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

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

# Was ist ein PUP?

In Sicherheitswissen by Jochen on December 23, 2013 | Deutsch, English, Français, Italiano

Wenn es um Anti-Malware-Technologie geht, so gibt es einiges an Fachbegriffen, die sich im Netz finden. Das trifft auf die meisten Sachverhalte zu, die mit Informatik zu tun haben. Da gibt es *Bits* und *Bytes*, *.exe* und *.mp3*. *Trojaner*, *Rootkits*, *Social Media* und *RSS-Feeds*. *Plattformen*, *Konsolen*, *Betriebssysteme*, *Anwendungen*. Artikel auf Websites werden auf *Blogs* veröffentlicht.

Das kann alles sehr verwirrend sein, insbesondere wenn sich Begriffe überschneiden. In der Anti-Malware-Welt ist einer besonders problematisch, und zwar der der **PUPs**.

## Zunächst einmal: ein PUP ist kein Spielzeug

Obwohl es vom Namen her dem ähnelt, so hat ein PUP nichts mit einer Puppe zu tun. PUP steht für **Potentially Unwanted Program**, und die Programme, die unter diesem Spitznamen zusammengefasst werden, unterscheiden sich leicht von Malware.

Von einem technischen Standpunkt aus ist ein PUP keine Malware. PUPs werden nicht in der Absicht erstellt, Ihren Computer zu beschädigen oder sich Ihre persönlichen Informationen anzueignen. PUPs sind in der Regel vielmehr Marketing-Werkzeuge, die ihren Weg auf Ihren Computer durch ein wenig Social Engineering finden.

In der Vergangenheit bezeichnete man PUPs als Spyware und Ad-Ware, aber vielen Firmen, die diese Programme erstellen, gefielen diese Begriffe wenig. Sie fanden sie sogar eher kontraproduktiv, da man dadurch ihre Programme mit Malware in Verbindung brachte, was für Abschreckung sorgte. An und für sich gibt es jetzt eine klare gesetzliche Trennlinie zwischen PUPs und Malware, und jeder im IT-Sektor, der Programmen ein Etikett aufdrückt, sollte den jeweiligen Begriff mit Bedacht wählen.

## Wie kann ich mir PUPs einfangen?

Passenderweise fangen Sie sich ein PUP ebenso einfach wie zum Beispiel einen Welpen ein. Sehen wir uns zwei Szenarios an.

*Szenario 1*

Jeden Tag, wenn Sie von der Arbeit nach Hause kommen, fragt Sie Ihre 10-jährige Tochter, ob sie einen Hund haben kann. Sie ist dabei von Anfang sehr direkt. "Mama, können wir einen Hund haben?", fragt sie höflich. Sie verneinen, denn Sie wissen, was das alles mit sich bringt. Zerkaute Möbel, hartnäckige gelbe Flecken, überall Haare und Gott weiß, was sonst noch. All das wird nicht Ihr Haus zum Einsturz bringen, aber sicherlich optisch, geruchlich und vom Wohngefühl her für einige negativen Veränderungen sorgen.

Aber Ihre Tochter bleibt hartnäckig. Sie setzt ihre Hunde-Kampagne einen guten Monat lang fort und fragt jeden Tag nach der Arbeit, ob sie nicht einen kaufen können. Sie wird dabei immer kreativer, legt sich detaillierte Aktionspläne zurecht und vergleicht die Vorteile, einen Hund zu haben, mit den Kosten. "Das wird mich zu mehr Verantwortung erziehen", sagt sie. Das geht so weiter, bis Sie eines Tages genug haben und in einem Moment der Schwäche antworten: "In Ordnung, du bekommst schon einen."

Doch da hört es noch lange nicht auf. Eines Samstagmorgens gehen Sie zur Tierhandlung, betreten das Geschäft und sehen sich mit einem Sonderverkauf für Hunde konfrontiert. Überall sind Welpen, und eine junge, dynamische Verkäuferin teilt Ihnen mit, dass es heute ein Sonderangebot mit zwei Hunden zum Preis von einem gibt! Die Augen Ihrer Tochter leuchten. Am liebsten würden Sie die Verkäuferin schlagen, besinnen sich jedoch eines Besseren und erkennen, dass es zu spät ist. Sie gehen mit zwei Welpen nach Hause, ob Sie nun wollen oder nicht.

*Szenario 2*

Jeden Tag kommen Sie von der Arbeit nach Hause, melden sich an Ihrem PC an und surfen im Netz. Sie haben kürzlich einen neuen Laptop gekauft, und meine Güte, geht das schnell! Sie können bis zu 30 Fenster gleichzeitig offen haben, und bei der Suche nach neuer Unterhaltung oder Informationen sind Sie nicht zu stoppen.

Sie sind begeistert, denn das Internet scheint geradezu explodieren angesichts der Fülle neue Plug-ins und Anwendungen. Die meisten sind kostenlos, und viele sogar nützlich. Jeden Tag finden Sie etwas Neues und Aufregendes, das Sie einfach ausprobieren müssen, und Sie verfallen in die Routine, einfach immer wieder auf INSTALLIEREN zu klicken, bis alles beendet ist.

Sie sind gewissermaßen wie das aufgeregte Kind, das einen Welpen möchte. Sie möchten einfach alles ausprobieren, was Spaß macht, und denken nicht an die Langzeitfolgen Ihres Handelns. Was sogar noch schlimmer ist: Sie können unmittelbar haben, was Sie möchten, und brauchen nicht erst Ihre Mutter oder Ihren Vater darum anbetteln.

Anders gesagt sind Sie ein bisschen wie die überforderten Eltern. Sie wissen, dass das Herunterladen jeder Art von Freeware nichts Gutes verheißen kann, aber Sie sind müde von der Arbeit und kümmern sich nicht großartig um das Kleingedruckte jeder Installation. Sie möchten sich einfach entspannen und Ihre Freeware genießen.

## Was geht aber wirklich vor sich?

Freeware ist toll, aber der Grund dafür, dass sie kostenlos ist, liegt darin begründet, dass sie als Werbemittel für proprietäre Software genutzt wird. Wie kann das passieren? Im Falle einer von der Installation herrührenden Begeisterung oder des Gefühls, **"einfach zu müde zu sein, das Kleingedruckte zu lesen"**, installieren die meisten viel mehr als das, was sie ursprünglich wollten.

Autoren von PUPs wissen um diesen Umstand. Sie wissen, dass die meisten sich nicht die Zeit nehmen, durch alle Schritte jedes Installationsassistenten zu lesen, und da sie Softwareentwickler sind, sehen Sie darin eine erstklassige Gelegenheit, umsonst für ihre Software zu werben.

Was handeln Sie sich ein? Nun, das kommt auf den Entwickler an. Manchmal handelt es sich um einen Internet-Toolbar, der zusätzliche Funktionen bietet, während groß darüber das Logo des Autors prangt, sodass Sie dieses jedes Mal vor Augen haben, wenn Sie eine Suche starten. In anderen Fällen handelt es sich um eine Wetteranzeige, die Sie über die Wetterbedingungen in Dubai oder anderswo von Ihrem aktuellen Standort aus informiert. In wieder anderen Fällen sind PUPs einfach Spyware (wiederholen Sie das nicht!), die Ihre Suchgewohnheiten überwachen und Sie dazu verleiten, Dinge zu kaufen, die Sie eigentlich nicht brauchen.

An und für sich ist ein einzelnes PUP relativ harmlos. Betreten Sie aber die Tierhandlung während einer Sonderaktion für Welpen, und Sie können sich sicher sein, dass Sie mit mehr den Laden verlassen, als Sie ursprünglich wollten.

## Das Problem mit PUPs

Das Problem mit den PUPs liegt darin, dass die meisten nicht nur eines, sondern einen ganzen Stall davon voll haben. Das passiert, da die meisten Computernutzer im Laufe der Zeit einiges an Freeware herunterladen – und die meiste Freeware wird mit mindestens einem PUP im Paket geliefert.

Überladen Sie Ihren Computer mit allem möglichen, und Sie können sich sicher sein, dass er immer langsamer wird. Letztendlich haben PUPs daher ihren Namen. "Potenziell unerwünscht", weil Ihr Computer irgendwann nur noch im Schneckentempo arbeitet, wenn Sie nur genug davon installieren. Genau wie ein Welpe genug Zerstörungspotenzial mitbringt, Ihren Teppich oder Ihre Couch zu ruinieren, werden 2 oder 3 Welpen Sie an den Rand der Verzweiflung und dazu bringen, Ihr Haus niederzubrennen.

Anders gesagt sind PUPs das Junkfood Ihres PCs. Einmal ist keinmal, aber essen Sie eine ganze Tüte davon, wissen Sie schon, wie das endet…

## PUP-Arten

Ebenso wie unsere Hunde gibt es PUPs in beinahe unbegrenzten Varianten, von groß zu klein, von tollpatschig zu sabbernd, zu überdreht und in jeder Art und Weise schlichtweg nervtötend. Ein paar sehen folgendermaßen aus:


Wenn Sie auf das Bild klicken und sich das Ganze genauer ansehen, werden Sie ein paar Dinge feststellen. Eines ist eine neue Verknüpfung **(das blaue P)** in der Windows-Taskleiste unten. In diesem spezifischen Screenshot hat der Nutzer auf die Verknüpfung geklickt. Das es sich bei der Verknüpfung allerdings um ein PUP handelt, wurde der Nutzer automatisch zur Internetadresse in der Adressleiste weitergeleitet, statt dass ein Programm gestartet wurde. Hierbei handelt es sich im Grunde um eine automatische Werbung für PC-Sicherheitssoftware, und die Werbung soll Ihnen vorgaukeln, Ihr Computer sei untersucht worden und Sie befänden sich in einer ausweglosen Lage.

Oftmals machen sich PUPs die Windows-Taskleiste zu Nutze, um so weniger auffällig zu erscheinen. Einige PUPs gehen sogar so weit, Windows-Funktionen zu "verbessern", indem sie neue Elemente hinzufügen. Ein kürzlich aufgetauchtes PUP versuchte seine Opfer damit zu beeindrucken, indem es den Start-Knopf in Windows zurückbrachte. Warum das? In den meisten Fällen handelt es sich um einen Fall mit Hundeaugen. PUPs wissen, dass sie nichts Gutes verheißen, aber möchten dennoch, dass Sie sie mögen. Wieder andere PUPs kommen wie folgt daher:


Man beachte die Überfülle an Internet-Toolbars im oberen Bildschirmbereich. Jedes davon ist ein PUP, das darauf wartet, dass sie darauf klicken, damit eine neue lästige Werbung angezeigt wird. Bei genug PUP-Toolbars wird Ihr Browser letztendlich abstürzen, da jedes PUP gleichzeitig um Ihre Aufmerksamkeit buhlt (d. h. Speicherressourcen verbraucht). Hier hat der Kampf der PUPs um die Vorherrschaft dazu geführt, dass ein PUP so weit geht, einen "Systemfehler" anzuzeigen, der Sie darauf hinweist, dass Sie zu viele PUPs heruntergeladen haben. Die Lösung? Noch mehr PUPs herunterladen natürlich!

# Wie kann ich PUPs aus dem Weg gehen?

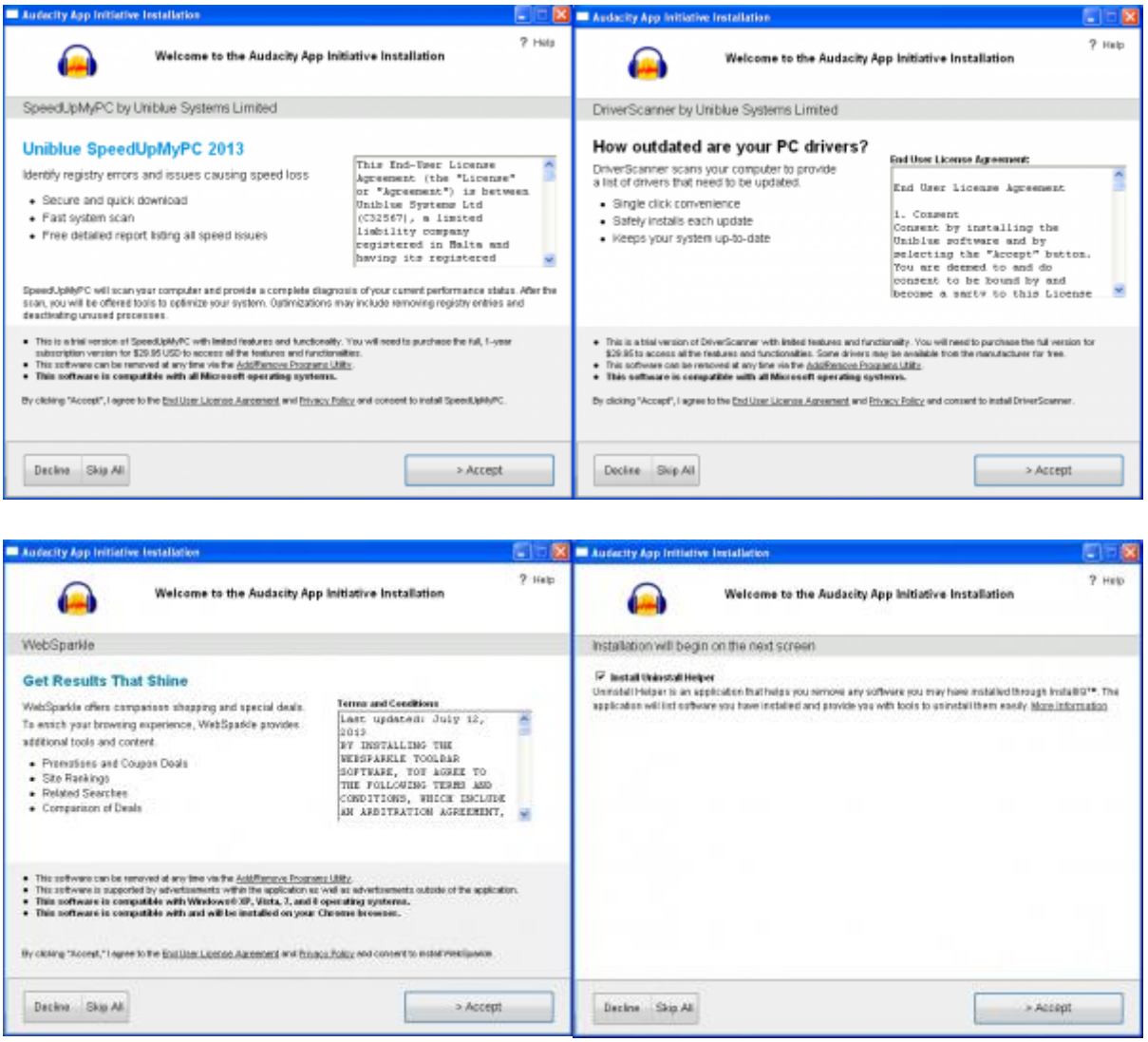
Glücklicherweise ist es um einiges leichter, PUPs aus dem Weg zu gehen, als Ihrem Kind einen Wunsch auszuschlagen. Computer sind nicht so süß wie Kinder (zumindest noch nicht), und es ist ihnen egal, was Sie mit ihnen machen.

