

## Was ist HiJackThis?

Der Autor, [Merijn Bellekom](#), entwickelte in erster Linie das Freeware-Tool HiJackThis, um hartnäckige [Browser Hijacker](#), wie z.B. CoolWebSearch, zu entfernen, aber auch andere [Malware](#) 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 [Download](#) oder [Direkt-Download](#), solltest Du mittels [WinZip](#) 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! -> [VBRUN60.exe](#) installieren

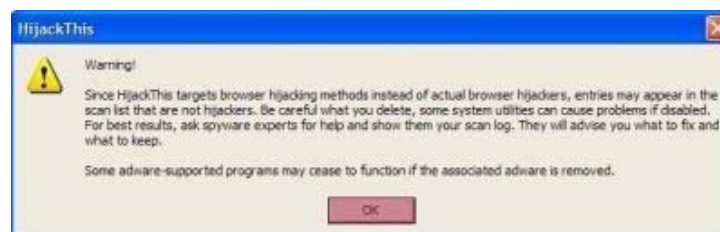
- Unexpected error -> [HJT-FAQ](#)

- [Zitat von Markus Klaffke

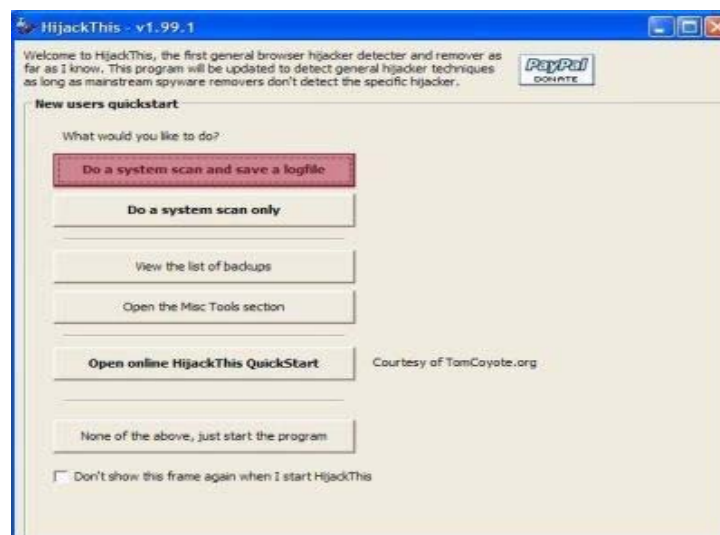
**Tipp:** Lässt sich bedingt durch eine aktive Malware die HijackThis.exe nicht starten, bitte einfach letztgenannte z.B. in pruefung.com umbenennen und dann ausführen. -- Wichtig hierbei: Die Dateieindung "exe" muss durch "com" ersetzt werden!] Quelle: [Markus Klaffke](#)

## Einsetzen von HJT – Log-File erstellen:

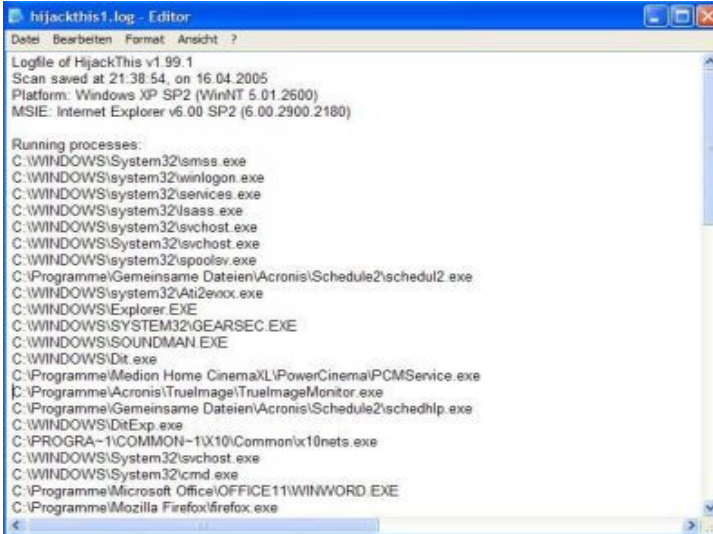
1. Navigiere nun zum Ordner '**C:\Programme\HiJackThis**' und starte HJT per Doppelklick auf '**HiJackThis.exe**'.
2. Beim ersten Start erhältst Du eventuell folgende Warnung und bestätigst diese, nach sorgfältigem Lesen, mit '**OK**':



