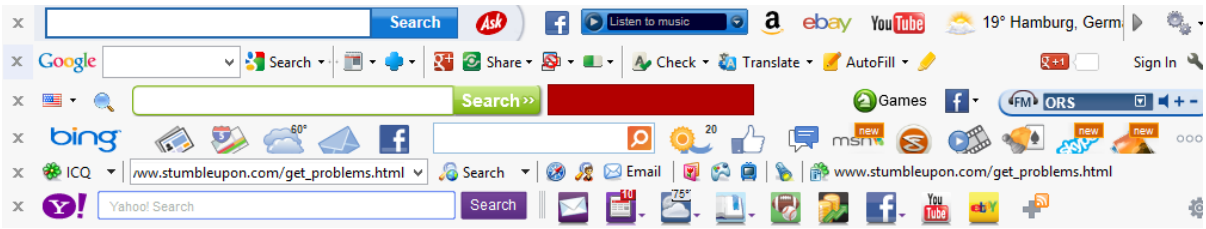
DIETMAR WALKER - PC-BLITZHELFER-NOTDIENST
Nationalgasse 14 • 72124 Pliezhausen • ∅ Tel. 07127 / 89194 - Fax 89118
Internet: http://www.pc-blitzhelfer.de – Mobil 0172-882 79 55

Ist der Antiviren-Sektor nicht mehr ganz bei Trost?!

Wir beobachten einen Besorgnis erregenden Trend, der langsam außer Kontrolle gerät: Potenziell unerwünschte Programme (PUPs) sind weiterhin auf dem Vormarsch. Was jedoch noch Besorgnis erregender ist: *wie* die Verbreitung vonstatten geht. Seit große Anbieter wie Oracle (Java) und Microsoft (Bing und Skype) damit begonnen haben, ihre Software im Paket mit anderer Software zu verkaufen, sind jetzt Antiviren-Softwarenanbieter jetzt auf diesen Zug aufgesprungen. Wir haben Recherchen zu den häufigsten Vorgehensweisen mit PUPs unter Freeware-Antiviren-Softwareanbietern angestellt, und die Ergebnisse sind recht verstörend.

PUPs sollen sich auf Ihren PC einschleichen, damit man mit Ihnen Geld verdienen kann.

Zunächst fassen wir einmal kurz zusammen, was PUPs sind und warum sie sich wie ein Lauffeuer verbreiten. PUPs sind Programme, die sich als **Toolbars, Adware, Plug-ins oder andere Downloads präsentieren und sich auf Ihrem PC einnisten.** PUPs gelten (noch?) nicht als Malware, da sie nicht immer eine Gefahr darstellen, aber recht häufig nervtötend sind, daher auch der Name "potenziell unerwünscht". Dennoch werden PUPs immer unerwünschter denn je: allein die Tatsache, dass Sie keine Ahnung davon haben, dass das, was Sie installieren, unerwünscht ist. Falls Sie urplötzlich Veränderungen an der Arbeitsgeschwindigkeit Ihres Computers, an der Suchmaschine in Ihrem Browser, nervige Pop-up-Werbeanzeigen, neue Toolbars in Ihrem Browser-Menüleiste oder anderweitige Veränderungen im Verhalten Ihres Computers oder seines Aufbaus bemerken, besteht eine sehr große Wahrscheinlichkeit, dass auf Ihrem PC ein oder mehrere PUPs installiert wurden.



PUPs präsentieren sich in vielerlei Formen und Arten, aber alle haben sie ein paar Dinge gemeinsam:

- **PUPs möchten mit Ihrer Hilfe Geld verdienen**. PUPs sollen sich aus einem Grund auf Ihren PC einschleichen: damit man mit Ihnen Geld verdienen kann. Die häufigste Art und Weise ist durch Hijacking Ihres Browsers: dann können Ihnen Werbeanzeigen gezeigt werden, aus Ihnen Kapital geschlagen werden oder Ihre Suchergebnisse und/oder Ihr Surfverhalten verkauft werden oder gar Ihre Homepage verändert werden.
- **PUPs setzen auf aggressive Verteilungsmethoden, um sich auf Ihrem PC einzunisten:** "einschleichen" im wahrsten Sinne des Wortes, da Sie in den meisten Fällen nicht dessen bewusst sind, dass ein PUP installiert wird.
- **Die meisten PUPs haben keinen echten Mehrwert oder Vorteil,** weshalb PUP-Hersteller anderen Software-Anbietern oder -Vertreibern wie Download-Portalen für jede erreichte Neuinstallation Geld bezahlen müssen.

- **PUPs werden Ihnen oft von Freeware-Anbietern geliefert:** oftmals landen sie im Paket mit Freeware-Programmen auf Ihrem Computer. Während der Installation von Programm A installieren Sie ein oder mehr PUPs, oftmals ohne sich dessen bewusst zu sein. Der Freeware-Anbieter erhält von dem PUP-Hersteller dafür Geld, und zwar bis zu 2 $ pro Installation.

Achtung, Gefahr! Probieren Sie das nicht zu Hause aus: laden Sie Top-10-Anwendungen von Download.com herunter.

PUPs sind nichts Neues. Aber das stellt einen alarmierenden Trend dar, da immer mehr Freeware-Anbieter und -Vertreiber, wie z. B. Download-Portale, PUPs in hohen Auflagen verteilen – und all das für schnelles Geld. Selbst Sourceforge, eine Hosting-Plattform für Open-Source-Projekte, hat damit begonnen, PUPs ihren Downloads beizugeben, ohne dass die Entwickler, die dort ihre Projekte einstellen, dazu ihre Zustimmung gegeben hätten. Die Tech-Website HowtoGeek zeigte vor kurzem, was geschieht, wenn Sie die Top-10-Anwendungen bei Download.com herunterladen, die nach Download-Volumen aufgelistet sind:

“Wir haben die Top-10-Anwendungen von Download.com installiert, und Sie werden uns kaum glauben, was passiert ist! Nun, ich denke, Sie werden sich das schon gut vorstellen können. Nichts Gutes. Überhaupt nichts Gutes. Wir wettern seit Jahren gegen Freeware-Downloads, weshalb wir dachten: warum erlauben wir uns nicht einen Spaß und lassen es einmal *wirklich* darauf ankommen, indem wir Software herunterladen, wie es jeder arglose Nutzer tun könnte?”

Das Ergebnis dieses Tests: **ALLE Top-10-Anwendungen auf Download.com werden mit PUPs geliefert, einige strotzten nur so davor**. HowtoGeek rät Nutzern sogar davon ab, dies zu Hause auf ihrem Hauptrechner auszuprobieren, es sei denn, Sie möchten Ihren Computer in einen “nutzlosen Haufen Plastik” verwandeln.

Antiviren-Programme sind auch auf diesen Zug mit aufgesprungen

Hier jetzt die Top-10-Liste von Download.com, die HowtoGeek für ihren Test einsetzte:

Most Popular Downloads

DOWNLOADS FOR LAST WEEK

1.	Avast Free Antivirus 2015	1,071,404
2.	KMPlayer	741,420
3.	AVG AntiVirus Free 2015	675,369
4.	YAC	435,763
5.	CCleaner	423,181
6.	Advanced SystemCare Free	258,909
7.	Free YouTube Downloader	255,731
8.	YTD Video Downloader	246,517
9.	IObit Uninstaller	138,991
10.	Download App	134,587

Top-10-Downloads von Download.com von Januar 2015

Sticht Ihnen irgendetwas auf dieser Liste ins Auge? **Es finden sich zwei Antiviren-Programme auf dieser Liste!** Ethik scheint dem Software-Sektor vollkommen abhanden gekommen zu sein, wenn selbst Antiviren-Softwareanbieter mit ihrer Software PUPs anbieten. Sehen Sie sich einmal die Download-Volumen im Screenshot oben an: bis zu einer Million Downloads pro Woche. Addieren Sie dazu die Downloads aus anderen Quellen und die Tatsache, dass PUP-Hersteller bereit sind, alles von ein paar Pennys bist zu 2 US-$ zu zahlen, und schon haben Sie eine ungefähre Vorstellung davon, wie viel Geld dabei hier im Spiel ist: Tausende, wenn nicht sogar Millionen Dollar. Wir erfuhren dies bereits vorher, als jemand mit einem ähnlichen Angebot an Emsisoft herantrat.

Tatsache: 7 von 8 getesteten kostenlosen Antiviren-Suites werden mit PUPs geliefert

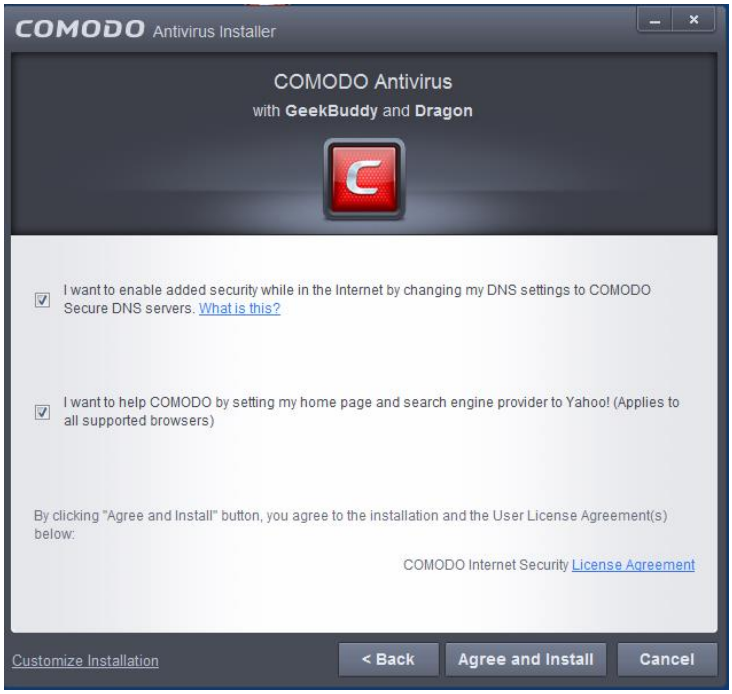
Wir entschieden uns dazu, einen genaueren Blick darauf zu werfen, und führten den gleichen Test mit allen anderen kostenlosen vollständigen Antiviren-Suites durch; die Ergebnisse waren ziemlich schockierend:

Alle getesteten kostenlosen Antiviren-Programme werden mit Toolbars oder PUPs irgendwelcher Art geliefert – außer Bitdefender Free. Viele verfügten über eine "rebrandete" Ask-Toolbar, die besonders Pay-per-Install (PPI)-Einkommen generieren, wobei diese als Teil der Sicherheitslösung des jeweiligen Herstellers verkauft wird. Andere legen offen, dass sie Ask einsetzen (z. B. Avira), andere wie AVG gehen sogar so weit, dass sie Pop-ups mit Coupon-Angeboten einbauen.

