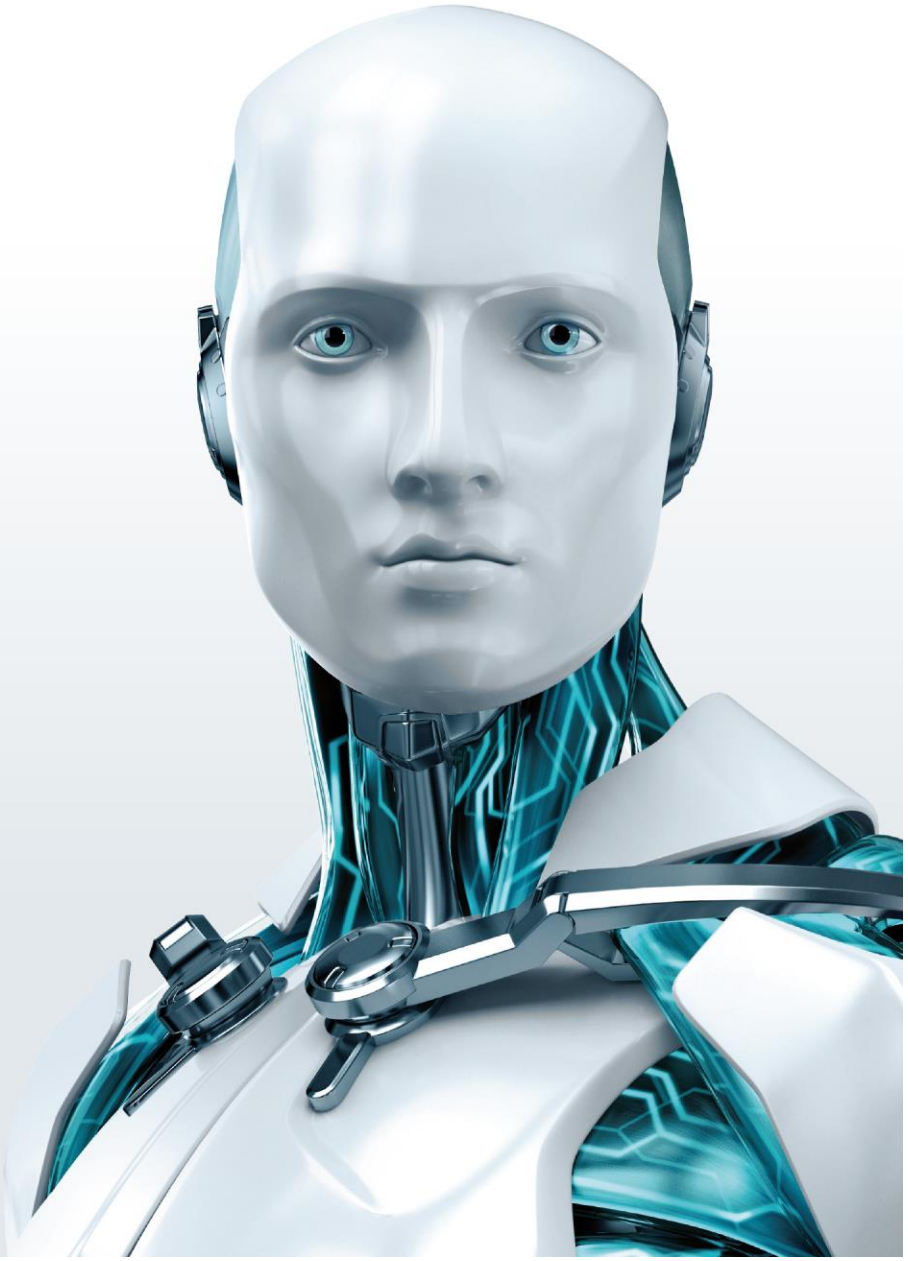
Aplicaciones Potencialmente Indeseables (PUA)



Autor: André Goujon, Especialista de Awareness & Research

Fecha: julio 2012

ESET
ENJOY SAFER TECHNOLOGY™

Índice

Introducción 3

¿Qué son los PUA? 3

Aplicaciones potencialmente peligrosas 4

Los PUA pueden impactar hogares y empresas 5

La detección de PUA es opcional 6

Conclusión: dificultades en la categorización 7

Introducción

Las siglas PUA son el acrónimo anglosajón de "***P**otentially **U**nwanted **A**pplication*", es decir, aplicaciones potencialmente indeseables. Se trata de programas informáticos que exhiben una serie de comportamientos probablemente indeseados por el usuario. Aunque los PUA pueden no presentar conductas típicas de códigos maliciosos (como expandirse a través de una red, cifrar archivos o dañar otros programas), sí llevan a cabo otras acciones. Entre ellas, suelen instalar aplicaciones adicionales, cambian el comportamiento del dispositivo en el cual son ejecutados o realizan acciones no esperadas por la persona que los instaló.

