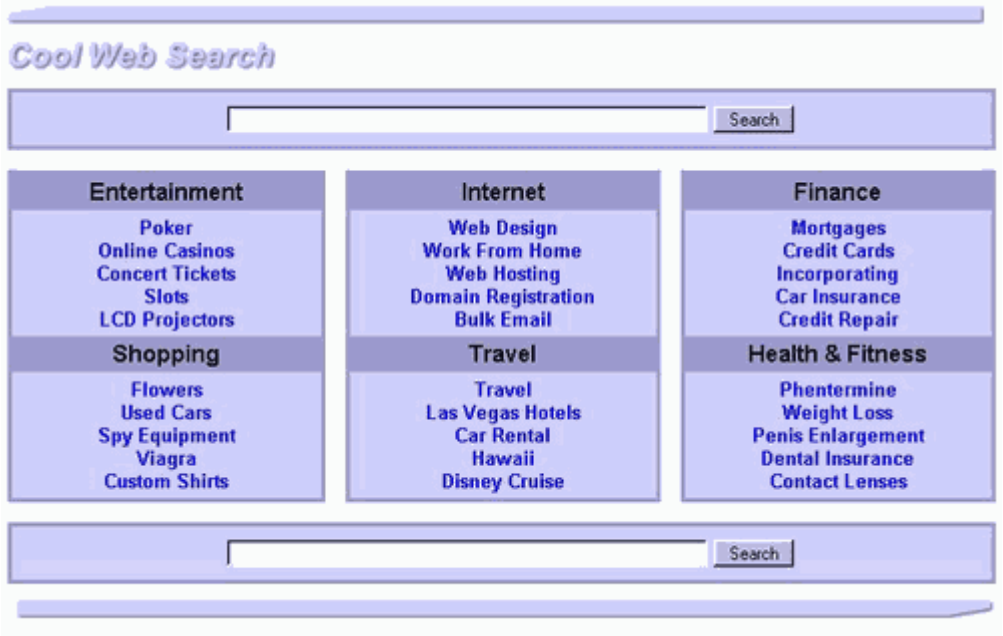
Dieser Service wird Ihnen bereitgestellt durch:

seit 1998 Trojaner - Info
Die deutsche Security-Seite

Browser-Hijacking - 'Entführung' auf unerwünschte Suchmaschine

---

Das Entführen (das sogenannte Hijacking) auf nicht gewünschte Internetseiten ist nicht neu. Zweifelhafte Berühmtheit erlangt hierbei die 'Suchmaschine' Cool Web Search. Die hinter diesem Webangebot stehende Firma 'Coolwebsearch' (CWS) verbreitet immer neue Varianten trojanischer Pferde, mit dem Zweck den Surfer auf die eigene Seite umzuleiten.



Die erste Form des Hijacking's auf die Seiten von *'Coolwebsearch'* wurde bereits im Mai 2003 entdeckt. Seit dem sind eine Vielzahl von Varianten hinzugekommen. Eine chronologische Auflistung der bisher bekannten Varianten befindet sich auf der Seite www.merijn.org/cwschronicles.html. Dieses Hijacking nutzt eine Sicherheitslücke in veralteten Versionen der **Virtual Machine** von Microsoft aus. Daher ist auch nur der **Internet Explorer** von Microsoft hiervon betroffen. Erste und wichtigste Regel ist daher auch hier das regelmäßige Updaten des Betriebssystems.

Der Niederländer **'Merijn'** hat mit dem **CWShredder** ein Programm geschrieben, welches in der Lage ist, die durch das Hijacking hervorgerufenen Veränderungen des Systems zurückzunehmen. Der CWShredder kann von dieser Seite kostenlos heruntergeladen werden: www.spywareinfo.com. Auf einem bereits betroffenen System kann das Aufsuchen der Seite ggf. scheitern. In diesem Fall kann der CWShredder auch direkt hier heruntergeladen werden: http://www.spywareinfo.com/~merijn/files/cwshredder.zip. **Achtung:** Bei diesem Direktlink startet **sofort** der Download!