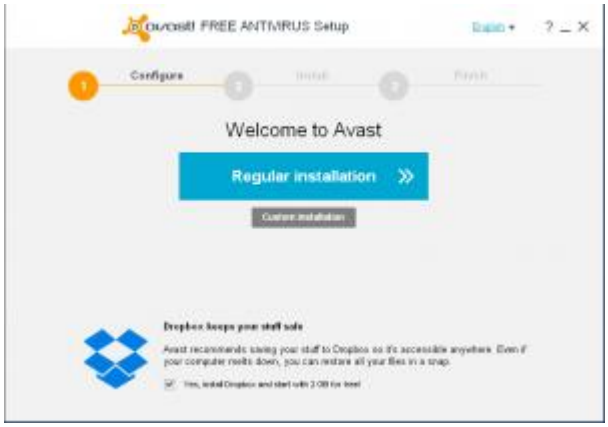
Antiviren-Programme sollen Ihren PC gegen Viren schützen; jedoch handeln viele Ihnen bei der Installation fragwürdige Programme ein, ohne dass dies klar offen gelegt wird. Unten finden Sie die Liste von 8 kostenlosen Antiviren-Programmen und welche Art von PUPs Sie sich bei der Installation einhandeln. Bitte beachten Sie, dass wir nur vollständige Antiviren-Suites, aber keine Produkt nur mit Scanner aufgenommen haben.

Bitdefender Free: wie bereits erwähnt ist Bitdefender Free einer der einzigen "sauberen" Antiviren-Softwareanbieter, die Ihnen keinerlei PUPs mitliefern.

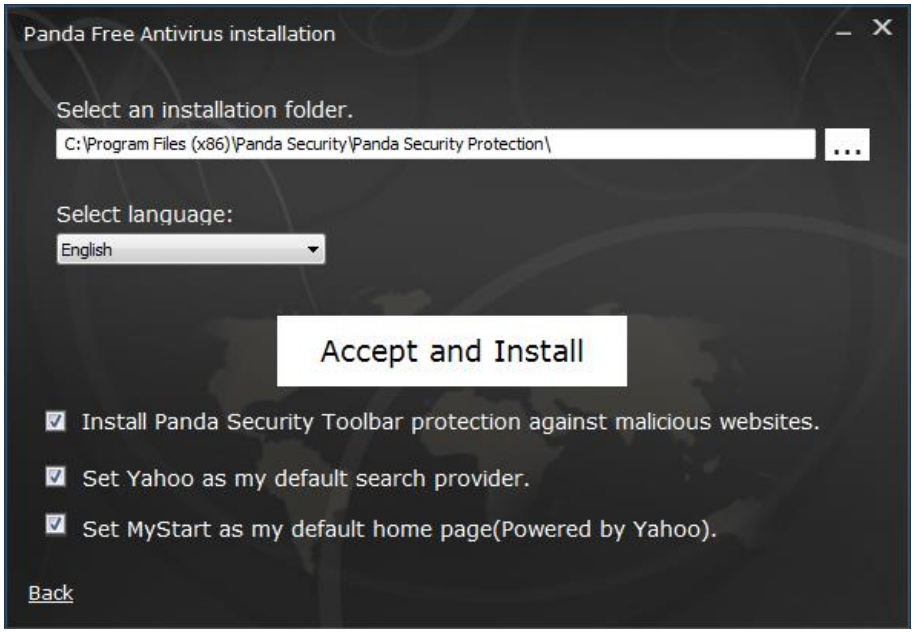
Comodo AV Free: ändert die Homepage und Suchmaschine auf Yahoo während der Installation, es sei denn, der Nutzer deaktiviert das Kontrollkästchen.



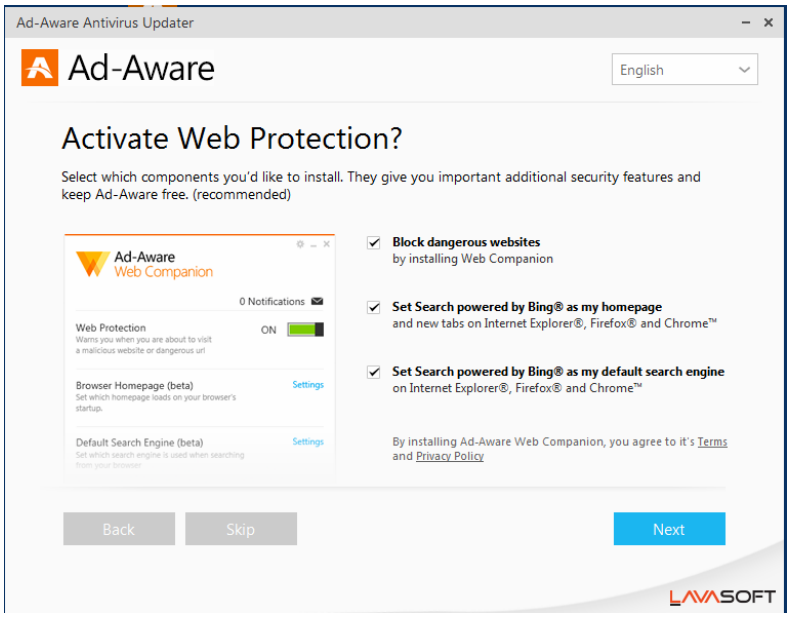
Avast Free: bietet Ihnen Dropbox standardmäßig zur Installation an, wenn Sie nicht das Kontrollkästchen deaktivieren.



Panda AV free: installiert die Panda Security-Toolbar, ändert die Suchmaschine auf Yahoo! und die Homepage auf MyStart (powered by Yahoo). Keine Produkt-Rebrands: wenigstens das Installationsprogramm weist klar aus, dass es sich um Yahoo-Produkte handelt.

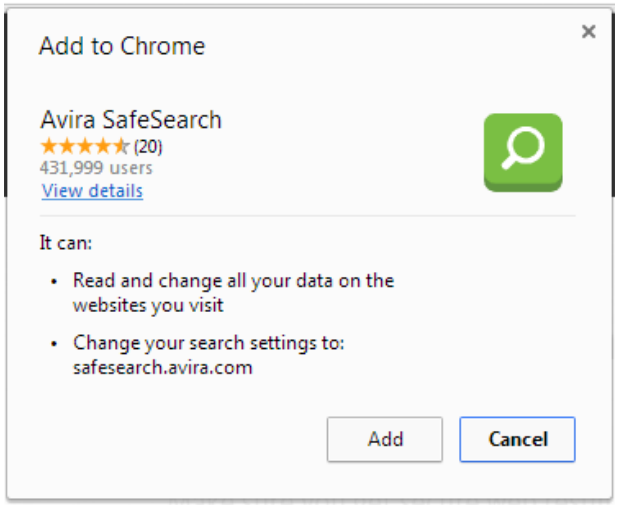


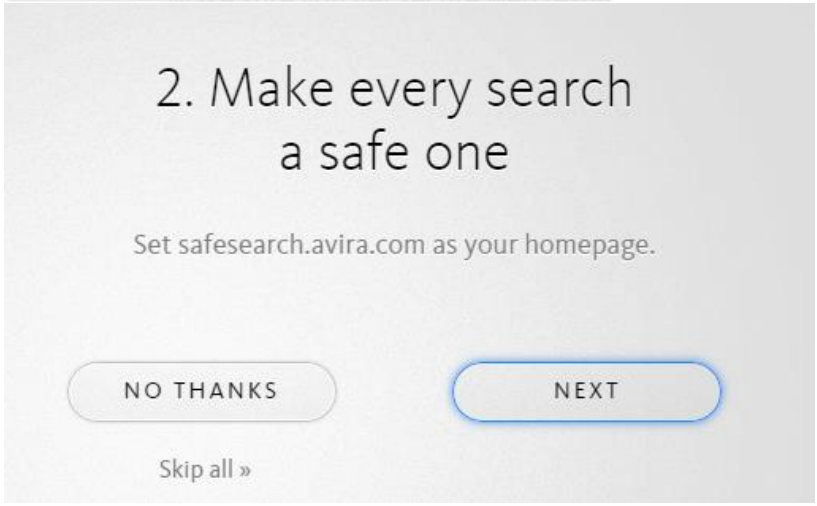
AdAware free: installiert WebCompanion standardmäßig, wenn Sie nicht das Kontrollkästchen deaktivieren. Ändert ebenso Ihre Homepage auf Bing und Ihre Suchmaschine auf Bing, wenn Sie sich nicht dagegen entscheiden. Es wird offen gelegt, dass AdAware diese Programme anbietet, damit die Software kostenlos bleiben kann.



