Problematic, Unloved and Argumentative: What is a potentially unwanted application (PUA)?

Revised 11-29-2011

Aryeh Goretsky, MVP, ZCSE

Table of Contents

Introduction

This paper was started as the result of a rather innocuous request: A co-worker asked for an explanation of what the class of software ESET calls ***potentially unwanted applications*** (PUAs)—also known as ***potentially unwanted programs*** (PUPs) or ***potentially unwanted software*** (PUS)—does. While he was already familiar with the more well-known types of malicious software, such as computer viruses and worms, he wanted to understand the difference between the outright threats posed by these types of malware and those that are classified as being ***potentially a*** threat. So, with question that in mind, just what is a potentially unwanted application?

The formal definition

A potentially unwanted application (PUA) is a type of computer program ***and*** a set of associated behaviors (which we will discuss in more detail later). While a PUA may ***not*** perform the same type of malicious activities typically associated with computer viruses or worms—such as causing damage to programs, altering data, spreading illicitly across network shares and so forth—it may instead install additional unwanted software, change the behavior of the digital device, or perform activities not approved or expected by the user.

Here's a real-world example of such an application:

A company in a heavily regulated industry (such as banking or health care) may restrict its employees' use of instant messaging (IM) due to regulatory concerns. To bypass this restriction, a new employee who wishes to chat with friends while at work brings in a USB flash drive with a portable instant messaging (IM) program on it. While free, the program is supported by advertising. It turns out that a criminal bought space on the advertising network used by the program, and uses a maliciously crafted advertisement to inject malware into the new employee's computer, which then acts as a springboard for stealing the company's intellectual property.

PUAs in the home and office

Potentially unwanted applications are not limited to the office. Imagine the following scenario: A child using a family computer downloads a "utility" program in order to add additional features to his or her instant messaging program. The child clicks through the program's installation process, ignoring the end user license agreement (EULA), and thus doesn't realize that installing the program will also install adware that monitors user behavior and displays targeted advertising, and that replaces standard search recommendations with paid search results. The adware may then go on to redirect search results to sites from which additional malicious software can be deployed.

Examples of PUA behavior:

Many types of program can be classified as potentially unwanted applications. Here are some of the most common reasons:

- Programs that install toolbars in the web browser. Such add-ons are not necessarily malicious, but if they install without clearly informing the user of their presence, don't offer the opportunity to opt out of installing, provide no means to effect a clean uninstall or fail to provide assistance with uninstalling; then they join the category of potentially unwanted applications.

- Programs that contain an adware component but do not clearly indicate the presence of such a component or provide a method or instructions for removing the adware after the parent application has been uninstalled.
- Software of dubious quality and reputation, including programs that make outlandish, unverifiable and unsupportable claims about their efficacy and/or generate deceptive false-positive alarm reports of threats that do not exist in order to mislead people into purchasing something they do not really want or need. Sometimes such programs make claims so misleading that they actually border on—or step across the border of—outright fraud.
- Programs sold through spam and/or sold through rogue affiliate marketing networks that pay a commission based on software installations (the "pay-per-install" business model).
- Programs that make changes to web browser settings such as the default home page or search engine selection in an unannounced or otherwise deceptive fashion.
- Programs compressed with packers or protectors that are widely used (or abused) by malicious software.
- Legitimate programs that are misused by malware to perform malicious activities.