3. Es öffnet sich das Programmfenster '**New user quickstart**'.  
Klicke auf den rot markierten Button '**Do a system scan and save a log file**':



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

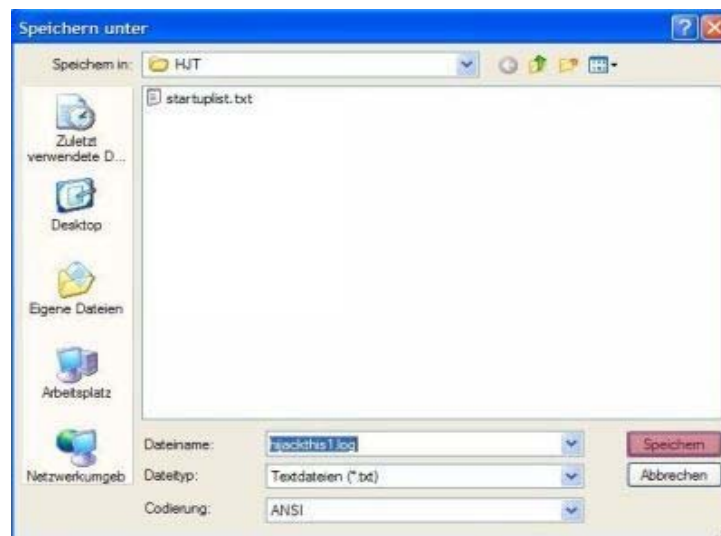
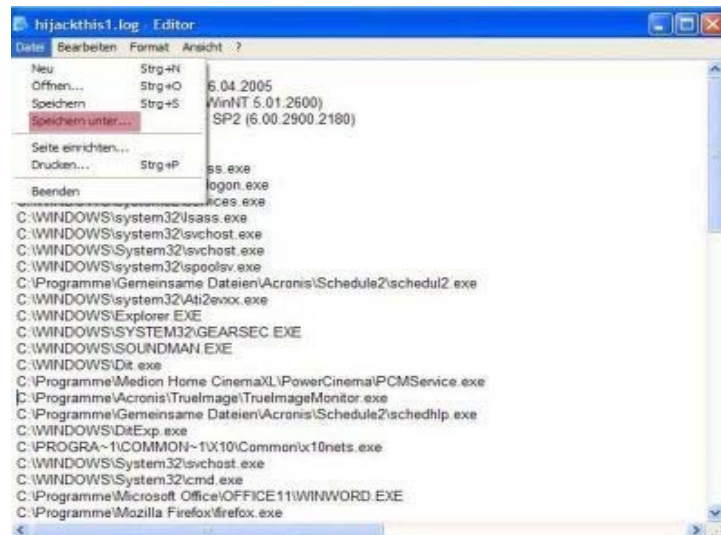


```

hijackthis1.log - Editor
Datei Bearbeiten Format Ansicht ?
Logfile of HijackThis v1.99.1
Scan saved at 21:38:54, on 16.04.2005
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.exe
C:\WINDOWS\system32\services.exe
C:\WINDOWS\system32\lsass.exe
C:\WINDOWS\system32\svchost.exe
C:\WINDOWS\System32\svchost.exe
C:\WINDOWS\system32\spoolsv.exe
C:\Programme\Gemeinsame Dateien\Acronis\Schedule2\schedul2.exe
C:\WINDOWS\system32\Ati2evxx.exe
C:\WINDOWS\Explorer.EXE
C:\WINDOWS\SYSTEM32\GEARSEC.EXE
C:\WINDOWS\SOUNDMAN.EXE
C:\WINDOWS\Dit.exe
C:\Programme\Medion Home CinemaXL\PowerCinema\PCMServise.exe
C:\Programme\Acronis\TrueImage\TrueImageMonitor.exe
C:\Programme\Gemeinsame Dateien\Acronis\Schedule2\schedhlp.exe
C:\WINDOWS\DitExp.exe
C:\PROGRA~1\COMMON~1\X10\Comman\10nets.exe
C:\WINDOWS\System32\svchost.exe
C:\WINDOWS\System32\cmd.exe
C:\Programme\Microsoft Office\OFFICE11\WINWORD.EXE
C:\Programme\Mozilla Firefox\firefox.exe
  
