

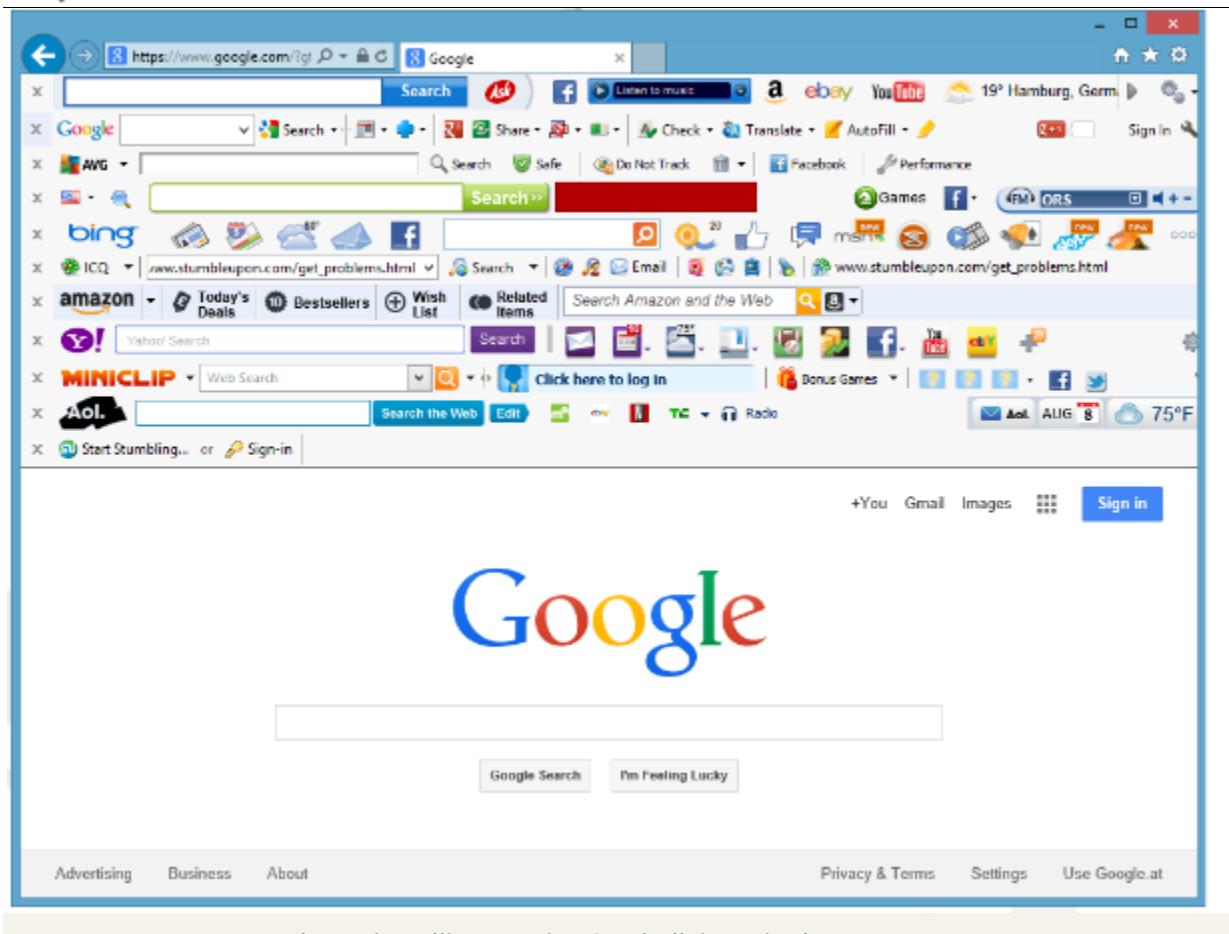


Was Sie über potentiell unerwünschte Programme (PUP) wissen müssen

Malware, Trojaner, Bugs – Begriffe, die in jedem von uns Panik verursachen und Bilder von fallendem Code, Totenköpfe hervorrufen. Diese bösartigen Programme sind der Schmutz des Internets und der Beweis, dass mit jedem Nutzen einer Technologie auch ein gleichwertig unangenehmer, unerwünschter oder sogar schädlicher Nachteil kommen kann.

