen' hinzufügt. Diese immer mit HijackThis fixen.

O12 - IE Plugins (Programmerweiterungen des IE)

Beispieleinträge:

O12 - Plugin for **.spop**: C:\Program Files\InternetExplorer\Plugins\NPDocBox.dll
O12 - Plugin for **.PDF**: C:\Program Files\InternetExplorer\PLUGINS\nppdf32.dll

Was zu unternehmen ist:

Die meisten Einträge in diesem Abschnitt sind sicher. Nur **OnFlow** fügt hier ein unerwünschtes Plugin ein. OnFlow-Plugins haben die Erweiterung *.ofb.

O13 - Veränderung der Standard Voreinstellungen (DefaultPrefix) des IE

Beispieleinträge:

O13 - DefaultPrefix: **http://www.pixpox.com/cgi-bin/click.pl?url=**
O13 - WWW Prefix: **http://prolivation.com/cgi-bin/r.cgi?**
O13 - WWW. Prefix: **http://ehttp.cc/?**

Was zu unternehmen ist:

Einträge in diesem Bereich sind immer 'schlecht' und sollten mit HijackThis gefixt werden.

O14 - Veränderungen unter 'Webeinstellungen zurücksetzen'

Beispieleinträge:

O14 - IERESET.INF: START_PAGE_URL=**http://www.searchalot.com**

Was zu unternehmen ist:

Handelt es sich bei diesen Einträgen nicht um die Adresse des PC-Händlers oder des 'Internet-Service-Provider (ISP)', sollten diese Einträge mit HijackThis gefixt werden.

O15 - Unerwünschte Seiten in 'Vertrauenswürdige Seiten'

Beispieleinträge:

O15 - Trusted Zone: **http://free.aol.com**
O15 - Trusted Zone: ***.coolwebsearch.com**
O15 - Trusted Zone: ***.msn.com**

Was zu unternehmen ist:

Die meisten automatisch platzierten Einträge in diesem Bereich sind entweder von **AOL** oder **Coolwebsearch**. Wenn hier aufgeführte Internet-Seiten nicht wissentlich unter 'Vertrauenswürdige Seiten' hinzugefügt wurden, sollten diese mit HijackThis gefixt werden.

O16 - ActiveX-Objekte (auch bekannt als Downloaded Program Files)

Beispieleinträge:

O16 - DPF: **Yahoo! Chat** - http://us.chat1.yimg.com/us.yimg.com/i/chat/applet/c381/chat.cab

O16 - DPF: {D27CDB6E-AE6D-11CF-96B8-444553540000} (**Shockwave Flash Object**) - http://download.macromedia.com/pub/shockwave/cabs/flash/swflash.cab

Was zu unternehmen ist:

Unbekannte ActiveX-Objekte, bzw. ActiveX-Objekte von unbekannten Seiten sollten mit HijackThis gefixt werden. **Beinhaltet der Name des ActiveX-Objekts bzw. die angegebene URL Worte wie 'dialer', 'casino', 'free_plugin' etc, sollten diese unbedingt gefixt werden!**
Javacool's SpywareBlaster beinhaltet eine große Datenbank gefährlicher ActiveX-Objekte. Dieses kostenlose Tool kann bequem nach CLSID's ('Class Identifier' -> Zahlen-/Buschstabenkolonnen in geschweiften Klammern {}) durchsucht werden. Dies geschieht mit einem Rechts-Klick in die Liste zum Öffnen der Suchen-Funktion.

O17 - Lop.com-Domain Veränderungen

Beispieleinträge:

O17 - HKLM\System\CCS\Services\VxD\MSTCP: Domain = **aoldsl.net**
O17 - HKLM\System\CCS\Services\Tcpip\Parameters: Domain = **W21944.find-quick.com**
O17 - HKLM\Software\..\Telephony: DomainName = **W21944.find-quick.com**
O17 - HKLM\System\CCS\Services\Tcpip\..\{D196AB38-4D1F-45C1-9108-46D367F19F7E}: Domain = **W21944.find-quick.com**
O17 - HKLM\System\CS1\Services\Tcpip\Parameters: SearchList = **gla.ac.uk**
O17 - HKLM\System\CS1\Services\VxD\MSTCP: NameServer = **69.57.146.14,69.57.147.175**

Was zu unternehmen ist:

Wenn die hier angegebene Domäne nicht zum ISP, bzw. des Firmen-Netzwerks ist, sollte dieser Eintrag mit HijackThis gefixt werden. Das Gleiche gilt für die 'SearchList'-Einträge (Suchlisten-Einträge).
Für vorhandene 'NameServer' (DNS Server) Einträge, hilft im Zweifel eine Suche mit Google nach den IP-Adressen bei der Entscheidung, ob diese Einträge 'gut' oder 'schlecht' sind.

O18 - Zusätzliche bzw. veränderte Protokolle

Beispieleinträge:

O18 - Protocol: **relatedlinks** - {5AB65DD4-01FB-44D5-9537-3767AB80F790} - C:\PROGRA~1\COMMON~1\MSIETS\msielink.dll
O18 - Protocol: **mctp** - {d7b95390-b1c5-11d0-b111-0080c712fe82}
O18 - **Protocol hijack: http** - {66993893-61B8-47DC-B10D-21E0C86DD9C8}

Was zu unternehmen ist:

Nur wenige Hijacker werden hier angezeigt. Die bekannten sind **'cn' (CommonName)**, **'ayb' (Lop.com)** und **'relatedlinks' (Huntbar)**. Diese sollten mit HijackThis gefixt werden.
Weitere Einträge können nicht als Sicher eingestuft werden, bzw. es handelt es sich um Veränderungen durch einen Hijacker (z.B. wenn die CLSID durch Spyware verändert wurde.) In letzterem Fall sollten diese Einträge ebenfalls mit HijackThis gefixt werden.