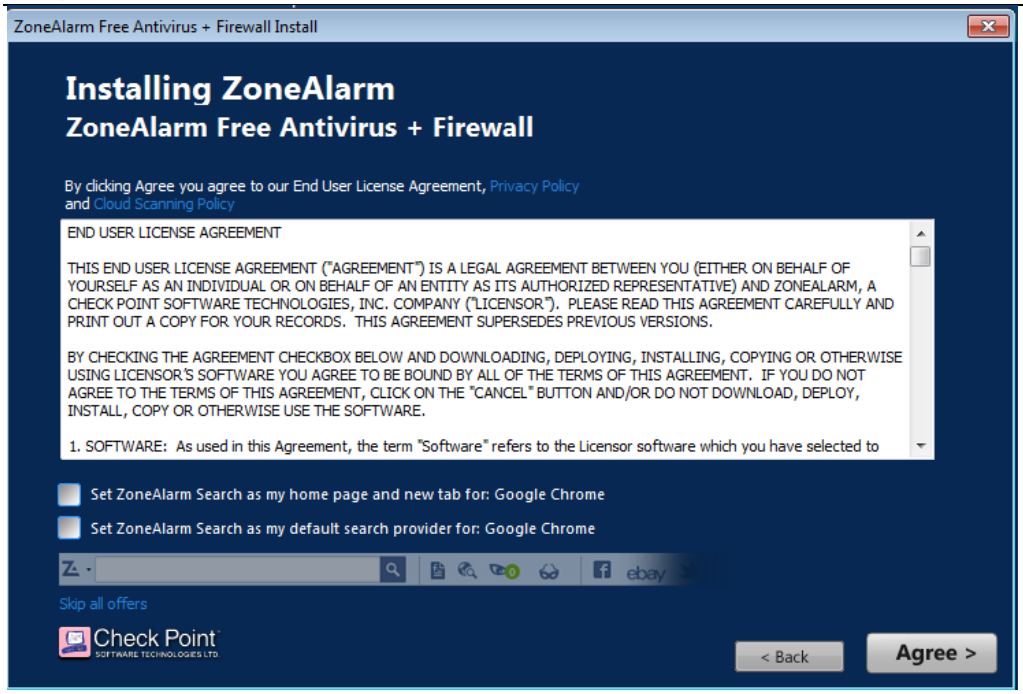
Avira free: bietet Dropbox nach der Installation an. Ändert Ihre Suchmaschine zu Avira Safe Search, wobei es sich um eine Version der Ask-Toolbar handelt. Avira legt die Partnerschaft mit Ask offen und gibt an, dass "*man Ask.com als Partner gewählt habe, um den*

Nutzern die SearchFree-Toolbar anzubieten, da Ask.com einer der vielen Anbieter sei, dessen Produkte Funktionen bieten, welche die Nutzer schätzen würden".

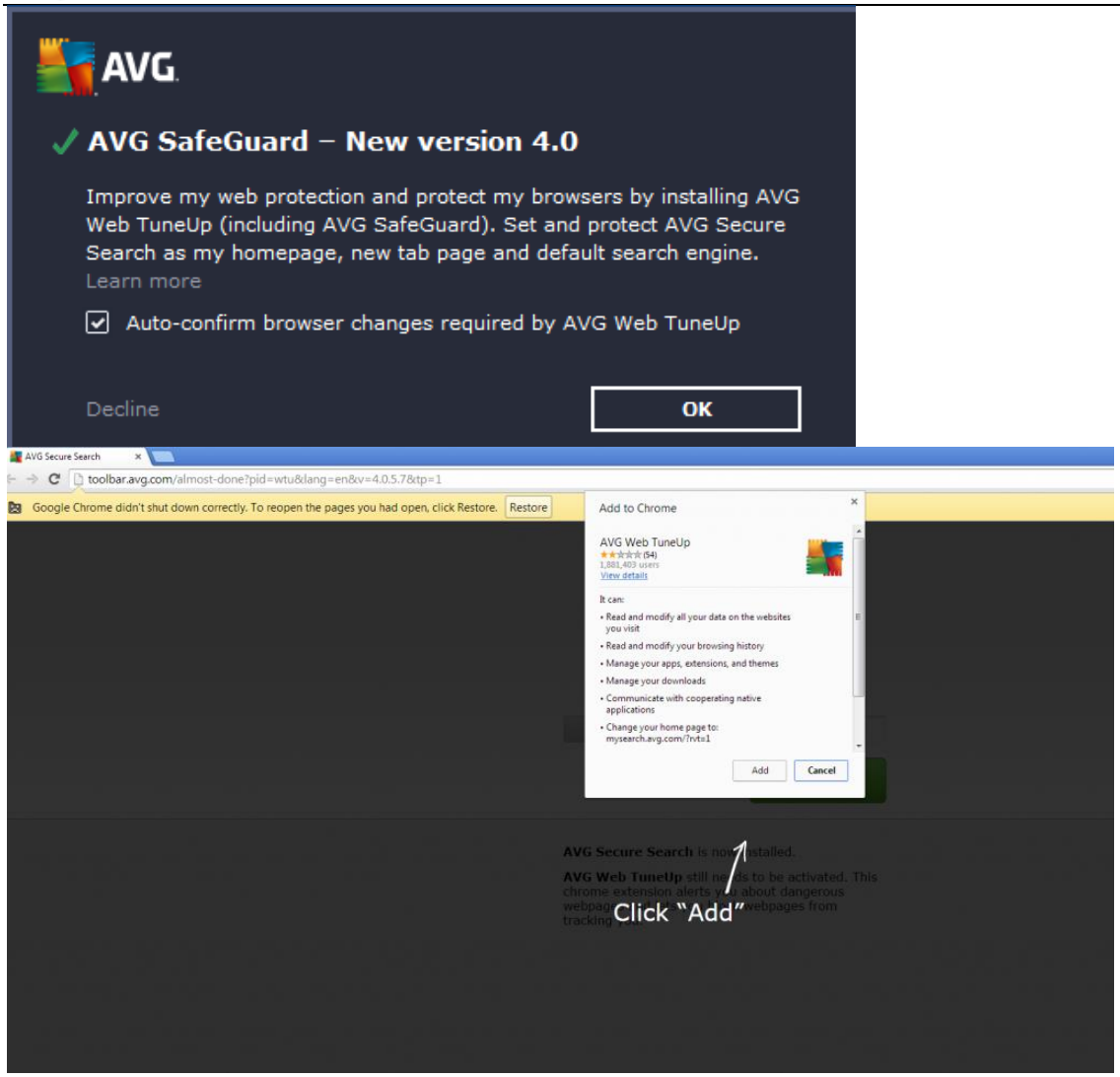




ZoneAlarm free AV + Firewall: bei benutzerdefinierter Installation: ändert Ihre Homepage auf ZoneAlarm und Ihre Suchmaschine. Dabei handelt es sich um eine rebrandete Ask-Toolbar, was allerdings auf der Website von ZoneAlarm keinerlei Erwähnung findet.



☹ **AVG free:** installiert Web Tuneup, einschließlich AVG SafeGuard. Stellt AVG Secure Search als Homepage, neue Tab-Seite und Standard-Suchmaschine ein. Die Toolbar wird von Ask geliefert, obgleich das nicht explizit erwähnt wird. Bietet ebenso AVG Rewards, wodurch Pop-up-Werbeanzeigen mit Coupons und Angeboten angezeigt werden.

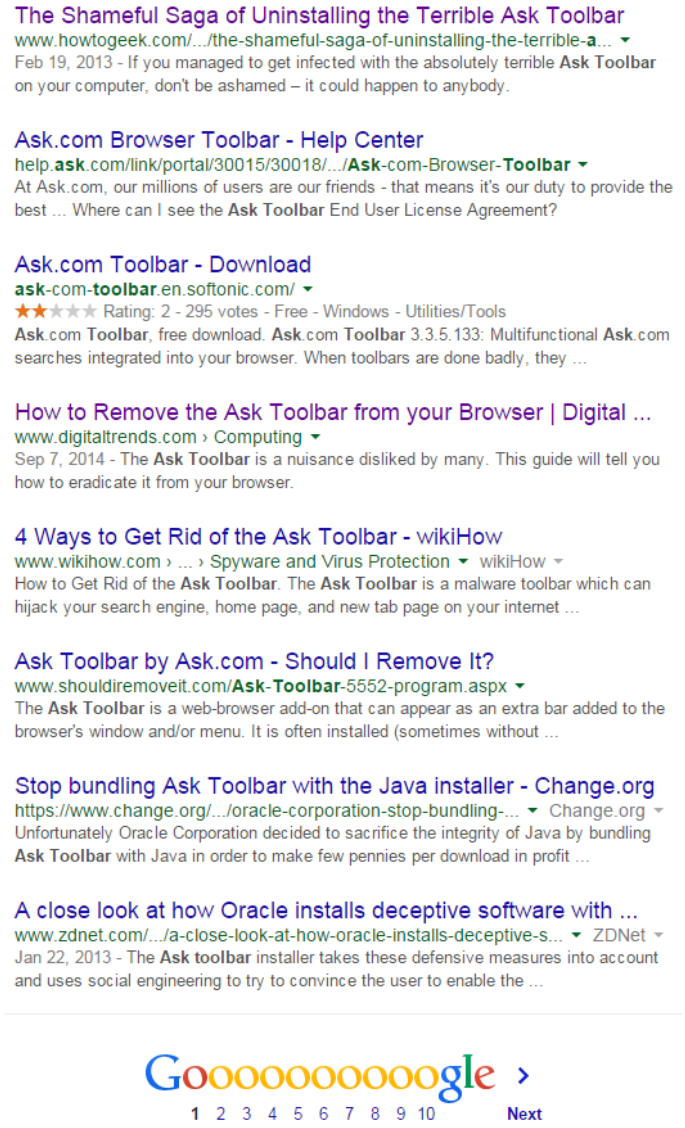


Beliebte Mittel und Wege bei kostenlosen Antiviren-Programmen mit PUPs Geld zu machen

Sehen Sie sich einmal die Screenshots oben an, und Sie werden sehen, dass Antiviren-Softwareanbieter mehrere Mittel und Wege gefunden haben, um mit PUPs Geld zu machen:

- **Änderung der Suchmaschine:** Ihre Standard-Suchmaschine wird auf diejenige nach Wahl des Softwareanbieters geändert, hier gibt es viel Geld zu holen. Denken Sie nur einmal an die Firma namens Google.
- **Ask-Toolbar:** suchen Sie einmal schnell auf Google nach der Ask-Toolbar, und Sie werden erstaunt sein, wie viele Suchergebnisse mit dem Titel "Wie entferne ich die

Ask-Toolbar?" und "Wie werde ich die Ask-Toolbar los?" Sie auf der ersten



Ergebnisseite finden werden.