Ein potentiell unerwünschtes Programm (PUP) ist genau das, was der Name schon ankündigt: Software, die auf Ihrem System erwünscht sein kann (meistens jedoch nicht ist). PUPs sind Malware insofern sehr ähnlich, dass sie nach dem Herunterladen und Installieren für Probleme sorgen können. Der wohl einzige Unterschied ist, dass es mit Ihrer Zustimmung geschieht.

Der Begriff PUP wurde erstmals geprägt, um diese Art von Adware oder Crapware (engl.: crap = Unsinn, Müll) von anderweitig schädlicher Software zu unterscheiden. Auch wenn PUPs nicht als bösartig oder schädlich gelten, verbrauchen sie häufig Unmengen an Systemressourcen und sind damit in der Regel der Grund für ein behäbiges Betriebssystem. Außerdem erstellen die Störenfriede beispielsweise neue Symbolleisten für Onlineshops in Ihrem Internetbrowser, wechseln ohne Grund den Suchanbieter von Google zu Bing, zeigen Werbeanzeigen an oder informieren Sie regelmäßig über das Wetter in Swasiland. Einige sind sogar so aggressiv, dass sie Ihren Computer absichtlich verlangsamen, um Ihnen dann Programme zum Tunen oder Beschleunigen des Systems zu verkaufen.



Weshalb gibt es dann PUPs? Software-Entwickler können Geld verdienen, indem sie die Programme „kostenlos“ anbieten. Für jede erfolgreich installierte Symbolleiste kann ein Freeware-Hersteller beispielsweise ungefähr 2 USD verdienen. Einige PUPs gibt es schlicht, um Geld zu verdienen, ohne Ihnen irgendwelchen Nutzen zu bringen.

Ist das Ganze rechtes?

Das Verhalten eines PUP ist meistens in seiner Endbenutzerlizenzvereinbarung (EULA) angegeben. EULAs sind diese langen Rechtsdokumente, die Ihnen angezeigt werden, wenn Sie sich beim Installieren durch die vielen Meldungen klicken müssen. In diesen scheinbar unsinnigen Rechtsformulierungen wird jedoch der Zweck eines Programms ausgeführt. Sie schützt die Software-Entwickler auch vor rechtlichen Schritten. Denn ein PUP kann nur installiert werden, wenn Sie am Ende des Dokuments zustimmen. Viele Anbieter verlassen sich darauf, dass Sie die Installation durch einfaches Klicken auf „Weiter“ schnellstmöglich abschließen möchten und die EULA gar nicht erst lesen, sondern am Ende schlicht auf „Zustimmen“ klicken.

Wie gelangt dann ein PUP (oder zehn) auf Ihren Computer?



Wie das Geschenkpapier um das Spielzeug unter dem Weihnachtsbaum sind auch die PUPs um Ihre Downloads gewickelt – nicht nur bei kleinen Anbietern. Auch Produkte vieler großer Firmen kommen im Paket mit PUPs.

Step: 1 of 3

Adobe Acrobat Reader DC



Version 2015.016.20039
[System requirements](#)

Your system:
Mac OS (Intel) 10.5.8 - 10.11, English
[Do you have a different language or operating system?](#)

Are you an IT manager or OEM?

About:

Adobe Acrobat Reader DC software is the free global standard for reliably viewing, printing, and commenting on PDF documents.

And now, it's connected to the Adobe Document Cloud – making it easier than ever to work across computers and mobile devices.

It's the only PDF viewer that can open and interact with all types of PDF content, including forms and multimedia.

Terms & conditions:

By clicking the "Install now" button, you agree to the automatic installation of updates to Adobe Acrobat Reader DC, and to the [Adobe Software Licensing Agreement](#).

Note: Your antivirus software must allow you to install software.

