Resumen de la solución

Protección frente a los programas potencialmente no deseados

En el **informe de McAfee® Labs sobre amenazas de febrero de 2015** se analizan en profundidad los programas potencialmente no deseados (PUP). Pueden considerarse PUP las aplicaciones que los usuarios encuentran útiles, pero que sin embargo ocultan un riesgo tangible. Por lo general estas aplicaciones no informan a los usuarios de estos riesgos. A diferencia de los troyanos, virus, rootkits y otras formas de malware, el objetivo de los PUP no suele ser obtener las credenciales del usuario (para redes sociales o banca electrónica, por ejemplo) ni modificar los archivos del sistema para provocar daños. Los PUP podrían ubicarse en una "zona gris" en la clasificación, ya que al mismo tiempo que son de utilidad para el usuario, también conllevan un riesgo. Normalmente son difíciles de detectar y clasificar.

Estos son algunos de los comportamientos habituales de los PUP:

- Modifican sin autorización la configuración del sistema, como los ajustes del navegador.
- Ocultan un programa no solicitado dentro de una aplicación legítima.
- Recopilan de forma furtiva información del usuario, como sus hábitos de navegación y la configuración de su sistema.
- Instalan aplicaciones sin que el usuario lo perciba.
- Dificultan su desinstalación.
- Se distribuyen con publicidad confusa o engañosa.

Los PUP pueden adoptar diversas formas:

- **Adware**: distribuye publicidad, principalmente a través de los navegadores.
- **Descifrador/revelador de contraseñas**: muestra la contraseña oculta de una aplicación.
- **Herramienta de administración remota**: controla las actividades de los usuarios en el equipo en el que se ha instalado o permite el control remoto del sistema sin el conocimiento ni el consentimiento del usuario.
- **Keygen (o generador de claves)**: genera claves de producto para aplicaciones legítimas.

intel Security

- **Secuestrador del navegador**: cambia la página de inicio, la página de búsqueda, la configuración del navegador, etc.
- **Herramientas de ataque**: aplicaciones independientes que pueden facilitar la intrusión en el sistema o la fuga de datos importantes.
- **Proxy**: redirige u oculta información relacionada con la dirección IP.
- **Herramientas de rastreo:** spyware o aplicaciones de registro de pulsaciones que graban las teclas que ha pulsado el usuario, registran sus comunicaciones personales, supervisan sus actividades online o capturan pantallas sin su conocimiento.

Aquí se indican las diferencias entre los PUP y otros tipos de malware, como troyanos, ransomware, redes de bots y virus:

Técnicas	Programas potencialmente no deseados	Otro malware: troyanos, virus, redes de bots
Método de instalación	Procedimiento de instalación de aplicaciones estándar, a veces con acuerdo de licencia. A menudo precisan la aceptación e interacción del usuario para instalarse completamente en el sistema.	Se instalan como programas independientes sin la interacción del usuario. Suelen funcionar como archivos independientes.
Paquetes	Vienen unidos a aplicaciones legítimas y se instalan de manera desapercibida para el usuario, junto a ellas.	Son archivos independientes con pocos componentes adicionales. No vienen en paquetes de instalación.
Desinstalación	A veces el paquete contiene un desinstalador, lo que permite su eliminación. El procedimiento de desinstalación suele ser difícil.	Los ejecutables aumentan la complejidad de la propia eliminación del malware, ya que se "enlazan" a otros procesos, controladores de procesos u otros vínculos complejos. Como no se trata de paquetes de instalación, no aparecen en el panel de control.
Comportamiento	Muestran publicidad no consentida y ventanas emergentes, ya sea encima o debajo del navegador. Modifican la configuración del navegador, recopilan datos de los usuarios y el sistema, o permiten el control remoto del sistema sin el conocimiento ni el consentimiento del usuario.	Roban los datos de identificación y bancarios del usuario, modifican archivos del sistema, inutilizan el sistema, solicitan un rescate, etc.
Capacidad para ocultarse	No suelen ocultar su conducta.	Pueden ocultar archivos, carpetas, entradas del registro y tráfico de la red.