Der beste Weg, PUPs zu vermeiden, besteht darin, den Installationsvorgang zu entschleunigen. PUPs können mit jeder neuen Software, Freeware oder nicht, geliefert werden, und alles, was es braucht, um sie von Ihrem PC fernzuhalten, ist, alles genau zu lesen und vorab ausgewählte Kontrollkästchen abzuwählen.


Dieses spezifische Beispiel zeigt, wie vielschichtig PUPs bei der Installation sein können. "**Delta Search**" ist selbst eine PUP-Toolbar, und bei seiner Installation wird standardmäßig noch ein weiteres PUP installiert. RealPlayer ist ein angesehenes Produkt, aber es wird mit so viel Marketing-Werkzeugen geliefert, auf die viele Nutzer getrost verzichten könnten. Das ist für sich nicht übermäßig, doch klicken Sie nur auf "Weiter", und Sie sehen noch eine weitere Installationsaufforderung für ein PUP.


Dieses Mal handelt es sich um eine kostenlose Testversion von **TuneUp Utility 2013**, was in PUP-Begriffen ein kostenloses Werbemittel darstellt. Wie bei PC Speed Up oben ist TuneUp Utility 2013 so konzipiert, Sie davon zu überzeugen, dass Ihr Computer kaputt ist und die einzige Rettung im Kauf von

TuneUp Utility besteht. Das ist nicht böswillig, aber man könnte dies durchaus als aggressives Marketing ansehen. Ein Programm, das diese aggressive Mentalität auf eine ganze neue Ebene hebt, ist **Install IQ.**




Das sind 4 separate Installationsfenster für 4 separate PUPs! Wie wahrscheinlich ist es, dass Sie sich alles Kleingedruckte durchlesen? Das sagt Ihnen, wie anfällig Ihr Computer für PUPs ist.

## Die PUP-Signaturdatenbank von Emsisoft

Neben aufmerksamem Lesen besteht eine weitere Methode der Vorbeugung gegen PUPs in der Verwendung einer Antiviren-Software, welche die Erkennung von PUPs unterstützt, **wie Emsisoft Anti-Malware**. Emsisoft legt besonderes Augenmerk auf PUPs, die mit Freeware geliefert werden, da sie die am weitesten verbreiteten sind. In der Tat kennt unsere umfassende Signaturdatenbank 1.000 PUPs, sodass Sie sich nicht darum kümmern müssen, da die Software Sie auf diese aufmerksam macht, bevor Sie auf INSTALLIEREN klicken.

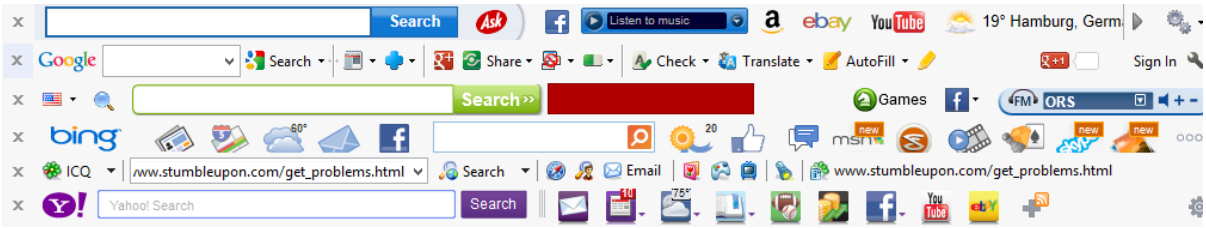

Betrachten Sie uns als die Ohrfeige, die Sie der übereifrigen Tierhändlerin geben wollten, bevor sie Sie auf das Angebot über 2 Welpen zum Preis von 1 hinweist. Und seien Sie unbesorgt, *unsere* Installationsroutine ist vollkommen frei von PUPs.

Quelle: http://blog.emsisoft.com/de/2013/12/23/was-ist-ein-pup/

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

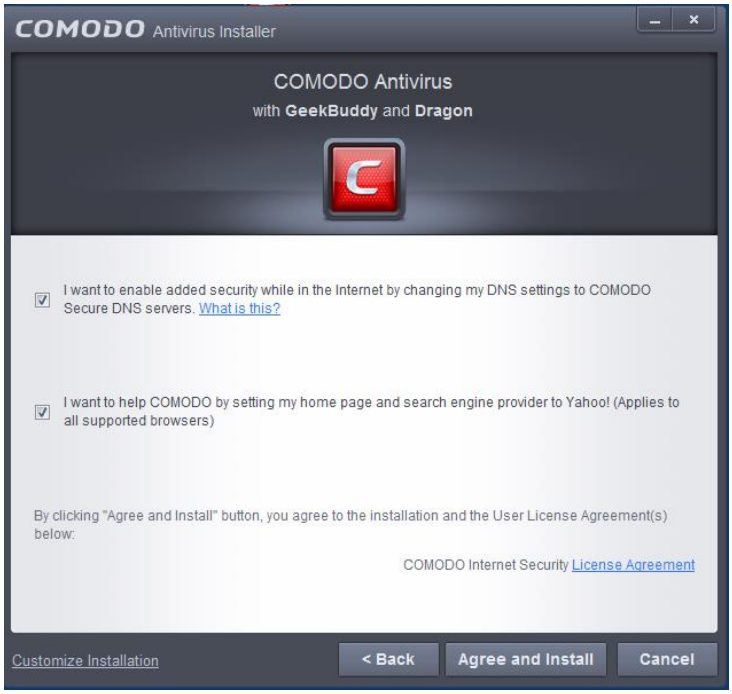
Wir entschieden uns dazu, einen genaueren Blick darauf zu werfen, und führten den gleichen Test mit allen anderen kostenlosen vollständigen Antiviren-Suites durch; die Ergebnisse waren ziemlich schockierend:

**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.

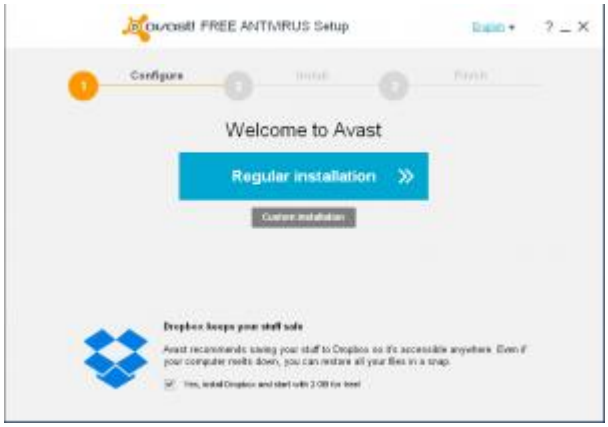
Antiviren-Programme sollen Ihren PC gegen Viren schützen; jedoch handeln viele Ihnen bei der Installation fragwürdige Programme ein, ohne dass dies klar offen gelegt wird. Unten finden Sie die Liste von 8 kostenlosen Antiviren-Programmen und welche Art von PUPs Sie sich bei der Installation einhandeln. 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.

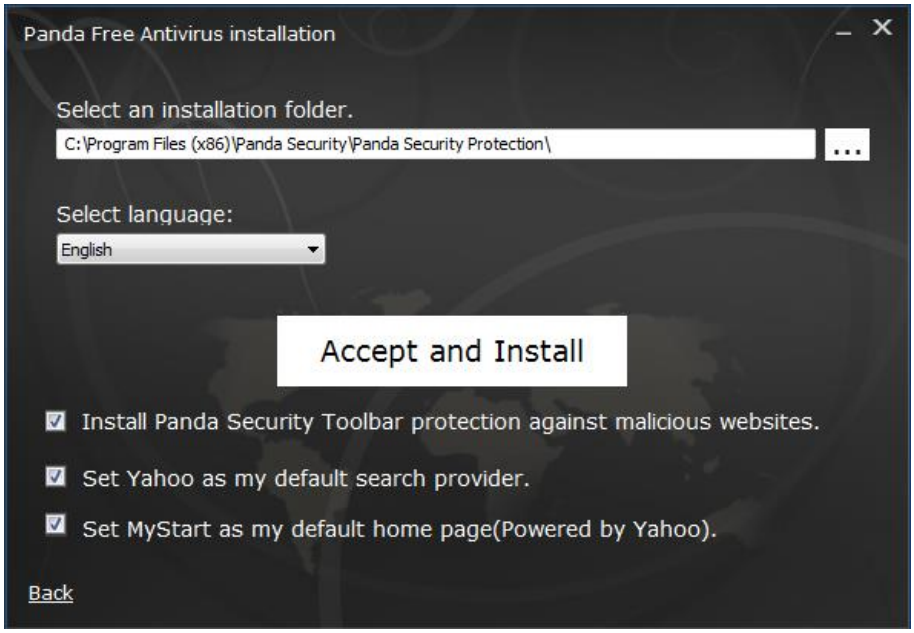
**Comodo AV Free:** ändert die Homepage und Suchmaschine auf Yahoo während der Installation, es sei denn, der Nutzer deaktiviert das Kontrollkästchen.



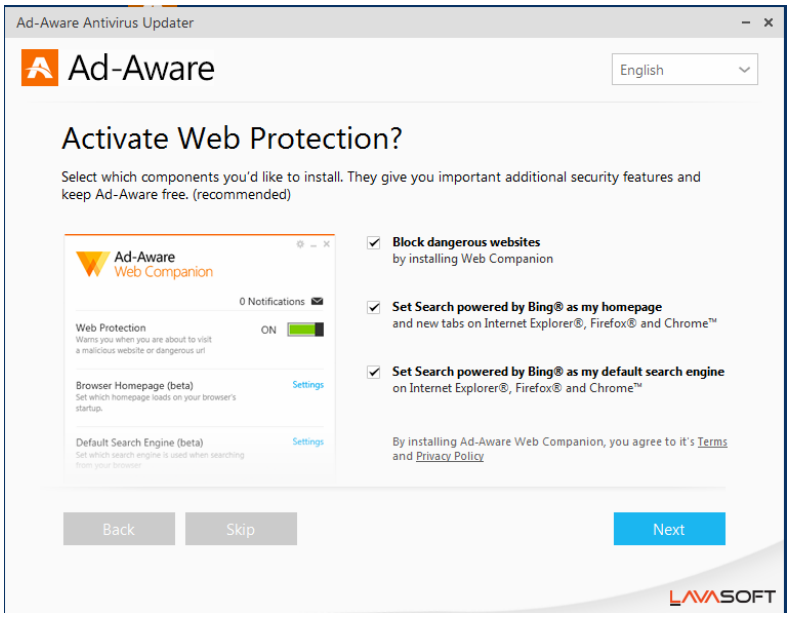

**Avast Free:** bietet Ihnen Dropbox standardmäßig zur Installation an, wenn Sie nicht das Kontrollkästchen deaktivieren.



**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.

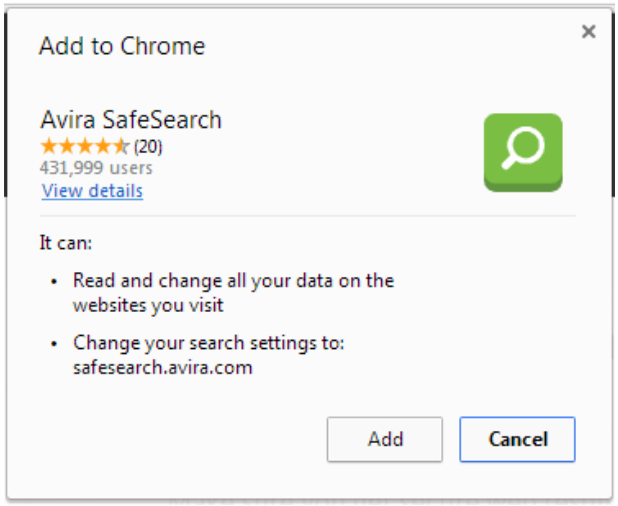


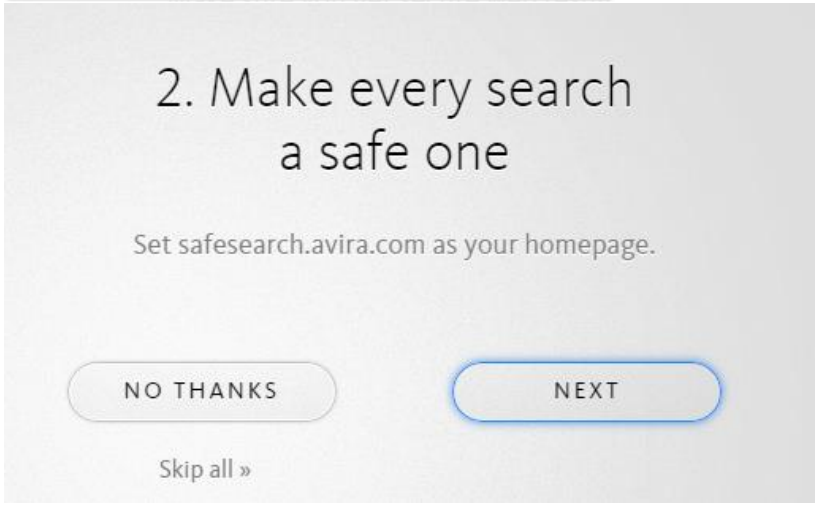

**AdAware free:** installiert WebCompanion standardmäßig, wenn Sie nicht das Kontrollkästchen deaktivieren. Ändert ebenso Ihre Homepage auf Bing und Ihre Suchmaschine auf Bing, wenn Sie sich nicht dagegen entscheiden. Es wird offen gelegt, dass AdAware diese Programme anbietet, damit die Software kostenlos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



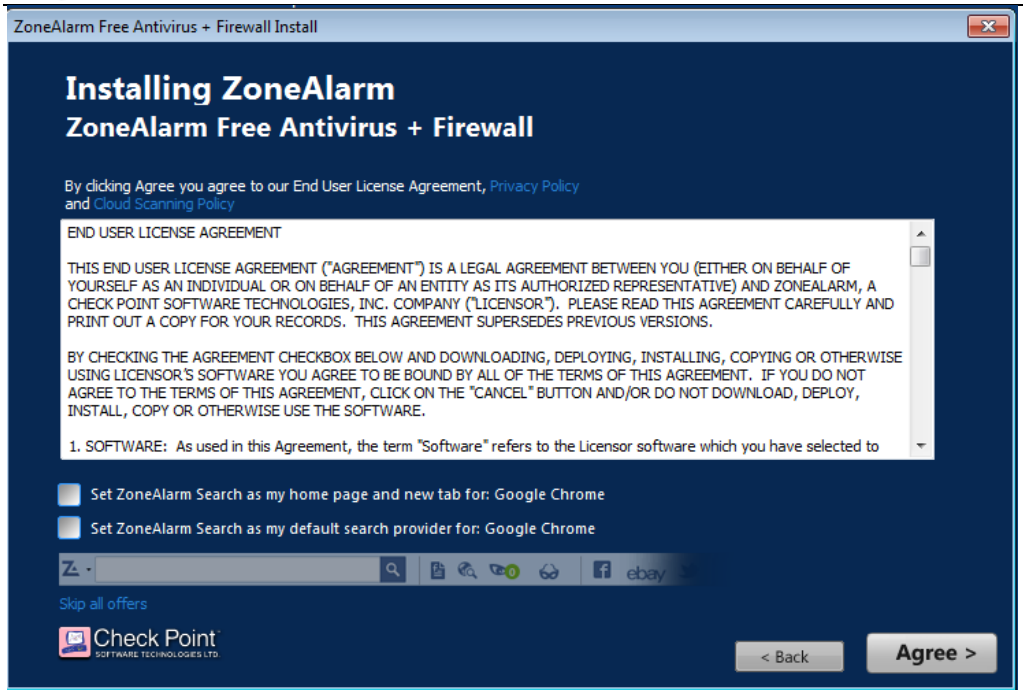

**Avira free:** bietet Dropbox nach der Installation an. Ändert Ihre Suchmaschine zu Avira Safe Search, wobei es sich um eine Version der Ask-Toolbar handelt. Avira legt die Partnerschaft mit Ask offen und gibt an, dass "*man Ask.com als Partner gewählt habe, um den*