Este tipo de aplicaciones han despertado la curiosidad y muchas dudas por parte de los usuarios, especialmente en casos donde su equipo baja el rendimiento, o cuando aparecen funcionalidades activas que el usuario no recuerda haber aplicado, e incluso en los casos donde la solución antivirus detecta el archivo.

Por tal motivo, el presente artículo buscará explicar en mayor detalle qué son las aplicaciones potencialmente indeseables, cómo pueden perjudicar al usuario y por qué éstas son detectadas por muchas soluciones de seguridad.

¿Qué son los PUA?

Un archivo es catalogado como PUA cuando, según un análisis previo y exhaustivo por parte de nuestros laboratorios, presenta uno o varios de los siguientes comportamientos:

- Programas que instalan algún componente *adware* sin explicitarlo o que no proveen un método eficaz para su posterior remoción del sistema.
- Software que emite alertas y encuentra gran cantidad de errores, sin que todos sean reales (falsos positivos). Generalmente estos desarrolladores ofrecen productos de dudosa calidad y procedencia.

Muchos de estos programas prometen resolver gran cantidad de problemas encontrados en el registro del sistema operativo o amenazas detectadas en la computadora, aunque no siempre estos problemas son reales o de la gravedad indicada por la aplicación. Determinar fehacientemente la verdadera intención que hay tras dicho comportamiento y el nivel de peligrosidad en comparación con la utilidad, son factores claves para poder saber si estamos frente a un PUA o un código malicioso[1].

Algunos de los comportamientos o aplicaciones que pueden ser catalogados como PUA son las siguientes:

- **Barras de herramientas (*toolbars*)** que se instalan sin el consentimiento adecuado del usuario y no poseen un mecanismo de desinstalación eficaz. Aunque existen casos en que estas aplicaciones son de utilidad, al no informar explícitamente sobre su instalación, pueden entrar en la categoría de PUA.

[1] Más información sobre este tema puede ser encontrada en el documento "FAKE BUT FREE AND WORTH EVERY CENT" de Robert Lipovský, Daniel Novomeský y Juraj Malcho.

- **Programas que modifican configuraciones de navegadores de Internet**. Por ejemplo alteran la página de inicio o el buscador predeterminado.
- **Instaladores (o "*software wrappers*") que se comportan como parásito**, es decir, que tienen encapsulado un programa completamente genuino que instalan en conjunto con otros componentes inesperados como una barra de herramientas. Hay que tener en cuenta que en un ejemplo como este, sólo el instalador y la segunda aplicación son considerados potencialmente indeseados, y no el componente legítimo del mismo. En la mayoría de los casos, los desarrolladores del programa genuino no encapsulan sus productos de esta forma[2].
- **Aplicaciones que son distribuidas mediante el modelo de negocio "pagar por instalar"** (*pay-per-install*). En algunos casos, esto significa que el programa es expandido mediante métodos poco ortodoxos como malware o campañas masivas de correo electrónico basura (spam).
- **Programas protegidos por empaquetadores en tiempo real** que hayan sido ampliamente utilizados con fines maliciosos para evitar y dificultar su detección.
- **Software legítimo** que ha sido **utilizado por programas maliciosos** de forma masiva**.**

Este último caso **puede ser controvertido y difícil de determinar, puesto que se trata de programas que son genuinos** y que en un contexto de buen uso, no tendrían que ser detectados, o en el peor de los casos, sólo podrían catalogarse como potencialmente **peligrosos**, clasificación que será presentada más adelante.

Por ejemplo, si una determinada versión de un programa de acceso remoto y administración de procesos es utilizada de forma masiva por códigos maliciosos, ESET clasificaría esa edición en particular del programa como PUA. Esto se debe a que la presencia de dicha herramienta de administración remota en el sistema de los usuarios podría permitir encontrar y detectar malware que de lo contrario, pasaría inadvertido.

En caso que e haya hecho mal uso de varias versiones de un mismo programa, entonces todas las ediciones de ese software podrían entrar en la categoría de PUA y ser detectadas como tal, incluso aquellas actualizaciones que pudieran ser lanzadas en el futuro.

Aplicaciones potencialmente peligrosas

A diferencia de las aplicaciones potencialmente **indeseables**, las **peligrosas** representan una posible amenaza si quien las utiliza lo hace con fines maliciosos, o en determinados entornos y situaciones.