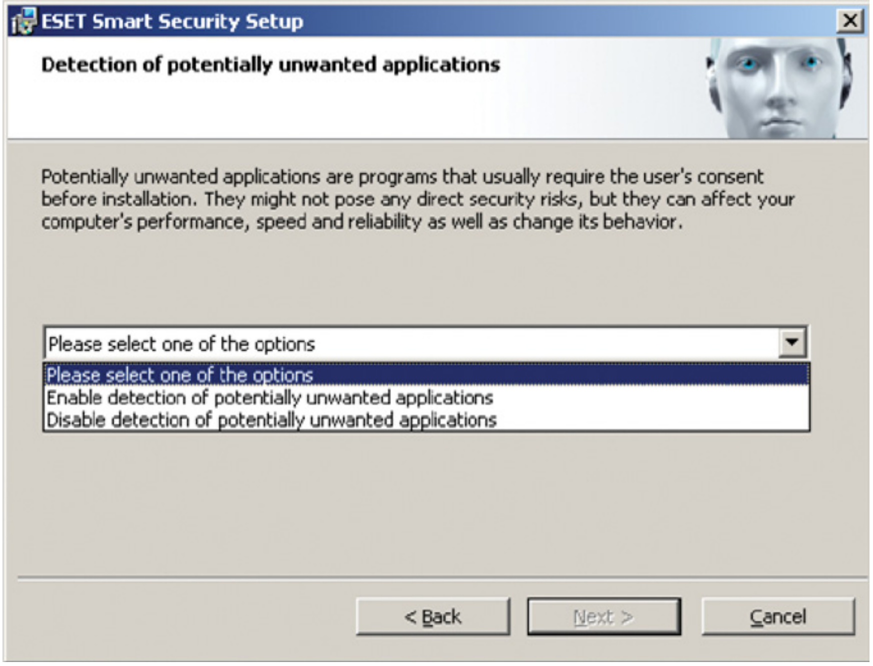
The latter case is interesting because it involves a program that is legitimate, or that might at least otherwise normally be classified as a potentially unsafe application (a category we will discuss further on). In these instances, a program that has legitimate uses has been surreptitiously installed onto a computer by other malware in order to perform a clandestine activity. Examples include programs that perform such activities as remote administration, process management and Bitcoin mining. While none of these actions may itself qualify as unwanted activity by the computer user, when a specific version of such as program is installed by malware to such an extent that its presence stands a good chance of indicating an infection, it is classified as a PUA. This provides the user with an opportunity to be alerted to the presence of additional malicious software that might otherwise be undetected. Programs that fall into this category are subject to careful scrutiny: If only one particular version of a program is widely distributed by malware, ESET will only classify that particular version as a PUA. If, on the hand, multiple versions of the program are used by malware, it may be necessary to flag all versions of the program, including future versions.

Another emerging case is the use of software wrappers. A "software wrapper" is a program that wraps—or encapsulates—another program. The technology itself is not new and has been used for various purposes over many years. Back during the DOS era, parasitic file-infecting viruses commonly infected their host files by prepending and/or appending malicious code to them, and runtime file packers have also been used to compress executable files to make them smaller or resistant to reverse engineering. However, unlike a computer virus, software wrappers have no replicating component, and unlike a runtime packer, they do not seek to compress or obfuscate the original program file. What software wrappers do have, though, is a potentially unwanted application as their payload, which means they install a program or perform an activity such as those described, above. While this makes software wrappers de facto members of the potentially unwanted application family, it is important to distinguish between the two components: The PUA, in this case, is the software wrapper, **not** the encapsulated program, which may be a legitimate application. It is also important to note that in most instances, software wrappers are not applied by the original developer of a program but rather by someone seeking to benefit from distributing it for download and installation. Of course, because any program can, in theory, be wrapped, it is possible we might one day come across a PUA that has been wrapped in another PUA.

These, then, are some of the most frequently observed types of potentially unwanted programs. But it is important to keep in mind that there are additional reasons for classifying a program as potentially unwanted. More examples can be found in Robert Lipovský, Daniel Novomeský and Juraj Malcho's paper from the Virus Bulletin 2011 Conference, "**Fake but Free and Worth Every Cent.**"[1]

Potentially unwanted: It's your decision

There are some situations in which a person may consider that the benefits of a potentially unwanted application outweigh its risks, and this is the reason ESET antivirus software assigns such applications to a lower-risk category than other types of malicious software, such as trojans or worms. In fact, ESET's antivirus software requires the user to determine whether potentially unwanted applications should be looked for when the security program is installed. (See Figure 1.)



