



## **Anleitung Was ist ein PUP? PUP=Potentiell unerwünschtes Programm**

Als unerwünscht gelten Programme, die ein Nutzer unwissentlich installiert oder über deren Zweck er bewusst getäuscht wurde. PUAs, auch PUP (Potentially Unwanted Program) genannt, werden häufig mit legitimen Programmen gebündelt. Deren Installer weist möglicherweise auf die Installation zusätzlicher Software hin, versucht dann aber häufig über schwer verständliche Dialoge oder vorausgewählte Einstellungen den Nutzer dazu zu bringen, diese Software zu akzeptieren. In einigen Fällen wird die Einrichtung zusätzlicher Programme sogar komplett verschwiegen und im Hintergrund durchgeführt.

PUAs sind unter anderem in der Lage, unerwünschte und aufdringliche Werbung anzuzeigen und alle Internetaktivitäten eines Nutzer aufzuzeichnen, um diese Daten an Werbetreibende zu verkaufen. PUAs verändern aber auch Browsereinstellungen wie Startseite und Suchmaschine. Einige versuchen auch, Root-Zertifikate zu installieren und Sicherheitsfunktionen abzuschalten.



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 Welpen 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.

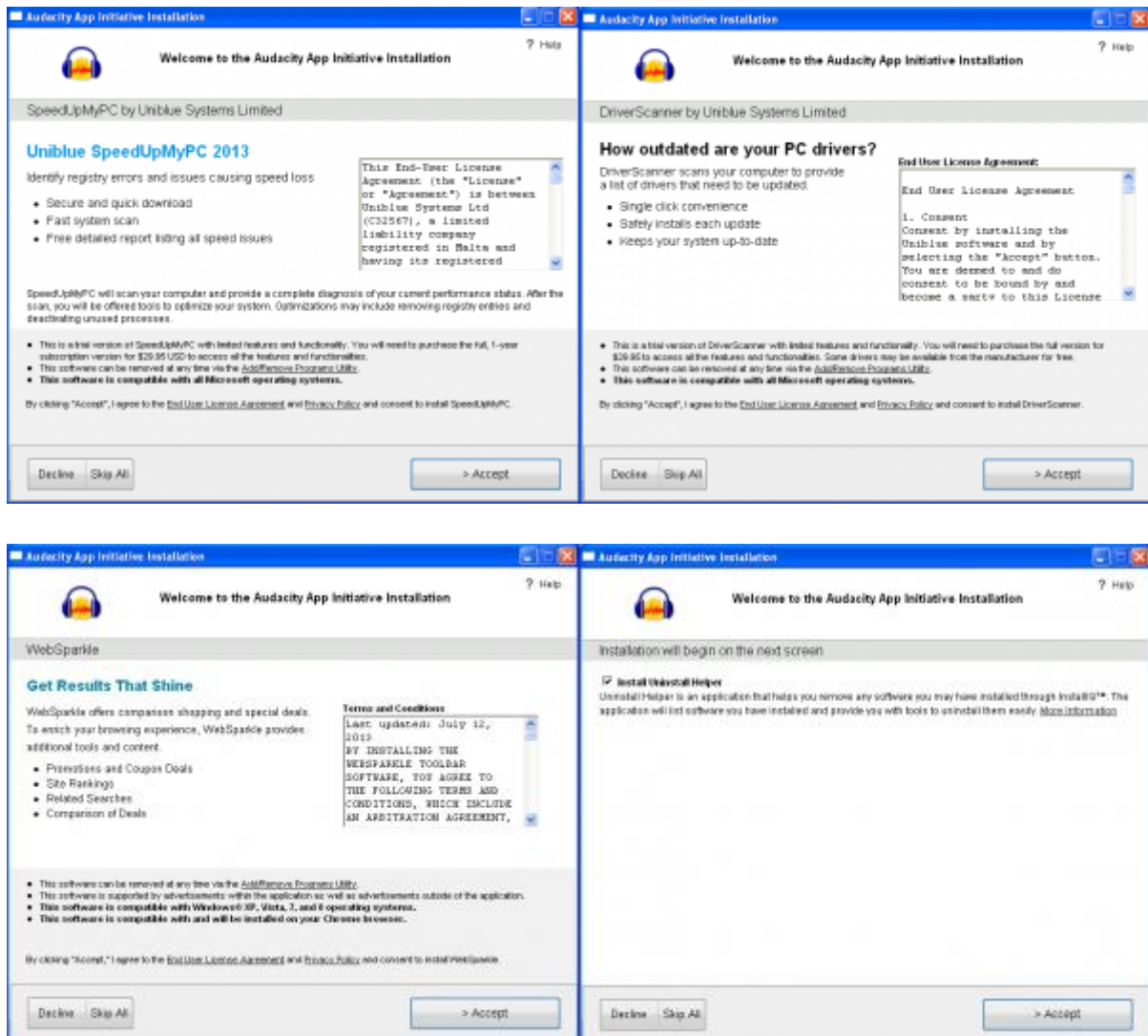


Dieses Mal handelt es sich um eine kostenlose Testversion von **TuneUp Utility 2013**, was in PUP-Begriffen ein kostenloses Werbemittel darstellt. Wie bei PC Speed Up oben ist TuneUp Utility 2013 so konzipiert, Sie davon zu überzeugen, dass Ihr Computer kaputt ist und die einzige Rettung im Kauf von 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: <https://blog.emsisoft.com/de/2013/12/23/was-ist-ein-pup/>