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

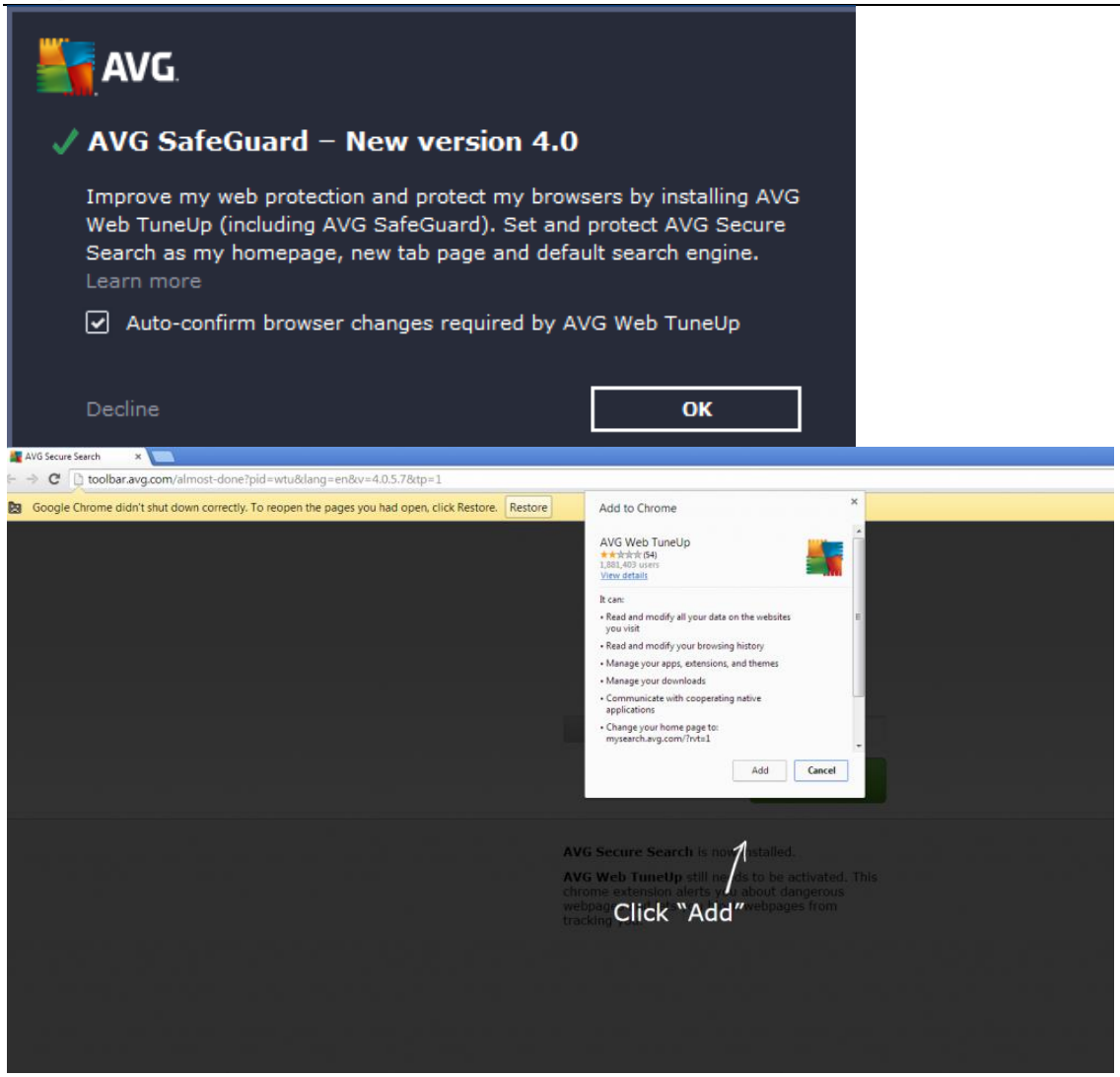



**ZoneAlarm free AV + Firewall:** bei benutzerdefinierter Installation: ändert Ihre Homepage auf ZoneAlarm und Ihre Suchmaschine. Dabei handelt es sich um eine rebrandete Ask-Toolbar, was allerdings auf der Website von ZoneAlarm keinerlei Erwähnung findet.




**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.

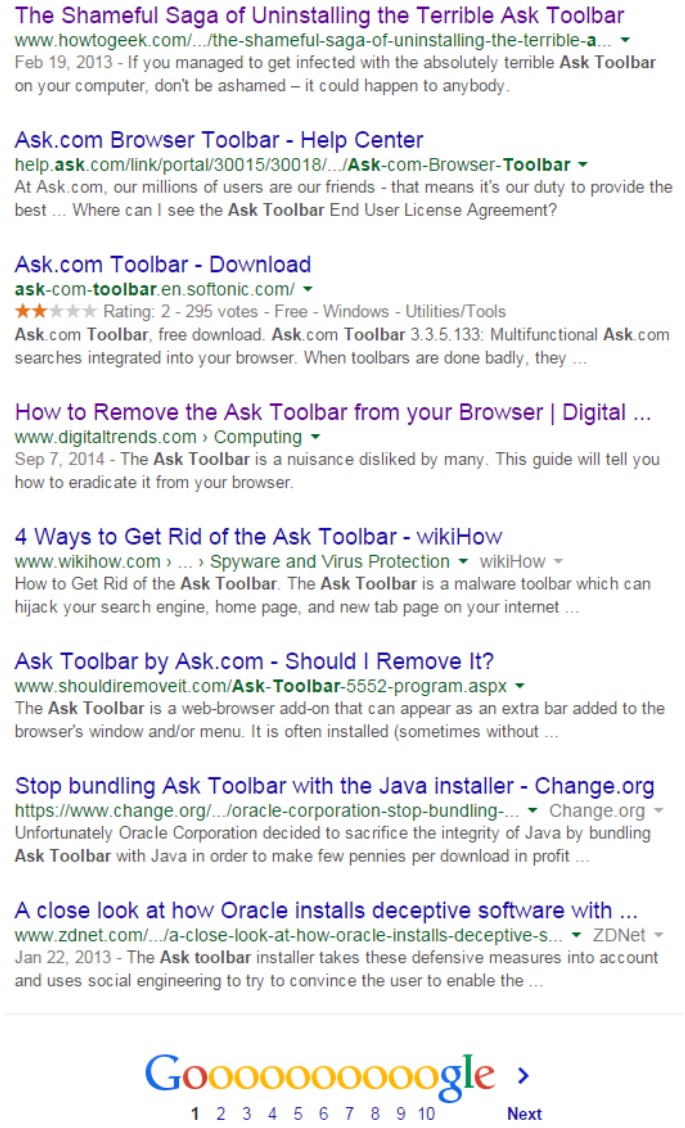



## Beliebte Mittel und Wege bei kostenlosen Antiviren-Programmen mit PUPs Geld zu machen

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

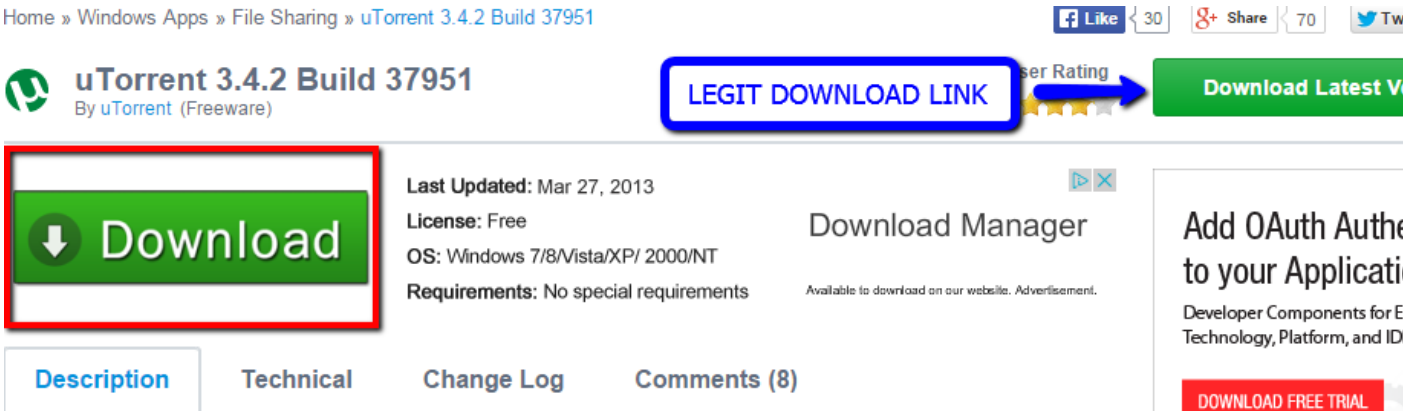
# 10 Wege, wie sich PUPs auf Ihren Computer schummeln. Und wie Sie das verhindern.

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.

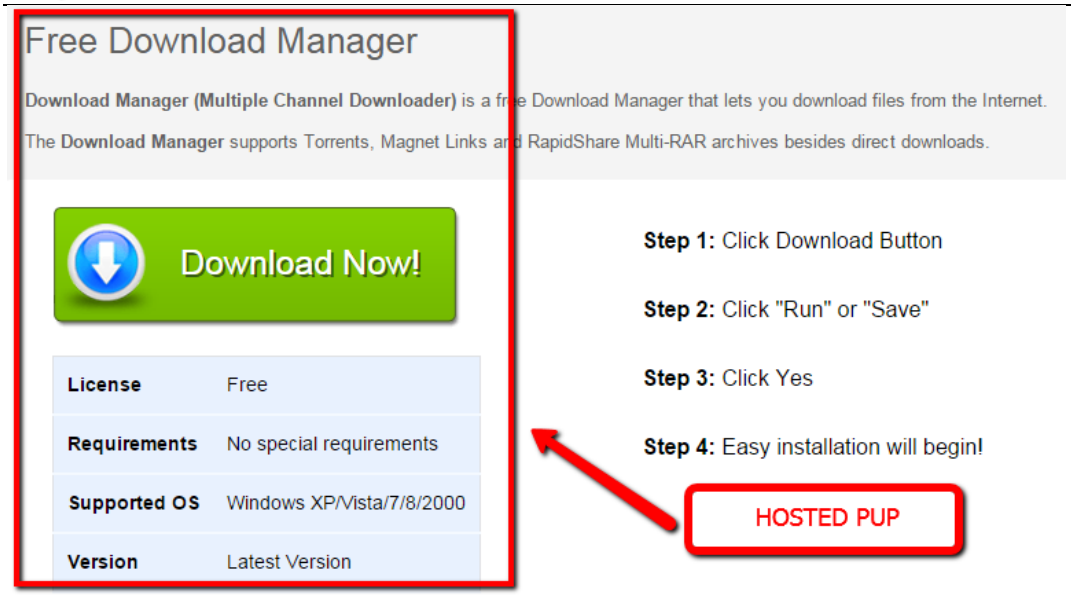
Angesichts Tausender neuer PUPs, jeden Tag und der Grauzone, in der PUPs operieren (zwischen nervender Software und Malware), besteht immer eine gute Möglichkeit, dass Sie auf PUPs treffen. Hier hat ein Kollege von Emsisoft Ihnen ein paar Methoden zusammengestellt, wie sie sich einnisten:

## 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.



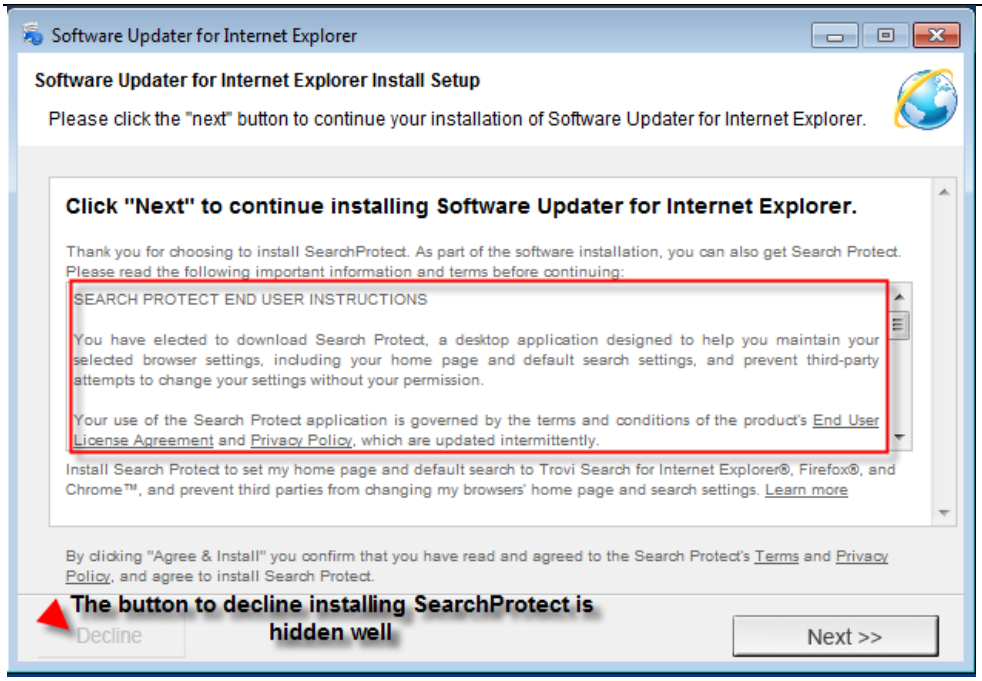

Moment – Wir wollten Utorrent, aber das sieht nicht ganz wie Utorrent aus … Was ist falsch gelaufen? Hierbei handelt es sich um eine sehr weit verbreitete Methode, bei dem Nutzer tagtäglich zum Download von PUPs verleitet werden. Ein beliebtes Download-Portal bietet Freeware-Software an. Klar, die Software 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.