- **Rebrandete Ask-Toolbar:** noch schlimmer als die Ask-Toolbar, da bei dieser Version der Toolbar dieser ein neuer Name und ein neues Aussehen vom Softwareanbieter gegeben wird, es sich aber letzten Endes ebenso um die Ask-Toolbar handelt.
- **Änderung der Homepage oder neuer Tabs**: "Kostenloser" sicherer Traffic für eine Website Ihrer Wahl gefällig?
- **Ihre Daten sowie Ihr Such- und Surfverhalten:** niemand weiß, was Antiviren-Softwareanbieter mit Ihren Daten anstellen. Bekannt ist jedoch, dass man sie beobachtet und verfolgt. Vertrauen Sie darauf, dass man mit Ihren Daten nichts anstellt? Die Online-Verfolgung von Personen und der Verkauf von Surfdaten und persönlichen Informationen ist seit Jahren schon ein großes Geschäft im Internet, wer weiß also, was damit getrieben wird.

Das Besorgnis Erregende an all diesen Mitteln und Wegen, die Antiviren-Softwareanbieter zum Einsatz bringen, ist die Tatsache, dass die PUPs bei der Standardinstallation mitgeliefert werden, es sei denn, ein Nutzer entscheidet sich dagegen oder liest genau das Kleingedruckte. Manchmal wird die Installation von PUPs noch nicht einmal offen gelegt oder gar verschwiegen. Selten wird überhaupt erklärt, wozu das installierte PUP gut ist. Das ist ein **fragwürdiges Gebaren, um sich auf den Computer unwissender Nutzer einzunisten**

Während das Produkt kostenlos angeboten wird, sind in Wahrheit SIE das Produkt

Wie HowToGeek ebenfalls feststellt, spielt es keine Rolle, welches Downloadportal Sie nutzen. **Diejenigen, welche die Freeware herstellen, bieten Ihnen die Pakete an.** Einige Downloadportale bieten darüber hinaus Pakete an, doch liegt nicht hier des Übels Wurzel. Sie machen bei diesem Spiel mit. Wie HowToGeek in seinem Artikel feststellt:

"Es gibt ebenso wenig sichere Downloadportale …, weil nicht nur bei CNET-Downloads Pakete angeboten werden, wie Sie diesen Screenshots entnehmen können, sondern JEDER macht es. Freeware-Autoren bieten unnötige Software im Paket an, und dann packen lausige Download-Quellen noch einmal mehr davon oben drauf. Eine wahre Flut unnötiger Software. Jedes Mal, dass wir diesen Text über die letzten Monate durchgeführt haben, sahen wir uns mit anderer Software im Paket konfrontiert, aber **jede Software, die im Paket geliefert wird, liefert Ihnen die gleichen Verdächtigen mit: Browser-Hijacker, die Ihre Suchmaschine, Ihre Homepage ändern und Sie mit Werbung überschwemmen.** Denn während das Produkt kostenlos angeboten wird, sind in Wahrheit SIE das Produkt."

Machen Freeware-Nutzer das PUP-Geschäft erst "möglich"?

Folgendes sei klargestellt: nicht jede Freeware ist schlecht und setzt auf PUPs, aber gute Freeware ist leider eine Ausnahme geworden. Hier ein paar wenige Beispiele für gute Freeware:

1. Eingeschränkte Versionen von Vollversionen, bei denen Sie mit der kostenlosen Version eine Vorstellung des Produkts erhalten und über grundlegende Funktionen verfügen, während der Anbieter darauf aus ist, Ihnen eine höherwertige Ausgabe der gleichen Software zu verkaufen.
2. Die Open-Source-Community. Ein Ort, an dem man Software aus Spaß an der Freude herstellt oder um die Welt zu verbessern. Es mag schwierig erscheinen, aber manchmal nutzen andere Open-Source-Projekte, die sie durch gefälschte Imitationen um Werbung ergänzen.
3. Projekte, die sich durch Spenden finanzieren, die allerdings eine Seltenheit geworden sind.

Die verbleibenden Freeware-Anbieter müssen auf die Auslieferung im Paket mit anderer Software zurückgreifen. Ermöglichen und unterhalten Freeware-Nutzer die zunehmende Verteilung von PUPs? In gewisser Weise ja, aber man kann ihnen nicht ernsthaft die Schuld geben. Die meisten sind einfach der Meinung, kostenlose Software höre sich gut an, haben aber keine Ahnung davon, was sie sich einhandeln (können).

Bestenfalls kann man ihnen vorhalten, *warum* sie sich keine Gedanken darüber machen, dass eine Software kostenlos angeboten wird.

PUP-Hersteller wissen, dass sie Nutzer hinters Licht führen; Freeware-Anbieter wissen, dass PUPs eine äußerst fragwürdige Angelegenheit sind, und Antiviren-Softwareanbieter wissen sehr wohl, dass die ganze Sache ethisch nicht astrein ist. Daher nehmen alle Beteiligten einiges auf sich, um die Tatsache zu verschleiern, dass sie Ihnen PUPs im Paket mitliefern. Sie tragen Sorge dafür, alle rechtlichen Auflagen aufs Wort zu erfüllen, aber nutzen alle möglichen Mittel und Wege zur Verbreitung dieser unerwünschten Programme. Die Bereitschaft von Anbietern, alle ethischen Bedenken außen vor zu lassen und ihr Ansehen für schnelles Geld aufs Spiel zu setzen, sprechen schon für sich. **PUP-Vertreiber nutzen den "unwissenden" Durchschnittsnutzer aus.**

Fazit: seien Sie vorsichtig mit Freeware, kostenpflichtige Software wird normalerweise nicht mit PUPs oder anderer Software im Paket geliefert.

PUPs werden sich weiterhin massiv ausbreiten und gar noch nerviger und hinterhältiger werden, wenn niemand dagegen vorgeht. Nur gemeinsam ist eine Veränderung möglich. Selbst wenn Sie eine Antiviren-Lösung nutzen, die frei von PUPs ist, sind Sie von der drastischen Zunahme von PUPs betroffen. Sie werden mehr davon hören, es werden mehr PUPs blockiert, Sie erhalten immer mehr Signatur-Updates für Ihre Antiviren-Software, damit alle verschiedenen Arten erkannt werden. Beispielsweise verwenden die Malware-Analysten von Emsisoft mittlerweile die Hälfte ihrer Zeit auf die Analyse von PUPs, während wir diese Zeit für andere Ressourcen und anderen Malware-Arten nutzen könnten, um Sie bestmöglich gegen andere Online-Bedrohungen zu schützen. Zumindest müssen Nutzer vollständige Offenlegung einfordern, damit sie die Möglichkeit besitzen, eine bewusste Entscheidung darüber zu treffen, ob Sie eine Software herunterladen oder nicht, und wissen, was sie da herunterladen. Im Grunde heißt das: seien Sie vorsichtig mit Freeware, kostenpflichtige Software wird normalerweise nicht mit PUPs oder anderer Software im Paket geliefert.

Sind Sie jemals auf PUPs auf Ihrem PC gestoßen? Sind Sie von derartiger Nutzung von PUPs und der Tatsache überrascht, dass Freeware- und Antiviren-Softwareanbieter bei diesem Spiel mitmachen? Sagen Sie uns Ihre Meinung und hinterlassen Sie einen Kommentar unter diesem Post.

Wir wünschen eine schöne (PUP-freie) Zeit!

Quelle: http://blog.emsisoft.com/de/2015/01/17/ist-der-antiviren-sektor-ist-nicht-mehr-ganz-bei-trost

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

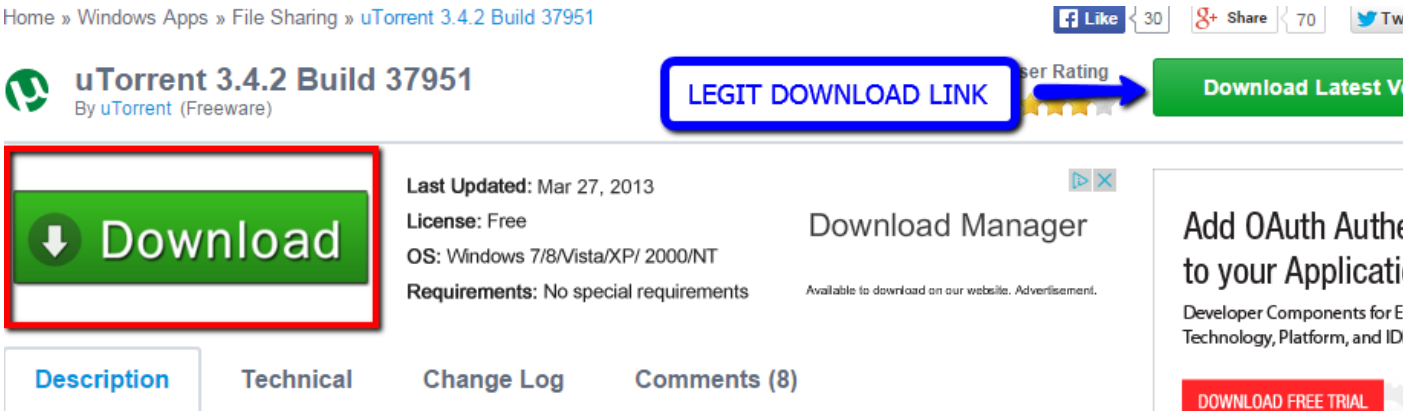
10 Wege, wie sich PUPs auf Ihren Computer schummeln. Und wie Sie das verhindern.

