Resumen de la solución

Protección contra exploits de Adobe Flash

La plataforma multimedia y de software Adobe Flash es una forma popular de distribuir contenido web enriquecido, como juegos, sitios web, aplicaciones, etc. Desafortunadamente, su popularidad la convierte en un objetivo atractivo para los ciberdelincuentes, que aprovechan sin miramientos las nuevas vulnerabilidades sin parche para comprometer a usuarios desprevenidos.

Prevalencia de los exploits de Adobe Flash

Los exploits de Flash se analizan en profundidad en el ***Informe de McAfee Labs sobre amenazas: Mayo de 2015***. Los exploits de Flash empezaron a aumentar drásticamente a principios del primer trimestre de 2014. Las vulnerabilidades de Flash se encuentran ahora entre los principales objetivos de los creadores de exploits. McAfee Labs cree que esto se debe a varios factores: el aumento constante del número de vulnerabilidades de Flash; demora por parte de los usuarios en la aplicación de los parches de software para esas vulnerabilidades de Flash; nuevos y creativos métodos de aprovechar esas vulnerabilidades; un pronunciado aumento del número de dispositivos móviles que pueden reproducir archivos .swf de Flash; y la dificultad de detectar exploits de Flash.

Entre los kits que distribuyen exploits de Flash, Angler se ha convertido en el más popular. Este potente kit, analizado en profundidad en el ***Informe de McAfee Labs sobre amenazas: Febrero de 2015*** es un toolkit comercial, fácil de utilizar que puede distribuir una gran variedad de cargas útiles a través del aprovechamiento de vulnerabilidades.

Cómo protegerse contra los exploits de Flash

A continuación incluimos algunas buenas prácticas y procedimientos para protegerse contra los exploits de Flash:

- Active las actualizaciones automáticas de los sistemas operativos o descargue con regularidad las actualizaciones para que estos cuenten con los parches necesarios para estar protegidos frente a las vulnerabilidades conocidas.
- Configure software antivirus para bloquear los adjuntos que contengan la extensión .swf.
- Establezca la configuración de seguridad del navegador como mínimo al nivel medio.
- Utilice un complemento del navegador para bloquear la ejecución de secuencias de comandos y elementos iframe.

intel Security

- No instale complementos de navegador desconocidos.
- Preste especial atención al abrir adjuntos, sobre todo si tienen la extensión .swf.
- No abra nunca mensajes de correo electrónico no deseados ni archivos adjuntos que no espere recibir, incluso aunque provengan de personas que conoce.
- Tenga cuidado con el phishing basado en spam. No haga clic en enlaces de mensajes instantáneos o de correo electrónico.
- Escriba las URL o cópielas en la barra de direcciones del navegador y compruebe la dirección en lugar de hacer clic en anuncios web.
- No haga clic en películas Flash en sitios web que no sean de confianza.

Cómo puede ayudarle Intel Security a protegerse frente a los exploits de Flash

McAfee Web Gateway

Para distribuir los ataques que aprovechan exploits de Flash 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. La emulación y los análisis de comportamiento ofrecen protección de forma proactiva frente a los ataques selectivos y de tipo zero-day. McAfee Gateway Anti-Malware Engine inspecciona los archivos e impide que los usuarios los puedan descargar si son maliciosos.
- **Integración con McAfee Global Threat Intelligence (McAfee GTI):** la información en tiempo real sobre la reputación de archivos, la reputación de la Web y la categorización de la Web de McAfee GTI ofrecen 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.

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. Para combatir la creciente tendencia de exploits de Flash es fundamental garantizar que su empresa está protegida contra las aplicaciones vulnerables.

- **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 reduce su exposición a exploits de Flash gracias a que garantiza que no se ejecutan en su entorno versiones de Flash sin parche.
- **Reputación de archivos:** la integración con McAfee GTI permite a McAfee Application Control consultar información en tiempo real sobre tipos de archivos legítimos conocidos, maliciosos y desconocidos para asegurarse de que su empresa esté al tanto de vulnerabilidades o ataques desde aplicaciones que pueden haber sido alteradas.
- **Protección con conexión o sin ella:** implemente controles en los servidores, las máquinas virtuales, los endpoints y los dispositivos de función fija, como los terminales punto de venta, tanto conectados como no conectados.

