Was ist HiJackThis?

Ursprünglich von **Merijn Bellekom**, entwickelt um hartnäckige **Browser HiJacker**, wie z.B. CoolWebSearch, zu entfernen, wird das Freeware-Tool **HijackThis** seit einiger Zeit von TrendMicro weiterentwickelt. Da das Programm noch immer einen guten ersten Eindruck von infizierten Windows-Systemen vermittelt, ist es in vielen Foren auch heute noch ein von den dortigen Helfern gerne verwendetes Analysetool.

Download und Installation HJT:

Nach dem **Download** oder **Direkt-Download**, solltest Du die Installation durch einen Doppelklick auf die *HJTInstall.exe* starten. Nach einem Klick auf *Install* und der Bestätigung der Lizenzvereinbarung, sollte einer Verwendung von HijackThis nichts mehr im Wege stehen.

Fehlermeldung beim Start von HJT:

- MSVBVM60.DLL fehlt! -> **VBRun60.exe installieren**

Zitat:

> ***Original 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!

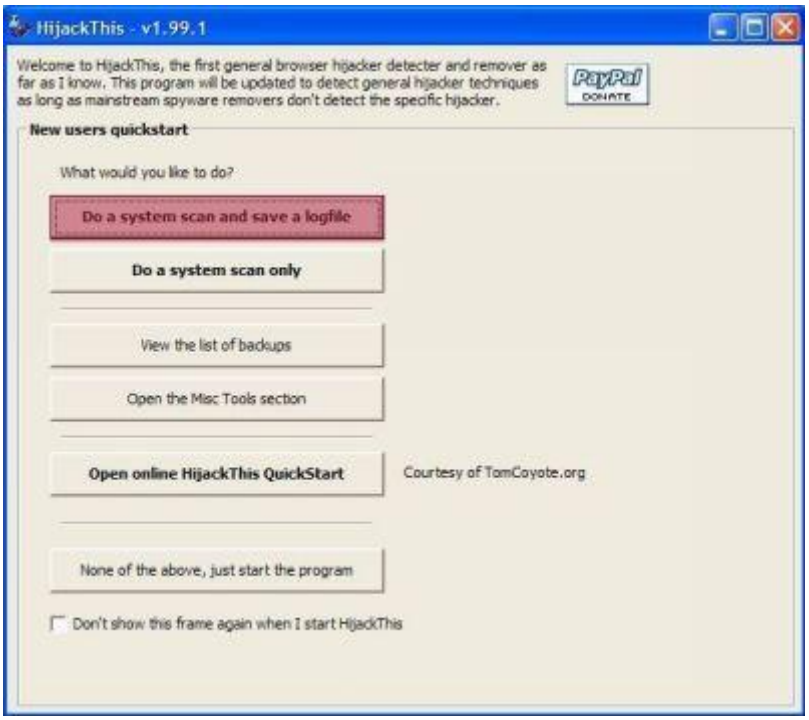
Quelle: **Markus Klaffke**

Einsetzen von HJT – Log-File erstellen:

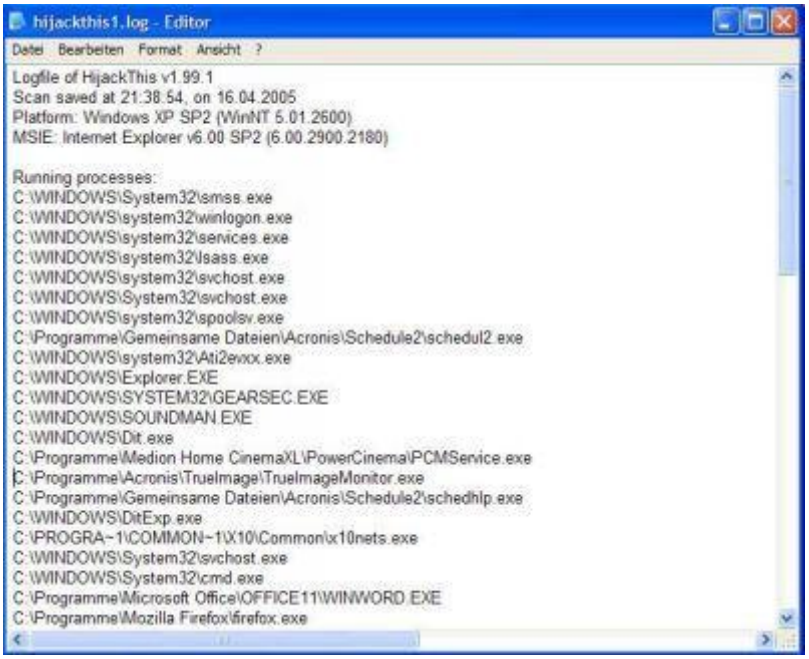
1. Nach erfolgter Installation lässt sich HijackThis durch einen Doppelklick auf das zugehörige Desktopsymbol starten. (Alternative: Navigiere zum Ordner '**C:\Programme\Trend Micro\HijackThis**' und starte HJT per Doppelklick auf '**HiJackThis.exe**')

