Anleitung: HiJackThis

Was ist HiJackThis?

Der Autor, <u>Merijn Bellekom</u>, entwickelte in erster Linie das Freeware-Tool HiJackThis, um hartnäckige <u>Browser</u> <u>HiJacker</u>, wie z.B. CoolWebSearch, zu entfernen, aber auch andere <u>Malware</u> lässt sich so aufspüren und ggf. entfernen.

Mittlerweile ist das mächtige HJT aus keinem Forum mehr wegzudenken, da es den dortigen Helfern die Analyse der infizierten Systeme erheblich erleichtert.

Download und entpacken von HJT:

Nach dem <u>Download</u> oder <u>Direkt-Download</u>, solltest Du mittels <u>WinZip</u> das Archiv in einem zuvor eigens erstellten Ordner entpacken [1], damit HJT Backups von den gefixten Einträgen anlegen kann. Wichtig: Bei Fehlbedienung kann im Bedarfsfall auf die Backups zurückgegriffen werden.

[1] z.B. C:\Programme\HiJackThis

Fehlermeldung beim Start von HJT:

- MSVBVM60.DLL fehlt! -> <u>VBRun60.exe</u> installieren

- Unexpected error -> HJT-FAQ
- [Zitat von Markus Klaffke

Tipp: Lässt sich bedingt durch eine aktive Malware die HijackThis.exe nicht starten, bitte einfach letztgenannte z.B. in pruefung.com umbenennen und dann ausführen. -- Wichtig hierbei: Die Dateiendung "exe" muss durch "com" ersetzt werden!] Quelle: <u>Markus Klaffke</u>

Einsetzen von HJT – Log-File erstellen:

Navigiere nun zum Ordner 'C:\Programme\HiJackThis' und starte HJT per Doppelklick auf 'HiJackThis.exe'.
Beim ersten Start erhältst Du eventuell folgende Warnung und bestätigst diese, nach sorgfältigem Lesen, mit 'OK':



3. Es öffnet sich das Programmfenster 'New user quickstart'.

Klicke auf den rot markierten Button 'Do a system scan and save a log file':

isers quickstart	
Do a system scan and save a logfile	
Do a system scan only]
View the list of backups]
Open the Misc Tools section]
Open online HijackThis QuickStart	Courtesy of TomCoyote.org
None of the above, just start the program	1
Don't show this frame aciain when I start Hilad	_l (This

4. Nach dem Scan erscheint nun das HJT Log-File im geöffneten Notepad. Dieses Log-File speicherst [2] Du unter C:\Programme\HiJackThis ab:

hijackthis1.log - Editor		
Datei Bearbeiten Format Ansicht ?		
Logfile of HijackThis v1.99.1		^
Scan saved at 21:38:54, on 16:04:200	15	
Platform: Windows XP SP2 (WinNT 5	.01.2600)	
MSIE: Internet Explorer v6.00 SP2 (6.	00.2900.2180)	
Running processes:		
C \WINDOWS\System32\smss exe		
C:\WINDOWS\system32\winlogon.ex	e	
C:\WINDOWS\system32\services.exe	3	
C:\WINDOWS\system32\Isass.exe		
C:\WINDOWS\system32\svchost.exe		
C:\WINDOWS\System32\svchost.exe		
C:\WINDOWS\system32\spoolsv.exe	1	
C: Programme/Gemeinsame Dateien	Acronis/Schedule2/schedul2.exe	
C.WINDOWSISystem32/Att2evox.ext	e	
C.WINDOWSIEXPIDEREAD	EVE	
C-WINDOWSISOUNDMAN EXE	J.EAE	
C-WINDOWS/Dit eve		
C \Programme\Medion Home Cinema	XI \PowerCinema\PCMService.exe	
C:\Programme\Acronis\TrueImage\Tru	elmageMonitor.exe	
C:\Programme\Gemeinsame Dateien\	Acronis\Schedule2\schedhlp.exe	
C:\WINDOWS\DitExp.exe		
C:\PROGRA~1\COMMON~1\X10\Con	nmon/x10nets.exe	
C:\WINDOWS\System32\svchost.exe		
C:\WINDOWS\System32\cmd.exe	Constant of the second second	
C \Programme\Microsoft Office\OFFIC	E11WINWORD EXE	
C:/Programme/Mozilla Firefox/firefox.e	BX0	~
< · · · · · · · · · · · · · · · · · · ·		2

[2] Datei -> Speichern unter... -> hijackthis1.log eingeben -> Speichern



Speichem in:	O HJT		S 0 0 0 0	9-
Zuletzt verwendete D Desktop Desktop Bigene Dateien	startuplist.tx	E		
	Dateiname:	TOSTORY.	*	Speichem
1.10			1	
Vetzwerkumgeb	Dateityp:	Textdateien (* txt)	(20)	Abbrechen

Das erstellte Log-File besteht aus 3 Bereichen: **Oberer Bereich:** Systeminformationen - Patchstand **Mittlerer Bereich:** Aktuell laufende Prozesse **Unterer Bereich:** <u>R0 bis O23 Einträge</u>

Einsetzen von HJT – Auswertung:

<u>1. Möglichkeit:</u> Du wertest dein Log-File selbst mit Hilfe der nachfolgenden Seiten aus: <u>Pacmans-Startuplist</u> <u>Answer that work</u> <u>CLSID List</u> <u>Reger24 FBJ's O18, 20 and 21, 23</u> <u>Google</u> Info zu diverser Malware: <u>viruslist.com</u> <u>VGrep</u>

Allerdings musst du bei der Auswertung ganz genau wissen, was du tust. Sicherheitshalber solltest du das 1. Logfile auch nicht löschen oder überschreiben. Falls bei der Auswertung und dem anschließenden "Fixen" etwas schief geht, können wir daraus den Ausgangszustand ersehen.