Resumen de la solución

McAfee Vulnerability Manager
McAfee Vulnerability Manager ayuda a su empresa a comprender las consecuencias de disponer de versiones antiguas de Flash en su entorno y adopta las medidas necesarias para reducir eficazmente esa exposición.

- **Análisis completo de vulnerabilidades:** McAfee Vulnerability Manager es un producto independiente y altamente escalable de descubrimiento de hosts, administración de activos, evaluación de vulnerabilidades y generación de informes en cualquier dispositivo conectado a la red. McAfee Vulnerability Manager puede evaluar la exposición de su entorno a exploits de Flash mediante el análisis de los sistemas que ejecutan versiones antiguas de Flash.
- **Generación de informes y medidas correctivas de gran flexibilidad:** McAfee Vulnerability Manager y **McAfee Asset Manager** funcionan en colaboración para proporcionar una supervisión y una administración automatizadas de los análisis, las medidas correctivas, la implementación y la generación de informes. De esta manera, podrá evitar laboriosos simulacros de emergencia y procesos ad hoc, eliminar errores y proteger un mayor número de sistemas de forma más eficaz.
- **Información sobre su exposición:** McAfee Asset Manager permite a su empresa saber qué sistemas son vulnerables a exploits de Flash mediante la correlación de análisis de vulnerabilidades con análisis de descubrimiento de hosts. La identificación en tiempo real de los sistemas que están ejecutando versiones vulnerables de Flash permite reducir el tiempo para saber si se corren riesgos, y disponer de más tiempo para aplicar medidas correctivas.

McAfee Threat Intelligence Exchange
Es importante disponer de una plataforma inteligente que pueda adaptarse 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 aprovechan vulnerabilidades de Flash en el entorno de su empresa.

- **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 de ejecución y medidas correctivas:** McAfee Threat Intelligence Exchange puede intervenir e impedir que se ejecuten 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.
- **Visibilidad:** McAfee Threat Intelligence Exchange puede realizar un seguimiento de todos los archivos ejecutables empaquetados y de su ejecución inicial en el entorno, así como de todos los cambios que se produzcan a partir de ahí. Gracias a este grado de visibilidad de las operaciones de una aplicación o un proceso desde la instalación inicial hasta el momento actual, la respuesta y la resolución pueden ser más rápidas.
- **Indicadores de peligro (del inglés, IoC):** importe hashes de archivos maliciosos conocidos para que McAfee Threat Intelligence Exchange inmunice su entorno contra estos archivos maliciosos conocidos mediante la implementación de las directivas adecuadas. Si se activa alguno de los IoC en el entorno, McAfee Threat Intelligence Exchange puede eliminar todos los procesos y las aplicaciones asociados.

McAfee VirusScan Enterprise

Detectar y eliminar del malware que aprovecha vulnerabilidades de Flash para infiltrarse en su entorno es muy sencillo con **McAfee VirusScan® Enterprise**. McAfee VirusScan Enterprise emplea el galardonado motor de análisis de McAfee para proteger sus archivos 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:** protege contra 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.

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 contra exploits de Flash y otros por medio de las funciones siguientes:

- **Inteligencia basada en la correlación de vectores:** recopila y correlaciona datos de todos los vectores de amenazas principales (archivos, Web, correo electrónico y redes), para detectar amenazas combinadas.
- **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.
- **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 exploits de Flash.

McAfee VirusScan Mobile

McAfee VirusScan Mobile es un sistema antimalware que analiza y limpia los datos de los dispositivos móviles, evitando que se produzcan daños por virus, troyanos y otros programas maliciosos. McAfee VirusScan Mobile protege sus dispositivos móviles en los puntos de mayor exposición, como son los mensajes de correo electrónico entrantes y salientes, los mensajes de texto, los archivos adjuntos del correo electrónico y las descargas de Internet.

- Detección de amenazas en tiempo real: bloquea el malware del correo electrónico, los mensajes de texto y los archivos adjuntos sin que se produzcan demoras apreciables. McAfee VirusScan Mobile busca una amplia gama de amenazas maliciosas en menos de 200 milisegundos, lo que representa una protección automática y completa para los smartphones.

La creciente prevalencia de las vulnerabilidades de Flash que aprovechan los agresores no muestra signo alguno de remitir. La tecnología de seguridad de Intel Security puede ayudar a su empresa a protegerse de forma proactiva frente a amenazas que buscan aprovecharse de esas vulnerabilidades.

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