Install now

Total size: 148 MB

Choose your region | Copyright © 2016 Adobe Systems Incorporated. All rights reserved.
[Terms of use](#) | [Privacy](#) | [Cookies](#)

Adobe Acrobat Reader bittet Sie, automatischen Aktualisierungen zuzustimmen.



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

Updating Skype

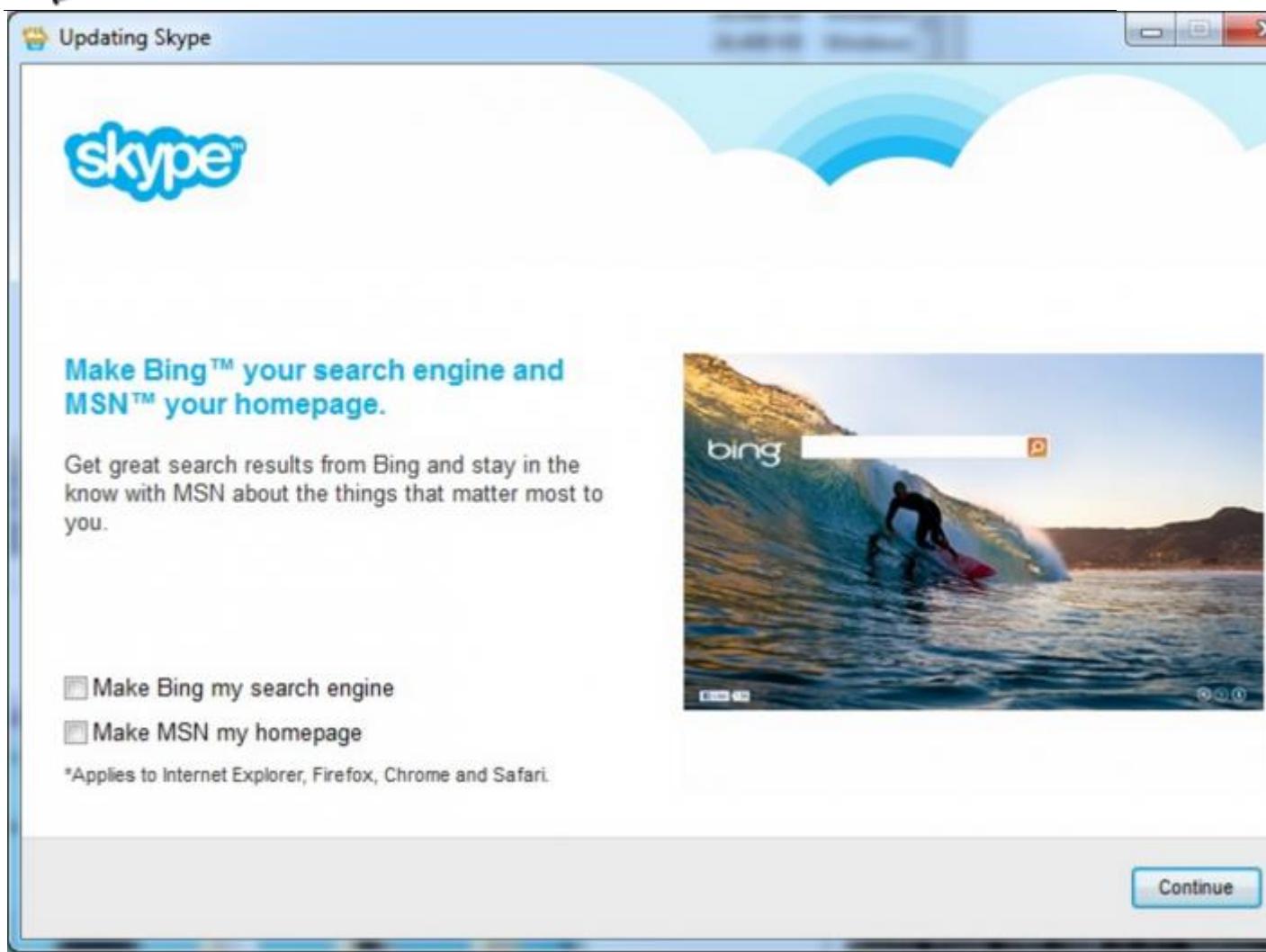
skype™

Make Bing™ your search engine and MSN™ your homepage.

