DIETMAR **W**ALKER - **P**C-**B**LITZHELFER-**N**OTDIENST
Nationalgasse 14 • **7**2124 **P**liezhausen • ∅ **T**el. 07127 / 89194 - **F**ax 89118
Internet: http://www.pc-blitzhelfer.de – **M**obil 0172-882 79 55

Anleitung zur manuellen Entfernung von PUPs

n diesem Beitrag widmen wir uns einer sehr häufig vorkommenden Malware-Kategorie: potenziell unerwünschte Programme (kurz PUPs).

Was ist ein potenziell unerwünschtes Programm?

Bevor wir erläutern, wie Sie PUPs richtig entfernen, sei zunächst erst einmal erklärt, was das überhaupt ist – und was nicht. Unsere Emsisoft-Experten werden regelmäßig gefragt, weshalb bestimmte Anwendungen nicht als PUP erkannt werden.

Schauen wir uns beispielsweise Symbolleisten, Browser-Plug-ins oder PC-Optimierungsprogramme an. Auch wenn sich über die Nützlichkeit derartiger Anwendungen streiten lässt, ist keine von ihnen von Grund auf bösartig oder unerwünscht. „Unerwünscht“ werden sie erst, wenn sie auf unlautere oder betrügerische Weise verbreitet werden oder sogar falsche oder irreführende Informationen anzeigen.

Auf alle Einzelheiten und Unterschiede einzugehen, würde den Rahmen dieses Artikels sprengen. Wir werden uns jedoch in unserem Webinar zur manuellen PUP-Entfernung näher damit befassen. Weitere Informationen hierzu finden Sie am Ende des Artikels.

Umgang mit hartnäckigen PUPs

Damit sind wir auch schon beim ersten Schritt zur manuellen Entfernung von PUPs angekommen. Bevor Sie irgendwelche anderen Maßnahmen ergreifen, deinstallieren Sie zunächst alle unerwünschten Programme über das Menü „Programme und Features“. Um es unabhängig von Ihrer Windows-Version aufzurufen, drücken Sie gleichzeitig die Windows-Taste und R. Geben Sie dann in das Textfeld des Ausführen-Dialogs **appwiz.cpl** ein und drücken Sie die Eingabetaste. Überprüfen Sie bei unbekannten Einträgen unbedingt, ob sie in der Tat unerwünscht sind und/oder zu einem PUP gehören.

Mitunter kann es jedoch vorkommen, dass selbst nach der Deinstallation des unerwünschten Programms noch nervige Probleme auftreten. Natürlich können wir wieder auf die Hilfsmittel zurückgreifen, die wir in unserem letzten Artikel eingesetzt haben. Bei PUPs ist es aber in der Regel einfacher, sich einen Überblick zu verschaffen, was genau von dem Problem betroffen ist. Tauchen nervige Werbe-Popups beispielsweise in Ihrem Browser auf, müssen Sie in anderen Bereichen suchen, als wenn sie in der Windows-Taskleiste oder im Infobereich angezeigt werden. Bei Browser-Problemen lässt sich das Ganze schnell weiter eingrenzen, indem Sie prüfen, ob alle Browser betroffen sind oder nur ein bestimmter.

Zusammenfassung zum Umgang mit PUPs:

1. Bevor Sie sich überhaupt um die PUPs kümmern, überprüfen Sie den Computer zunächst auf echte Schädlinge. Das hat immer Vorrang. Schließlich sind Werbe-Popups zwar nervig, aber nicht so gefährlich wie Malware, die Ihre Kennwörter stiehlt.
2. Gehen Sie die im Menü „Programme und Features“ aufgelisteten Programme durch und deinstallieren Sie unerwünschte Anwendungen. Das mag selbstverständlich klingen, doch viele Anwender vergessen diesen Schritt.

3. Beobachten Sie, welche Probleme danach eventuell weiterhin bestehen und kategorisieren Sie diese nach den betroffenen Anwendungen (z. B. Browser, Windows-Meldungen, Suchergebnisse, usw.)
4. Grenzen Sie das Problem für jede der erkannten Komponenten so weit wie möglich ein.

