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

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.

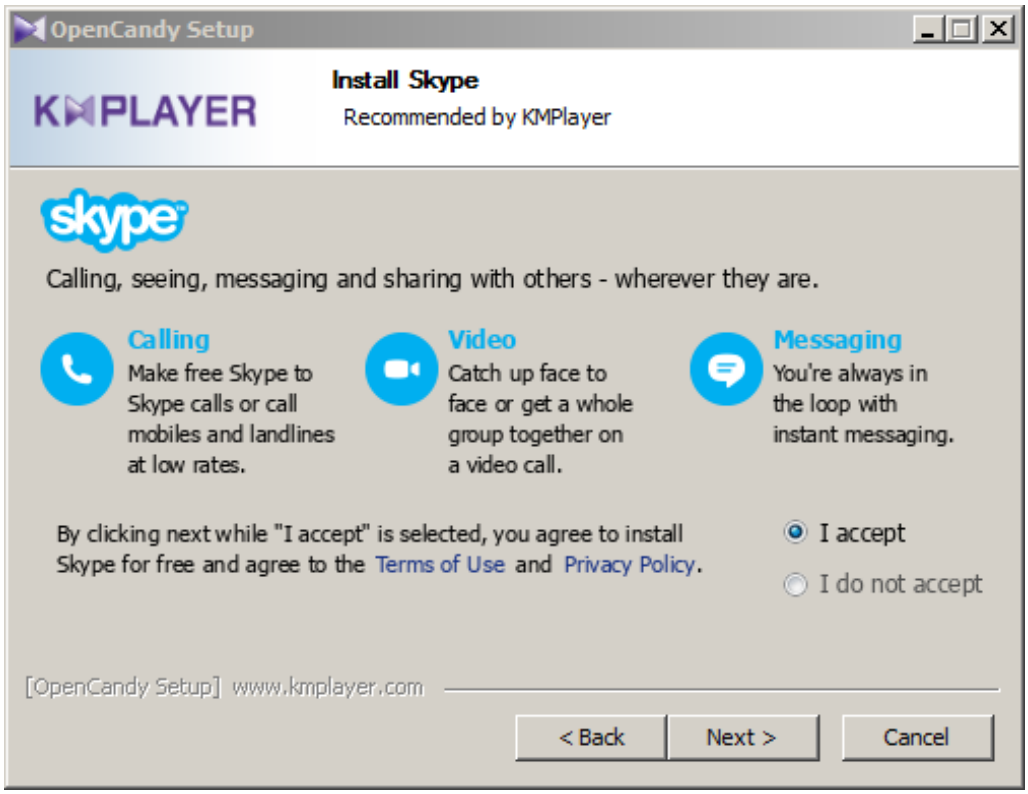
Beispiel von Kaskaden-PUPs

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.

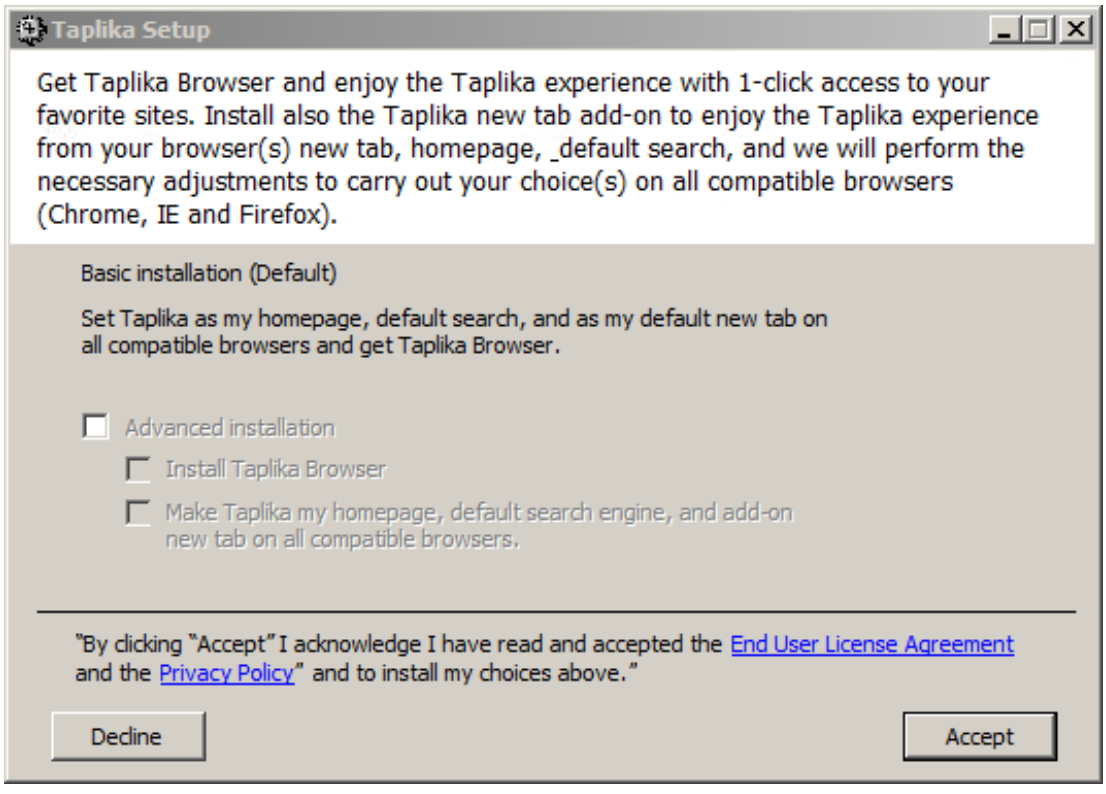
1) Über den Software-Anbieter installierte PUPs