Get great search results from Bing and stay in the know with MSN about the things that matter most to you.

Make Bing my search engine
 Make MSN my homepage

*Applies to Internet Explorer, Firefox, Chrome and Safari.



Microsoft Skype bittet Sie, Ihren Browser und Ihre Startseite zu ändern.



Java Setup



ORACLE

Offer to Install the FREE Browser Add-on from Ask



Get Facebook status updates directly in your browser, listen to top radio stations, and get easy access to search and weather. Toolbar installs and settings apply in Internet Explorer.

- Install the Ask Toolbar in Internet Explorer
- Set and keep Ask as my default search provider
- Set and keep Ask.com as my browser home page and new tabs page

By installing this toolbar and associated updater from Ask.com, your use is subject to the Ask.com [Terms and Conditions](#) and [Privacy Policy](#). The Ask Toolbar is a product of APN, LLC.

Cancel

Next >

Oracle fügt durch die Installation von Java eine Symbolleiste hinzu.

Eine weitere Möglichkeit, wie PUPs auf Ihren Computer gelangen können, sind Software-Portale. Das sind die Seiten, über die Sie Ihre Adobe-Produkte aktualisieren oder einen vernünftigen Medienplayer suchen. Viele Portale werben damit, „saubere und sichere Downloads“ anzubieten. Doch auch das Vertrauen in dieses Angebot ist inzwischen mit Risiko behaftet. PUPs tauchen in Verbindung mit Programmbeurteilungen auf, die nicht immer rechtmäßig wirken.

Wir haben uns angesehen, wie viele PUPs in die 50 beliebtesten Anwendungen auf Download.com integriert sind und fanden heraus, dass **31 von den 50 auf Download.com getesteten Programmen PUPs enthalten**. Lesen Sie hierzu auch [62 % der Top-50-Anwendungen auf Download.com werden mit Toolbars und anderen PUPs beliefert](#).



Von diesem Ergebnis negativ überrascht haben wir uns das Verhalten der zehn beliebtesten Download-Portale (andere als Download.com) angesehen. Wir wollten herausfinden, ob es überhaupt sichere unter ihnen gibt. Dazu haben wir deren Top-10-Anwendungen heruntergeladen und dokumentiert, wie viel „Crapware“ dabei ist. Leider mussten wir feststellen, dass bei nahezu jedem Portal mindestens ein PUP dabei war. Näheres dazu im Artikel [Top-Downloadportale, die Sie links liegen lassen sollten.](#)

Die Sache mit der grünen Schaltfläche

Sie kennen das sicher: Sie möchten gern wieder einmal Ihre Fotos sortieren, die wild verteilt in allen möglichen Ordnern auf Ihrem Computer gespeichert sind und ein zielgerichtetes Ansehen unmöglich machen. Also laden Sie sich ein Fotoprogramm herunter, um sie zu ordnen und bei Bedarf auch zu bearbeiten. Direkt auf der Startseite von Download.com sind bereits etliche aufgeführt. Sie wählen ein Programm aus und Ihnen strahlt eine leuchtend grüne Schaltfläche „Jetzt herunterladen“ entgegen. Das Einzige, das jetzt noch zwischen Ihnen und der Lösung für Ihre Fotoprobleme steht ... weshalb Sie natürlich darauf klicken. Endlich Ordnung. Dummerweise sind bei dieser Schaltfläche auch gleich noch drei PUPs dabei gewesen.

The screenshot shows the Download.com homepage with a search bar and navigation icons for Windows, Mac, and iOS. Below the search bar, there's a red callout box with a skull icon and the text "Download with bundled PUPs". To the right, there's a large green "Start Download" button with the subtext "3 steps for a faster install". To the left of the main content area, there's a "PhotoS" software card with a "SAFE" badge, a "Download Now" button, and a user rating of 4 stars out of 5. A green speech bubble points from the "Safe download option" badge towards the "Start Download" button. On the right side, there's another "Start Download" button with the same "3 steps for a faster install" subtext, accompanied by a small Mac Optimizer note. At the bottom, a message says "Der sichere Link ist auch die sicherere Option zum Herunterladen."