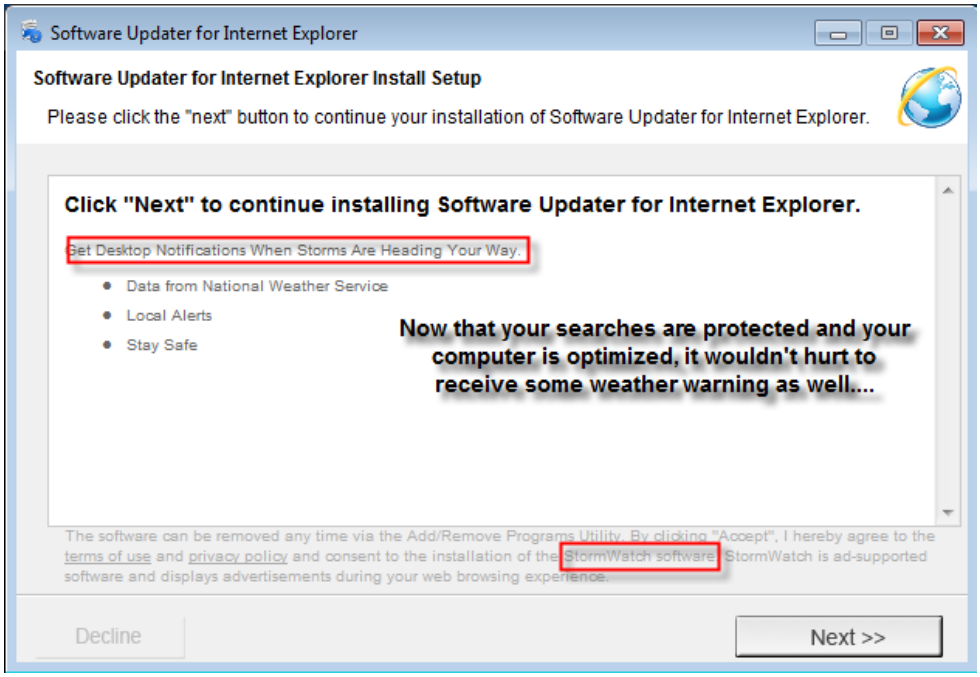
**So vermeiden Sie das Problem:** Am besten gehen Sie Download-Portalen schlichtweg vollständig aus dem Weg. Falls Sie sie dennoch nutzen, lassen Sie beim Download von Dateien größte Sorgfalt walten, verwenden Sie aktuelle Antiviren-Software mit aktivierter PUP-Erkennung, achten Sie auf Dateinamen und, 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!



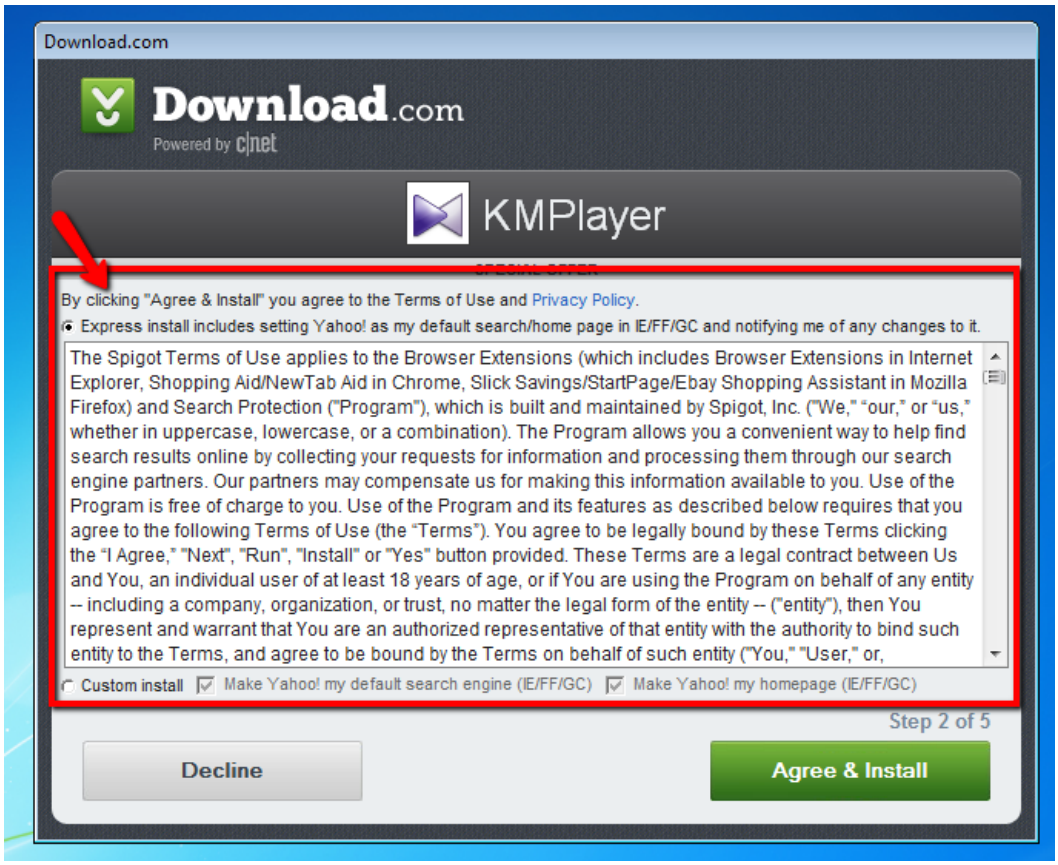

Die beiden Installationsprogramme oben machen dem Nutzer nette Angebote. Jedoch sind diese Angebote alles andere als toll oder nett. Nach der Installation ändert Seach Protect Ihre Browser-Einstellungen (Suchmaschine, Homepage, Tab-Einstellungen) und kann sogar manche Ihrer Surfdaten an unbekannte Quellen 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.



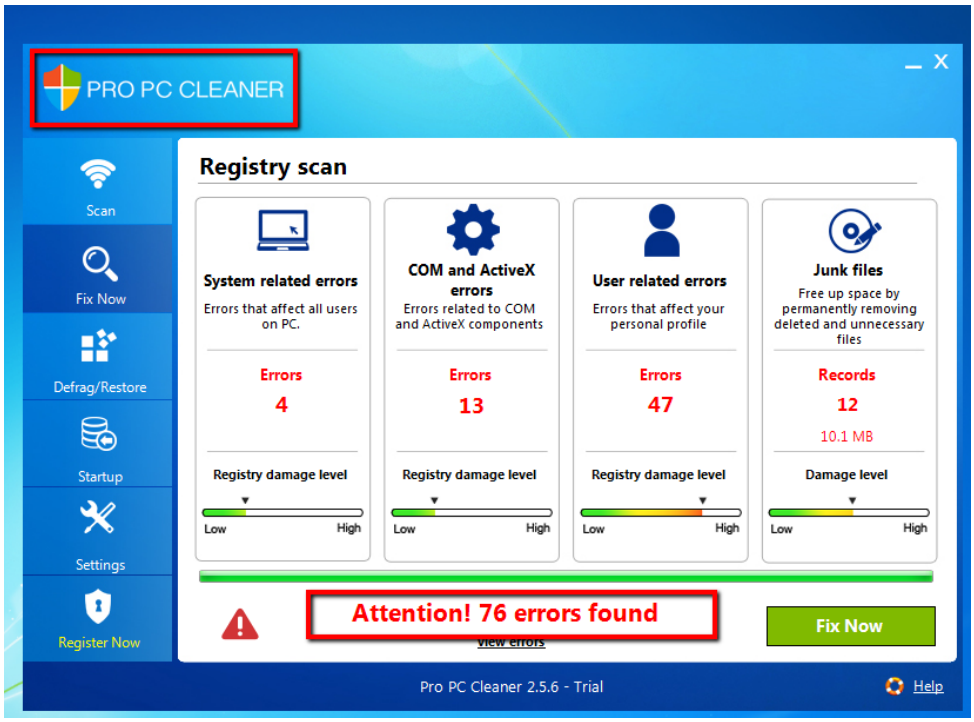

Hierbei handelt es sich um die zweite Welle potenziell unerwünschter "Sonderangebote", bevor Sie endlich zum legitimen Installationsprogramm gelangen. "Pro PC Cleaner" wird klammheimlch auf Ihrem PC installiert und bombardiert Sie dann mit gefälschten Funden, die auf vielerlei Art und Weise den letzten 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:

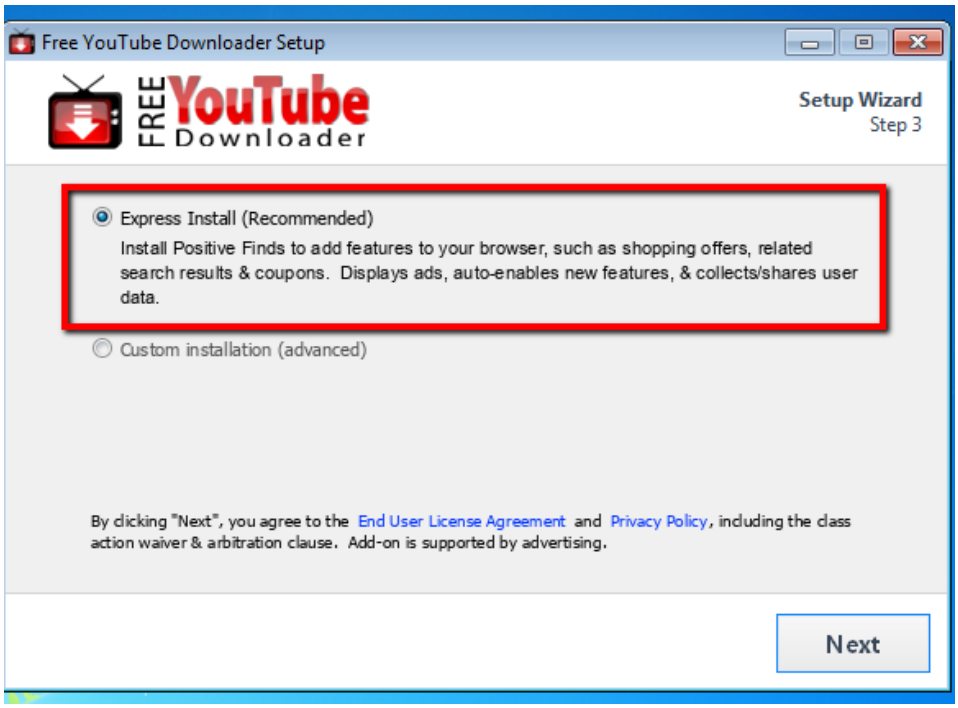


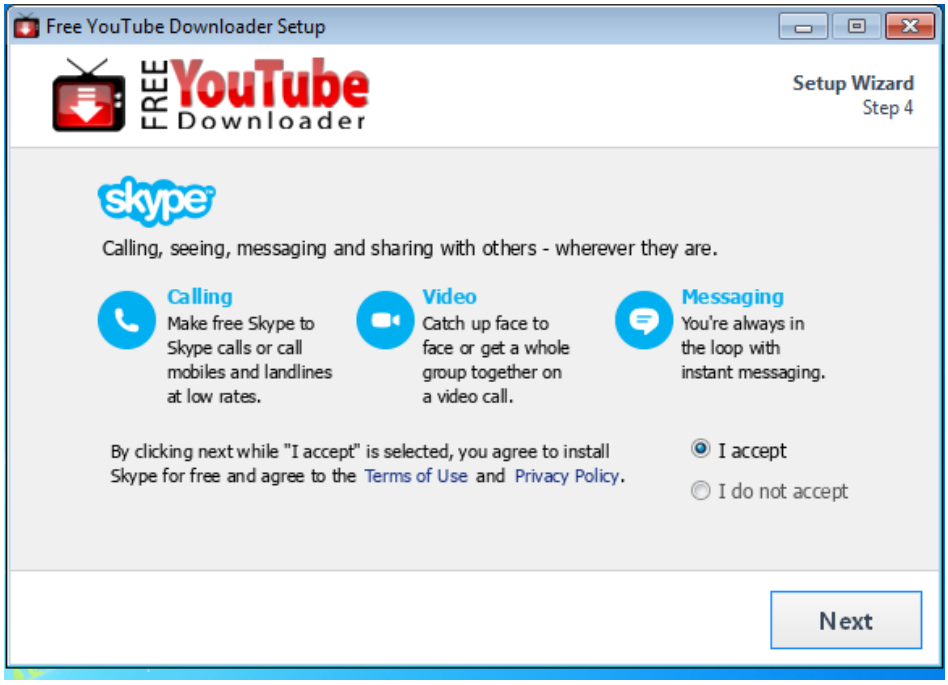

Das oben gezeigte PUP wurde in Wahrheit im Hintergrund durch Annahme der Bestimmungen des EULA des Downloaders von Download.com für KMPlayer heruntergeladen. Das ist erschreckend, aber leider wahr. Ein potenziell unerwünschtes Programm lädt ein anderes ebensowenig erwünschtes Programm herunter. Pro PC 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:



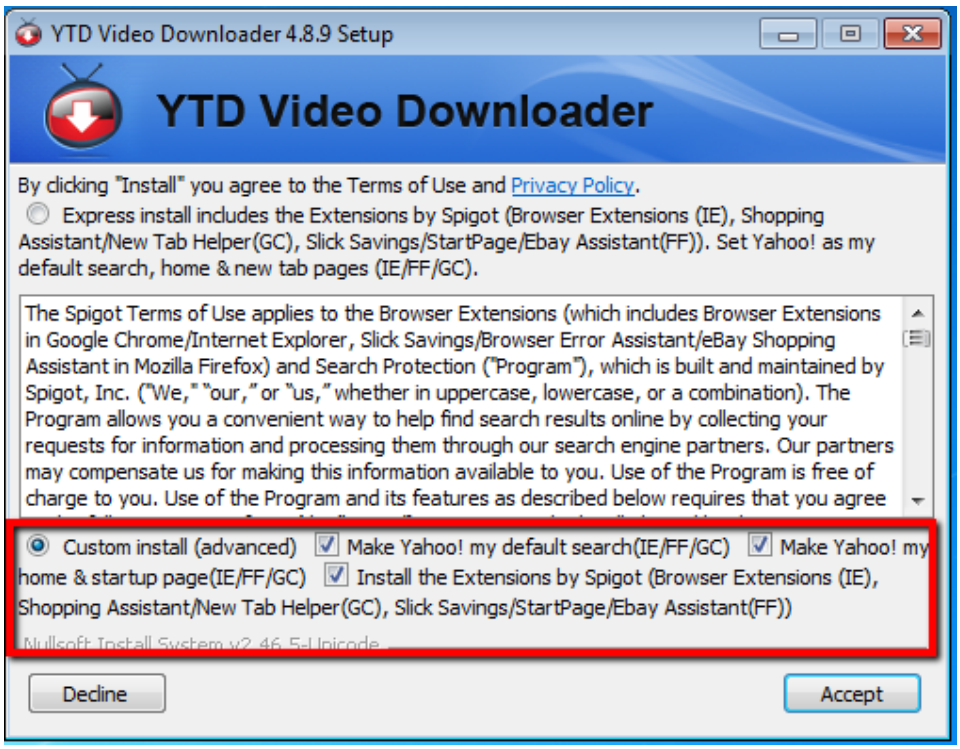

Da schau einer an. Die Express-Installation ist nicht immer der beste Weg. Ja, es stimmt schon, eine Express-Installation erfordert nur wenige Klicks, aber ist es wirklich das Risiko wert, potenziell unerwünschte Programme zu installieren? Skype ist eine legitime Anwendung; jedoch kann es sich für einen 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.