Kürzlich berichteten wir von potenziell unerwünschten Programmen (PUPs), was sie sind und wie sie Ihnen inzwischen sogar von Anbietern kostenloser Antiviren-Software frei Haus geliefert werden. In diesem Artikel gehen wir nun detailliert darauf ein, wie Ihnen PUPs geliefert werden. Vorweg: jede Anwendung kann als potenziell unerwünscht betrachtet werden, wenn Sie ohne **"ausdrückliche Zustimmung"** eines Nutzers installiert wird.

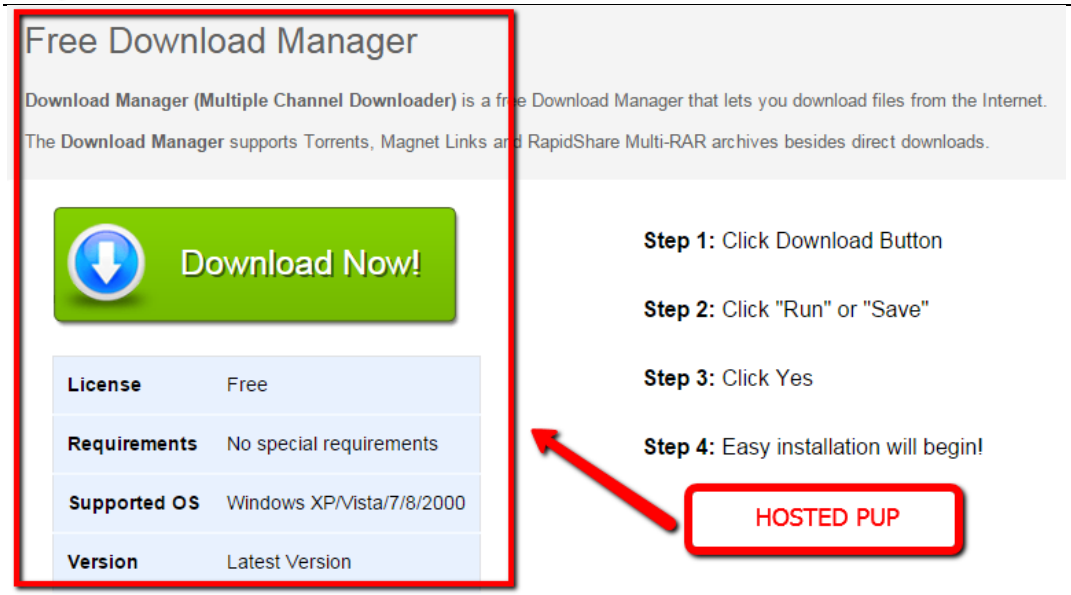
Angesichts Tausender neuer PUPs, jeden Tag und der Grauzone, in der PUPs operieren (zwischen nervender Software und Malware), besteht immer eine gute Möglichkeit, dass Sie auf PUPs treffen. Hier hat ein Kollege von Emsisoft Ihnen ein paar Methoden zusammengestellt, wie sie sich einnisten:

Beispiel 1: Verbreitung durch Download-Portale

Beim Besuch von Filehippo.com, einem der meist genutzten Download-Portale, begegnen Sie den schönsten grünen Download-Buttons, die Sie jemals gesehen haben. Jedoch ist die ganze Sache nicht mehr annähernd so schön, wenn Sie jedes Mal die falsche Download-Option auswählen. Weiter unten finden Sie, was genau dabei vor sich geht.



Hmm …. Das ist interessant, hier wird ein "Free Download Manager" angeboten … Wow! Das ist doch toll von "Filehippo". Da wollen wir unbedingt Utorrent installieren …los geht's.



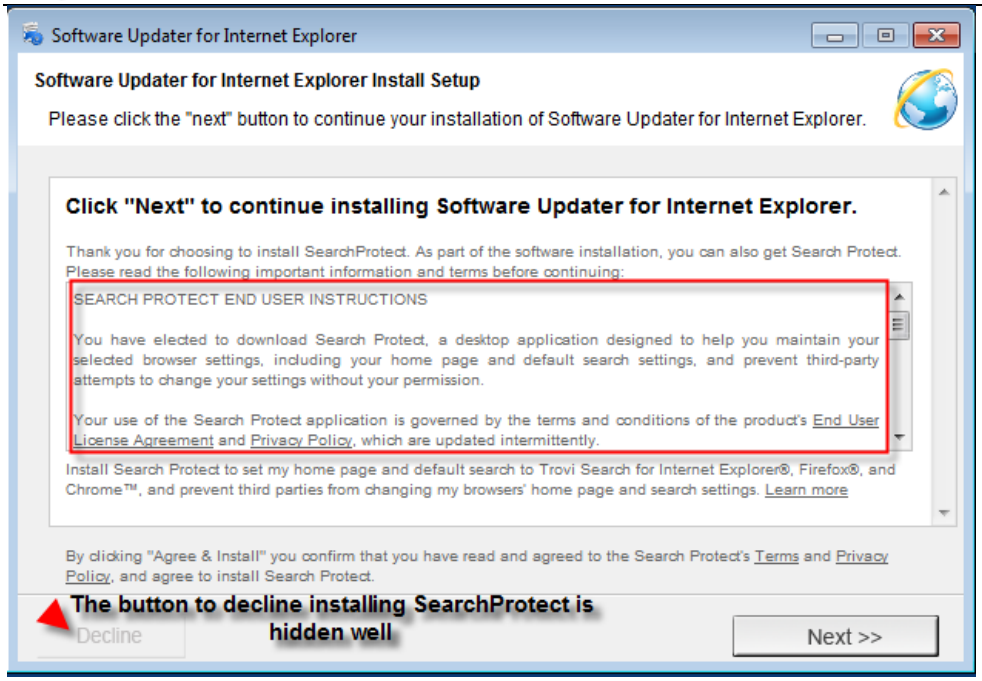
Moment – Wir wollten Utorrent, aber das sieht nicht ganz wie Utorrent aus … Was ist falsch gelaufen? Hierbei handelt es sich um eine sehr weit verbreitete Methode, bei dem Nutzer tagtäglich zum Download von PUPs verleitet werden. Ein beliebtes Download-Portal bietet Freeware-Software an. Klar, die Software ist "kostenlos" (und kostenlos ist ja etwas Gutes, oder?). Wer also auf "Download" klickt und übersieht, dass es neben dem Direktdownload noch eine zweite, offensichtlich legitime Download-Option geben würde, staunt: Herzlichen Glückwunsch, die Invasion der PUPs hat begonnen! Aber keine Sorge, es gibt Abhilfe.

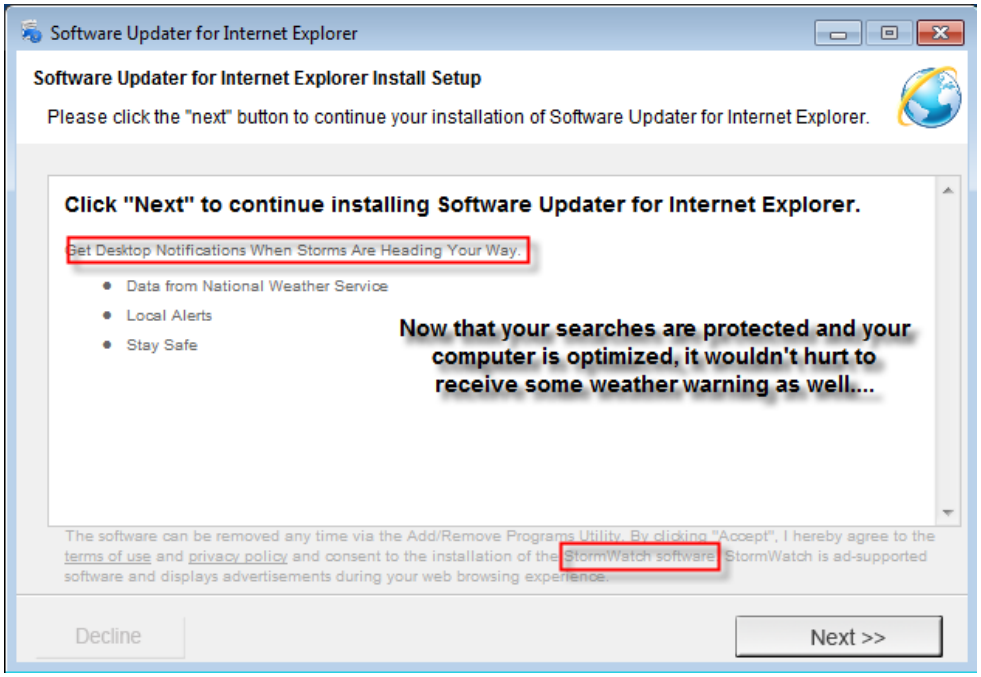
So vermeiden Sie das Problem: Am besten gehen Sie Download-Portalen schlichtweg vollständig aus dem Weg. Falls Sie sie dennoch nutzen, lassen Sie beim Download von Dateien größte Sorgfalt walten, verwenden Sie aktuelle Antiviren-Software mit aktivierter PUP-Erkennung, achten Sie auf Dateinamen und, dass die Software, die Sie herunterladen, wirklich diejenige ist, die Sie möchten. Sollte es sich nicht um den richtigen Dateinamen handeln, lassen Sie die Finger davon.

Beispiel 2: Über gefälschte Updates, die über temporäre Websites ausgeliefert werden

Updates werden oftmals über temporär erstellte Websites ausgeliefert, die für Adsense entwickelt wurden. Häufig wird Open-Source-Software angeboten, die in Downloader verpackt ist, welche Nutzer zur Aktualisierung von Flash Player, Java, Service Packs usw. auffordern. Es gibt Firmen, die Hunderte von Websites am Tag erstellen, um die Nutzer hinters Licht zu führen und auf diese Weise ihren Website Traffic zu verbessern.