Es gibt auch Seiten, auf denen eine automatische Auswertung angeboten wird. Von dem Einsatz raten wir ab, da die automatische Auswertung nicht ausgereift ist.

<u>2. Möglichkeit</u>: Bei Unsicherheit wendest Du Dich an das Board und postest ein aktuelles HJT Log-File [3]. **Wichtig:** Durchsuche das Log-File nach persönlichen Informationen, wie z.B. deinen Realname, und editiere diese, bevor Du es postest.

Alle Links im Log-File sollten wie folgt editiert werden -> z.B. <u> $h^{**}p://trojaner-board.de</u>$. Einfach, damit niemand auf die Idee kommt, auf die Links zu klicken.</u>

[3] Navigiere zum Ordner C:\Programme\HiJackThis -> Doppelklick auf hijackthis1.log -> Strg+A (alles markieren) -> Strg+C (kopieren) -> Strg+V (in deinen erstellten Thread einfügen).

<u>Einsetzen von HJT – Einträge fixen:</u>

Die Auswertung ist nun abgeschlossen und die verdächtigen Einträge sollten im <u>abgesicherten Modus bei</u> <u>deaktivierter Systemwiederherstellung</u> wie folgt entfernt werden: Vor den genannten Einträgen einen Haken setzen und auf **'Fix Checked'** klicken.

010 - Einträge dürfen nicht gefixt werden. Winsock-Veränderungen werden mit dem Programm <u>LSP-Fix</u> repariert. O23 - Einträge sollten erst gefixt werden, wenn zuvor der Dienst beendet wurde: Start -> Ausführen -> services.msc -> OK -> Rechtsklick auf z.B. Remote Procedure Call (RPC) Helper -> Eigenschaften -> "Starttyp" deaktiviert und "Dienststatus" beenden einstellen -> Übernehmen

🖢 HijackThis - v1.99.1	
Below are the results of the scan. Be careful what determine what is bad and what merely customiz is save a log file and show it to knowledgable folk	It you delete, HijackThis cannot ed by you. The best thing to do s.
R0 - HKCU\Software\Microsoft\Internet Explo R1 - HKLM\Software\Microsoft\Internet Explo R0 - HKCU\Software\Microsoft\Internet Explo Q2 - BHO: AcroIEHprobj Q2 - BHO: AcroIEHprobj Q3 - HKCU\Software\Microsoft\Internet Explo Q2 - BHO: AcroIEHprobj Q3 - Toolbar: &Radio - (8E71888-423F-11D) Q3 - Toolbar: &Radio - (8E71888-423F-11D) Q3 - Toolbar: &Radio - (8E71888-423F-11D) Q4 - HKLM . Run: [ATIPTA] C: \VINDOWS\ Q4 - HKLM . Run: [SoundMan] SOUNDMAN. Q4 - HKLM . Run: [Dit] Dit.exe Q4 - HKLM . Run: [ITOBL SpeedMe] 'C: \VINDOWS\ Q4 - HKLM . Run: [Coll PCHService] 'C: \VINDOWS\ Q4 - HKLM . Run: [Coll SpeedMe] 'C: \VINDOWS\ Q4 - HKLM . Run: [Dit] Dit.exe Q4 - HKLM . Run: [ITOBL SpeedMe] 'C: \VINDOWS\	prer Wain, Start Page = http://dedies-board prer Wain, Default_Page_URL = http://www prer Wain, Local Page = (207 -4059-8370-78487068E083) - C: \Pro ; Neikeisoft - {49E0E0F0-5C30-11D4-945D 38-01D0-4d91-8333-CF10577473F7} - c: \pro 2-876E-00A0C9082467} - C: \WINDOWS\S 44-9818-009027A5CD4F} - c: \programme\g httpatch.exe XTI Technologies \ATI Control Panel\atiptax: EXE OWS\System 32\VOBREGCheck.exe -Check4 Ime\Wedion Home CinemaXI_PowerCinema \gramme\f_05L SpeedMansgen SpeedMars
Scan & fix stuff	Other stuff
Scan Fix checked	Info Config
the second	and the second s

Abschliessende Frage noch mit 'Ja' bestätigen.



Anschliessend sollten auch die Malware Dateien entfernt werden, denn sonst hat die ganze Prozedur keinen Sinn.

In Zusammenarbeit mit dedies-Team.