```

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



Das erstellte Log-File besteht aus 3 Bereichen:  
**Oberer Bereich:** Systeminformationen - Patchstand  
**Mittlerer Bereich:** Aktuell laufende Prozesse  
**Unterer Bereich:** [R0 bis O23 Einträge](#)

### Einsetzen von HJT – Auswertung:

**1. Möglichkeit:** Du wertest dein Log-File selbst mit Hilfe der nachfolgenden Seiten aus:

[Pacmans-Startuplist](#) [Answer that work](#) [CLSID List](#) [Reger24](#) [FBJ's O18, 20 and 21, 23](#) [Google](#)  
Info zu diverser Malware: [viruslist.com](#) [VGrep](#)

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.

**2. Möglichkeit:** 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. [h\\*\\*p://trojaner-board.de](http://h**p://trojaner-board.de). Einfach, damit niemand auf die Idee kommt, auf die Links zu klicken.

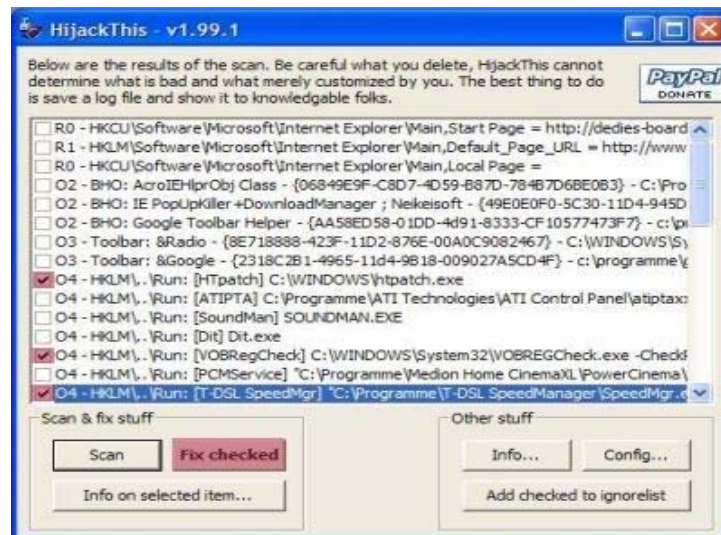
[3] Navigiere zum Ordner C:\Programme\HiJackThis -> Doppelklick auf hijackthis1.log -> Strg+A (alles markieren) -> Strg+C (kopieren) -> Strg+V (in deinen erstellten Thread einfügen).

### Einsetzen von HJT – Einträge fixen:

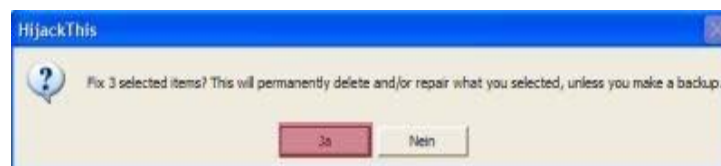
Die Auswertung ist nun abgeschlossen und die verdächtigen Einträge sollten im [abgesicherten Modus bei deaktivierter Systemwiederherstellung](#) wie folgt entfernt werden:

Vor den genannten Einträgen einen Haken setzen und auf 'Fix Checked' klicken.

010 - Einträge dürfen nicht gefixt werden. Winsock-Veränderungen werden mit dem Programm [LSP-Fix](#) repariert.  
023 - 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



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](#).