O19 - Veränderungen des 'User Style Sheet' (CSS)

Beispieleinträge:

O19 - User style sheet: c:\WINDOWS\Java**my.css**

Was zu unternehmen ist:

Zeigt sich der InternetExplorer ungewohnt langsam, bzw. es kommt immer wieder zu 'unkontrollierten' Popups, sollten die Einträge mit HijackThis gefixt werden.
Werden diese CSS-Veränderungen in den Coolwebsearch-Chronicles aufgeführt, ist es besser, den kostenlosen CWShredder zum Entfernen dieser Einträge zu benutzen.

O20 - *AppInit_DLLs*-Autostarteinträge in der Registry

Beispieleinträge:
O20 - AppInit_DLLs: **msconfd.dll**

Was zu unternehmen ist:
Dieser Registry-Wert, zu finden unter
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Windows,
lädt bei der Benutzer-Anmeldung eine DLL in den Speicher, die auch nach der Abmeldung dort verbleibt. Nur sehr wenige Programme nutzen diese Vorgehensweise auf legale Art (z. B. Norton CleanSweep benutzt die APITRAP.DLL). Wesentlich öfter wird diese Vorgehensweise jedoch von einem Trojaner oder einem agressiven Browser-Hijacker verwandt.

Falls eine 'verborgene' DLL durch diesen Registry-Wert (nur sichtbar, wenn im Registrierungs-Editor unter Ansicht die Option 'Binärdaten anzeigen' verwendet wird) geladen wird, kann dem dll-Namen das Zeichen '|' vorangestellt sein, um diesen Eintrag im Log sichtbar zu machen.

O21 - *ShellServiceObjectDelayLoad (SSODL)*-Autostarteinträge in der Registry

Beispieleinträge:
O21 - SSODL - AUHOOK - {11566B38-955B-4549-930F-7B7482668782} - **C:\WINDOWS\System\auhook.dll**

Was zu unternehmen ist:
Hierbei handelt es sich um eine undokumentierte Autostart-Methode, welche normalerweise von einigen wenigen Windows System Komponenten genutzt wird. Einträge unter
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\ShellServiceObjectDelayLoad
werden beim Windows-Start durch den Explorer mit gestartet. HijackThis benutzt eine Whitelist verschiedener 'SSODL'-Einträge. Wird ein solcher Eintrag im Log angezeigt handelt es sich um einen unbekannten Eintrag, der **möglicherweise** schadhaft.
Hier gefundene Einträge sollten mit besonderer Vorsicht behandelt werden.

O22 - *SharedTaskScheduler*-Autostarteinträge in der Registry

Beispieleinträge:
O22 - SharedTaskScheduler: (no name - {3F143C3A-1457-6CCA-03A7-7AA23B61E40F} - **c:\windows\system32\mtwirl32.dll**

Was zu unternehmen ist:
Hierbei handelt es sich ebenfalls um eine undokumentierte Autostart-Methode unter **Windows NT/2000/XP**, welche nur äußerst selten angewandt wird. Bisher ist nur CWS.Smartfinder für die Verwendung dieser Methode bekannt.
Hier gefundene Einträge sollten ebenfalls mit besonderer Vorsicht behandelt werden.

O23 - *Windows NT Services*-Dienste unter Windows NT
Beispieleinträge: O23 - Service: Kerio Personal Firewall (PersFw) - Kerio Technologies - **C:\Program Files\Kerio\Personal Firewall\persfw.exe** Was zu unternehmen ist: Hier werden alle **nichtwindowseigenen Dienste** aufgelistet. Diese Liste sollte identisch sein, mit den Autostarteinträgen des Msconfig-Tools unter Windows XP. Diverse Hijacking-Trojaner benutzen in Verbindung mit weiteren Autostartmöglichkeiten einen eigenen Dienst um sich immer wieder selbst neu zu installieren. Der komplette Name eines solchen Dienstes klingt zumeist äußerst wichtig, z. B. 'Network Security Service', 'Workstation Logon Service' oder 'Remote Procedure Call Helper', aber der interne Name (in Klammern) ist eine Sammlung unsinniger Zeichen, z. B. 'O?'ŽrtñåÈ²$Ó'. Der hintere Teil der jeweiligen Zeile zeigt den Namen der Datei an, welche zu diesem Dienst gehört. Achtung: Das 'Fixen' eines 023-Eintrages beendet und deaktiviert lediglich einen solchen Dienst. Es ist daher erforderlich, den Dienst entweder manuell oder mit einem entsprechenden Tool aus der Registry zu entfernen. In HijackThis 1.99.1 oder höher kann die Option 'Delete NT Service' unter 'Misc Tools' hierfür genutzt werden.

Das BrowserHijacking nutzt eine (von vielen) Schwachstellen des Internet Explorers von Microsoft aus. Deshalb kann HijackThis auch 'nur' die Veränderungen durch BrowserHijacker reparieren, aber es bietet keinen vorbeugenden Schutz vor erneuten Infektionen.

Wer nicht -zum Beispiel aus beruflichen Zwängen- auf die Nutzung des Internet Explorers angewiesen ist, sollte sich Gedanken über einen Wechsel zu einem alternativen Browser machen.
Mozilla,
Mozilla Firefox oder
Opera
bieten mindestens den gleichen Surfkomfort wie der Internet Explorer bei einem Mehr an Sicherheit. Ganz gleich, welcher Browser favorisiert wird. Ein regelmäßiges **Windowsupdate** ist auf jeden Fall unerläßlich.

Lutz (lk) 01.07.2004
(zuletzt ergänzt am 24. Jan. 2004)