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 bekanntesAdware-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.

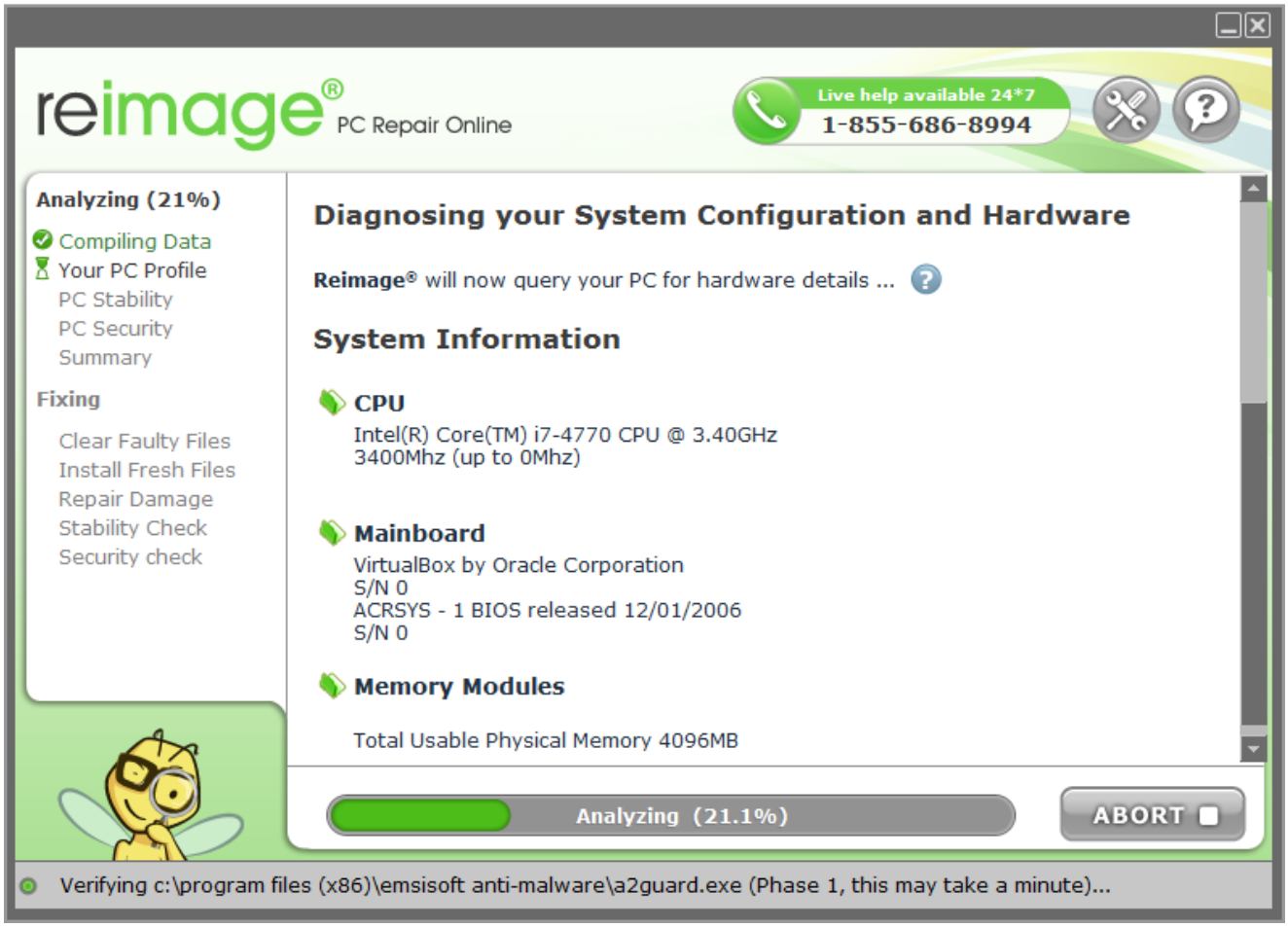
Beim Starten der "sicheren Installations-Software" von CNET wird bei der Installation von KMPlayer das "Sonderangebot" Pro PC Cleaner von Download.com präsentiert. Wie andere bösartige Software scannt Pro PC Cleaner Ihren Computer auf angebliche Probleme und zeigt dann verschiedene lästige Pop-ups und 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 gutesBeispiel.

