Problematic, Unloved and Argumentative:

What is a potentially unwanted application (PUA)?

Aryeh Goretsky, MVP, ZCSE

Table of Contents

Introduction

This paper was started as the result of a rather innocuous request: A new co-worker asked me to explain to him what the class of software ESET calls ***Potentially Unwanted Applications*** (PUAs)—also known as ***Potentially Unwanted Programs*** (PUP) or ***Potentially Unwanted Software*** (PUS)—did. While he was already familiar with some malicious types of 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 which are classified as being ***potentially unwanted***. 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 set of associated behaviors (more on this 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, they 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 healthcare) 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 its 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 it will install adware that monitors user behavior and displays targeted advertising, and replaces search recommendations using paid search results. The adware may then go on to redirect search results to sites from which additional malicious software can be deployed.

Some other examples of PUAs include:

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 migrate towards the category of potentially unwanted applications.

- Programs that contain an adware component but do not clearly indicate the presence of such a component, nor provide a method or instructions for removing the adware after the parent application have been uninstalled.

- Software of dubious quality and reputation, which include programs that make outlandish, unverifiable and unsupportable claims about their efficacy, and/or generate deceptive false positive alarm reports of threats where none exists in order to mislead people into purchasing something they do not really want or need. Sometimes such programs make claims so misleading that the actually border on—or step across the border of—outright fraud.
- Programs sold through spam, installed by malware and/or sold through rogue affiliate marketing networks that pay a commission based on software installations (the pay-per-install business model).
- Programs compressed with packers or protectors that are widely (ab)used by malware.

Of course, there are additional reasons a program might be classified as potentially unwanted, these are just some of the most frequently observed ones.

Potentially unwanted: it's your decision

There are some situations where a person may consider that the benefits of a potentially unwanted application outweigh its risks, and this is the reason ESET antivirus software assigns them 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)

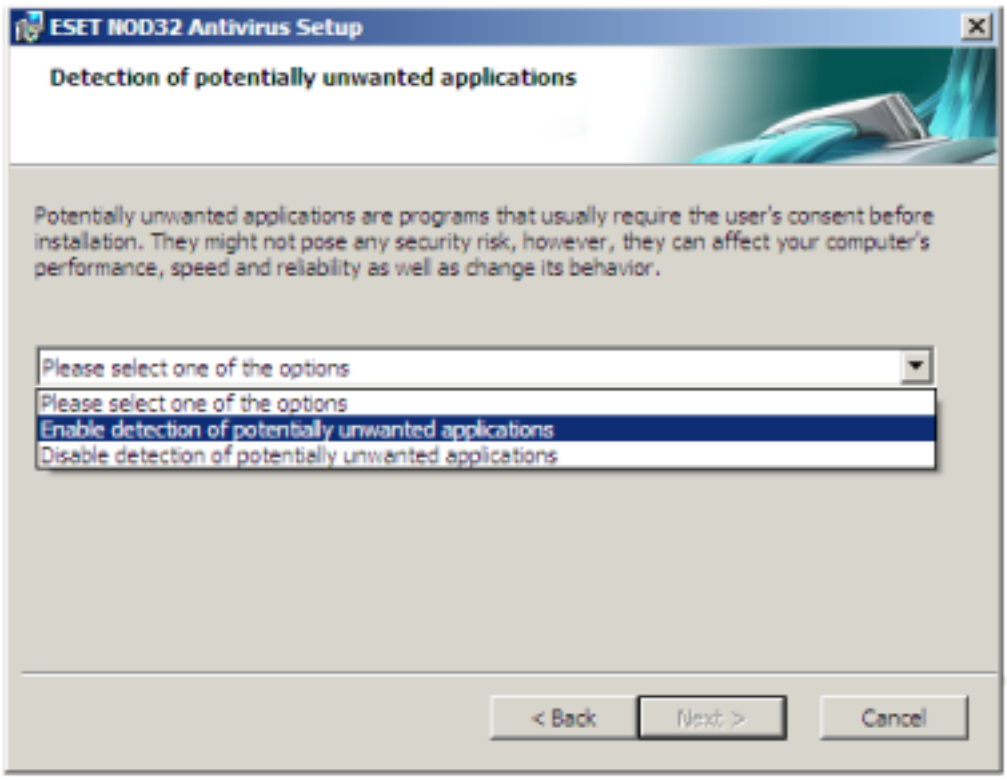

Figure 1: PUA detection configuration

This is not a permanent option, and can be toggled on and off as the user desires. For instructions see ESET Knowledgebase article # 2198 [1], "How do I configure my ESET security product to detect unwanted or unsafe applications?".

