Dieser Service wird Ihnen bereitgestellt durch:

http://www.trojaner-info.de

Internet Explorer: Unerwünschte Startseite real-yellow-page.com - Anleitung zur Entfernung

Browser-Hijacker sind zur Zeit so etwas wie die 'neue Pest' im Internet. Wir berichteten bereits Anfang des Jahres darüber und auch diverse Foren zum Thema Internet-Sicherheit laufen über mit Anfragen verzweifelter Anwender, die sich auf ihrem PC einen der zahlreichen Hijacker eingefangen haben.

Einer der zähesten Vertreter dieser Browser-Hijacker ist die **real-yellow-page**-Variante. Lt. cwchronicles - *englischsprachiger Link*- handelt es sich hierbei bereits um die 39. Variante von CoolWebSearch! Erstmals bekannt geworden ist diese Variante am 16. März 2004 und lässt sich aufgrund seiner Komplexität zur Zeit weder mit dem CWShredder dauerhaft entfernen, noch können die entsprechenden Veränderungen in einem Log von HijackThis angezeigt werden. Die Seiten des Internet Explorers werden nach **real-yellow-page.com**, **drxcount.biz**, **list2004.com** oder **linklist.cc** umgeleitet. Da diese Variante jedoch des öfteren im Zusammenspiel mit der Searchx-Variante beobachtet wird, sollte der CWShredder dennoch unbedingt eingesetzt werden (dazu später mehr).

Auf der Suche nach einer dauerhaften Entfernung dieses Hijackers hat sich folgende Vorgehensweise als erfolgreich herausgestellt. **Bitte die folgenden Schritte genau in der aufgeführten Reihenfolge durchführen, da ansonsten eine dauerhafte Entfernung nicht möglich ist. Wir empfehlen dringend, sich vor Beginn der Entfernung diese Seite auszudrucken!**

Schritt 1:
Download der erforderlichen Tools
Achtung: Es handelt sich jeweils um direkte Download-Links!

- Prozess-Viewer von zerosrealm.com erforderlich für Schritt 3
- TheKillbox erforderlich für Schritt 5
- CWShredder erforderlich für Schritt 6
- IEFIX.reg für Schritt 11
- HijackThis für eine abschließende Kontrolle (Schritt 13)

Schritt 2:

nur bei Windows ME und Windows XP!
Schließe alle Anwendungen und deaktiviere die Systemwiederherstellung.
Fahre den Rechner herunter und starte ihn neu.
Aktiviere (bei Bedarf) die Systemwiederherstellung.
Erläuterung zur Systemwiederherstellung

Schritt 3:
Entpacke die gezippte Datei "**pv.zip**" auf dem Desktop (der Prozess-Viewer funktioniert nicht, wenn er direkt aus der ZIP-Datei gestartet wird).Nach dem Entpacken gehe auf den Desktop und öffne den neu erstellten Ordner **pv**.

Starte aus diesem Ordner die Datei **runme.bat** (unter Win2000 bzw. WinXP), bzw. die Datei **runme9x.bat** (unter Win95-, Win98- oder WinME) mit einem Doppelklick. Es öffnet sich ein DOS-Fenster.
Wähle Option 1 für **explorer dll's** (Drücke 1 und anschließend [Enter]).
Es öffnet sich ein Notepad-Fenster mit einer Vielzahl an Informationen über laufende Prozesse und dergleichen.

Schritt 4:
Win2000 bzw. WinXP
Klicke auf "**Format**" und vergewissere Dich, das die Option "**Zeilenumbruch**" **nicht aktiviert** ist. Klicke auf "**Bearbeiten**" und dann auf "**Suchen**"

Windows 95, 98 und ME
Notepad unter Windows9x kennt die Option "Zeilenumbruch" nicht. Dieser Schritt entfällt bei einem solchen System.
Außerdem wird die Suche hier unter "**Suchen**" und dann erneut "**Suchen**" gestartet.

Gib in der Suche folgenden Wert ein: **61c00000 61440** und klicke anschließend auf "**Weitersuchen**".
Wenn die hier behandelte Version von CWS gefunden wurde, erhältst Du ein Ergebnis welches dem folgenden ähnelt:
"**logignh.dll 61c00000 61440 c:\windows\system32\logignh.dll**".
Achtung: Der Dateiname ist bei jeder Infektion ein anderer (loginh.dll ist nur ein Beispiel von vielen möglichen!). Dieser Umstand macht auch die Suche und die Entfernung des Hijacks so schwierig. Konstant bei allen Infektionen mit dieser HiJack-Variante ist allerdings der Wert: **61c00000 61440**.

Schritt 5:
Entpacke die Datei "**Killbox.exe**" in einen eigenen Ordner und starte sie mit einem Doppelklick.
In der Eingabebox "**Paste Full Path of File to Delete**" trage den unter Schritt 4 gefundenen Dateipfad ein (im obigen

Beispiel wäre das: c:\windows\system32\logignh.dll)
Bitte beachte, dass Du den bei Dir gefundenen Namen der dll einträgst und nicht den aus diesem Beispiel!
Klicke auf keinen der vorhandenen Buttons, sondern klicke in der Menü-Leiste (oben) auf "**Action**" und wähle den Eintrag "**Delete on Reboot**".
In dem sich nun öffnenden Fenster klicke auf das "**File**"-Menü und wähle "**Add File**" aus.
Der von Dir ausgewählte Dateiname inclusive vollständigem Pfad sollte nun angezeigt werden. Wenn dieser Schritt erfolgreich war, wähle in diesem Fenster das "**Action**"-Menü und dort "**Process and Reboot**". Du wirst nun aufgefordert Deinen Rechner neu zu booten. Führe diesen Schritt aus.