2. Beim ersten Start erhältst Du *eventuell* folgende Warnung und bestätigst diese, nach sorgfältigem Lesen, mit '**OK**':

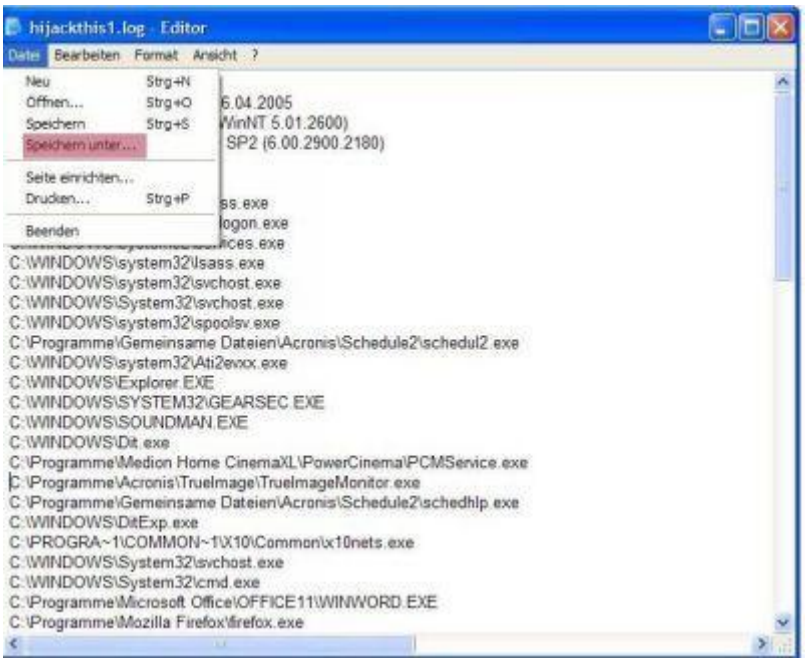
3. Es öffnet sich das Programmfenster '**New user quickstart**'.
Klicke auf den rot markierten Button '**Do a system scan and save a log file**':