Bei der Verteilung von potenziell unerwünschten Programmen (PUP) sind mehrere Parteien beteiligt. Daher kann es passieren, dass Sie mitunter auch in ein regelrechtes Schneeballsystem geraten. Dabei wird beim Installieren nicht nur ein PUP angeboten, sondern mehrere nacheinander.

Eine Variante hierbei ist, dass ein PUP im Paket mit weiteren PUPs heruntergeladen wird. Während Sie also das gewünschte Programm herunterladen, haben Sie möglicherweise



versehentlich einem Symbolleisten-PUP zugestimmt. Das kommt jetzt allerdings nicht allein, sondern in Kombination mit weiteren PUPs, die ohne Ihr Wissen installiert werden.

Wir haben uns die Auswirkungen dieses PUP-Schneeballsystems etwas genauer angeschaut, indem wir den beliebten KPlayer herunterluden und dessen Installationsverfahren beobachteten. Dafür, dass wir eigentlich ein Programm herunterladen wollten, hatten wir nach der Aktion ganze 6 PUPs. Mehr dazu in unserem älteren Blog-Beitrag [*Wie Ihnen das Herunterladen von einem Programm sechs \(!\) PUPs bescheren kann.*](#)

Achten Sie auch auf falsche Software-Aktualisierungen. Diese werden häufig über kurzzeitig verfügbare Websites verbreitet, die speziell für Google AdSense entwickelt wurden und Sie zu dazu auffordern, Ihren Flash-Player oder Java zu aktualisieren. Es gibt Unternehmen, die täglich Hunderte dieser Seiten entwickeln, um Sie zu täuschen und auf ihre Seiten zu locken.

Es gibt noch unzählige weitere Möglichkeiten, wie Sie mit PUPs überschwemmt werden können. Um Ihnen einen Überblick darüber zu verschaffen, haben wir die wichtigsten für Sie zusammengestellt: [*10 Wege, wie sich PUPs auf Ihren Computer schummeln. Und wie Sie das verhindern.*](#)

Für wen sind PUPs nützlich?

Software-Anbieter: Software-Anbieter (Händler) werden von den PUP-Entwicklern (Urheber der Adware) für jede Installation bezahlt. Beispiele dafür werden auch in diesem Artikel erwähnt.

Download-Portale: Auch die Download-Portale werden für jedes PUP bezahlt, das über eines ihrer Installationsprogramme (die besagten leuchtend grünen Schaltflächen) installiert werden. Die Software-Anbieter sind hierbei nicht beteiligt und haben keine Vorteile davon.

PUP-Entwickler: Einige Entwickler arbeiten zusammen, um ihre Programme gegenseitig zu vertreiben / zu installieren und bezahlen sich entsprechend untereinander.

Aber es geht noch beunruhigender:

Eine aktuelle Entwicklung bei PUPs ist die Verwendung von Rootkits. Das sind also Codes, die sich in den eigenen Daten oder anderen Dateien verstecken, damit sie von Ihnen oder Ihrem Computer nicht entdeckt werden können. Diese fangen dann ein- und ausgehende



Meldungen Ihres Computers ab und leiten beliebige Informationen an Server außerhalb weiter. Durch die Verwendung dieser Rootkits werden die Grenzen zwischen unerwünschtem Ballast und aktiver Malware verwischt.

Das lässt sich besonders gut an dem neuen PUP „Faster Internet“ erkennen, das nach der Installation einen Fingerabdruck Ihres Computers erstellt. Diese Informationen werden zusammen mit Screenshots der aktuellen Anzeige auf Ihrem Monitor und Ihrer IP-Adresse an die Server des Entwicklers gesendet. Ein derartig Spyware-ähnliches Verhalten ist nicht mehr nur Adware sondern eine grobe Verletzung Ihrer Privatsphäre.