Nach dem Download liegt der CWShredder in gezippter (komprimierter) Form vor und muss zunächst entpackt werden. Gezippte Dateien können beispielsweise mit WinZip entpackt werden. Für die Ausführung des Tools werden die Visual Basic 6 Runtime Libraries benötigt, die bei den meisten

Systemen bereits vorhanden sind. Sollte es beim Start des CWShredders zu der Meldung kommen, dass die Datei MSVBVM60.DLL fehlt, kann diese bei Microsoft kostenlos heruntergeladen werden.

Der CWShredder startet mit folgender Maske:

Um die Veränderungen durch das Hijacking rückgängig zu machen (zu fixen) genügt ein Klick auf den Button **Next ->**.
Achtung: Damit der CWShredder die Veränderungen fixen kann, ist es wichtig, dass alle evtl. geöffneten Browserfenster vorher geschlossen werden.
Mit **Scan only** wird das System auf evtl. Veränderungen überprüft, **ohne** dass eine Reparatur erfolgt.
Der CWShredder wird häufig aktualisiert, da immer wieder neue Varianten des Hijacking's auftauchen. Ist der Shredder einmal installiert, empfiehlt sich vor der Ausführung eine Überprüfung, ob bereits ein Update vorliegt. Dies geschieht am einfachsten mit einem Klick auf **Check for update**.

Viele Anwender melden sich seit den Weihnachtsfeiertagen in diversen Security-Foren mit Meldungen wie dieser:

> ***Auf einmal hat "ntsearch" auf alle möglichen Wörter einen Hyperlink gesetzt und nun gehen einige Homepages nicht mehr richtig! Z. B. wird eine Seite geladen, und sobald diese geladen ist, ist die Seite nur noch grau...***

Einmal gestartet, versucht der durch den Trojaner eingeschleppte Prozess **sp.exe** den Internet-Surfer auf die Seite *www.ntsearch.com* zu entführen (hinter dieser Adresse verbirgt sich ebenfalls die Suchmaschine *Cool Web Search*). Diese neueste Variante des Browser-Hijacking wird zum Zeitpunkt dieses Berichts vom CWShredder noch nicht erkannt, da der Programmierer lt. eigener Homepage zur Zeit erkrankt ist!

Bei auf NT basierenden Betriebssystemen (WinNT 4.0, Windows2000, WinXP) funktioniert die Entfernung des Trojaners vielfach durch die folgenden Schritte:

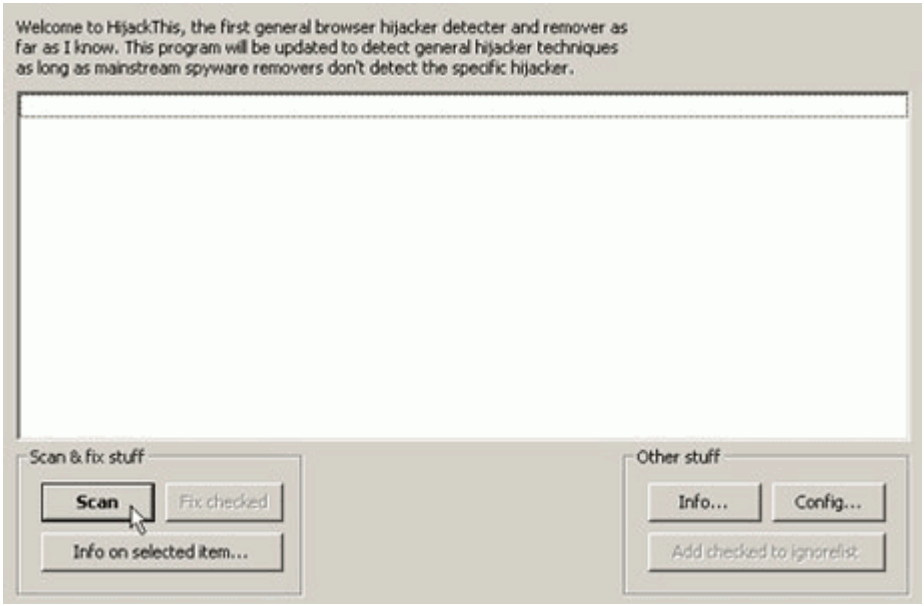
1. Im Taskmanager den Prozess sp.exe beenden
2. Die Datei sp.exe im Ordner C:\WINDOWS löschen