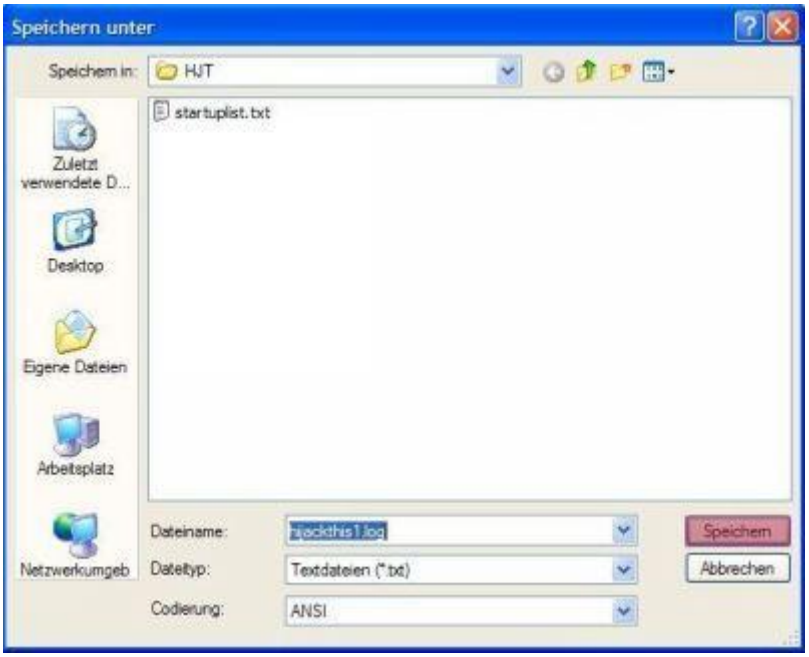


4. Nach dem Scan erscheint nun das HJT Log-File im geöffneten Notepad. Dieses Log-File speicherst **[2]** Du unter C:\Programme\Trend Micro\HiJackThis ab:



[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** **Reger24** **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.

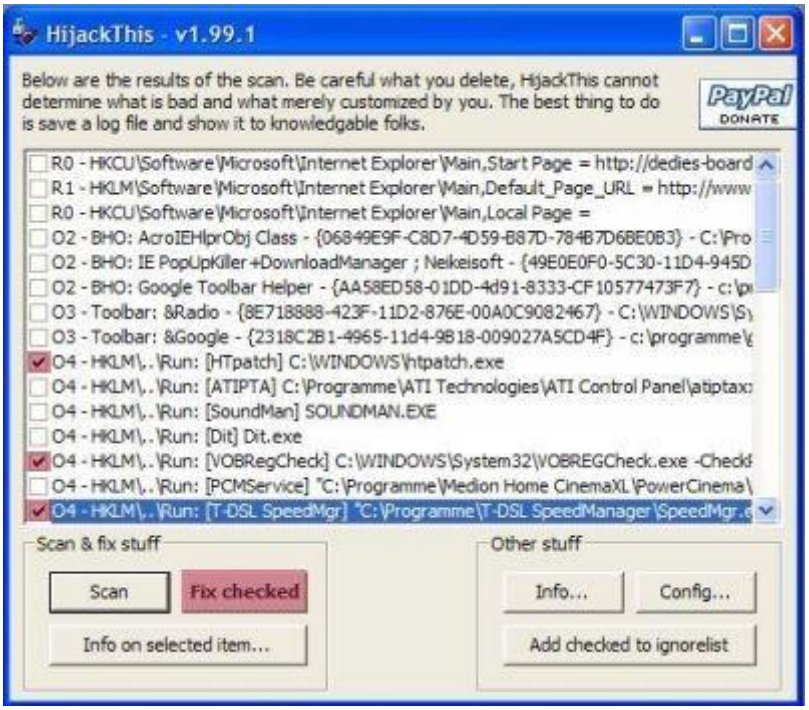
Alle Links im Log-File sollten wie folgt editiert werden -> z.B. hp://dedies-board.de. Einfach, damit niemand auf die Idee kommt, auf die Links zu klicken.**
Alternativ, je nach verwendete Forensoftware:
Woltlab Burning Board: Optionen -> Haken entfernen bei 'Urls automatisch umwandeln'!
vBulletin Board: Zusätzliche Einstellungen -> Haken entfernen bei 'Links automatisch umwandeln'!

[3] Navigiere zum Ordner C:\Programme\Trend Micro\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 abgesichert 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.
O23 - Einträge sollten erst gefixed 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.

Damit Ihr die Anleitung auch offline betrachten könnt', steht diese, ab sofort zum Download im PDF Format zur Verfügung!

Wenn etwas unklar sein sollte, dann eröffne bitte einen neuen Thread und stelle dort deine Fragen.

In Zusammenarbeit mit dedies - Team

Edit:
2010-11-04 Links aktualisiert
dedie

Gruß, Cidre
S-Mod d-b

Neuaufsetzen des Systems/Absicherung - Wie poste ich falsch? - Wie man Fragen richtig stellt!