Browser-Hijacker

Verhält sich der Internet Explorer merkwürdig, leitet bei URL-Vertippern auf Werbeseiten um und hat plötzlich neue Toolbars und Lesezeichen, hat man sich wahrscheinlich einen Browser-Hijacker eingefangen. So werden Sie die Plagegeister wieder los.

Wird der Internet-Nutzer beim Surfen ohne sein Zutun auf Werbeseiten entführt, spricht man von Browser-Hijacking. Eine Malware, der Browser-Hijacker, hat die Einstellungen so manipuliert, dass beliebige Seitenaufrufe, URL-Vertipper oder Suchanfragen auf Websites mit Werbung umgeleitet werden. Darüber hinaus werden regelmäßig Popups mit Werbung geöffnet, Links zu Werbeseiten auf den angezeigten Seiten eingeblendet und auch neue Toolbars, Buttons und Lesezeichen finden sich plötzlich im Browser.

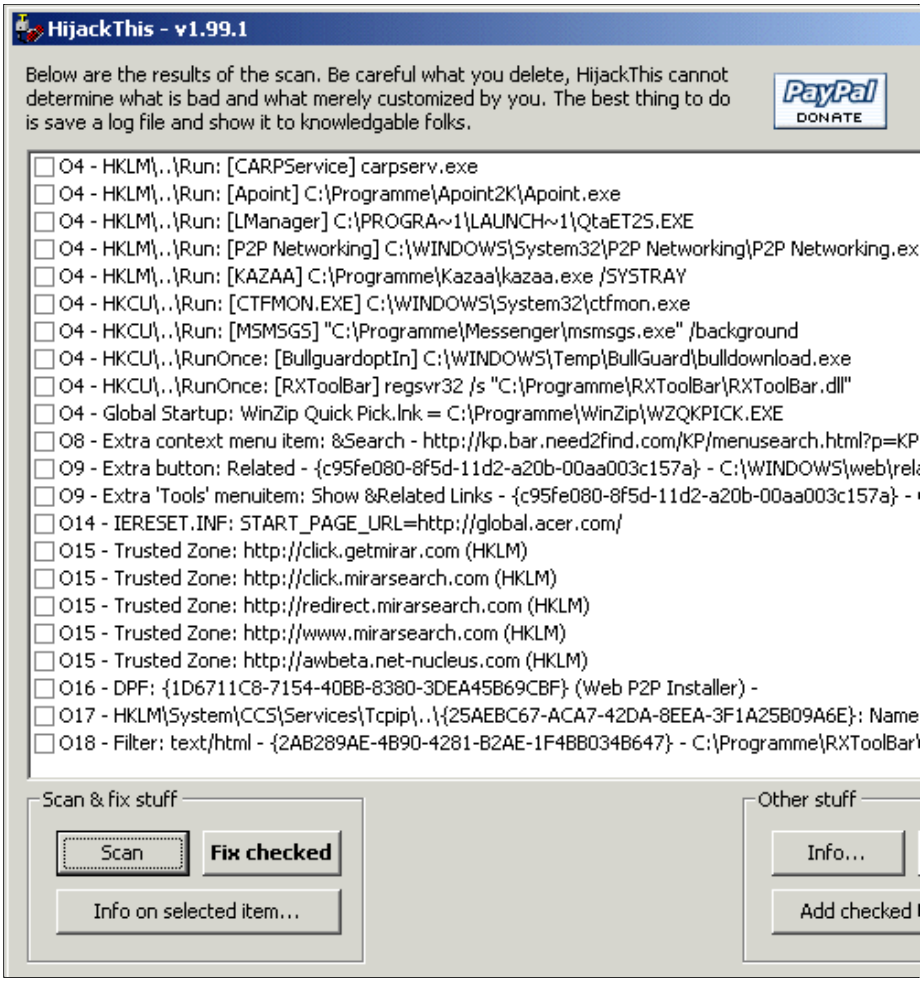
Betroffen ist in erster Linie der **Internet Explorer**, dem die Schadprogramme durch Sicherheitslücken oder niedrige Sicherheitseinstellungen unbemerkt untergeschoben werden können, zumeist mithilfe aktiver Inhalte wie Javascript und ActiveX. Zumindest prinzipiell ist Browser-Hijacking aber auch bei anderen Browsern möglich, denn die Hijacker gelangen nicht zwangsläufig über Websites auf den Rechner. Einige kommen huckepack mit einem vorgeblich nützlichen Programm, das sich der Anwender installiert, andere ganz profan via Mail. Ein Virenscanner auf dem PC, gesundes Misstrauen gegenüber unverlangt zugesandten Dateianhängen und unbekannten Gratisprogrammen sorgen ebenso wie das Deaktivieren von AciveX im Internet Explorer für einen gewissen Grundschutz.

Besser ist es allerdings, so weit wie möglich auf den Internet Explorer zu verzichten und auf alternative Browser wie Firefox und Opera umzusteigen. Diese werden von ungleich weniger Hijacker attackiert, und die Schadprogramme haben kaum eine Chance, sich unbemerkt einzunisten, und besitzen weit weniger Manipulationsmöglichkeiten.