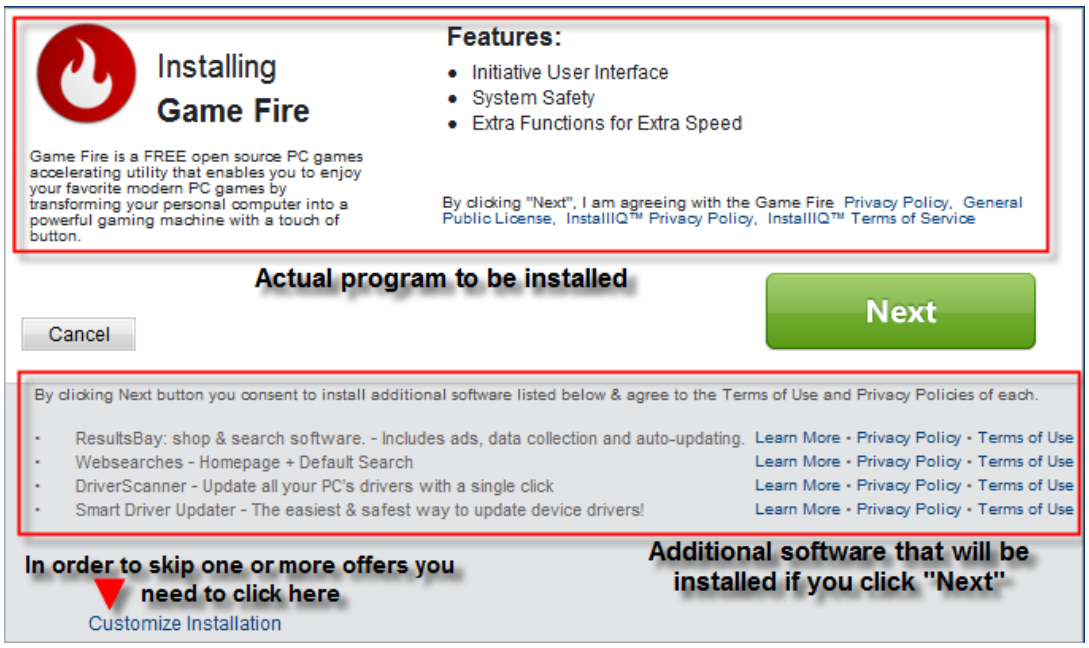



Man muss kein Wissenschafter sein, um zu erkennen, dass auch bei einer benutzerdefinierten Installation PUPs präsent sein können. Jedoch besteht zwischen einer Express- und einer benutzerdefinierten Installation ein signifikanter Unterschied: bei ersterer wird dem Nutzer keinerlei Option zur Änderung 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.

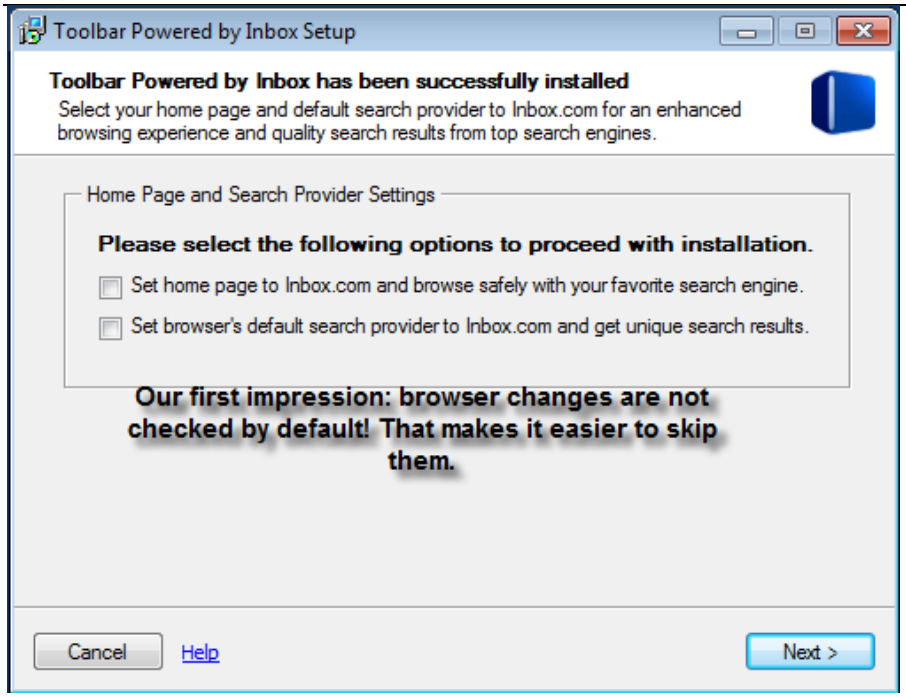


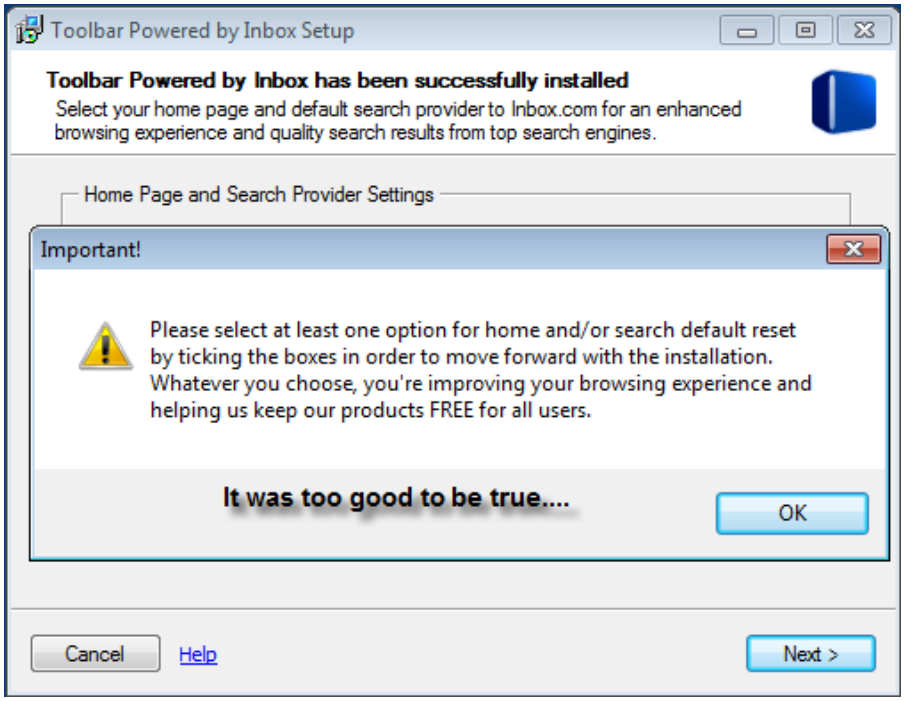

Wie im Screenshot oben zu sehen, wird ein Nutzer mit mehreren potenziell unerwünschten Zusätzen konfrontiert. Die Bilder zeigen: Game Fire, ResultsBay, WebSearches, Driver Scanner und Smart Driver Updater, die allesamt von einer einzigen Installation herrühren. Wow! Das ist einiges! PUPs übernehmen Installationsprogramme. 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

## Angebot der Woche



## Meist gelesen

Das Internet ist ein gefährlicher Ort

Wozu gibt es eigentlich Firewalls?
So scannen und reinigen Sie einen Computer mit Emsisoft Emergency Kit


Was ist ein PUP?
Malware und Viren – was ist eigentlich der Unterschied?

## Newsletter

Name:

E-Mail:

## Kategorien

- Alarme & Ausbrüche (128)
- Emsisoft Lab (4)
- Emsisoft News (35)
- Sicherheitswissen (100)
- Testberichte & Awards (19)

## NEUESTE AWARDS & REZENSIONEN

Video Review: Emsisoft Internet Security vs 500 malware samples

VB100 Award: Emsisoft ranks 2nd out of 27 in PC slowdown test


Emsisoft awarded “Top Rated Product of 2014″ by AV-Comparatives


Fourth time in a row: Advanced+ ranking in Real-World Protection Test


Video Review: Emsisoft Internet Security 9 scores 100%

## Archiv

- March 2015 (12)
- February 2015 (11)
- January 2015 (18)
- December 2014 (14)
- November 2014 (4)
- October 2014 (14)

Mehr sehen

## DIE NEUESTEN SCHLAGZEILEN


Anti-Virus, Anti-Malware, Anti-PUP? Was ist Emsisoft wirklich?


Sicherheitslücke zeigt, dass BIOS-Versionen der meisten Hersteller anfällig für Infektionen sind

Anspruchsvolle neue Variante von Point-of-Sale Malware entdeckt


SMS-Trojaner "Podec" umgeht CAPTCHA auf Android-Handys


Neue Cryptolocker-Variante greift Spiele an


Das Ende von FREAK: Riesige SSL-Sicherheitslücke endlich behoben


Top-Downloadportale, die Sie links liegen lassen sollten



# Top-Downloadportale, die Sie links liegen lassen sollten

In Sicherheitswissen by Jochen on March 11, 2015 | Deutsch, English, Français

Kürzlich berichteten wir davon, wie viele potenziell unerwünschte Programme (PUPs) mit den 50 beliebtesten Downloads auf Download.com mitgeliefert werden. In Anbetracht der recht besorgniserregenden Ergebnisse entschlossen wir uns, die Gepflogenheiten auf anderen beliebten Downloadportalen einmal genauer anzusehen, ob es hier besser aussieht oder Sie Downloadportale schlichtweg allesamt links liegen lassen sollten. Die meisten behaupten, "saubere und sichere Downloads" anzubieten, und dies schreiben sie auch auf ihren Websites. Jedoch wird es für die meisten zunehmend schwierig, Downloadportalen zu vertrauen, da die Zahl mitgelieferter PUPs rapide steigt und die Software-Rezensionen auf den Websites selbst nicht ernsthaft objektiv scheinen.

Wir haben uns die zehn beliebtesten Downloadportale angesehen, die zehn dort beliebtesten Anwendungen heruntergeladen und geprüft, wie viele Toolbars, Adware, Homepage-Hijacker und anderen PUPs mitgeliefert werden, und so ihre Sauberkeit und Sicherheit auf die Probe zu stellen.

## Welche sind die zehn beliebtesten Anwendungen auf jedem Downloadportal?

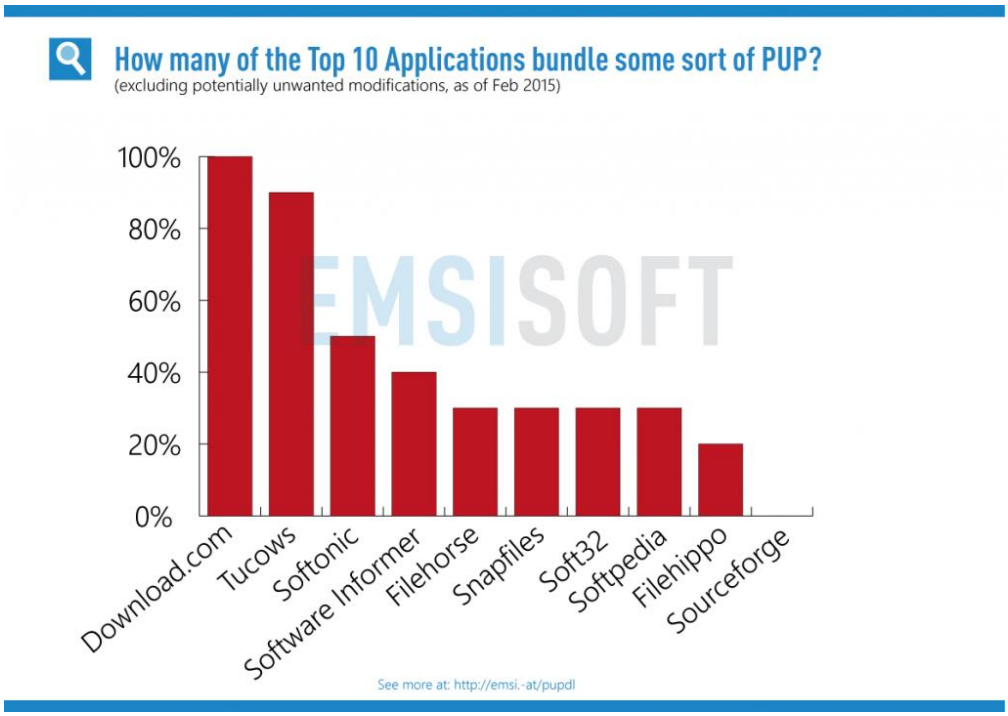
Zunächst schicken wir eine Liste der zehn beliebtesten Downloads nach Downloadportal voraus, die in diesen Artikel eingeflossen sind:

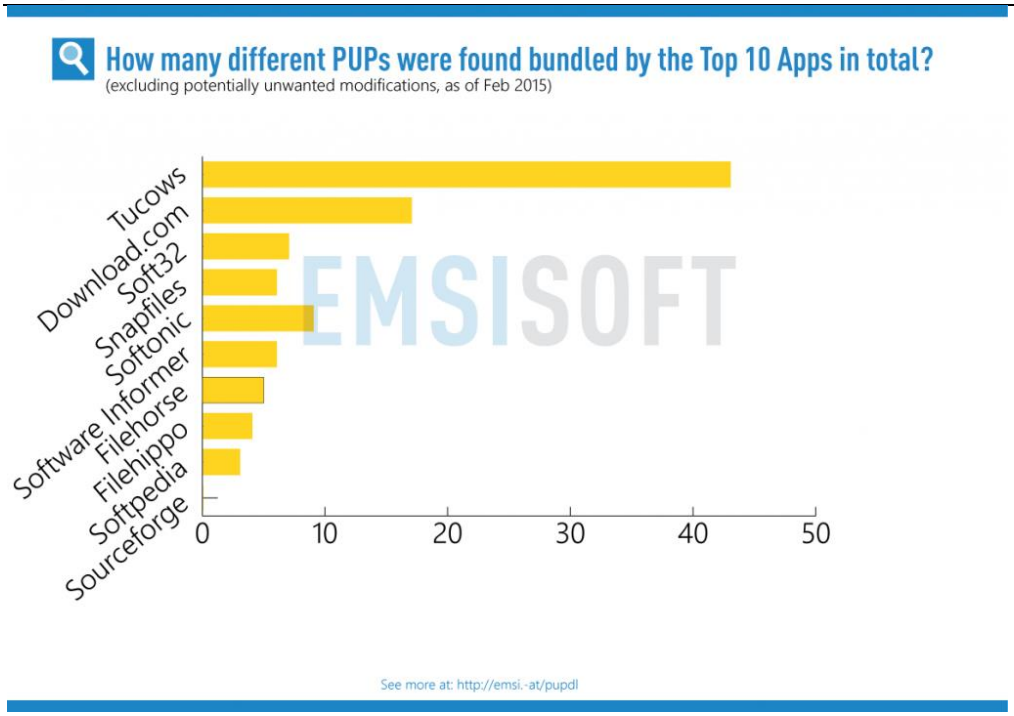
- **Download.com –** Avast Free Antivirus, AVG Free Antivirus, CCleaner, YAC, KMPlayer, YTD Video Downloader, Advanced System Care Free, DownloadApp, iObit Uninstaller, Free YouTube Downloader
- **Filehippo –** Adobe Reader, CCleaner, Mozilla Firefox, Picasa, Java, Recuva, Skype, uTorrent, VLC Media Player, WINRAR
- **Snapfiles –** Avast Free Antivirus, CCleaner, Comodo Internet Security Premium, Auslogics Disk Defrag, Eusing Free Registry Cleaner, Freemake Video Converter, GIMP, PDFX Viewer, Recuva, Revo Uninstaller
- **Softonic –** Avast Free Antivirus, BSplayer, Mozilla Firefox, Hotspot Shield, Adobe Flash Player, iObit Malware Fighter, Skype, uTorrent, VLC Media Player, YTD Video Downloader
- **Softpedia –** Google Chrome, Malwarebytes Antimalware, Nero Free, Orca, Super Simple Video Converter, Picasa, Image Burn, Skype, Unlocker, Yahoo Messenger