Ihnen wurde eine Meldung angezeigt, die Ihnen Hilfe versprach? Diese interaktiven PUPs sollen dem Normalverbraucher Angst einjagen, indem sie Online-Meldungen anzeigen, laut denen auf Ihrem Computer angeblich ein schwerwiegendes Problem vorliegt. Auf diese Weise werden Sie dazu verleitet, die Telefonnummer eines Kundendienstes anzurufen, der Ihnen dann noch mehr Angst einjagen soll, damit Sie die angebotenen Produkte kaufen.



System Detected (2) Potentially Malicious Viruses.
Your Personal Financial Information **IS NOT SAFE**
(24/7 - Toll Free - High Priority Virus Removal Call Line)

To Remove Viruses, Call Tech Support Now:

Falschmeldungen fordern Sie auf, ein Anti-Virus-Unternehmen anzurufen.

Leider werden immer wieder neue Wege gefunden, um Ihren Computer zu infizieren. Dadurch, dass es – wenn überhaupt – nur minimale gesetzliche Vorgaben für Adware gibt, bleiben aufrichtige Entwickler wehrlos.



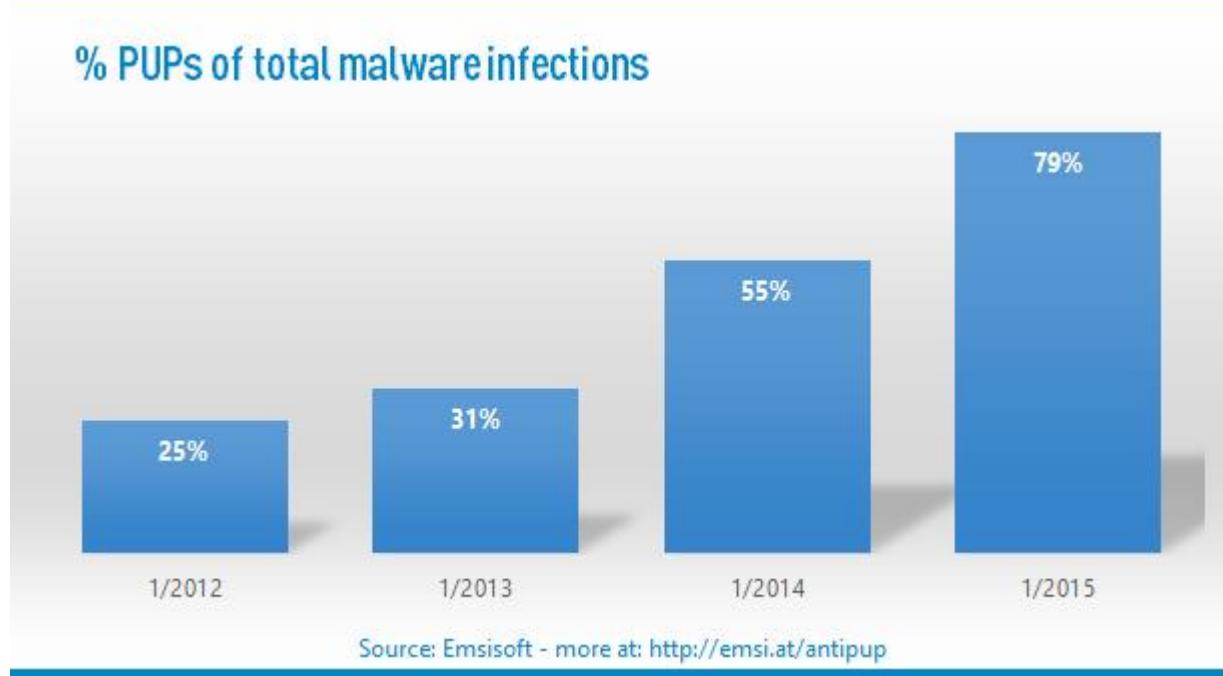
PUPs und die Antivirus-Industrie