Entre todas las categorías de PUP, el adware es el que ha captado más atención entre los proveedores de seguridad, no por sus molestos anuncios, sino por el abuso de confianza que supone. Gracias a la implementación de varias técnicas para garantizar su presencia permanente en los sistemas infectados, el adware es ahora más inteligente. A continuación se incluyen algunos de los métodos:

- Ejecución de procesos independientes en la memoria
- Archivos DLL de modelo de objetos componentes (COM) y no COM con funciones incorporadas expresamente para la aplicación
- Claves del registro para objetos auxiliares del navegador (BHO)
- Archivos DLL enlazados a procesos del sistema
- Extensiones y complementos en el navegador
- Servicios del sistema registrados
- Componentes de controladores de dispositivos que realizan funciones de control del dispositivo
- Controladores de filtro de bajo nivel
- Troyanos distribuidos como carga útil

Normalmente los PUP se propagan abusando de la confianza de usuarios inocentes, como se explica en el **informe de McAfee Labs sobre amenazas de noviembre de 2014**. Entre las técnicas de distribución de PUP más habituales figuran:

- Anexión encubierta a una aplicación legítima
- Ingeniería social
- Venta de "Me gusta" para Facebook
- Publicación de timos en Facebook
- Secuestro de Google AdSense
- Extensiones y complementos no consentidos en el navegador
- Instalación forzosa junto a aplicaciones legítimas

Cómo puede ayudarle Intel Security a protegerse frente a los PUP

McAfee Application Control

McAfee Application Control permite a su empresa controlar qué aplicaciones se pueden ejecutar en su entorno por medio de listas blancas dinámicas y directivas de implementación, tanto en los endpoints conectados como en los desconectados. De esta manera puede ayudarle a proteger su negocio de los PUP.

- **Listas blancas dinámicas**: permita que su organización administre de forma eficaz sus aplicaciones desarrollando de forma automática una lista blanca a medida que los sistemas se revisen con parches y se actualicen. McAfee Application Control no permite la ejecución de adware conocido y de esa forma reduce el riesgo ante los PUP.
- **Reputación de archivos**: la integración con **McAfee Global Threat Intelligence** (McAfee GTI) permite a McAfee Application Control consultar información en tiempo real sobre tipos de archivos conocidos, ya sean legítimos o maliciosos, y desconocidos para ayudar a crear listas blancas y mantener a su empresa al tanto de aplicaciones clasificadas como PUP.
- **Protección con conexión o sin ella**: implemente controles en los servidores, las máquinas virtuales, los endpoints y los dispositivos fijos, como los terminales punto de venta, tanto si están conectados como si no.

McAfee Web Gateway

Para distribuir PUP se utilizan métodos como la publicidad engañosa, las descargas inadvertidas y las URL maliciosas incrustadas en sitios web de confianza. **McAfee Web Gateway** es un producto robusto que mejorará significativamente la protección de su empresa frente a este tipo de amenazas.

- **McAfee Gateway Anti-Malware Engine**: el análisis de intenciones sin firmas filtra el contenido malicioso del tráfico de la Web en tiempo real. McAfee Gateway Anti-Malware Engine inspecciona los archivos e impide que los usuarios los puedan descargar si son maliciosos.
- **Integración con McAfee GTI**: el flujo de información sobre la reputación de archivos, la reputación de la Web y la categorización de los sitios web que proporciona McAfee GTI facilita la protección frente las últimas amenazas, ya que McAfee Web Gateway deniega los intentos de conexión a sitios web maliciosos o sitios web que hacen uso de redes de publicidad engañosa.

Resumen de la solución

McAfee Global Threat Intelligence

McAfee Global Threat Intelligence (McAfee GTI) es un servicio de información sobre amenazas integral, en tiempo real y basado en la nube, que permite a los productos de McAfee bloquear las ciberamenazas procedentes de todos los vectores: archivos, la Web, mensajes y redes. Ofrece protección de forma proactiva frente los PUP por medio de las funciones siguientes:

- **Inteligencia basada en la correlación de vectores**: recopila y correlaciona datos de todos los vectores de amenazas principales, incluidos archivos, Web, correo electrónico y redes, para detectar amenazas combinadas, como las redes de publicidad que distribuyen malware firmado.
- **Plataforma de información integral sobre amenazas**: reúne información sobre amenazas de millones de sensores de productos de McAfee desplegados por los clientes, como las soluciones para endpoints, la Web y el correo electrónico, los sistemas de prevención de intrusiones y los dispositivos de firewall.
- **Reputación de certificados**: consulte la información en tiempo real sobre certificados conocidos legítimos y maliciosos con el fin de proteger su empresa frente a amenazas, como el malware firmado, que se pueden distribuir por medio de redes de publicidad fraudulenta.
- **Security Connected**: integración con otros productos de seguridad de McAfee para ofrecer la información sobre amenazas más amplia, la correlación de datos más profunda y la integración de productos más completa disponibles actualmente, y garantizar así una sólida protección frente al adware.