- **Tucows –** Express Files, Karaoke Player Software, Network Inventory Advisor, Internet Download Manager, Internet Explorer 8, IrFan View, Internet Explorer 9, Outlook Express, PDF Converter, PDF Reader
- **SourceForge –** 7Zip, Audacity, Camstudio, DVD Styler, FileZilla, KeePass, Media Player Classic, Process Hacker, Password Safe, VLC Media Player
- **Filehorse –** Avast Free Antivirus, Advanced System Care Free, Adobe Reader, AVG Free Antivirus, Java, Moborobo, Skype, iTunes, VLC Media Player, Winamp Media Player
- **Software Informer –** Free Download Manager, Avira Free Antivirus, Avast Free Antivirus, Free 3GP Video Converter, Free MP3 WMA Converter, AVG Free Antivirus, Free Sound Recorder, Free Video to JPG Converter, Free DWG Viewer, 123 Solitaire Free
- **Soft32 –** Counterstrike, DC++, Mozilla Firefox, Google Chrome, Google Earth, Virtual DJ, Internet Explorer 9, Yahoo Messenger, VLC Media Player, MSN Messenger

## Ein Chaos unter Downloadportalen: wie vielen können Sie blind vertrauen?

Wir haben alle o. g. Downloads nach Portal darauf geprüft, wie viele PUPs mitgeliefert werden. Bitte beachten Sie, dass nur PUPs gezählt wurden; potenziell unerwünschte Modifikationen oder Änderungen (wie z. B. Änderung des Suchseitentabs ohne Installation eines Programms) wurden außer Acht gelassen. Hier das Gesamtergebnis:

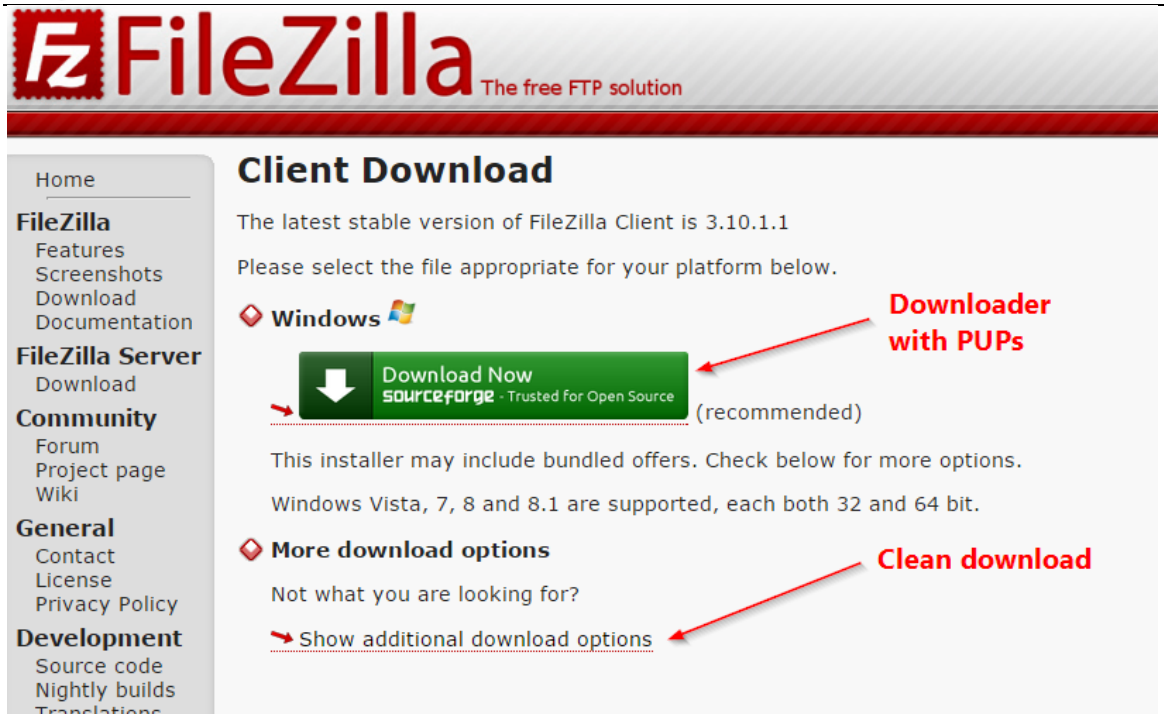





Wie Sie sehen können, **lieferte fast jedes Downloadportal ein oder mehr PUPs mit**. Von den zehn Downloadportalen im Test gelang es lediglich SourceForge, die beliebteste Software frei von PUPs zu halten. Die Downloadportale, die Sie auf jeden Fall links liegen lassen sollten, sind: Download.com, Tucows und Softonic.

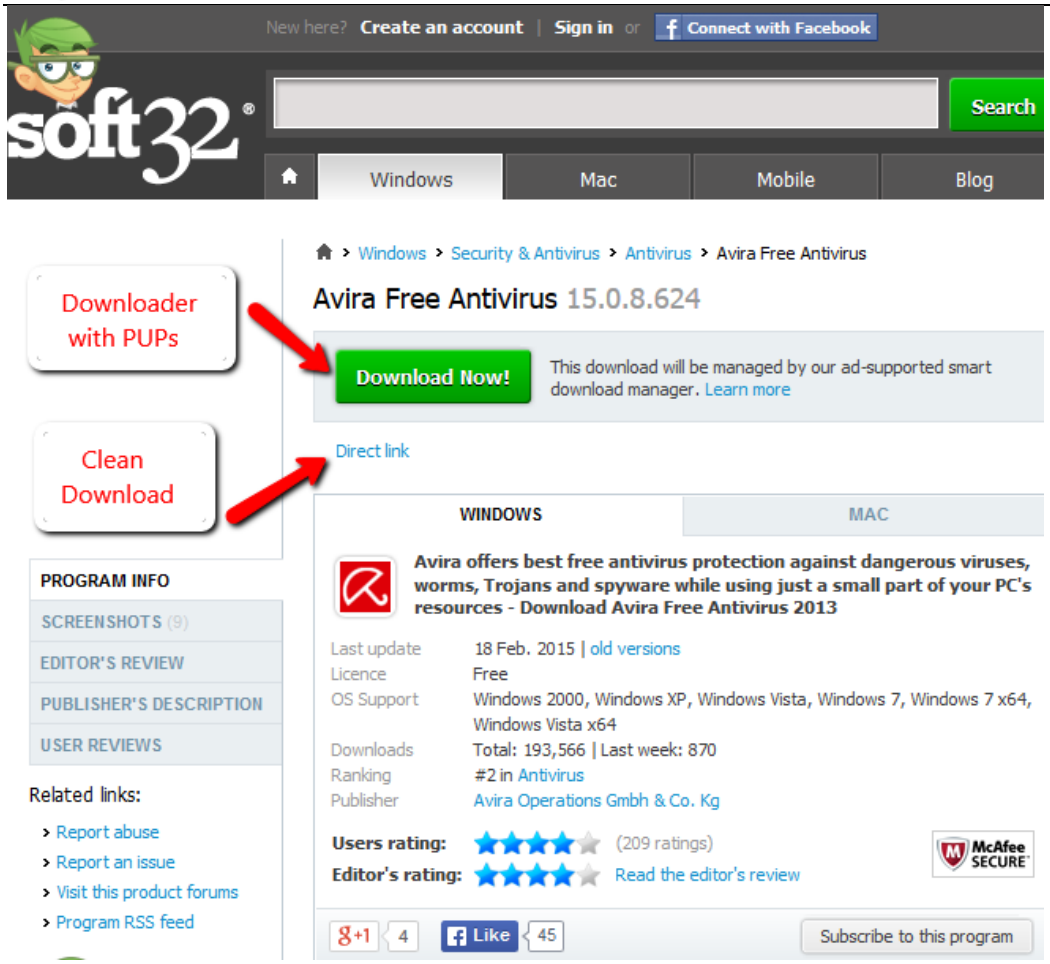
## Augen auf beim Klick auf den großen grünen Download-Button

Der große grüne "Download Now"-Button sieht auf den ersten Blick angenehm einladend aus; doch was verbirgt sich wirklich dahinter? Eine große Zahl "Download Now"-Buttons auf mehreren der großen Downloadportale und Websites von Softwareanbietern sind unsicher, da es sich bei ihnen in Wahrheit um clever verschleierte PUP-Installationsprogramme handelt. Ihre gewünschte Software sehen Sie ganz am Ende der Installation, nachdem Ihnen Tonnen an Junkware und PUPs vorgesetzt wurden. Seien Sie gewarnt: der direkte Downloadlink wird sehr wahrscheinlich verschleiert oder ganz versteckt; Sie müssen erst mühsam danach suchen. Unten finden Sie ein paar Beispiele in Screenshots von Installationsprogrammen, bei denen eben dieses Szenario eintritt:



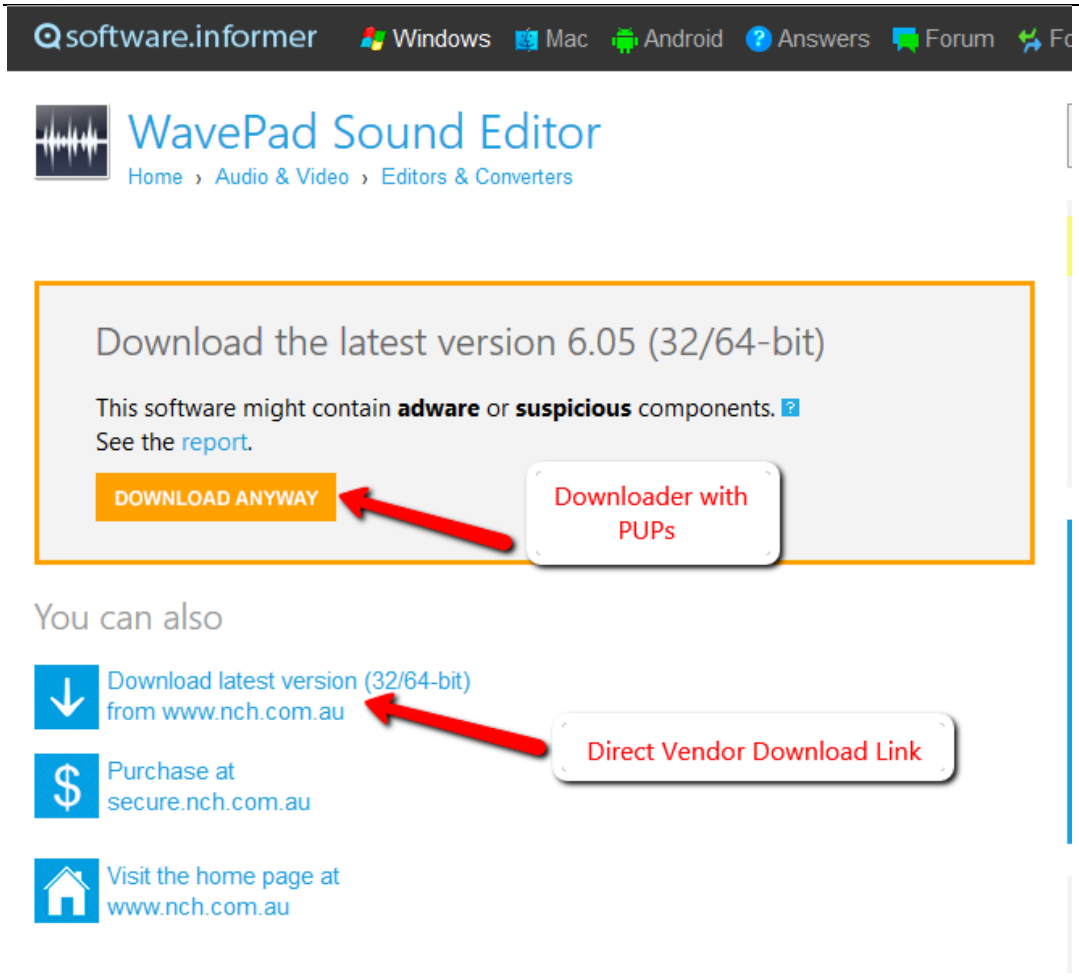

SourceForge schafft es wohl ganz gut, seine zehn beliebtesten Anwendungen frei von PUPs zu halten, doch einige PUPs werden durch optionale Installation von den Freewareanbietern mitgeliefert. SourceForge bietet Softwareentwicklern die Möglichkeit, mit ihrer Freeware durch Software-Bundles Geld zu verdienen, und augenscheinlich entscheiden sich manche Softwareanbieter zu diesem Schritt, wie Sie dem Screenshot der auf SourceForge beliebten Anwendung “FileZilla” oben entnehmen können.

Soft32 macht keinen Hehl daraus, seinen “Smart Download Manager” zu bewerben, der auf “smarte” Art und Weise Unmengen von PUPs auf Ihren Computer herunterlädt. Wieder einmal wird mit dem scheinbar sicheren “grünen” Download-Button der Nutzer hinters Licht geführt, und der sichere direkte Downloadlink für Avira findet sich darunter in ganz kleiner Schrift. Ironischerweise werden PUPs oft im Pack mit verschiedenen kostenlosen Antivirenprogrammen geliefert, die Ihren Computer eigentlich frei von diesen Eindringlingen halten sollen.




Diese Website ist derart “clever”, sogar das McAfee Secure-Logo zu führen, um den Nutzer beim Herunterladen dieser Software mit ihrem “Smart Download Manager” in falscher Sicherheit zu wägen.

Zu guter Letzt hostet Software Informer nicht nur einen PUP-Downloader, sondern warnt sogar die Nutzer davor, dass Adware oder verdächtige Komponenten enthalten sein “könnten”. Dies ist ein klarer Hinweis darauf, dass Sie sich mit einer Vielzahl unerwünschter Angebote und sogar mehr konfrontiert sehen, bevor die eigentliche Installation überhaupt erst beginnt. Als weiterer augenscheinlich verdächtniserregender Faktor ist die Farbgebung der Download-Buttons in Betracht zu ziehen. Der “Download anyway”-Button ist tatsächlich in Orange gehalten, was ein klarer Hinweis darauf ist, dass Sie Vorsicht walten lassen sollten, bevor Sie darauf klicken.




Unter dem PUP-Downloader sehen Sie weitere anderslautende Optionen. Unter den drei Optionen finden Sie einen "Download latest version"-Button, mit dem Sie zum direkten Downloadlink beim Anbieter gelangen. Verwenden Sie wann immer möglich diesen Link, damit Ihr PC frei von PUPs bleibt.