Ein Beispiel: Endlich ein Update für Internet Explorer, worauf Nutzer dieses Programms bereits lange gewartet haben. Sorgt dieses Update-Programm wirklich dafür, dass ich die neueste Version von Internet Explorer habe? Moment, das sieht nicht ganz wie ein Update-Programm aus. Aber fein, dass ich mit Internet Explorer Search Protect und Desktop-Benachrichtigungen zum Wetter angeboten bekomme. Diese aktualisierte IE-Version scheint wirklich etwas Anderes zu sein!





Die beiden Installationsprogramme oben machen dem Nutzer nette Angebote. Jedoch sind diese Angebote alles andere als toll oder nett. Nach der Installation ändert Seach Protect Ihre Browser-Einstellungen (Suchmaschine, Homepage, Tab-Einstellungen) und kann sogar manche Ihrer Surfdaten an unbekannte Quellen übermitteln. Die StormWatch-Software zeigt Ihnen Werbung im Browser an und sehr wahrscheinlich zahllose unerwünschte Pop-ups zum "Wetter". Aufgepasst! Durch gefälschte Updates wird Ihr Computer auf potenziell unerwünschte Weise aktualisiert.

So vermeiden Sie das Problem: Es kann mit Sicherheit gesagt werden, dass Nutzer keine aktualisierte Software oder Wetterberichte von diesem Update-Programm wünschen. Am besten vermeiden Sie die Installation solcher Junkware, indem Sie auf "Ablehnen" klicken und jegliche

eventuell vorhandene Kontrollkästchen kontrollieren und ggf. deaktivieren. Wieder einmal gilt es, VORSICHT WALTEN ZU LASSEN!

Beispiel 3: Installationsprogramme – Verbreitung durch Downloader und EULAs

Eines der beliebtesten Software-Programme aller Zeiten … "KMPlayer". Wow, da gibt es wirklich viel zu lesen. Am besten klicken Sie einfach auf "Zustimmen" und "Installieren"! BUMM! Jetzt installiert Spigot Browser-Erweiterungen, Shopping Aid, NewTab, eBay Shopping Assistant und Search Protect. Das ist noch lange nicht alles – Homepage und Suchmaschine Ihres Browsers werden auf Yahoo geändert.

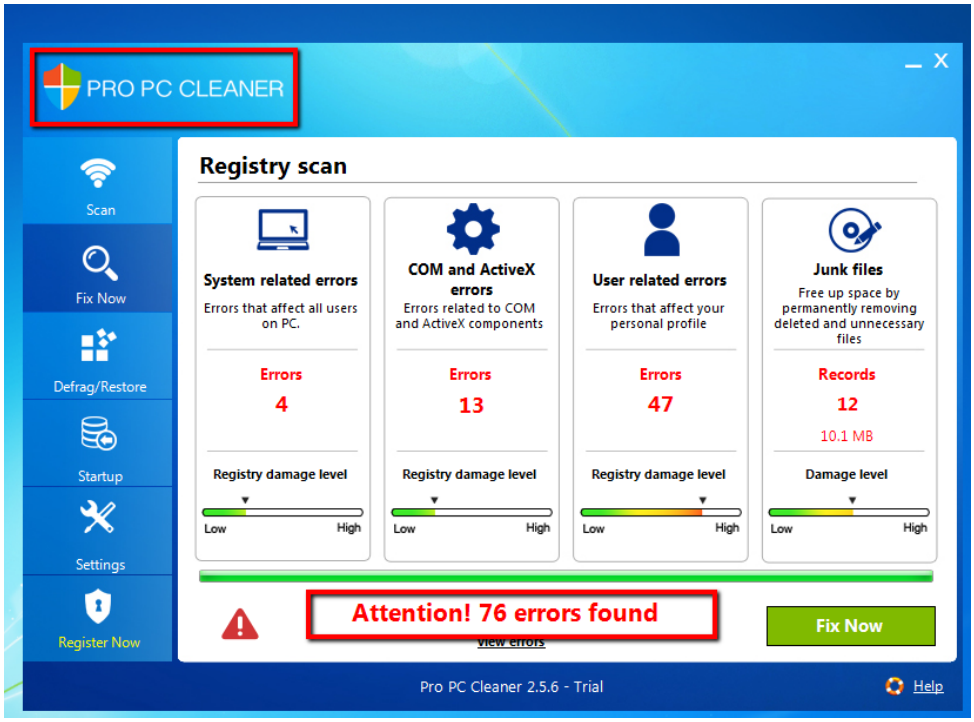
Hierbei handelt es sich um die zweite Welle potenziell unerwünschter "Sonderangebote", bevor Sie endlich zum legitimen Installationsprogramm gelangen. "Pro PC Cleaner" wird klammheimlch auf Ihrem PC installiert und bombardiert Sie dann mit gefälschten Funden, die auf vielerlei Art und Weise den letzten Nerv rauben. Angebote bei Downloadern (auch "Wrapper" genannt) von Websites wie Download.com, Filehippo, Brothersoft u.Ä. versuchen, Nutzer zur Installation und Zustimmung zur Installation von Junkware zu verleiten. Die meisten Nutzer haben wenig Lust, einen Haufen Unsinn zu lesen. Sie wollen einfach die gewünschte Software installieren.

So vermeiden Sie das Problem: Ein Weg, dieser Art potenziell unerwünschter Programme aus dem Weg zu gehen, besteht darin, auf "Ablehnen" zu klicken, alles aufmerksam durchzulesen, nichts ungelesen zu installieren und sich erst einmal anzusehen, was mitgeliefert wird. Ebenso überprüfen Sie

das Download-Portal auf Informationen zu dem jeweiligen Installationsprogramm, die Aufschluss darüber geben, was mit der Software mitgeliefert wird.

Beispiel 4: PUP über PUP – ein PUP lädt andere PUPs herunter?

Recherchen zufolge handelt es sich bei "Pro PC Cleaner" um ein sehr weit verbreitetes potenziell unerwünschtes Programm, das auf vielen Download-Portalen mit Freeware im Paket angeboten wird. Sie fragen, wie effizient dieses Programm wirklich einen PC reinigen kann? Theoretisch lässt sich dieses PUP ziemlich genau mit einem gefälschten (Rogue-) Produkt vergleichen. Schauen wir uns das einmal an:



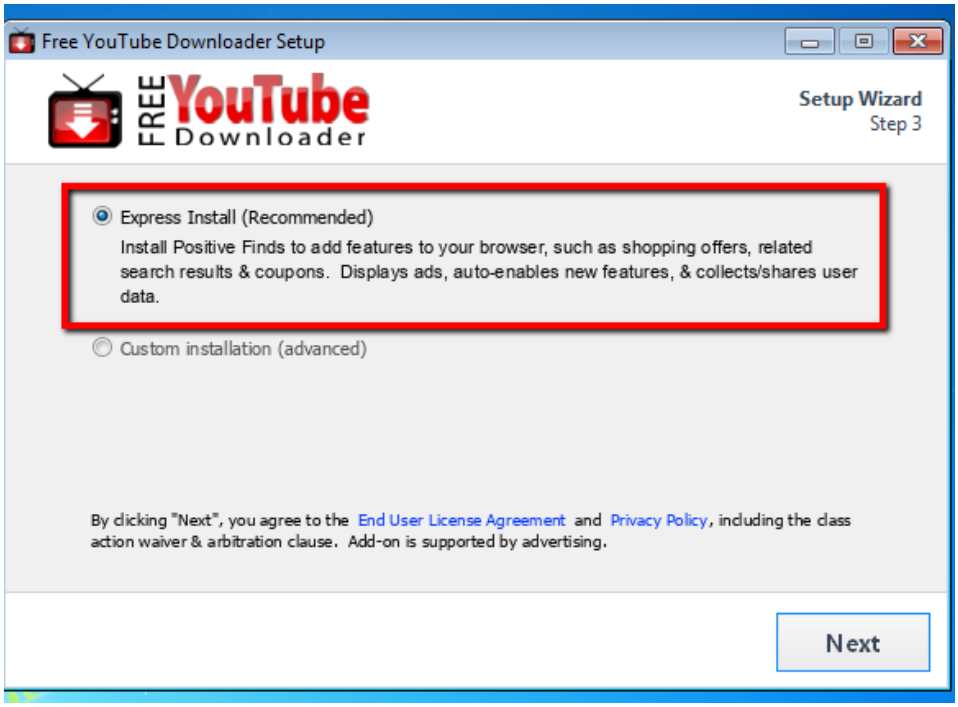
Das oben gezeigte PUP wurde in Wahrheit im Hintergrund durch Annahme der Bestimmungen des EULA des Downloaders von Download.com für KMPlayer heruntergeladen. Das ist erschreckend, aber leider wahr. Ein potenziell unerwünschtes Programm lädt ein anderes ebensowenig erwünschtes Programm herunter. Pro PC Cleaner versucht den Nutzer dazu zu verleiten, die kostenpflichtige Version zu erwerben (wie bei Rogue-Software). Eine Installation von Download.com reicht aus, und schon taucht ein nerviges PUP auf.