3. In der Registry unter
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run den Eintrag
'C:\WINDOWS\sp.exe' löschen
4. Bei Windows ME und Windows XP die Systemwiederherstellung deaktivieren
5. PC neu starten
6. Bei Windows ME und Windows XP die Systemwiederherstellung wieder aktivieren

Die Punkte 4 und 6 gelten nur bei den Betriebssystemen Windows ME und Windows XP. Bei allen anderen Windowsbetriebssystemen kann nach der Löschung des Registry-Schlüssels gleich der PC neugestartet werden.

Bei älteren Betriebssystemen, oder falls diese schnelle Version zu keinem Erfolg führt, hilft das kostenlose Tool **HijackThis**. Dieses Tool - ebenfalls entwickelt von 'Merijn' - ist auch auf der Seite www.spywareinfo.com zu bekommen. Mit HijackThis bekommt man auf einen Blick all das angezeigt, was auf dem Rechner automatisch gestartet wird (bzw. wurde) und mit ein bisschen Erfahrung sieht man schnell, was zum System gehört und was nicht.
Ein englischsprachiges **HijackThis Log Tutorial** auf der Seite http://www.merijn.org/htlogtutorial.html hilft bei der Identifizierung und Zuordnung der einzelnen Einträge weiter.

Wenn HijackThis als gezippte Datei heruntergeladen wurde, muss diese zunächst wieder entpackt werden. Für die Ausführung von HijackThis werden ebenfalls die Visual Basic 6 Runtime Libraries benötigt (Downloadmöglichkeit s. oben). Nach dem Starten von *HijackThis.exe* erscheint folgende Maske:



Hier auf **Scan** klicken.

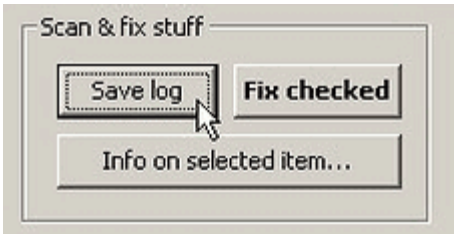
Ein solcher Scan enthält beispielsweise die folgenden Angaben:

```
Logfile of HijackThis v1.97.7
Scan saved at 13:38:20, on 30.12.2003
Platform: Windows XP (WinNT 5.01.2600)
MSIE: Internet Explorer v6.00 SP1 (6.00.2600.0000)

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
'
'

R0 - HKCU\Software\Microsoft\Internet Explorer\Main,Start Page = http://www.trojaner-info.de/
'
O2 - BHO: (no name) - {06849E9F-C8D7-4D59-B87D-784B7D6BE0B3} - g:\Programme\Adobe\Acrobat 5.
0\Acrobat\ActiveX\AcroIEHelper.ocx
'
O4 - HKLM\..\Run: [Disc Detector] C:\Programme\Creative\ShareDLL\CtNotify.exe
O4 - HKLM\..\Run: [Creative Launcher] C:\Programme\Creative\Launcher\CTLauncher.exe
O4 - HKLM\..\Run: [NeroCheck] C:\WINDOWS\system32\NeroCheck.exe
'
O8 - Extra context menu item: Open with GetRight Browser - C:\Programme\GetRight\GRbrowse.htm
O9 - Extra 'Tools' menuitem: Sun Java Console (HKLM)
O9 - Extra button: ICQ Pro (HKLM)
O9 - Extra 'Tools' menuitem: ICQ (HKLM)
O9 - Extra button: Recherche-Assistent (HKLM)
O9 - Extra button: Real.com (HKLM)
O12 - Plugin for .mp3: C:\Programme\Internet Explorer\PLUGINS\npqtplugin4.dll
O12 - Plugin for .spop: C:\Programme\Internet Explorer\Plugins\NPDocBox.dll
O16 - DPF: {41F17733-B041-4099-A042-B518BB6A408C} - http://a1540.g.akamai.net/7/1540/52/20021126/qtinstall
info.apple.com/dribnif/de/win/QuickTimeInstaller.exe
O16 - DPF: {D27CDB6E-AE6D-11CF-96B8-444553540000} (Shockwave Flash Object) - http://download.macromedia.co
pub/shockwave/cabs/flash/swflash.cab
```