Die Arbeit der Hijacker
Gelangt ein Browser-Hijacker auf den PC, ändert er in der Registry zahlreiche Werte, um das Verhalten des Internet Explorers seinen Wünschen anzupassen. Dazu zählen in den meisten Fällen die Schlüssel unter

HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main
HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Search
HKEY_LOCAL_MACHINE\Software\Microsoft\Internet Explorer\Main
HKEY_LOCAL_MACHINE\Software\Microsoft\Internet Explorer\Search

Hierüber werden die Start- und Suchseiten festgelegt. Ein weiterer Trick der Browser-Hijacker ist es, das Zonenkonzept des Internet Explorers auszuhebeln, indem eigene Seiten in der Zone **Vertrauenswürdige Sites** abgelegt werden. Sie können dann trotz restriktiver Sicherheitseinstellungen weiter Javascript und AcriveX ausführen.



Durch Einträge in der Datei **hosts** unter **C:\WINDOWS\system32\drivers\etc** manipuliert der Hijacker die Namensauflösung von URLs in IP-Adressen. In der Datei – eine einfache Textdatei, wenn auch ohne Endung – werden Host-Namen IP-Adressen zugeordnet. Bevor das System nach Eingabe einer Internet-Adresse den DNS-Server konsultiert, wird in der **hosts**-Datei nachgeschlagen. Hat der Hijacker dort nun beispielsweise **www.google.com** die IP eines eigenen Servers zugeordnet, landet der Anwender bei diesem, statt auf den Google-Seiten.

Auch so genannte **Browser Helper Objects** (BHO) werden von den Hijackern genutzt, um auf eigene Seiten umzuleiten, das Verhalten des Benutzers aufzuzeichnen und Formulardaten wie Kreditkartennummern oder Passwörter abzufangen. Eigentlich sind BHO nützliche kleine Programme, die den Funktionsumfang des Internet Explorers erweitern. Sie machen es erst möglich, dass der Browser beispielsweise PDF-Dokumente anzeigen kann und sich mit Toolbars erweitern lässt.

Oft bringen Browser-Hijacker eine Trojaner-Komponente mit, die beim Windows-Start automatisch geladen wird und alle Änderungen erneut vornimmt, falls der Anwender einige Einstellungen zurückgesetzt haben sollte.

Systembereinigung
Einen Browser-Hijacker wieder loszuwerden, ist nicht ganz einfach. Schließlich lässt er sich nicht bequem über die Systemsteuerung deinstallieren. Erste Hilfe bieten bereits Tools wie Ad-Aware und Spybot Search & Destroy, die auf Adware und Spyware spezialisiert sind und auch viele Browser-Hijacker aufspüren. Hartnäckige Hijacker lassen sich allerdings nur mit HijackThis entdecken.

HijackThis stammt vom holländischen Entwickler Merijn Bellekom und wurde kürzlich von Trend Micro übernommen. Das Programm kann direkt nach dem Entpacken ohne Installation gestartet werden. Taucht eine Fehlermeldung wegen fehlender DLLs auf, werden noch die Visual Basic Runtime Libraries benötigt. Verhindert eine Malware den Programmstart, benennen Sie einfach die EXE- in eine COM-Datei mit beliebigem Namen um, etwa **scan.com**.

Läuft HijackThis, starten Sie mit **Do a system scan and save a logfile** die Analyse ihres Systems. Das Tool listet anschließend verschiedene Systeminformationen auf, darunter auch Angaben zu Browser-Einstellungen, Schadprogrammen, installierten Toolbars, Plugins und BHOs. Nicht benötigte oder gefährliche Komponenten

können dann per Checkbox ausgewählt und mit einem Klick auf **Fix Checked** beseitigt werden. Nähere Informationen zu den einzelnen Einträgen liefert der Button **Info on selected item...**.

Wird ein Objekt versehentlich gelöscht, kann es über die Backup-Funktion wiederhergestellt werden. Empfehlenswert ist es, sich vor dem Löschen online ein paar Informationen zu besorgen. So kann unter hijackthis.de das Logfile hochgeladen und eine einfache, automatische Auswertung erstellt werden, welche Objekte sicher sind und welche nicht.

Detailliertere Informationen liefern die User des HijackThis-Forums, in das Sie die Scan-Ergebnisse einstellen können. Zudem können Sie die in der HijackThis-Auswertung aufgeführten 36stelligen GUIDs (Globally Unique Identifier) Online nachschlagen und auf diese Weise feststellen, ob ein Eintrag einer Spyware oder einem erwünschten Programm zuzuordnen ist.

Mehr Sicherheit mit Vista
Wer den Internet Explorer 7 unter Windows Vista nutzt, kann in den **Geschützten Modus** wechseln. Der Browser hat dann lediglich Schreibrechte für das Verzeichnis mit den temporären Internetdateien, auf andere Verzeichnisse und die Registry kann er nicht zugreifen. Fängt man sich einen Browser-Hijacker ein, kann der Browser einfach zurückgesetzt werden. Dabei gehen zwar auch Cookies und History verloren, aber die Malware wird zuverlässig entfernt. Gegen Hijacker, die Sie sich aufs System holen, indem Sie etwa eine Toolbar aus zweifelhafter Quelle installieren, hilft allerdings auch der **Geschützte Modus** nicht. (tm)

Erstveröffentlichung 20.06.2007

Über Daniel Dubsky

Freier Journalist für Computer-und Internet-Themen. Schrieb unter anderem für verschiedene gedruckte Fachzeitschriften. Website. Weitere Beiträge für Dr. Web: 14

Verwandte Artikel

Bitte beachten Sie: Werbung und Spam sind unerwünscht und können eine Rechnung zur Folge haben. Woher kommen die Bilder neben den Kommentaren?