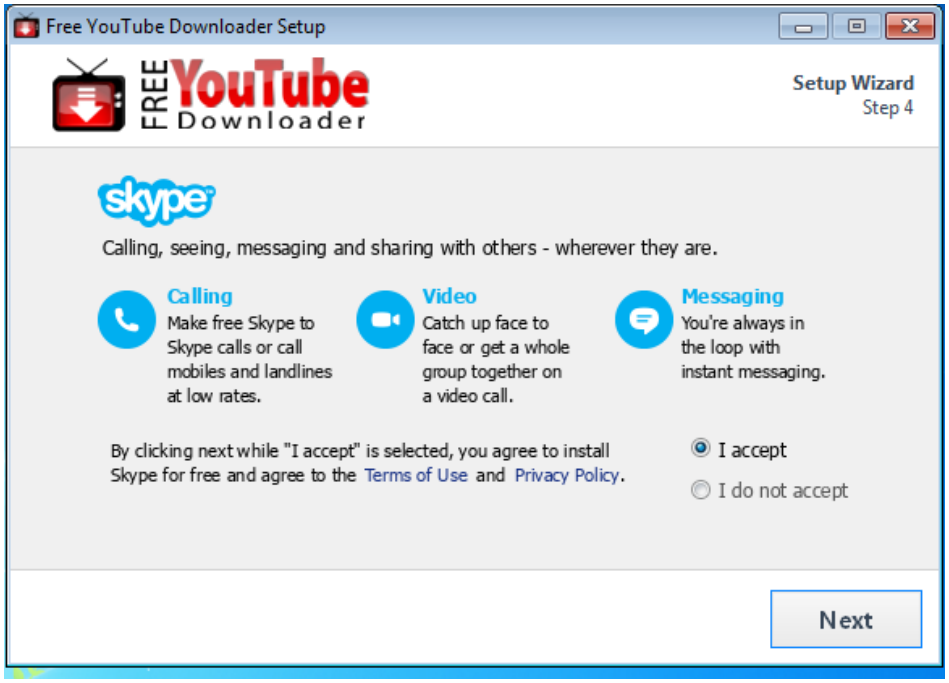
So vermeiden Sie das Problem: Bleiben Sie wachsam, lassen Sie den gesunden Menschenverstand walten und beachten und lesen Sie sorgsam ALLES vor der Installation. Wie bereits erwähnt sollte Ihre Antiviren-Software auf dem neuesten Stand und die PUP-Erkennung aktiviert sein.

Beispiel 5: Express-Installation = Express-Infektion?

In diesem Beispiel nutzen wir "Free YouTube Downloader", eine beliebte Freeware-Anwendung auf CNET.com zum Herunterladen von YouTube-Videos. Allerdings würden wir darauf wetten, dass CNET

den Nutzer über die mitgelieferten unerwünschten Angebote im Unklaren lässt. Schauen wir uns das einmal an:



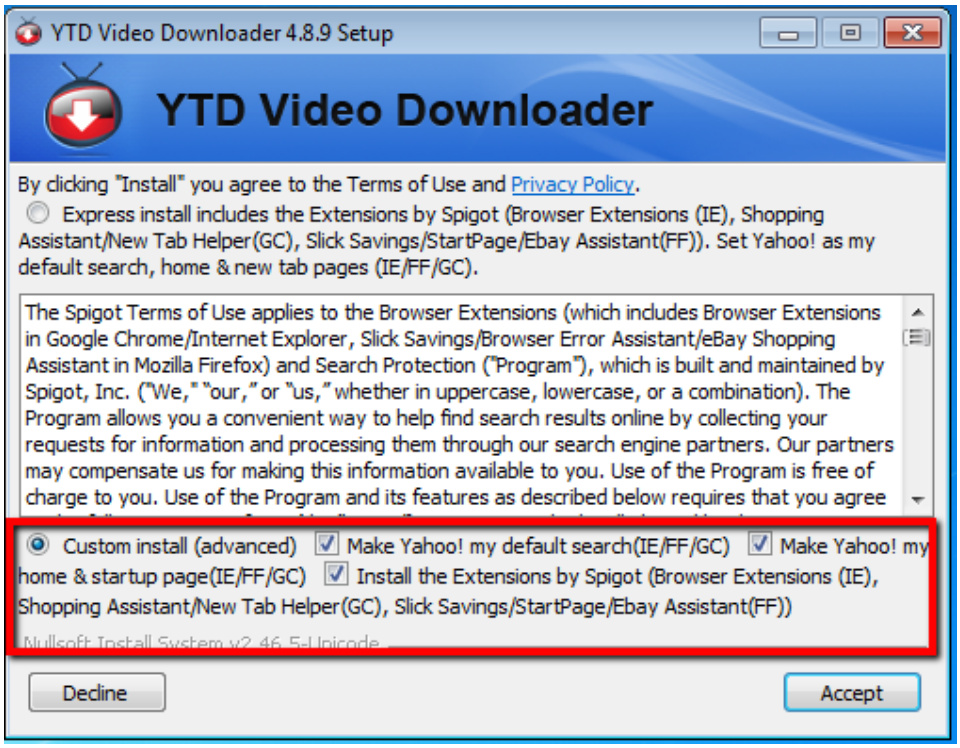


Da schau einer an. Die Express-Installation ist nicht immer der beste Weg. Ja, es stimmt schon, eine Express-Installation erfordert nur wenige Klicks, aber ist es wirklich das Risiko wert, potenziell unerwünschte Programme zu installieren? Skype ist eine legitime Anwendung; jedoch kann es sich für einen Nutzer, der es nicht benötigt, als unerwünscht erweisen. Bei der Express-Installation werden außerdem weitere potenziell unerwünschte Programme im Browser installiert, durch die Werbung angezeigt und Nutzerdaten gesammelt/geteilt werden. Das klingt gar nicht nett.

So vermeiden Sie das Problem: Niemals die angebotene Express-Installation nutzen. Diese liegt nur im besten Interesse des Herstellers, aber nicht Ihrem eigenen Interesse.

Beispiel 6: Benutzerdefinierte Installation – ist eine benutzerdefinierte besser als eine Express-Installation?

"YTD Video Downloader" ist eine weitere beliebte Freeware-Anwendung. Sind die Installationsoptionen weniger mit PUP-lastig bei einer benutzerdefinierten Installation als bei Free YouTube Downloader. Sieht das bei einer benutzerdefinierten Installation anders aus? Mal sehen.

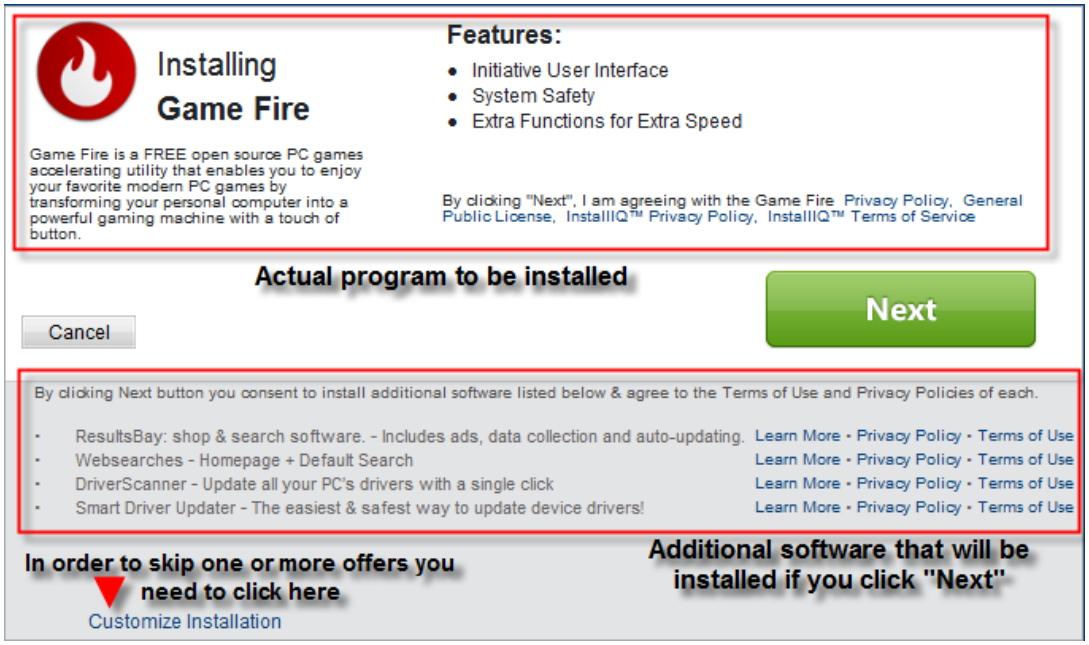


Man muss kein Wissenschafter sein, um zu erkennen, dass auch bei einer benutzerdefinierten Installation PUPs präsent sein können. Jedoch besteht zwischen einer Express- und einer benutzerdefinierten Installation ein signifikanter Unterschied: bei ersterer wird dem Nutzer keinerlei Option zur Änderung der Installation geboten, während man bei einer benutzerdefinierten der Nutzer genau auswählen kann, was auf seinem System installiert wird. Ein Benutzer kann alle unerwünschten Zusätze abnlehnen, wenn er Vorsicht walten lässt und sich gegen die Express-Installation entscheidet.

So vermeiden Sie das Problem: Bringen Sie die gleiche Taktik wie bereits erwähnt zum Einsatz und entscheiden sich zusätzlich für eine benutzerdefinierte Installation. Wie oben erwähnt wird eine benutzerdefinierte Installation dringend angeraten, um Kontrolle darüber zu haben, was auf Ihrem System installiert wird. Wählen Sie wann immer möglich eine benutzerdefinierte Installation.

Beispiel 7: Neue Homepage, Suchmaschine und aktualisierte Treiber

Unter normalen Umständen ist die Änderungsmöglichkeit der Homepage und der Suchmaschine Ihres Browsers eine gute Sache. Allerdings kommen bei potenziell unerwünschten Programmen jetzt Täuschungsmethoden in Installationsprogrammen zum Einsatz, die diese Änderungen und weitere Einstellungen für neue Tabs automatisch vornehmen. Selbst bei benutzerdefinierter Installation sind Sie gegen diese teuflischen PUP-Tricks nicht gefeit.