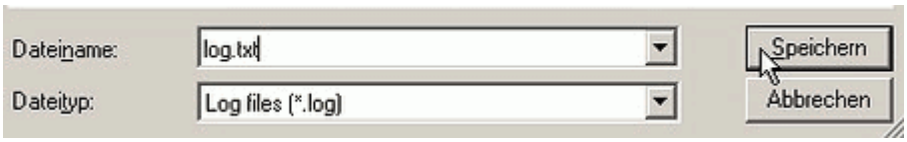
Anhand der Informationen aus dem **HijackThis Log Tutorial** (Link: siehe oben) können die Einträge herausgesucht und markiert (checked) werden, die für das Browser-Hijacking verantwortlich sind.
Über **Fix checked** werden die markierten Einträge gesäubert (fixed).
Für die hier beschriebene Form des Hijackings ist das beispielsweise der Eintrag **O4 - HKCU\..\Run: [sp] C:\WINDOWS\sp.exe**
Achtung: Vor dem 'fixen' müssen alle Browserfenster geschlossen sein!

Selbstverständlich erwarten wir nicht von jedem Anwender ein perfektes englisch, bzw. tiefergehende Erkenntnisse über die einzelnen Einträge von HijackThis. Wer sich nicht sicher ist, ob und wenn ja, welche Einträge zu reparieren sind, kann eine Log-Datei des Scans anlegen und in unser Support-Forum schreiben.

Nach Beendigung des Scans ändert sich der Button **Scan** automatisch auf **Save log**.



Die Logdatei kann z. B. unter dem Namen **log.txt** gespeichert



und mit dem Editor geöffnet werden. Mittels Copy&Paste (kopieren und einfügen) kann der Inhalt der Logdatei in die Forennachricht eingefügt werden.

Mittlerweile gibt es einige Removal-Tools, die darauf spezialisiert sind, diesen Hijacker von der Festplatte zu verbannen. Eines dieser Tools ist **SpoonWeg** von Multimedia Realisation Oberberg in Gummersbach.

SpoonWeg ist ein kleines, nur 9KB großes, in Assembler geschriebenes Tool, welches als erstes den aktiven Prozess **sp.exe** im System sucht, diesen -sofern vorhanden- beendet und den Pfad zum Aufruf in der Registry sucht. Anschließend wird die Datei sp.exe gelöscht (ein evtl. Schreibschutz der Datei wird aufgehoben) und der Registry-Key, welcher für den Aufruf der Datei sp.exe verantwortlich, entfernt.

Spoonweg kann hier kostenlos heruntergeladen werden:**http://mmrealisation.de.vu/**

Bei Anfragen in unserem Support-Forum bitte die folgenden Punkte beachten:

1. Bitte **j e d e r** in einem neuen, eigenen Thema schreiben. Wenn alles in einem Thema geschrieben wird, verliert jeder (Ratsuchender und Ratgeber) die Übersicht.
2. Bitte immer daran denken, dass alle Ratgebenden nur freiwillig und zeitweise im Forum anwesend sind. Auch wenn eine Antwort mal länger dauert, es wird niemand vergessen.
3. In anderen Themen suchen, ob schon Lösungsvorschläge zu finden sind.
4. Ruhe bewahren - Hektik schadet nur.

Weiterführende Links:
Virenticker von Trojaner-Info
Cleaner Tools und Programme von Trojaner-Info
Trojaner-Board - Das Forum zum Thema Trojaner
Windowsupdate
Spybot Search & Destroy
Ad-aware

alternative Browser
Mozilla
Mozilla Firebird
Opera

tschööö, DerBilk (Forenuser)

Vielen Dank an unseren Forenuser Lutz für diesen Artikel.

(tt) 02.01.2004

Trojaner-Info.de
Deutschlands große Security-Seite

Besuchen Sie uns auch im Internet unter: http://www.trojaner-info.de