ESET Smart Security Setup

Detection of potentially unwanted applications

Potentially unwanted applications are programs that usually require the user's consent before installation. They might not pose any direct security risks, but they can affect your computer's performance, speed and reliability as well as change its behavior.

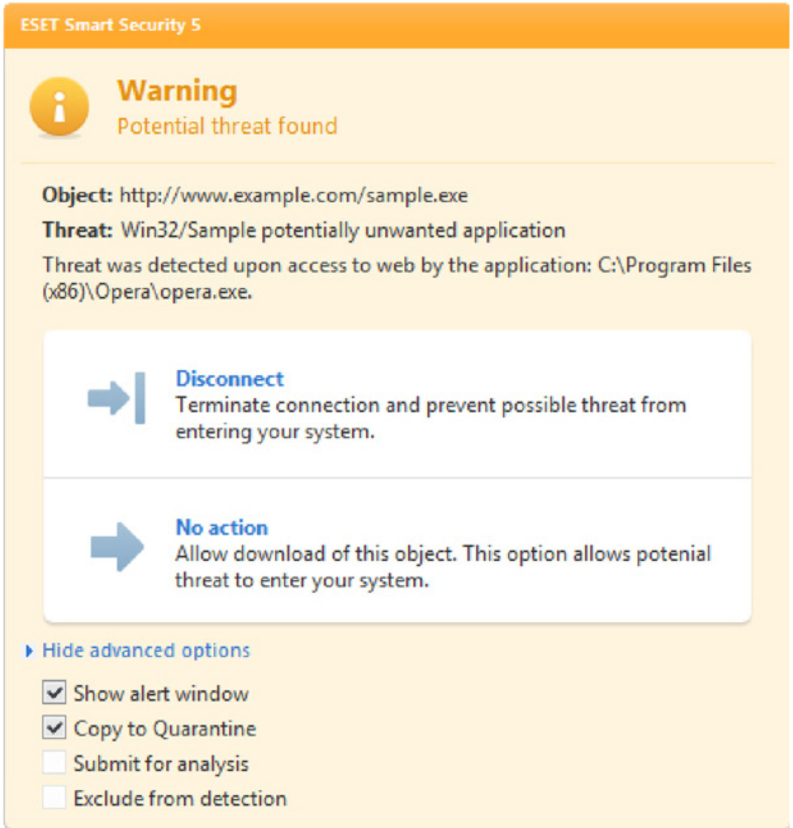
Please select one of the options

Please select one of the options
Enable detection of potentially unwanted applications
Disable detection of potentially unwanted applications

Figure 1: PUA detection configuration

This is not a permanent option, and can be toggled on and off as the user desires. For instructions, see ESET Knowledgebase article # 2198, "**How do I configure my ESET security product to detect or ignore unwanted or unsafe applications**?" [2]

Additionally, ESET users are able to decide what actions should be taken upon detection of a potentially unwanted application. (See Figure 2 for a simulated screenshot.)



ESET Smart Security 5

Warning

Potential threat found

Object: http://www.example.com/sample.exe

Threat: Win32/Sample potentially unwanted application

Threat was detected upon access to web by the application: C:\Program Files (x86)\Opera\opera.exe.

Disconnect

Terminate connection and prevent possible threat from entering your system.

No action

Allow download of this object. This option allows potenial threat to enter your system.

Hide advanced options

☑ Show alert window

☑ Copy to Quarantine

□ Submit for analysis

□ Exclude from detection

Figure 2: Detection of a PUA

Clicking on the ***Show Advanced Options*** item allows the user to "white list" (ignore) programs categorized as lower-risk threats so they may run on the computer.