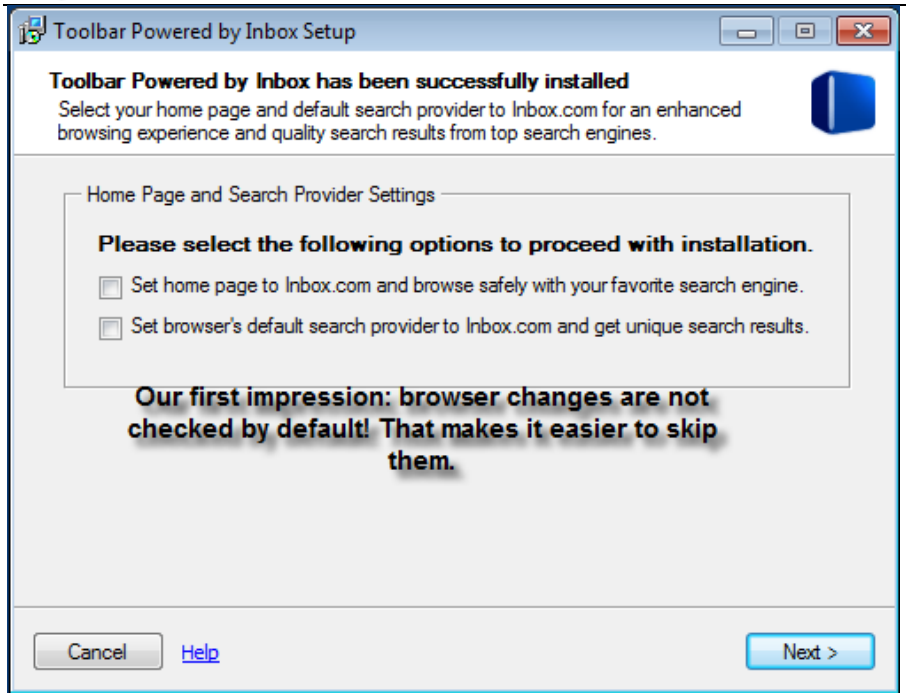


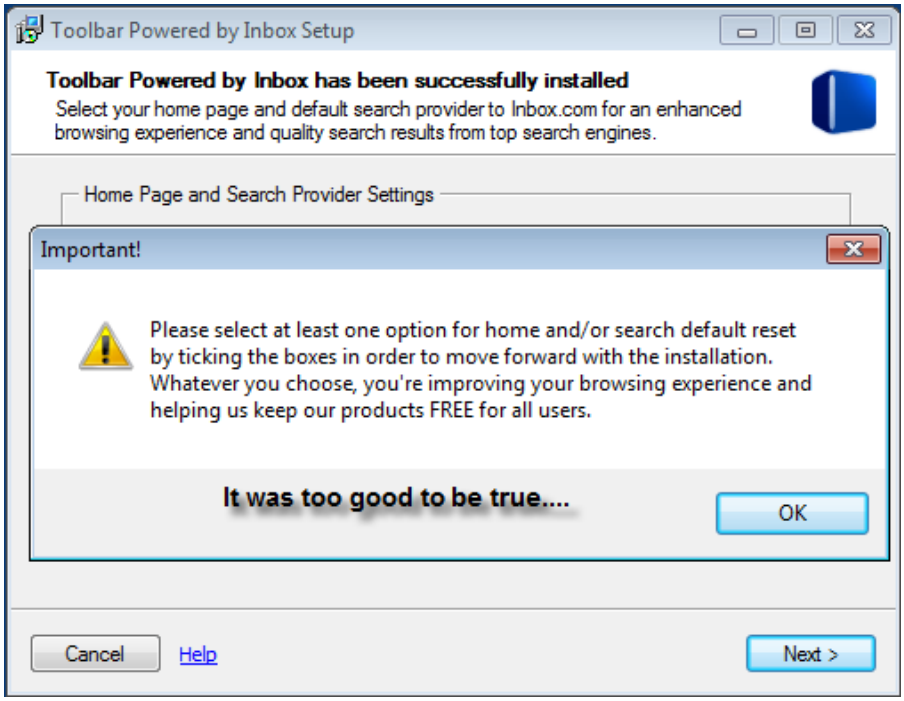
Wie im Screenshot oben zu sehen, wird ein Nutzer mit mehreren potenziell unerwünschten Zusätzen konfrontiert. Die Bilder zeigen: Game Fire, ResultsBay, WebSearches, Driver Scanner und Smart Driver Updater, die allesamt von einer einzigen Installation herrühren. Wow! Das ist einiges! PUPs übernehmen Installationsprogramme. Fahren Sie mit Vorsicht fort! Benutzerdefinierte Installationen sind nicht mehr so "sicher", wie manche das gerne glauben würden.

So vermeiden Sie das Problem: Die Möglichkeit, diesen "Angeboten" aus dem Weg zu gehen, ist von enormer Wichtigkeit. Deaktivieren Sie mit Bedacht alle Kontrollkästchen, durch die offenbar Änderungen an Ihrem System vornehmen. Sie sollten eventuell sogar bei manchen Installationsprogrammen auf "Abbrechen" klicken, um die PUP-Installation zu unterbinden. Wieder möchten wir betonen, dass Sie größte Sorgfalt walten lassen und sich die Installationsoptionen sorgsam durchlesen sollten, bevor Sie fortfahren.

Beispiel 8: Gewaltsame Verbreitung – die (fast) auswegslose Methode

Was hier angestellt wird, ist alles andere als lustig. Kurz gesagt soll die "Inbox-Toolbar", ein typisches PUP, installiert werden. Diese treibt jedoch ein übles Spiel. Dabei wird der Nutzer nämlich im Vorfeld dazu gezwungen, seine Homepage oder Suchmaschine anzupassen um überhaupt mit der Installation der eigentlichen Software fortfahren zu können. Diese Toolbar sollten Sie lieber direkt in den Papierkorb verfrachten!





Keine Sorge, es besteht noch Hoffnung! Für einen kurzen Augenblick sah alles ziemlich trübe aus. Die oben gezeigten aufgezwungenen potenziell unerwünschten Angebote können doch übersprungen werden. Dieses PUP brachte alle Finesse zum Einsatz, um den Nutzer zur Änderung seiner Browser-Einstellungen zu bewegen. Die o. g. Art von PUPs ist mit höchster Vorsicht zu genießen, bevor Sie mit der verbleibenden Installation fortfahren.

So vermeiden Sie das Problem: Es ist nicht ganz einfach, diesem Angebot aus dem Weg zu gehen, aber es kann während der Installation tatsächlich alles abgewählt werden.

Beispiel 9: Eine andere Person nutzt Ihren Computer

Vielleicht teilen Sie Ihren Computer mit Ihren Kindern, Mitarbeitern oder Ihrem Partner. Nicht alle sind möglicherweise so vorsichtig wie Sie und bringen PUPs auf Ihren Computer. Dies könnte insbesondere dann der Fall sein, wenn sie Torrent-, Streaming- oder Online-Gaming-Websites besuchen, die einen oftmals mit Downloads und Werbung überschütten.

 **So vermeiden Sie das Problem:** Die einzige Möglichkeit besteht darin, Ihren Computer nur für sich allein zu verwenden.

Beispiel 10: Ihr Arbeitgeber lässt Sie Recherchen zu PUPs anstellen ;)

Selbst wenn Sie darauf achten und genau auf PUPs achten (um diese für eine Studie gezielt aufzuspüren), kann sich eine vermeintlich einfache Installation als äußerst schwierig erweisen. Die Hersteller mancher PUPs geben sich größte Mühe, Antiviren-Programme zu umgehen und Programme zu (de)installieren, und das manchmal mit einer einzigen Codezeile. Einige PUPs sind wahrlich schwer zu erkennen selbst für einen versierten PC-Nutzer, von Otto Normalverbraucher einmal ganz zu schweigen.

 **So vermeiden Sie das Problem:** Nutzen Sie eine Virtual Machine und/oder erstellen Sie einen Snapshot zur Wiederherstellung Ihres Betriebssystems, bevor Sie sich in die Recherchen stürzen. Dies mag ein wenig übertrieben klingen, ist aber der beste Weg zur Vermeidung einer Ausbremsung Ihres Systems, selbst wenn es sich “lediglich” um den Rechner an Ihrem Arbeitsplatz handelt.

Wichtige Fakten zur Vermeidung von PUPs

Letzten Endes fällt jeder irgendwann vermutlich einem unerwünschten Programm zum Opfer. Der Softwaresektor muss eine klare Wendung vollziehen und sich gegen PUPs aussprechen, damit man sich entweder explizit dagegen entscheiden kann oder Antiviren-Programme sie offiziell als schadhaft blockieren dürfen. Hier noch einmal die wichtigsten Fakten zur Vermeidung potenziell unerwünschter Programme, die Sie im Hinterkopf behalten sollten:

- Seien Sie vorsichtig, verlassen Sie sich auf Ihren gesunden Menschenverstand und lassen Sie sich Zeit.
- Installieren, aktualisieren und nutzen Sie eine renommierte Antiviren-Software wie Emsisoft Anti-Malware, die Echtzeitschutz gegen PUPs bietet.
- Setzen Sie lediglich auf vertrauenswürdige Download-Quellen.
- Laden oder installieren Sie **NIEMALS** Anwendungen, die verdächtig oder bösartig erscheinen.
- Suchen Sie Optionen zur benutzerdefinierten Installation und nutzten Sie sie auch.
- Suchen Sie nach versteckten Buttons wie “Ablehnen” oder “Überspringen”, die oftmals in wenig auffälligen Schriftarten und Farben im Gegensatz zu großen auffälligen Buttons mit der Aufschrift “Weiter” gehalten sind.
- Prüfen Sie Ihren Computer auf PUPs und bereinigen Sie ihn regelmäßig, zum Beispiel auch mit dem kostenlosen Emsisoft Emergency Kit.

Wir wünschen eine schöne (PUP-freie) Zeit!

Quelle: http://blog.emsisoft.com/de/2015/01/27/10-wege-wie-sich-pups-auf-ihren-computer-schummeln-und-wie-sie-das-verhindern