## Die 5 häufigsten PUPS auf allen Downloadportalen

Viele Downloadportale scheinen ähnliche unerwünschte Programme im Pack anzubieten. Einige der u. g. PUPs mögen harmlos erscheinen, werden aber ohne Wissen der Nutzer im Pack angeboten, und darüber hinaus können Sie Datenschutzprobleme bereiten oder potenziell Sicherheitslücken aufweisen.

| PUP | Portale, auf denen es zu finden war |
|---|---|
| Dropbox | Download.com, Snapfiles, Filehorse, Software Informer |
| AVG SafeGuard Toolbar | Download.com, Snapfiles, Softonic, Filehorse, Software Informer |
| Spigot | Download.com, Filehorse, Software Informer, Soft32 |
| Search Protect | Download.com, Tucows, Filehippo, Softonic |
| Pro PC Cleaner | Download.com, Tucows, Softonic |

Unter all den ähnlichen PUPs sind Dropbox und AVG SafeGuard Toolbar die am häufigsten zu findenden Programme auf allen Downloadportalen. Dropbox wird augenscheinlich mit einer Vielzahl

von Antiviren-Programmen angeboten. Spigot und Pro PC Cleaner fanden sich am häufigsten auf Download.com. Search Protect trat sehr oft auf, häufig Hand in Hand mit Spigot.

## Fazit: Bleiben Sie Downloadportalen am besten fern

Von den zehn beliebtesten Downloadportalen boten 90 % PUPs zusammen mit ihren zehn beliebtesten Softwareanwendungen an. Die Gesamtzahl an PUPs, die auf allen Downloadportalen zu finden waren, belief sich auf **100 potenziell unerwünschte Programme.** Dieses Ergebnis ist recht alarmierend, wenn man bedenkt, dass lediglich die zehn beliebtesten Anwendungen jedes Portals untersucht wurden. Bleiben Sie also daher lieber einfach Downloadportalen fern.

Hier ein paar Tipps, wie Sie von PUPs verschont bleiben:

- Laden Sie namhafte Software nur aus verlässlichen Quellen herunter und handeln Sie bei Download und Installation mit Bedacht.
- Setzen Sie auf den Download direkt beim Anbieter und gehen Sie Downloadportalen ganz aus dem Weg. Obwohl viele Direktanbieter ebenso PUPs obendrauf packen, ist der Download direkt aus der Quelle immer noch am sichersten.
- Verlassen Sie sich auf ein aktuelles **Antiviren-Programm** wie Emsisoft Anti-Malware und führen Sie regelmäßig Scans auf Malware und PUPs durch.
- Alternativ dazu führen Sie Scans bei Bedarf mit Emsisoft Emergency Kit durch, welches Malware- und PUP-Infektionen völlig kostenlos findet und entfernt.

Quelle: http://blog.emsisoft.com/de/2015/03/11/top-downloadportale-die-sie-links-liegen-lassen-sollten/

# Wie Ihnen das Herunterladen von einem Programm sechs (!) PUPs bescheren kann

In Sicherheitswissen by Slade on April 2, 2015 | Deutsch, English, Français

An der Verbreitung von Potentiell Unerwünschten Programmen (PUPs) sind meist mehrere Mitwirkende beteiligt. So kann es passieren, dass Sie die unliebsame Begegnung mit sogenannten Kaskaden-PUPs machen könnten. Je nach Download-Methode kann sich unter Umständen eine regelrechte Lawine an PUP-Angeboten auf Ihrem Computer wiederfinden.

## Viele Wege führen zu einem PUP

Grundsätzlich gibt es mehrere Möglichkeiten, ein Potenziell Unerwünschtes Programm auf Ihr System zu bekommen:

**1) Direkt vom Software-Anbieter:** Der Software-Anbieter bündelt zusätzliche Angebote. Das bedeutet, dass Sie beim Besuch der original Webseite des Herstellers zum Herunterladen der Software auf PUPs treffen, weil dieser direkt mit den PUP-Herstellern zusammenarbeitet. Der Software-Anbieter erhält somit für jede Installation einen gewissen Betrag bezahlt. Wir haben in diesem Artikel ein paar Beispiele aufgeführt, die zeigen, dass die meisten Anbieter von kostenloser Antivirus-Software ebenfalls PUPs beim direkten Download von ihrer Webseite bündeln.

**2) Herunterladen von Software-Wrappern:** Viele Download-Portale nutzen Wrapper (besondere Installations-Software), die auch PUPs enthalten können. Diese verwenden nicht die originale Installations-Software des angebotenen Programms, sondern "verpacken" das Programm in ihrer eigenen Installations-Software – oft ohne die Genehmigung des eigentlichen Software-Herstellers. So verdient das Download-Portal Geld mit der Verbreitung von PUPs. Mit diesen zusätzlichen Downloads wird auf PPI-Werbenetzwerken (Pay Per Installation = Bezahlung pro Installation) Handel getrieben. Ähnlich wie eine Werbeeinschaltung auf Google, werden dabei die Anzeigen des Höchstbietenden angezeigt.

**3) Ein PUP bündelt zusätzliche PUPs:** Manchmal werden Symbolleisten und andere PUPs, die mit einem Programm installiert werden, mit noch mehr potentiell unerwünschten Programmen geliefert. Leider prüfen PPI-Netzwerke nicht, welche Software dahintersteckt und ob diese eventuell mit PUPs gebündelt ist.

**4) Vom PUP selbst:** PUPs werden auch über Werbung und Pop-ups auf bestimmten Webseiten verbreitet. Dabei handelt es sich oft um temporär erstellte Seiten mit Warnungen wie beispielsweise "Software XYZ muss aktualisiert werden". Diese Methode wird in diesem Artikel nicht berücksichtigt, weil wir uns auf PUPs konzentrieren, die man durch das Herunterladen eines anderen Programmes bekommt.

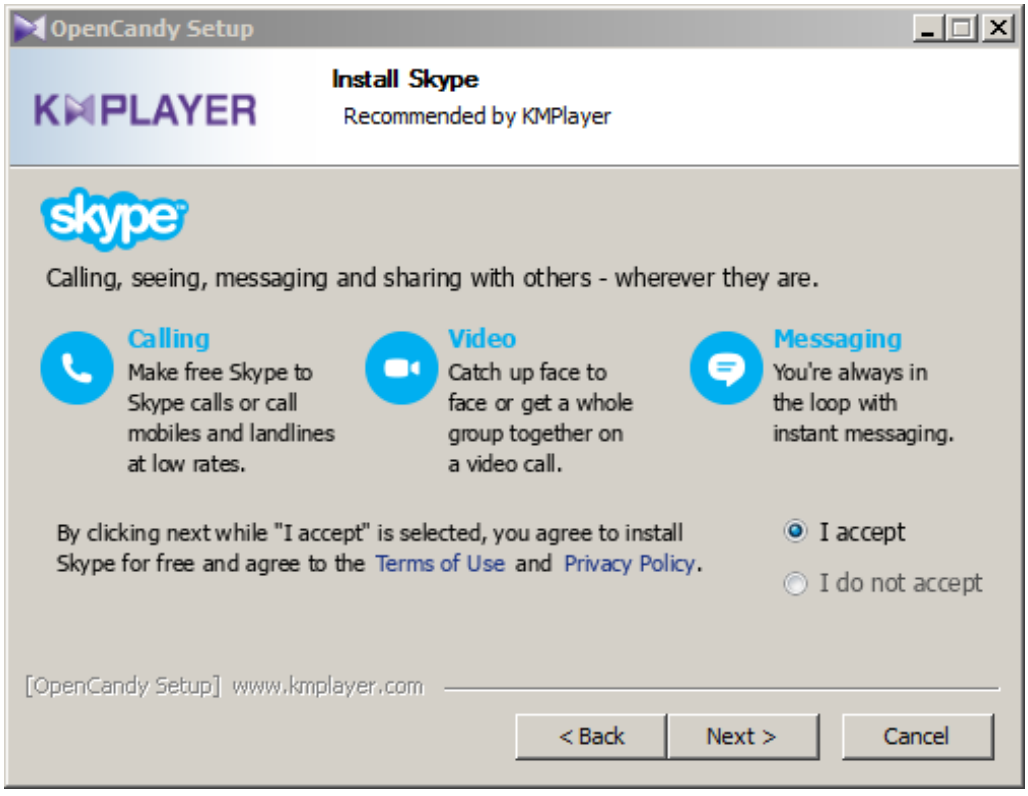
## Beispiel von Kaskaden-PUPs

Stellen Sie sich vor, Sie möchten KMPlayer installieren. Hierbei handelt es sich um einen sehr beliebten kostenlosen Video-Player, der hochwertige Wiedergabe von verschiedenen Medienformaten anbietet. Wir möchten Ihnen nun zeigen, wie sich durch das Herunterladen dieses Programms gleich mehrere PUPs von verschiedenen Quellen auf Ihrem Computer installieren können.

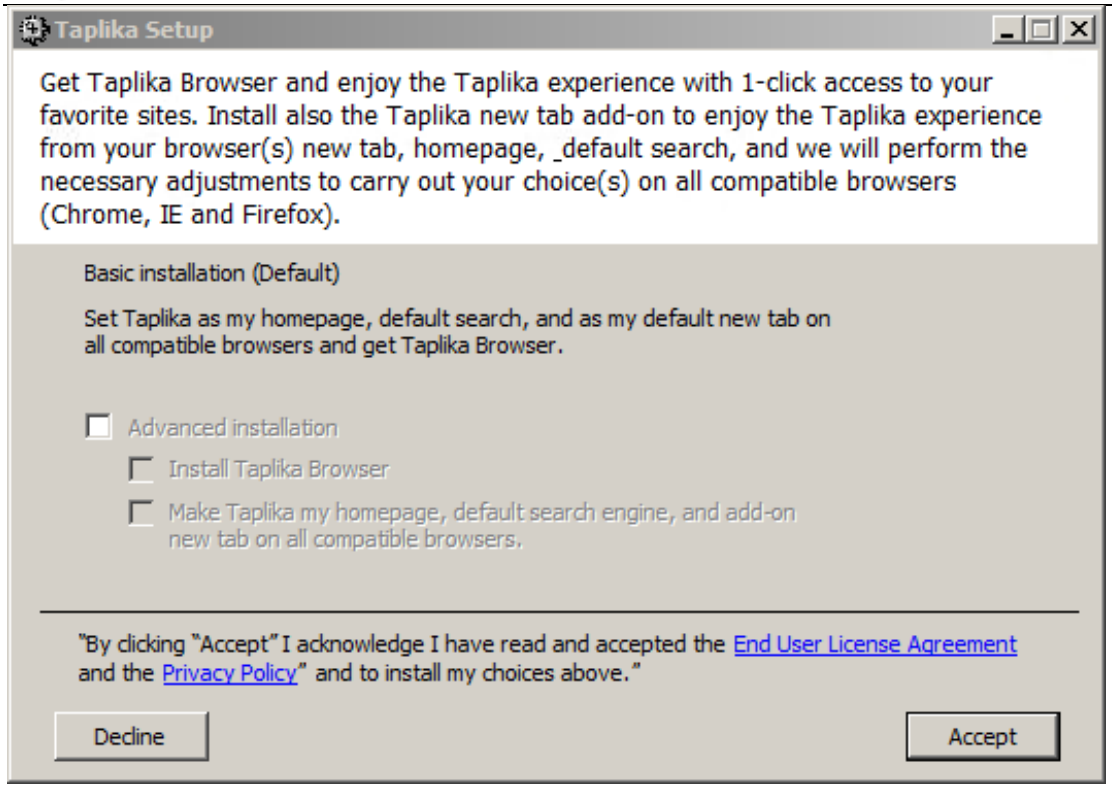
**1 ) Über den Software-Anbieter installierte PUPs**

Heutzutage werden immer mehr PUPs direkt vom Software-Programm verbreitet, das Sie herunterladen wollten. Selbst wenn Sie direkt die Webseite des Anbieters besuchen und sein Programm herunterladen, sind sie vor PUPs nicht sicher. Wir besuchten die Webseite von KMPlayer, um das Programm herunterzuladen, und das Folgende geschah:

Skype, eine nützliche Video-Chat-Anwendung, wird aktiv vom Anbieter angeboten. Aus der Installations-Software wird ersichtlich, dass Skype "Von KMPlayer empfohlen" wird.
Besonders besorgniserregend ist, dass Skype auch Teil des unerwünschten Angebots "Open Candy" ist. Dabei handelt es sich um ein bekanntes Adware-Programm.




Als nächstes bietet KMPlayer Ihnen SHAREit an, womit wir bei 2 PUPs wären. Am Ende des Installationsvorgangs fügt KMPlayer ein weiteres Programm namens Taplika hinzu. Taplika ändert Ihre Startseite, Suchmaschine und Tab-Einstellungen und installiert den auf Chromium basierten Taplika Web-Browser.




Der einst gute Ruf von KMPlayer steht durch dieses aggressive Bündeln auf dem Spiel. Im Zitat unten befindet sich die Meinung eines Nutzers von Software Informer zu den fragwürdigen Bündelungsmethoden von KMPlayer:

“Gut, aber ich HASSE den Installationsvorgang”

“Ich denke ernsthaft darüber nach, die Software zu deinstallieren. Der Installationsvorgang ist zu unseriös (zu viel Müll versucht, zusätzlich zum Player in meinem System installiert zu werden). Dadurch hasse ich die ganze App.”

PUP-Angebote aus dieser Download-Methode sind unvermeidbar, wenn die von Ihnen ausgewählte Software unerwünschte Programme gegen Bezahlung pro Installation bündelt.


PUP-Barometer: **3 PUPs**, falls Sie KMPlayer auf diese Weise herunterladen.