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.

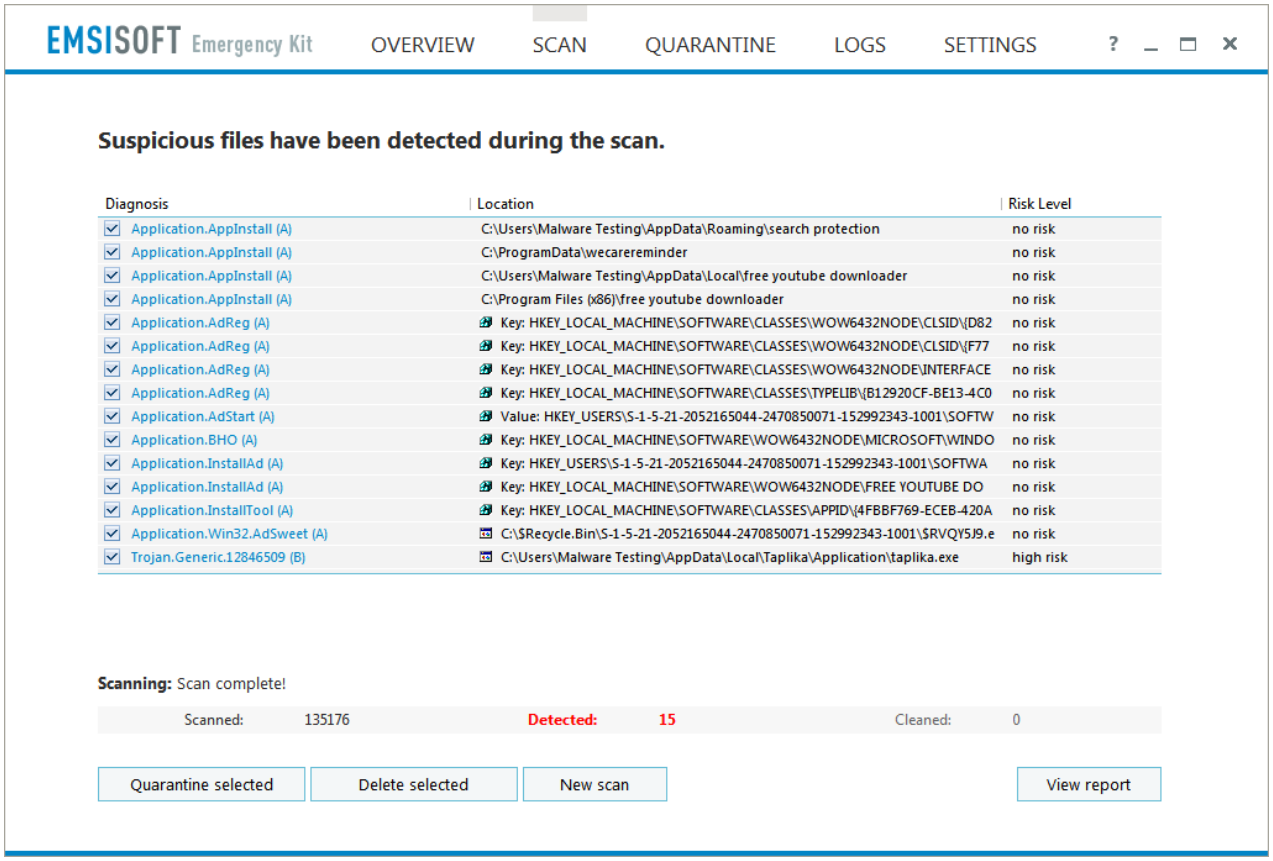
Tipp 1: Lassen Sie beim Herunterladen von Software Vorsicht walten; ein gutes Urteilsvermögen ist gefragt. Seien Sie achtsam und halten Sie Ausschau nach verdächtigen Dingen. Seien Sie auch bei Werbe-Bannern vorsichtig, die Download-Schaltflächen enthalten. Sie sind oft lästig und lenken vom echten Download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

Soforthilfe, Tools zur Entfernung von Malware und Viren hier: Nicos-EDVDienst Tel: +49 (0) 77 71 – 916 59 59