Erschreckenderweise scheint der Branche langsam ein gewisses Niveau an Ethik verloren zu gehen, nachdem selbst große Anbieter wie Oracle (Java) und Microsoft (Bing und Skype) ihre Produkte im Paket mit PUPs anbieten. Inzwischen gehen selbst Antivirus-Entwickler dazu über. Wir haben uns die Vorgehensweisen unter Anbietern von Antivirus-Freeware angesehen. Die Ergebnisse sind erschreckend. Wie Sie auch im Artikel [Ist der Antiviren-Sektor nicht mehr ganz bei Trost?!](#) nachlesen können, kamen 7 von 8 der getesteten kostenlosen Antivirus-Anwendungen im Paket mit PUPs.

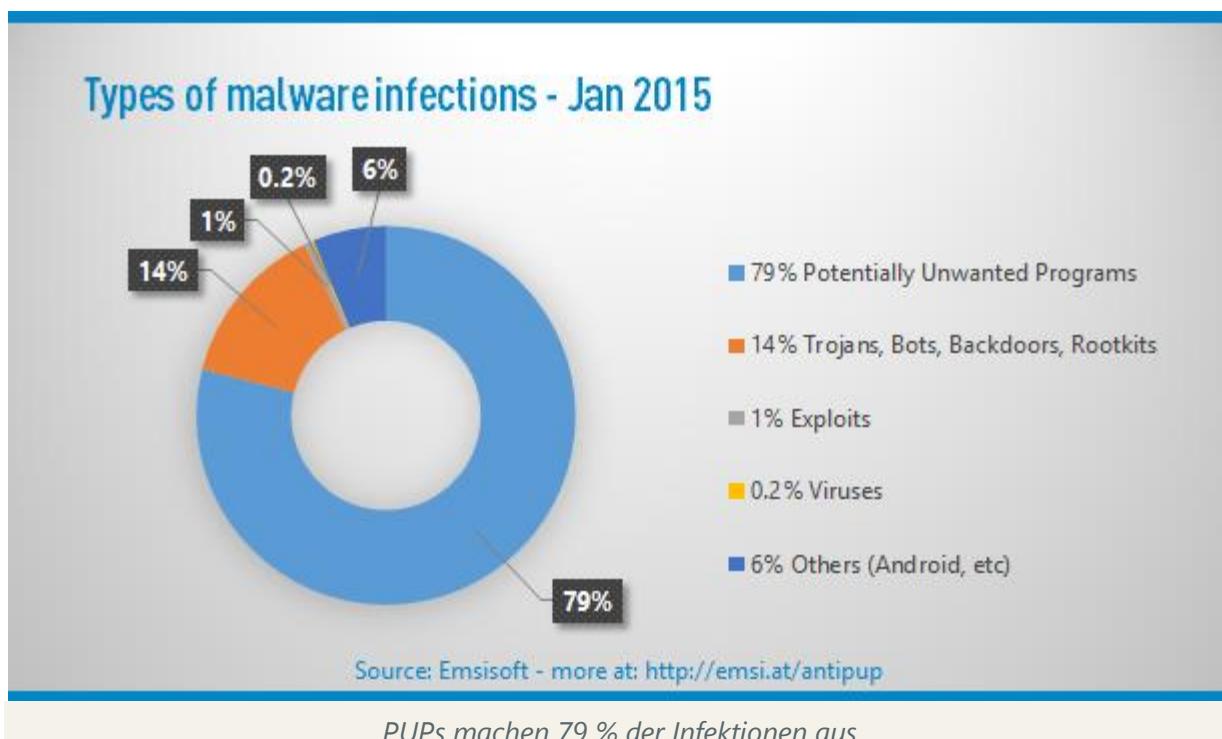
Emsisoft ist Anti-PUP

In den vergangenen Jahren hat sich die Art der Bedrohungen erheblich verändert. Als sich die Emsisoft-Experten letztes Jahr aktuelle Infektionsstatistiken vornahmen ([Anti-Virus, Anti-Malware, Anti-PUP? Was ist Emsisoft wirklich?](#)), stellten sie fest, dass Dreiviertel aller Funde von Emsisoft Anti-Malware im Zusammenhang mit PUPs standen. Diese Zahl hatte sich in den vergangenen Jahren erheblich erhöht.