**2) PUPs werden über einen Wrapper des Download-Portals heruntergeladen**

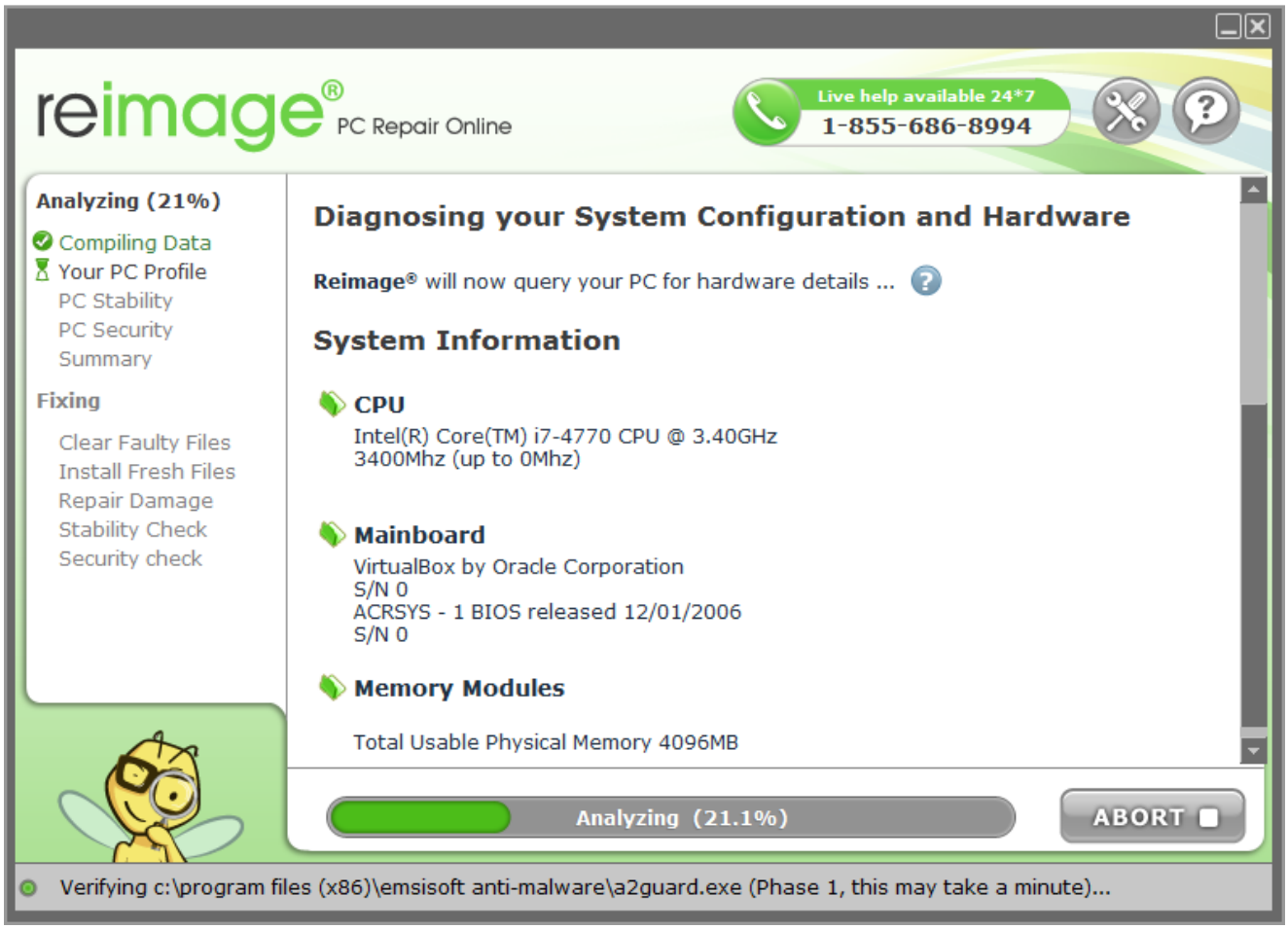
Wie Sie oben sehen, können Sie beim Herunterladen von KMPlayer direkt von dessen Webseite drei PUPs (Skype, SHAREit und Taplika) bekommen. Stellen Sie sich nun vor, dass Sie KMPlayer von einem Download-Portal herunterladen und nicht vom Anbieter direkt. In diesem Fall besuchten wir Download.com und benutzten deren “sichere” Installations-Software, um KMPlayer herunterzuladen. Noch bevor die eigentliche Anwendungsinstallation beginnen konnte, wurden uns verschiedene unerwünschte Angebote gemacht.


Beim Starten der "sicheren Installations-Software" von CNET wird bei der Installation von KMPlayer das "Sonderangebot" Pro PC Cleaner von Download.com präsentiert. Wie andere bösartige Software scannt Pro PC Cleaner Ihren Computer auf angebliche Probleme und zeigt dann verschiedene lästige Pop-ups und falsche Fehlerergebnisse an. Nach dem PRO-PC-Cleaner-Angebot bietet die Installations-Software als nächstes Spigot an, ein PUP, das oft von Download-Portalen gebündelt wird. Nach diesen zwei PUPs installiert Download.com endlich KMPlayer, der ja schon mit 3 PUPs vom Anbieter geliefert wird. Dadurch steigt die Gesamtzahl der PUPs auf 5 an.


PUP-Barometer: **5 PUPs**, falls Sie KMPlayer auf diese Weise herunterladen.

**3) Ein PUP installiert selbst noch mehr PUPs**

In diesem Fall wird ein unerwünschtes Programm mit einem oder mehreren weiteren unerwünschten Programmen geliefert. Hier installiert eins der fünf PUPs, die wir bei dieser Download-Methode gefunden haben, noch mehr PUPs: Taplika, das PUP, das beim direkten Herunterladen von KMPlayer von der Hersteller-Webseite hinzugefügt wird, installiert ein weiteres PUP. An dieser Stelle kommt Ihre Antivirus-Software womöglich zum Einsatz und blockiert das resultierende unerwünschte Programm in Echtzeit. Wenn dem aber nicht so ist, werden Sie niemals erfahren, wie dieses PUP in Ihren Computer gelangt ist.




Das Taplika-PUP hinterlässt Reimage PC Repair Online auf dem Computer. Hierbei handelt es sich um ein PUP-Beispiel, das **sich leise im Hintergrund installiert**. Es kann sein, dass sich PUPs zunehmend dieser Strategie bedienen, wenn zu viele Nutzer während der Installation Haken aus Kästchen entfernen. Reimage PC Repair scannt Ihren PC nach verschiedenen Kategorien und informiert über Ihren Systemstatus. Reimage gibt Fehler zur "PC-Sicherheit" und "Probleme mit PC-Stabilität" vor, die es reparieren kann. Viele PC-Techniker und Techies benutzen diese Software, um Systemoptimierungsaufgaben zu zentralisieren. Es wird jedoch dringend empfohlen, diese Software zu entfernen. In einer detaillierten Entfernungsanleitung machten wir eine interessante Entdeckung, die uns zeigte, dass diese Anwendung etwas vollkommen Anderes ist, als sie vorgibt.

"Reimage PC Repair Online ist technisch gesehen kein Virus, obwohl es viele der bösartigen Eigenschaften zeigt wie Rootkit-Fähigkeiten, um sich tief im Betriebssystem zu verhaken, Entführen vom Browser und allgemeines Stören der Nutzererfahrung."

PUP-Barometer: **6 PUPs**, falls Sie KMPlayer auf diese Weise herunterladen.

## Geld ist die Wurzel aller "PUPs" – Was haben alle Beteiligten davon?

Im Beispiel in diesem Artikel können Sie sich im schlimmsten Fall sechs unerwünschte Programme auf Ihrem Computer installieren. Warum sind alle an diesem Deal Beteiligten so bedacht darauf, PUPs auf Ihrem Computer zu hinterlassen? Das beliebte Sprichwort "Geld ist die Wurzel allen Übels" wird oft verwendet. Wie trifft es aber auf PUPs zu? Die Bündelung oder Erstellung von PUPs kann ein sehr lukratives Geschäft sein. In diesem Fall verdienen alle Beteiligten Geld: der Software-Anbieter, die Download-Portale und die PUPs selber.

**Software-Anbieter:** Der Software-Anbieter bekommt von den PUP-Entwicklern für jede durch ihn bewirkte Installation Geld. Im Beispiel in diesem Artikel bekommt KMPlayer Geld für jedes der drei PUPs, die ein Nutzer installiert. Mehr Beispiele gab es in diesem Artikel.
**Download-Portal:** Das Download-Portal bekommt Geld für die PUPs, die über ihre Installations-Software installiert werden. In diesem Fall von den Herstellern von Pro PC Cleaner und Spigot. Der Software-Anbieter ist allgemein nicht beteiligt und profitiert nicht von den Deals des Download-Portals.
**PUPs:** Manche PUPs arbeiten auch zusammen und installieren ihre Produkte gegenseitig, wofür sie einander bezahlen.

Wie vorher besprochen, gibt es für PUPs mehrere Methoden, um Geld zu verdienen. Die häufigste Methode ist durch Konfiguration Ihres Browsers: sie können Ihnen so bezahlte Werbung zeigen, Ihr Such- und/oder Browsing-Verhalten verkaufen oder Ihre Startseite umleiten. Jedes PUP verfügt normalerweise über seine eigene Datenschutzrichtlinie; ein weiterer Grund, weshalb Sie vorsichtig sein müssen. Außerdem können manche PUPs zu potentiellen Sicherheitslücken führen. Das PUP (Adware) Superfish ist dafür ein gutes Beispiel.

## Wie kann man am besten verhindern, dass man aggressiver PUP-Bündelung zum Opfer fällt?

Im Folgenden haben wir einige Tipps zusammengestellt, wie Sie Ihren PC vor PUPs schützen und potentielle Infektionen entfernen können, die sich womöglich einschleichen. Die ersten fünf davon stellen vorbeugende Maßnahmen in den Vordergrund. Beim letzten Tipp handelt es sich um eine nachträgliche "Heilmethode", also Entfernung im Fall einer Infektion.

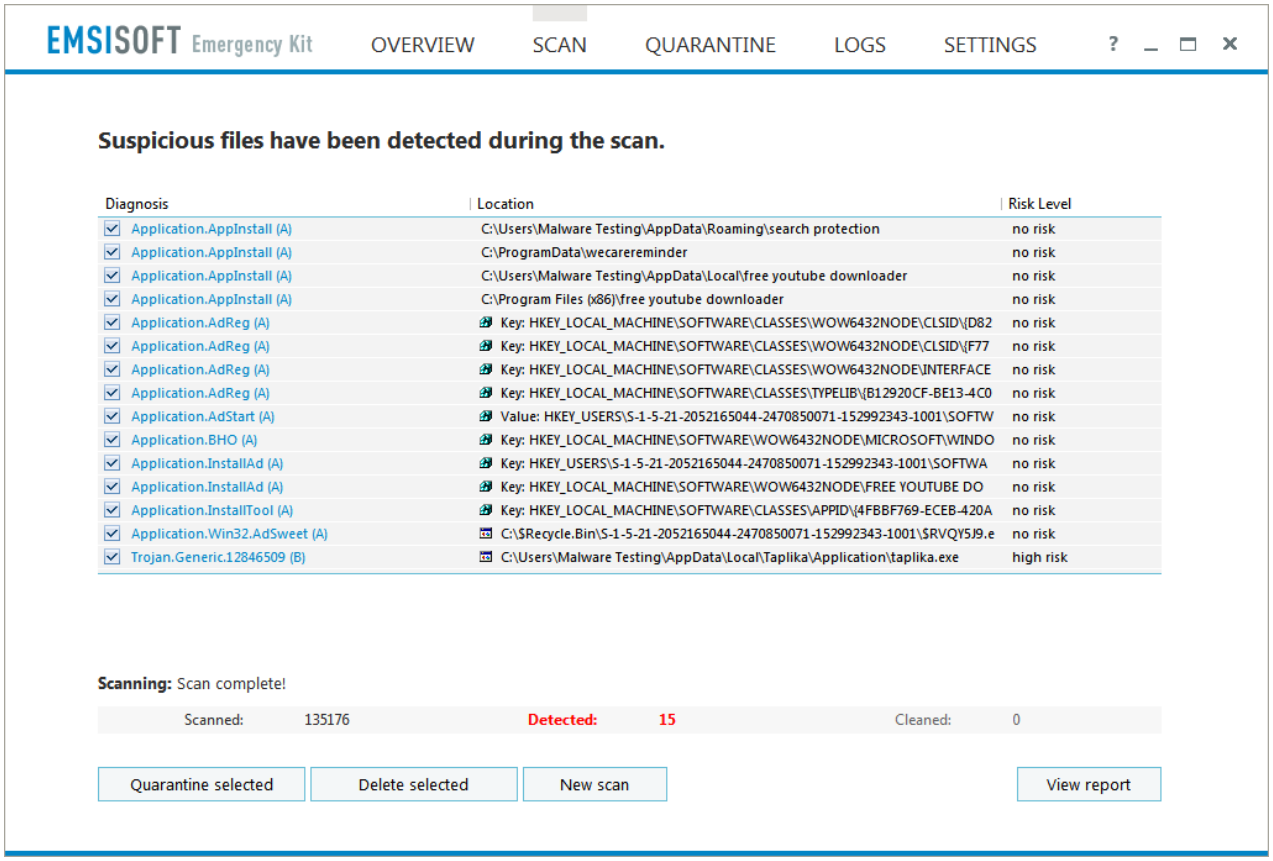
**Tipp 1:** Lassen Sie beim Herunterladen von Software Vorsicht walten; ein gutes Urteilsvermögen ist gefragt. Seien Sie achtsam und halten Sie Ausschau nach verdächtigen Dingen. Seien Sie auch bei Werbe-Bannern vorsichtig, die Download-Schaltflächen enthalten. Sie sind oft lästig und lenken vom echten Download auf dem Portal ab.

**Tipp 2:** Vermeiden Sie falls möglich den Gebrauch von Download-Portalen, von denen bekannt ist, dass sie PUPs und Junkware vom Software-Anbieter ohne deutliche Bekanntgabe oder Warnungen bündeln. Machen Sie es sich zum Prinzip, immer wachsam zu sein, selbst wenn Sie Software von Anbieter-Webseiten installieren, weil diese auch PUPs verbreiten könnten. Vermeiden Sie zu guter Letzt verdächtige Freeware-Anwendungen, weil "kostenlos" nicht immer die beste Wahl ist. Nicht jede Freeware ist schlecht, aber bedenken Sie vor einer etwaigen Installation, wie die von Ihnen verwendete Freeware an Ihnen Geld verdient. So können Sie entscheiden, ob Sie dem zustimmen oder nicht.

**Tipp 3:** Manche Nutzer verwenden gern ein Programm namens Unchecky, eine Anwendung, die bei der Installation die Haken aus Kästchen von unerwünschten Angeboten entfernt. Manche PUPs installieren

sich allerdings auch heimlich im Hintergrund oder verwenden andere Installationsmethoden als Opt-out. Seien Sie also weiterhin wachsam beim Installieren.

**Tipp 4:** Verwenden Sie aktuelle Antivirus-Software mit ausreichendem Schutz vor Zero-Day-Bedrohungen und wählen Sie ein Antivirus-Programm mit integrierter PUP-Erkennung wie Emsisoft Anti-Malware. Dieses Programm kann Malware und potentiell unerwünschte Programme erkennen, blockieren und entfernen. Wenn Sie über keinen Antivirus-Schutz verfügen oder eine andere Software als Emsisoft verwenden, können Sie Scan-Software als zweite Meinung einsetzen, so wie das kostenlose Notfallset Emsisoft Emergency Kit, um Anlass bezogen nach PUPs und anderer Malware zu suchen und sie zu entfernen.




**Tipp 5:** Obwohl dies ungeübten Nutzern nicht immer empfohlen wird, kann der Gebrauch einer Whitelisting-Anwendung eine Option für Fortgeschrittene sein. Whitelisting ist das genaue Gegenteil von Blacklisting, das von Antivirus-Software zur Erkennung von Gefahren verwendet wird. Eine Whitelist wird benutzt, um nicht berechtigte Software oder Programme zu blockieren, indem nur Programme aus der Liste starten dürfen. Ein Beispiel einer solchen Anwendung ist Microsoft Windows AppLocker.

Wenn Sie ausgezeichnete Sicherheitspraktiken einsetzen und alle notwendigen Vorsichtsmaßnahmen treffen, sollten Sie sich kaum oder gar keine Sorgen machen müssen. Falls Sie doch auf einen unerwünschten Eindringling treffen, ist es jedenfalls gut zu wissen, dass Ihnen zwei ausgezeichnete Helfer zur Seite stehen, die Sie beim Entfernen unterstützen.

Wir wünschen Ihnen einen schönen (PUP-freien) Tag!

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

Quelle: http://blog.emsisoft.com/de/2015/04/02/wie-ihnen-das-herunterladen-von-einem-programm-sechs-pups-bescheren-kann/?ref=ticker150402&utm_source=newsletter&utm_medium=newsletter&utm_content=blog&utm_campaign=ticker150402