Meet the potentially unsafe application

Closely related to potentially unwanted programs are potentially unsafe applications. This classification may include illegal software or software from unknown or untrustworthy vendors, but is generally applied where use is commonly accepted and is only a cause for concern in certain specific situations, such as when deployed by malware or used by a person with malicious intent. Potentially unsafe applications include the following:

- Software cracking tools and license key generators: These programs may be used to bypass copy protection. In some cases, this may be permissible (for example, if the software author is no longer in business).
- Hacking tools: These programs are used to compromise a digital device or network. A company might want to restrict access to such programs to security personnel.
- Product key finders: Typically, a user will never have to enter the serial number for software after it has been installed—if the software was pre-installed with the computer, he or she may not even know the serial number. There are times, though, when it may be necessary to look up a serial number, such as when hardware is being replaced. However, such programs might be misused to steal serial numbers for software.
- Remote control programs: A company's IT department might use this type of program to access a computer in a server room or repair a computer at a remote location, but they might not want their other employees to run such programs, which are, for instance, commonly used by fake support service centers.
- Software that displays advertising: This sort of software (i.e., adware) can feature advertising, possibly through a toolbar, or change the displayed pages or search query results in a web browser. This may or may not be acceptable to the user.

These examples are mainly geared towards inappropriate software use in a business environment; however, they also may be relevant in the home.

Conclusion

Malicious software has long since moved beyond traditional black or white, malicious or innocent, and has instead adopted varying shades of gray.

Determining when to classify a program as being either unwanted or unsafe can be particularly challenging, because a researcher has to look not just at what a program does, but what the intent is behind it. Business, ethical and legal questions come into play, too. For more information on this, I refer you to the head of ESET's virus lab, Juraj Malcho, who discussed this thoroughly in his virus conference paper from VB2009, "**Is there a lawyer in the lab**?" [3]

Recognizing that users may have legitimate reasons to occasionally run programs whose use might normally be considered questionable, ESET antivirus software allows for maximum flexibility in regards to filtering PUAs.

For additional information on potentially unwanted applications, I would suggest looking at our previous blog entry on **potentially unwanted applications** [4], as well as reading Wikipedia's **entry** [5] on potentially unwanted applications and this **description** [6] from Virus Bulletin magazine. If you are interested in some other categories of threat detected by ESET's software, the glossary in ESET Knowledgebase Article # 186, "**Viruses and other malware defined**" [7], is an excellent starting point.

A special thanks to my colleagues David Harley and Daniel Novomeský for their assistance with this article. If you have any questions or feedback, please feel free to contact us via the **AskESET@eset.com** mailbox.

Author bio

Aryeh Goretsky holds the position of Distinguished Researcher at global security provider ESET, where he is responsible for a variety of activities, including monitoring the threatscape, investigating technologies, working with ESET's developers, QA and support engineers, and liaising with other research organizations. He was the first employee at McAfee and is a veteran of several software and networking companies, including instant messaging pioneer Tribal Voice and VoIP hardware manufacturer Zultys Technologies. He is the recipient of Microsoft's Most Valuable Professional Award for contributions to making computing safer.

References

1. Lipovský, R., Novomeský, D. and Malcho, J. "Fake but Free and Worth Every Cent." Proceedings of the 21st Virus Bulletin International Conference. 2011: **http://go.eset.com/us/resources/white-papers/fake_but_free.pdf**

2. ESET Knowledgebase article #2198, "How do I configure my ESET security product to detect or ignore unwanted or unsafe applications?" **http://kb.eset.com/esetkb/index?page=content&id=SOLN2198**

3. Malcho, J. "Is there a lawyer in the lab?" Proceedings of the 19th Virus Bulletin International Conference. 2009: **http://go.eset.com/us/resources/white-papers/Lawyer_in_the_lab.pdf**

4. ESET Threat Blog: **http://blog.eset.com/?s=possibly+unwanted**

5. Wikipedia, "Privacy Invasive Software": **http://en.wikipedia.org/wiki/Potentially_Unwanted_Application**

6. Virus Bulletin, "Possibly Unwanted": **http://www.virusbtn.com/resources/glossary/potentially_unwanted.xml**

7. ESET Knowledgebase Article # 186, "Viruses and other malware defined": **http://kb.eset.com/esetkb/index?page=content&id=SOLN186**

www.eset.com

ESETPUAWP20111129