Aber für jedes Problem gibt es bekanntlich eine Lösung. Emsisoft hat sich [hohen ethischen Standards](#) verschrieben, die unseren Umgang mit Bedrohungen aller Art bestimmen. Dabei steht jedoch immer der Anwender im Mittelpunkt. Während viele Antiviren-Produkte selbst die häufigsten PUPs nicht erkennen – und sogar [selbst](#) welche mit dem eigenen Programm installieren – ist Emsisoft dafür bekannt, sie gründlich aufzuspüren und zu entfernen.



Die Anzahl der PUP-Erkennungen ist weiter zunehmend.



PUPs machen 79 % der Infektionen aus.

Auch wenn wir ein Teil der Lösung sind, ist es wichtig, dass Sie die PUPs erkennen, bevor Sie überhaupt erst auf Ihren Computer heruntergeladen werden und Probleme verursachen können.

Fazit:

- Potentiell unerwünschte Programme (PUPs) sollen mit Ihnen Geld machen. Das wohl üblichste Konzept ist es, sich in Ihrem Browser einzunisten. Sie zeigen Ihnen dann Werbung, verkaufen die Daten zu Ihrem Such- und Surfverhalten oder leiten Sie auf andere Websites weiter.
- Es werden zudem aggressive Vertriebsmethoden eingesetzt, um auf Ihren Computer zu gelangen, denn in den meisten Fällen wissen Sie nicht einmal, dass Sie ein PUP installieren.
- Der Großteil der PUPs bietet darüber hinaus keinerlei Mehrwert oder Vorteile. Die Entwickler vermeiden das, indem Sie Software-Händlern oder anderen Anbietern wie Download-Portalen pro Installation Geld zahlen.
- PUPs werden Ihnen häufig von Freeware-Anbietern „untergejubelt“ – also im Paket mit einem kostenlosen Programm. Während Sie Programm A installieren, werden (oft ohne Ihr Wissen) auch ein oder mehrere PUPs installiert. Die Freeware-Anbieter werden von den PUP-Entwicklern schließlich dafür bezahlt.



**Jetzt wissen Sie erst einmal, was PUPs sind und wie Sie sich den Ballast einfangen.
Doch wie können Sie sie vermeiden?**

- Bleiben Sie skeptisch, handeln Sie mit gesundem Menschenverstand und lassen Sie sich Zeit. Lesen Sie Installationsmeldungen gründlich durch. Stimmen Sie einer Endbenutzerlizenzvereinbarung (EULA) erst zu, wenn Sie auch wirklich mit allen Bedingungen/Angaben darin einverstanden sind.
- Verwenden Sie nur vertrauenswürdige Quellen zum Herunterladen von Programmen, etwa die offizielle Website des Software-Herstellers.
- Vermeiden Sie Download-Portale und laden Sie niemals Anwendungen herunter (von deren Installation ganz zu schweigen), die verdächtig oder gefährlich erscheinen.
- Installieren Sie eine seriöse Antivirus-Software (z. B. [Emsisoft Anti-Malware](#)), die immer im Hintergrund läuft, und halten Sie sie auch auf dem aktuellen Stand, um einen Echtzeitschutz gegen PUP zu haben.
- Für noch mehr Schutz, können Sie Ihren Computer auch regelmäßig mit dem [kostenlosen Emergency Kit Pro](#) reinigen.

Wir wünschen eine schöne (PUP-freie) Zeit!

Ihr Emsisoft-Team

Quelle: http://blog.emsisoft.com/de/2016/06/20/was-sie-ueber-potentiell-unerwuenschte-programme-pup-wissen-muessen/?ref=ticker160620&utm_source=newsletter&utm_medium=newsletter&utm_content=mainnews&utm_campaign=ticker160620