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

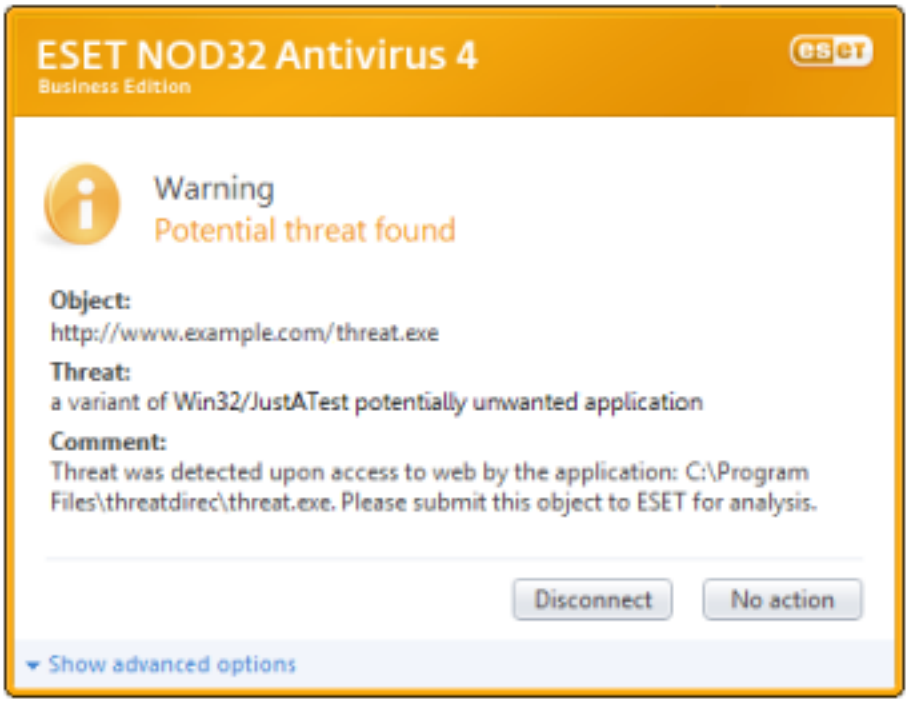

Figure 2: Detection of a PUA

Clicking on the ***Show Advanced Options*** item allows the user to white list (or 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 is in certain specific situations, such as when deployed by malware or used by a person with malicious intent.

- 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: Programs which 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, they 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: Software can feature advertising, possibly through a toolbar, or changes the displayed pages or search query results in a web browser, i.e., adware. 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 and white, malicious/innocent to varying shades of gray.

Determining when to classify a program as either being unwanted or unsafe can be particularly challenging, because a researcher has to not just look at what a program does, but what the intent is behind it. Business, ethical, and legal questions come in to 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 white paper, "Is there a lawyer in the lab?" [2].

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 [3], as well as reading Wikipedia's entry [4] on Potentially Unwanted Applications and this description [5] 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" [6] is an excellent starting point.

A special thanks to my colleagues David Harley and Daniel Novomesky 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 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. ESET Knowledgebase article # 2198, "How do I configure my ESET security product to detect unwanted or unsafe applications?": http://kb.eset.com/esetkb/index?page=content&id=SOLN2198
2. Juraj Malcho, "Is there a lawyer in the lab?": http://www.eset.com/resources/white-papers/Lawyer_in_the_lab.pdf
3. ESET ThreatBlog: http://blog.eset.com/?s=possibly+unwanted
4. Wikipedia, "Privacy Invasive Software": http://en.wikipedia.org/wiki/Potentially_Unwanted_Application
5. Virus Bulletin, "Possibly Unwanted": http://www.virusbtn.com/resources/glossary/potentially_unwanted.xml
6. ESET Knowledgebase Article # 186, "Viruses and other malware defined": http://kb.eset.com/esetkb/index?page=content&id=SOLN186

www.eset.com

ESETPUAWP20110718