



TRUST IN
GERMAN
SICHERHEIT

G DATA WHITEPAPER

POTENTIALLY UNWANTED PROGRAMS (PUP'S)



CONTENTS

Motivation · · · · · 03-03

What POTENTIALLY UNWANTED PROGRAMS do to trick users into installing them · · · · · 04-05

Are POTENTIALLY UNWANTED PROGRAMS a threat? · · · · · 06-06

How G DATA BROWSER CLEANER and FakeAVCleaner can help get rid of PUP’s again · · · · · 07-07

References · · · · · 08-08

MOTIVATION

Providers of freeware are increasingly relying on a particularly annoying business model in order to monetarize their free software. Software products from third-party suppliers are delivered along with the installation program, with varying degrees of concealment. The third-party providers pay a commission to the freeware provider with each successful installation; sources of shared income can include the direct display of advertising or the generation and sale of user profiles for personalized advertisements. Even trusted providers such as Adobe have links on their pages for unwanted add-on software as an "optional extra" for their products, but at least these are clearly identifiable and can be disabled before downloading.

The uninterrupted global demand for free software has led to the formation of a multi-million dollar industry. At the short end of the stick, however, are the users who find themselves facing ever more aggressive adware, spyware or all manner of ineffective software for fixing non-existent "computer problems" that allegedly slow the user’s system down. This type of software is generally referred to as "Potentially Unwanted Programs" (PUP's), because they do not inflict any direct damage, but instead cost the user’s time and in a lot of cases seriously tests their patience without bringing any benefits.

¹ <https://blog.gdata.de/artikel/potentiell-unerwuenschte-programme-viel-mehr-als-nur-nervig>
² http://www.pcwelt.de/ratgeber/Huckepack-Software-_Weg-mit-dem-Muell-7938592.html



Download portals such as CNET/ Download.com or Softonic have even made planting Potentially Unwanted Programs the focus of their business activity. Each program downloaded from there is packaged in an installer which installs additional software. As a result, even programs that are "clean" to begin with, will then bring along a "blind passenger" each time the program is installed. Other websites hide the link for downloading genuine and legitimate programs amidst numerous download buttons for dubious and/or useless software that make it very easy to download the wrong program. Anyone looking for a specific software title

who casually clicks on one of the top search results in Google can render their browser unusable in no time at all by inadvertently installing what is called a "browser hijacker" with toolbars, unknown search engines and advertising displays. The same happens with the careless installation of freeware – even if this has been downloaded from trustworthy download sites or from the provider. ^{1,2}



Providers of unwanted programs present their dubious activity as a legitimate business model and lure in freeware providers with additional revenues. (Source: Computer-Service-Remscheid.de)



WHAT POTENTIALLY UNWANTED PROGRAMS DO TO TRICK USERS INTO INSTALLING THEM

Of course, nobody will voluntarily install a program on their computer that only offers a very small benefit, if any. Likewise, no user will willingly install software that aggressively displays advertising or shows fake warning messages. The providers, however, use various methods to trick the user into installing the software:

- Web pages are deliberately designed to make it difficult to locate links for downloading genuine software. That way, users are more likely to click the download button for PUP's: The user mistakenly clicks on one of these buttons, supposedly starts installing the program he wants, and gets unwanted software instead.
- Websites display aggressive advertising which mimic the warning of a virus infection, registry error or tells the user that "320 PC problems have been detected". If the user heeds the warning, he will install a useless program promising a paid-for "full version" that will eliminate these alleged problems.
- The most widespread practice is bundling with legitimate freeware, as described in the introduction. Various methods are meant to ensure that the user overlooks the unwanted programs he receives during the installation, or gets the impression that installing them is mandatory.

The arsenal of tricks for duping users during the installation of freeware and tricking them into installing the Potentially Unwanted Program is diverse: ³

- The Potentially Unwanted Programs are installed if the user does not pay close attention and fails to disable the option for installing it.
- The option for preventing the installation of a Potentially Unwanted Program is hidden in the "user-defined" or "advanced" installation options. If the user uses the "express" or "recommended" installation option, he will not see any indication of the dummy passenger.
- The installation of the Potentially Unwanted Program is disguised as acceptance of the licence terms of the actual freeware; the only clue is the discrepancy in the program name in the small print. Declining the licence terms is the only way to prevent the installation. However, at first glance it looks to the users as if he would cancel the entire installation by doing so.



The installation of the unwanted add-on software is disguised as accepting the licence terms for the freeware. (Source: pcworld.com)

- The option for deselecting the Potentially Unwanted Program is greyed out so it looks like it has been disabled, but it can in fact be selected. Hence the user is left under the impression that the installation of the unwanted program is unavoidable.



The option to decline the licence terms or the installation is greyed out and apparently disabled, although it can be used. (Source: pcworld.com)

- The wording of the installation options is deliberately designed to be misleading with the use of a double negative. The supposed deactivation of the Potentially Unwanted Program actually initiates its installation. The user will only know about this when reading the text very carefully.

³<http://www.pcworld.com/article/2429418/how-to-spot-and-avoid-installing-potentially-unwanted-programs.html>

ARE POTENTIALLY UNWANTED PROGRAMS A THREAT?

Unlike real malware, PUP's do not have any direct malicious effect, nor any means of spreading autonomously. They do not steal account data, do not manipulate banking websites and do not infect any files. Furthermore, they are installed by the user himself, albeit unwittingly in many cases. In the light of this, the majority of security solutions do not categorize PUP's as malware, despite them being such a nuisance. There is also a legal side to this: if a program clearly does not cause any direct damage, a warning from a security program would potentially harm the business interests of the provider.