Beispiel eines typischen PUPs

Stellen Sie sich vor, Sie öffnen einen neuen Tab in Ihrem bevorzugten Browser. Allerdings wird nicht die Seite geöffnet, die Sie in Ihren Browser-Einstellungen festgelegt haben, sondern eine ganz andere. Darüber hinaus wird beim Suchen plötzlich auch noch eine ganz andere Suchmaschine verwendet. Und obwohl Sie die Einstellungen in Ihrem Browser immer wieder ändern, bleibt das Problem weiterhin bestehen.

Das ist zwar kein klarer Beweis für ein PUP, aber hier läuft eindeutig etwas anders, als es soll. Also in die Hände gespuckt zur manuellen PUP-Entfernung.

Lassen Sie uns für diese Erläuterungen bei dem oben genannten Beispiel bleiben. Es wurde keine Malware gefunden, es scheinen keine PUP installiert zu sein und die Browser-Einstellungen sehen auch normal aus. Wir erklären Ihnen die nächsten Schritte mit zwei beliebten Browsern: Google Chrome und Mozilla Firefox. Dafür benötigen wir auch keine speziellen Hilfsmittel. Ein gutes Hintergrundwissen zum Recherchieren im Internet und etwas Geduld reichen vollkommen aus.

Hinweis: Die Screenshots sind zwar auf Englisch, in den Erklärungen werden jedoch die Bezeichnungen der deutschen Benutzeroberflächen verwendet.

„Neuer Tab“ entfernen

Im folgenden Bild können Sie sehen, dass der Browser beim Öffnen eines neuen Tabs die Emsisoft-Website laden soll. Das tut er jedoch nicht. Stattdessen wird „Neuer Tab“ (Newtab) geladen. Auch wenn das in unserem Beispiel nicht schädlich ist, ist es doch eine Form von Browser-Manipulation.

Wenn wir online nach „Neuer Tab“ suchen, werden uns etliche Anleitungen zum Entfernen angezeigt. Viele davon sind jedoch eher Anweisungen zum Ausführen automatisierter Tools, ohne dass auf eine manuelle Entfernung eingegangen wird.

Schauen wir uns nun die Sucheinstellungen an (diesmal in Firefox, wobei es aber in Chrome ähnlich aussieht). Dort stellen wir interessanterweise fest, dass die Standardsuchmaschine (Default Search Engine) von der Erweiterung „FullTab“ verwaltet wird.

Natürlich können wir jetzt schlicht die Suchmaschine ändern und es dabei bleiben lassen. Es ist dennoch sinnvoll, die offensichtlich verantwortliche Erweiterung zu entfernen. In den meisten Browsern gibt es eine Übersicht, wo Sie die Erweiterungen verwalten können. Einige Exemplare nutzen jedoch Techniken, um sich zu verstecken oder vor Änderungen zu schützen. Daher sollten Sie sich gut informieren, wie Ihr Browser Erweiterungen verwaltet und wo diese und ihre zugehörigen Einstellungen gespeichert sind. Wie bereits erwähnt, nutzen wir für das Beispiel nur zwei Browser. Diese Informationen sind jedoch auch für nahezu alle anderen Browser verfügbar.

Wo verstecken sich die Erweiterungen?

Sowohl Mozilla Firefox als auch Google Chrome stellen Entwicklern eine ausführliche Dokumentation mit Erläuterungen bereit, wie Erweiterungen geladen werden können. Diese sind für jeden mit guten Recherchefähigkeiten schnell im Internet zu finden. In unserem Beispiel fanden wir für jeden Browser Folgendes:

- Chrome-Dokumentation für Erweiterungen (auf Englisch)
- Firefox-Dokumentation für Erweiterungen

Nachdem wir diese beiden Artikel gelesen haben, müssen wir also kurz gesagt Folgendes überprüfen:

Chrome

- %LOCALAPPDATA%\Google\Chrome\User Data\Default\Extensions\<Erweiterungs-ID>
  (Jeder Erweiterung ist eine ID aus 32 Zeichen zugewiesen.
- HKEY_LOCAL_MACHINE\SOFTWARE\Google\Chrome\Extensions\<Erweiterungs-ID>
- HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Google\Chrome\Extensions\<Erweiterungs-ID>
  (für 32-Bit-Browsers auf 64-Bit-Versionen von Windows)

Firefox

- %APPDATA%\Mozilla\Firefox\Profiles\<Profilordner>\extensions\{<Erweiterungs-ID>}.xpi
- %APPDATA%\Mozilla\Extensions\{<Erweiterungs-ID>}.xpi
- HKEY_CURRENT_USER\Software\Mozilla\Firefox\Extensions
- HKEY_LOCAL_MACHINE\SOFTWARE\Mozilla\Firefox\Extensions

Hinweis:
%APPDATA% bezieht sich auf den Pfad C:\Benutzer\<Benutzername>\AppData\Roaming.
%LOCALAPPDATA% bezieht sich auf den Pfad C:\Benutzer\<Benutzername>\AppData\Local.
„Default" ist der Name des zuerst registrierten Chrome-Profils. Zusätzliche Profile haben einen anderen Ordnernamen.