Por ejemplo, para un usuario hogareño, un programa de acceso remoto es potencialmente peligroso puesto que generalmente no necesita de uno, mientras que una empresa sí hace uso de este tipo de *software* para que el departamento IT pueda configurar las computadoras de una organización de forma sencilla y centralizada. Sin embargo, este tipo de herramientas también podrían provocar daños en un ambiente corporativo si caen en las

[2] Aryeh Goretsky entrega mayores antecedentes sobre algunas de las motivaciones existentes tras los *software wrappers* en su artículo "PROBLEMATIC, UNLOVED AND ARGUMENTATIVE: WHAT IS A POTENTIALLY UNWANTED APPLICATION (PUA)".

manos equivocadas.

Por lo tanto, esta clasificación aplica para aquellos programas que tienen un uso comúnmente aceptado pero que en algunos casos su utilización puede resultar riesgosa.

Algunos de los comportamientos o programas que pueden ser catalogados como aplicaciones potencialmente peligrosas son las siguientes:

- **Programas de cracks y generadores de números de licencia (keygen)**: Estos programas generan parches sin autorización del desarrollador del programa y tienen por objetivo modificar el comportamiento de un software original.
- **Herramientas de acceso ilegal (*hacker tools*)**: Generalmente estas herramientas están restringidas exclusivamente para personal autorizado dentro de una empresa.
- **Programas para obtener números de licencias**: Estos son capaces de conseguir los números de las licencias de aplicaciones instaladas en el sistema. Su uso es aceptado en casos donde se cambia el hardware y es necesario volver a activar dicho software escribiendo el serial.
- **Aplicaciones de acceso remoto**: los departamentos de IT suelen utilizar estos programas para administrar y reparar computadoras remotamente, sin embargo, un usuario malintencionado o una plataforma de soporte técnico falsa, podría darle un uso totalmente distinto en comparación a los propósitos originales por los cuales estas aplicaciones son desarrolladas.
- **Software que despliega publicidad:** es como un adware, pero que sí es mencionado durante la instalación del mismo y que presenta un comportamiento menos agresivo como permitir su posterior remoción del sistema con respecto a uno clasificado como potencialmente indeseable.

Los PUA pueden impactar hogares y empresas

Tanto en un ambiente corporativo como en uno hogareño, los PUA pueden ser una potencial amenaza para la información, seguridad, estabilidad y desempeño adecuado del entorno informático.

Ejemplo de caso hogareño:

Un niño descarga e instala, sin leer el contrato de licencia ni fijarse en los detalles, un programa que agrega supuestas nuevas funcionalidades a clientes de mensajería instantánea como Windows Live Messenger, ICQ, entre otros.

Ni el menor ni su familia se dan cuenta que ese software gratuito también instaló un componente *Adware* que monitorea el comportamiento del usuario. Esto lo hace con el objetivo de mostrarle publicidad y resultados de búsqueda acorde a sus gustos, preferencias y a la información personal recopilada de la computadora. Además, los resultados de búsqueda que le aparecen al usuario en pantalla pueden dirigir fácilmente a los usuarios a sitios maliciosos o inadecuados.

Ejemplo de caso corporativo

Una compañía mantiene una política de IT muy estricta, en donde se deben adoptar todos los resguardos necesarios para mantener los sistemas informáticos seguros. Entre varias restricciones se encuentra la imposibilidad de utilizar programas de mensajería instantánea y la de instalar aplicaciones sin el permiso del departamento correspondiente.

Sin embargo, un empleado contradice el reglamento y ejecuta mediante un dispositivo de almacenamiento masivo USB, un software portable gratuito para conversar con sus amigos en línea. Lo que ignora esta persona es que aunque ese cliente de mensajería no requiere de pago para poder ser utilizado, sí despliega anuncios publicitarios.

El peligro radica en que esos espacios publicitarios pueden ser adquiridos por ciberdelincuentes, quienes no dudarían en manipular maliciosamente un aviso. De esta forma, detrás de un anuncio podría esconderse malware destinado a robar datos sensibles de las computadoras que tengan instalada esa aplicación de mensajería. Esto podría ser una amenaza muy grave para el funcionamiento y la integridad de la información de la empresa.

La detección de PUA es opcional

En algunos casos particulares, los usuarios podrían optar por utilizar ciertos programas que podrían ser clasificados tanto en la categoría potencialmente indeseable como peligrosa como por ejemplo, en un entorno corporativo, el departamento de IT necesita utilizar programas de acceso remoto que a partir de determinados usos podrían llegar a ser catalogados como potencialmente peligrosos.

También, hay que tener en cuenta que un usuario hogareño tiene la opción de utilizar una aplicación cuyo comportamiento no es lo suficientemente agresivo para clasificarse como malware y sus acciones están bien documentadas en el contrato de licencia del software.