Schritt 6:
Wenn der Rechner neu gestartet ist, starte die neueste Version von CWShredder
Achtung: Es dürfen bei der Ausführung des CWShredders keine anderen Programme gestartet sein, ansonsten schlägt die Bereinigung unter Umständen fehl.

Schritt 7: **Nur bei Win95, Win98 bzw. WinME**
Boote Deinen Rechner neu im abgesicherten Modus.
Starte den **Registry-Editor**. "Start" -> "Ausführen" -> **regedit** eingeben und mit [Enter] bestätigen.
Erstelle zur Sicherheit zunächst ein Backup über das Menü "Registrierung" -> "Registrationsdatei exportieren" "Exportbereich Alles" und gebe einen freigewählten Dateinamen an. Speicher die Exportdatei an einem Ort, wo Du ihn bei Bedarf leicht wieder findest.
Gehe zum Pfad HKEY_LOCAL_MACHINE -> Software -> Microsoft -> Windows -> CurrentVersion -> RunServicesOnce
Wenn Du hier einen Eintrag mit der im Schritt 4 ermittelten dll findest lösche diesen.
Bei Win95, Win98 bzw. WinME-Systemen weiter mit Schritt 11!

Schritt 8: **Nur bei Win2000 bzw. WinXP**
Starte die **runme.bat** erneut. Jetzt wählst Du Option 6 für **"Appinit Contents"**. Notepad wird mit einer Log-Datei geöffnet. Die uns interessierende Zeile lautet:"**AppInit_DLLs"=" "**.
Achtung: Es können gültige und wichtige Dateien hier eingetragen sein. Wenn nur die unter Schritt 4 gefundene Datei angezeigt wird gehe weiter zu Schritt 9.
Wenn Du Dir an dieser Stelle unsicher bist, solltest Du den Inhalt dieser Log-Datei zunächst in einem aussagekräftigen Thread in unserem Forum posten und warten bis Dir einer der Experten weiterhilft.

Schritt 9: **Nur bei Win2000 bzw. WinXP**

Starte die Datei **runme.bat** ein weiteres Mal und wähle Option 7 für "**Appinit Clean**".

Schritt 10: **Nur bei Win2000 bzw. WinXP**
Starte die Datei **runme.bat** ein weiteres Mal und wähle erneut Option 6 für "**Appinit Contents**". Notepad öffnet sich erneut mit einer Log-Datei. Die Zeile **"AppInit_DLLs"=" "** sollte nun leer sein, bzw. nur gültige (erforderliche) Einträge enthalten. Die in Schritt 4 ermittelte dll darf jetzt nicht mehr im Log erscheinen.

Schritt 11:
Mit einem Doppelklick auf die Datei "**IEFIX.reg**" stellst Du die Startseite, Suchseite, etc. auf die Standard-Werte von Microsoft zurück.
Achtung: Lass diesen Schritt nicht aus, auch nicht, wenn Du eine andere Seite als Startseite eingetragen haben willst. Diese kannst Du zu einem späteren Zeitpunkt wieder einstellen.

Schritt 12:
Starte Deinen Rechner noch einmal neu.

Schritt 13:
Mach zum Abschluss eine Kontrolle mit HijackThis. Bei der Überprüfung der gefundenen Einträge kannst Du diese Anleitung zu Hilfe nehmen. Wenn Du Probleme bei der 'Entschlüsselung' des einen oder anderen Eintrags hast, kannst Du die Log-Datei von HijackThis in unserem Forum posten. Bitte erstelle einen **eigenen Thread** und stelle Deine Log-Datei nicht in einen bereits bestehenden Thread. Es ist sehr schwierig Hilfestellungen zu geben, wenn sich in einem Thread Logdateien von verschiedenen Rechnern befinden.

Zum Zeitpunkt dieses Berichts ist die für diese Form des Browser Hijackers verantwortliche Lücke des Internet Explorers von Microsoft noch nicht geschlossen. Eine Re-Infektion ist also jederzeit möglich. Deshalb und auch weil weitere bekannte Lücken des Internet-Explorers bisher ungepatcht sind , wird der Umstieg auf einen alternativen Browser dringend empfohlen.
Mozilla,
Mozilla Firefox oder
Opera
bieten mindestens den gleichen Surfkomfort wie der Internet Explorer bei einem Mehr an Sicherheit.
Ein regelmäßiges Windowsupdate ist zusätzlich unerläßlich.

---

*Ich bedanke mich ganz ausdrücklich bei **paff** und **raman**. Beide sind u.a. auch Mitglieder des Trojaner-Boards und haben mir mit ihrer intensiven Aufklärung im Board von Rokop-Security und im Protectus Securityforum diese Übersetzung der englischen Anleitung erst ermöglicht!*

, 30.04.04