Jetzt haben wir alle Speicherorte, an denen sich eine unerwünschte Erweiterung verstecken könnte. Schauen wir doch einmal, ob wir sie finden und entfernen können. Dazu müssen wir zunächst wissen, wie die Erweiterungs-ID lautet. (Die Erweiterung hat in jedem Browser eine andere ID.)

Geben Sie in Google Chrome in die Adressleiste „chrome://extensions" ein und drücken Sie die Eingabetaste. Jetzt wird eine Liste mit den installierten Erweiterungen geöffnet. Wenn Sie bei den einzelnen Einträgen auf die Option „Details" klicken, wird in der Adressleiste die jeweilige Erweiterungs-ID angezeigt.

Achten Sie dabei auf die für die Erweiterung angezeigten Berechtigungen (Permissions). In unserem Fall passen Sie genau zu den zuvor beschriebenen Problemen: Ändern der Seite beim Öffnen eines neuen Tabs (2. Punkt) sowie der Sucheinstellungen (4. Punkt).

Geben Sie in Mozilla Firefox in die Adressleiste**about:debugging#addons** ein und drücken Sie die Eingabetaste. Die gesuchte Erweiterung wird mit in der Liste angezeigt.

Wir müssen jetzt also nach folgenden Objekten suchen:

- **Oimkbkfjcjimpcamagdlepipkapmbjie** an den Speicherorten, die wir zuvor für die Erweiterungen in Google Chrome recherchiert haben.
- **{125f5269-2f69-401e-b072-40be97188078}** an den Speicherorten, die wir zuvor für die Erweiterungen in Mozilla Firefox recherchiert haben.

In unserem Fall finden wir die Erweiterung an folgenden Speicherorten:

Diese Objekte können leicht gelöscht werden. Damit sind wir aber noch nicht fertig. Firefox und Chrome nutzen beide eine Einstellungsdatei, in der auf die installierten Erweiterungen verwiesen wird. Hinweis: Legen Sie am besten immer eine Sicherung an, bevor Sie irgendwelche Objekte entfernen (falls doch einmal ein Fehler passiert).

Verweise bereinigen

Aus technischer Sicht wird in unserem Beispiel nichts weiter passieren, wenn die Browser-Verweise auf diese Erweiterung nicht entfernt werden. Die bessere Vorgehensweise ist auf jeden Fall, sie dennoch zu löschen.

In Google Chrome werden die Einstellungen in **%LOCALAPPDATA%\Google\Chrome\User Data\Default\Preferences** gespeichert (es handelt sich um eine Textdatei mit JSON-Markup).

In Mozilla Firefox werden die Einstellungen in **%APPDATA%\Mozilla\Firefox\Profiles\<Profilordner>\Prefs.js** gespeichert.

Sie können die beiden Dateien zwar mit einem Texteditor öffnen, allerdings ist das Entfernen von Verweisen auf diese Weise recht fehleranfällig. Sie müssen dann nämlich unter anderem sicherstellen, dass Sie das richtige Format einhalten. Selbst ein kleiner Fehler hierbei kann zu einer Beschädigung des Browser-Profils führen. Zum Glück gibt es andere Möglichkeiten – vom Ignorieren der Überbleibsel und Zurücksetzen der Browser-Einstellungen auf ihre Standardwerte einmal abgesehen.