En el caso de la detección de aplicaciones potencialmente **indeseables**, en todas las soluciones de ESET el usuario debe elegir entre activar o no dicha opción para poder continuar con el proceso de instalación:

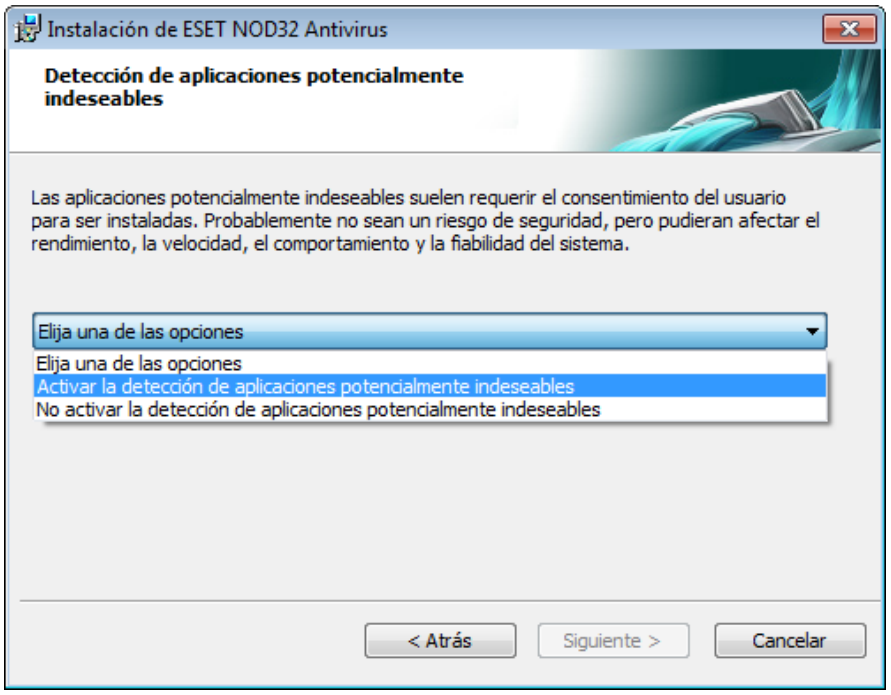


Imagen 1 – Detección de PUA en la instalación de soluciones de seguridad ESET

La funcionalidad de detección de aplicaciones potencialmente **peligrosas** viene desactivada de forma predeterminada. Ambas opciones pueden volver a ser configuradas una vez que el producto se encuentra instalado y de acuerdo a las necesidades particulares de cada usuario. El procedimiento de cómo hacerlo puede ser consultado en ESET Knowledgebase, nuestra Base de Conocimiento en español, haciendo clic en los siguientes enlaces:

- **Para la versión 5.x de productos ESET, presionar aquí (ID de solución: SOLN2912).**
- **Para la versión 4.x de productosESET, presionar aquí (ID de solución: SOLN2198).**

Conclusión: dificultades en la categorización

Actualmente, las cuestiones relacionadas a la detección de los PUA radican también en otros aspectos más allá de lo estrictamente técnico. En otras palabras, es importante determinar si la aplicación en cuestión es realmente legítima o no, en base a la verdadera intencionalidad de sus desarrolladores, y los posibles temas legales y éticos que conllevan detectar este tipo de programas.

Para poder establecer un criterio sobre qué tan malicioso es un software, y si reúne los antecedentes necesarios para que entre en la categoría de PUA, deben considerarse diversos factores. Entre ellas las funciones y utilidad que le otorgan al usuario, el modelo o canal de distribución a través del cual se obtiene la misma, y la potencial amenaza que pueda presentar para el entorno informático en cuanto a seguridad, estabilidad e integridad de la

información.

Los lineamientos específicos sobre clasificación de PUA se dificultan aún más con la existencia de aplicaciones discutiblemente útiles que contienen un componente de *adware* menos malicioso, con respecto a otras cuyo comportamiento es considerablemente más agresivo, pudiendo a estas últimas catalogársele directamente como malware, o específicamente un troyano. Juraj Malcho en su artículo titulado "Is there a lawyer in the lab" discute y explica la temática relacionada con la delgada barrera que diferencia una aplicación legítima de una que no lo es.

Como puede apreciarse, el tema no pasa por discernir entre blanco y negro sino de poder diferenciar de forma correcta, todas las tonalidades de grises existentes para darle a cada una, el lugar y utilización que le corresponde.

Debido a todo lo anteriormente mencionado y considerando que son los usuarios quienes en última instancia pueden decidir si las funcionalidades de una aplicación potencialmente indeseable y peligrosa superan los riesgos asociados a esta categoría de programas, las soluciones de ESET permiten activar o desactivar por separado, ambas opciones.