However, it is still possible for the user to be damaged indirectly by unwanted programs. The following consequences are conceivable, for example:

- By redirecting search queries to bogus search engines, the risk increases of the user ending up on fake websites or ones manipulated by malware.
- Unintentionally clicking on bogus or aggressive advertising leads to the installation of additional unwanted programs or malware.

- Eliminating bogus computer problems or virus infections for a fee leads to financial damages, even though the user pays the sum voluntarily.
- Blocking or disabling security functions in the browser can open up security holes for real malware.
- Functions for downloading additional program components open up potential security holes, via which malware or hackers can access the computer.

PUP's are therefore more than just a nuisance, they can potentially put the computer at risk.

HOW G DATA BROWSER CLEANER AND FAKEAVCLEANER CAN HELP GET RID OF PUP'S AGAIN

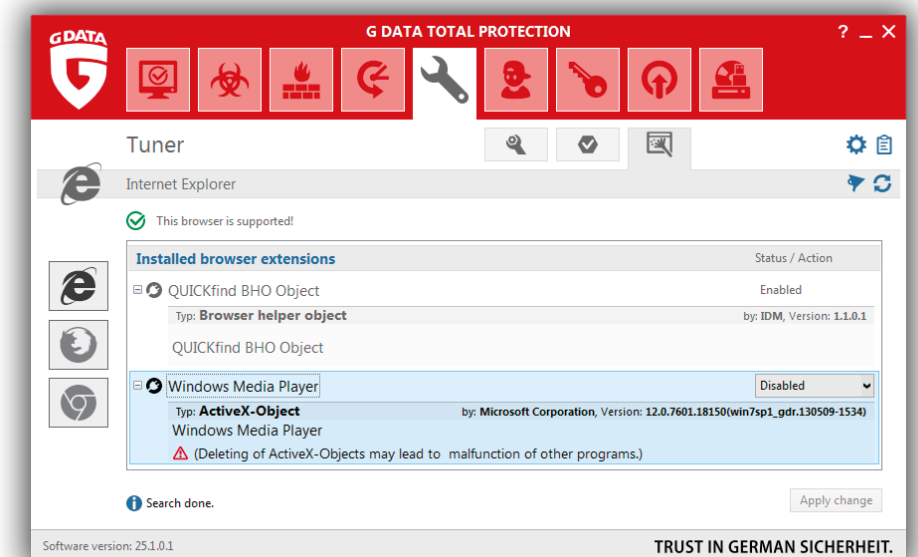
PUP's are inadvertently installed on the PC in no time, but are sometimes difficult to get rid of again. Many providers actually use the same programming techniques as authors of malware to embed their products deep in the system.⁴ Uninstalling via the Windows control panel is generally hard and usually unsuccessful for non-experts. The infamous browser hijacker Snap.do requires separate uninstalling for each browser. Other PUP's are installed in multiple parts that need to be fully removed prior to the next system start, otherwise they will reinstall themselves.

Even experienced users can make the task significantly easier by using G DATA BROWSER CLEANER and the G DATA FakeAVCleaner System Tool.

G DATA BROWSER CLEANER works with Microsoft Internet Explorer, Mozilla Firefox and Google Chrome and enables effortlessly easy management of all installed browser extensions. With a click of the mouse, all plug-ins in the list can be disabled or removed to free the browser of unwanted extensions. The tool optionally displays all plug-ins categorized as safe, so you can quickly and easily distinguish the unsafe or unwanted extensions. G DATA BROWSER CLEANER is included in the comprehensive solution G DATA TOTAL PROTECTION.

Users of G DATA INTERNET SECURITY and G DATA ANTIVIRUS can download the tool for free. G DATA FakeAVCleaner System Tool

removes fake AV tools that simulate a virus infection, scare the user and supposedly eliminate the danger again on payment of a fee. This category of programs includes PUP's such as Reimage Repair, which simulates PC problems rather than a virus infection. G DATA FakeAVCleaner System Tool can be downloaded from www.gdatasoftware.com/downloads for free by all users.



One click of the mouse is all it takes to remove unwanted browser extensions from Firefox, Internet Explorer or Chrome.

⁴<https://blog.malwarebytes.org/fraud-scams/2014/12/potentially-unwanted-program-borrows-tricks-from-malware-authors/>

TRUST IN
GERMAN
SICHERHEIT

REFERENCES

1. G DATA SecurityBlog: "Potentially Unwanted Programs": much more than just annoying
<https://blog.gdatasoftware.com/blog/article/potentially-unwanted-programs-much-more-than-just-annoying.html>
2. Peter Stelzel-Morawietz: "Huckepack-Software: Weg mit dem Müll!" (German)
<http://www.pcwelt.de/ratgeber/Huckepack-Software- Weg-mit-dem-Muell-7938592.html>
3. How to spot and avoid installing potentially unwanted programs
<http://www.pcworld.com/article/2429418/how-to-spot-and-avoid-installing-potentially-unwanted-programs.html>
4. Jérôme Segura: Potentially Unwanted Program borrows tricks from malware authors
<https://blog.malwarebytes.org/fraud-scam/2014/12/potentially-unwanted-program-borrows-tricks-from-malware-authors/>

TRUST IN
GERMAN
SICHERHEIT