McAfee SiteAdvisor® Enterprise

Mantenerse al día en la situación de evolución constante de las amenazas no es fácil, especialmente si se intenta proteger a los usuarios online frente a amenazas como los PUP sin imponerles estrictas directivas que estropeen su experiencia de navegación.

- **Identifique fácilmente amenazas tales como sitios web maliciosos que se hacen pasar por legítimos**: por medio de un intuitivo sistema de clasificación por colores, **McAfee SiteAdvisor Enterprise** proporciona un nivel adicional de protección en el escritorio. Esta aplicación deniega las conexiones a sitios web maliciosos conocidos e informa a los usuarios de estos peligros.
- **Seguridad mejorada con la tecnología de McAfee GTI**: McAfee GTI proporciona información sobre amenazas en tiempo real a McAfee SiteAdvisor Enterprise, que evalúa los sitios web basándose en los datos más actualizados.

McAfee Threat Intelligence Exchange

Es importante disponer de una plataforma inteligente que pueda adaptarse a medida que pasa el tiempo para responder a las necesidades de su entorno. **McAfee Threat Intelligence Exchange** reduce significativamente la exposición a este tipo de ataques gracias a la visibilidad de las amenazas inmediatas, como archivos o aplicaciones desconocidos que intentan ejecutarse en el entorno.

- **Información integral sobre amenazas**: combine fácilmente la información exhaustiva sobre amenazas que recibe de las fuentes de datos globales, como McAfee GTI o las aportaciones de terceros, con la información local procedente de los eventos en tiempo real y los datos históricos recibidos de endpoints, gateways y otros componentes de seguridad.
- **Prevención y corrección de ejecución**: McAfee Threat Intelligence Exchange puede intervenir para impedir la ejecución de aplicaciones desconocidas en el entorno. Si una aplicación cuya ejecución estaba autorizada se califica posteriormente como

maliciosa, McAfee Threat Intelligence Exchange puede desactivar en todo el entorno los procesos en ejecución asociados a dicha aplicación, gracias a sus potentes funciones de administración centralizada e implementación de directivas.

- **Reputación de certificados**: la integración con McAfee GTI protege a su empresa en tiempo real frente a los ataques que se basan en código malicioso firmado, para ello se consultan en tiempo real fuentes de información sobre certificados conocidos legítimos y maliciosos. McAfee Threat Intelligence Exchange puede proteger sus endpoints frente a certificados maliciosos por medio de directivas administradas de forma centralizada implementadas de manera que ofrezcan protección para los endpoints conectados y desconectados.

McAfee VirusScan® Enterprise

Con **McAfee VirusScan Enterprise** detectar y eliminar malware, incluido el adware, es muy fácil. McAfee VirusScan Enterprise emplea el galardonado motor de análisis de McAfee para proteger sus sistemas frente a virus, gusanos, rootkits, troyanos y otras amenazas avanzadas.

- **Protección proactiva contra ataques**: integra tecnología antimalware con prevención de intrusiones para proporcionar protección frente a los exploits que emplean desbordamiento del búfer aprovechando las vulnerabilidades de las aplicaciones.
- **Insuperable en detección y desinfección de malware**: protege frente a amenazas tales como rootkits y troyanos con análisis avanzado de comportamiento. Detiene el malware de raíz por medio de técnicas entre las que se incluyen el bloqueo de puertos, el bloqueo de nombres de archivo, el bloqueo de carpetas y directorios, el bloqueo del uso compartido de archivos, y el seguimiento y el bloqueo de infecciones.
- **Seguridad en tiempo real con integración en McAfee GTI**: protección frente a amenazas conocidas y desconocidas en todos los vectores de entrada —archivos, Web, correo electrónico y redes— con el respaldo de la plataforma de información sobre amenazas más exhaustiva del mercado.

Proteger su empresa frente a los PUP que pretenden burlar el modelo de confianza tradicional mediante un comportamiento sospechoso y no deseado puede ser difícil. Combinando las investigaciones de McAfee Labs, líder del sector, con la tecnología de Intel Security, puede ayudar a su empresa a protegerse de estos programas.

McAfee. Part of Intel Security.
Avenida de Bruselas n.º 22
Edificio Sauce
28108 Alcobendas
Madrid, España
Teléfono: +34 91 347 8500
www.intelsecurity.com