Firefox

Bei Firefox können Sie sich die Variablen der Prefs.js und die Anwendungseinstellungen bequem direkt im Browser anzeigen lassen, um sie zu ändern. Geben Sie dazu in die Adressleiste **about:config** ein und drücken Sie die Eingabetaste. Suchen wir nun nach der Erweiterungs-ID für unser Beispiel. Das Ergebnis sieht wie folgt aus:

Wie Sie sehen können, kommt die Erweiterungs-ID in zwei Variablen vor. Nun haben wir zwei Möglichkeiten: Wir bearbeiten die Variable (siehe Abbildung), indem wir einen Rechtsklick darauf machen und **Bearbeiten** wählen. Wir können die Variable auch einfach zurücksetzen, indem wir ebenfalls einen Rechtsklick darauf machen und **Zurücksetzen** wählen. Die zweite Option ist auf jeden Fall die sicherste. Sollte Ihr Browser viele Erweiterungen oder benutzerdefinierte Änderungen haben,

kann die Erste jedoch ratsamer sein, da anderenfalls die gesamte Variable mit all ihren Daten zurückgesetzt wird (unbedingt auf die richtige Datensyntax achten).

Chrome

Chrome bietet keine Möglichkeit zur Konfiguration. Hier müssen wir die betroffene Einstellung manuell über die Optionen chrome://settings und chrome://extensions anpassen. In unserem Beispiel gibt es unter „Erweiterungen“ immer noch Reste. Um sicherzustellen, dass Sie alle Spuren der Erweiterung entfernt haben, können Sie die Preferences-Datei anschließend in einem Texteditor öffnen und mit Strg+F nach der Erweiterungs-ID suchen. Wenn alles in Ordnung ist, sollte Ihnen eine Fehlermeldung angezeigt werden, dass der Text nicht gefunden werden konnte (siehe Abbildung).

Anmerkung: Für das Beispiel wurde Editor verwendet. Wir empfehlen jedoch die Nutzung eines vielseitigeren Texteditors.

Damit wurden alle Verweise bereinigt. Sollte es immer noch einen geben, überprüfen Sie, in welcher Variable er sich befindet. Wenn Sie nicht direkt in der Preferences-Datei arbeiten möchten, recherchieren Sie im Internet, um herauszufinden, wie Sie die Variable ändern können.
Diese abschließende Überprüfung können Sie natürlich auch mit der Prefs.js von Firefox vornehmen.

Hinweis: *Gehen Sie beim direkten Bearbeiten von Einstellungsdateien extrem vorsichtig vor. Speichern Sie außerdem immer eine Kopie der Originaldatei als Sicherung an einem anderen Ort, bevor Sie irgendwelche Änderungen vornehmen.*

Informationen auf andere PUPs anwenden

Dies ist nur ein Beispiel, wie Sie eine PUP-Komponente manuell und ohne zusätzliche Hilfsmittel entfernen können. Tools können Ihnen die Arbeit erleichtern. Dennoch ist es immer gut, die zugrunde liegenden Mechanismen zu verstehen. Um bei unserem Beispiel zu bleiben: Ein Protokollierungstool kann uns zwar eine Reihe von Browser-Einstellungen anzeigen, wir wissen aber immer noch nicht, wo genau sich diese befinden. Anfangs kann diese Herangehensweise etwas länger dauern, da auch einiges an Recherche erforderlich ist. Wenn Sie jedoch erst einmal wissen, wie ein Browser Erweiterungen verwaltet, haben Sie die Information beim nächsten Mal schnell wieder griffbereit. Dieses Vorgehen lässt sich auch auf andere häufig verwendete PUP-Komponenten anwenden, etwa bei Windows-Aufgaben, der Umleitung von Verknüpfungen oder der Änderung von Browser-Richtlinien.

Haftungsausschluss: Dieser Artikel und das Webinar dienen allein zu Präsentationszwecken. Es gibt die unterschiedlichsten PUP-Varianten und für viele von ihnen ist je nach Einsatzzweck ein anderer als der hier beschriebene Ansatz zum Entfernen erforderlich. Uns ist durchaus bewusst, dass es für jede Regel eine Ausnahme gibt und die Situation wesentlich komplexer ausfallen kann. Auf all diese Ausnahmen einzugehen, wäre jedoch nicht im Sinne dieses Blogartikels. Sollten Sie beim Entfernen von Malware Unterstützung benötigen, laden Sie sich gern unser kostenloses Emsisoft Emergency Kit herunter oder wenden Sie sich an unsere Malware-Analytiker unter support@emsisoft.com.

Wir wünschen eine schöne (Malware-freie) Zeit.

Quelle: https://blog.emsisoft.com/de/31499/anleitung-zur-manuellen-entfernung-von-pups/?ref=newsbox_ticker180618&utm_source=newsbox&utm_medium=software&utm_content=ticker180618&utm_campaign=ticker180618