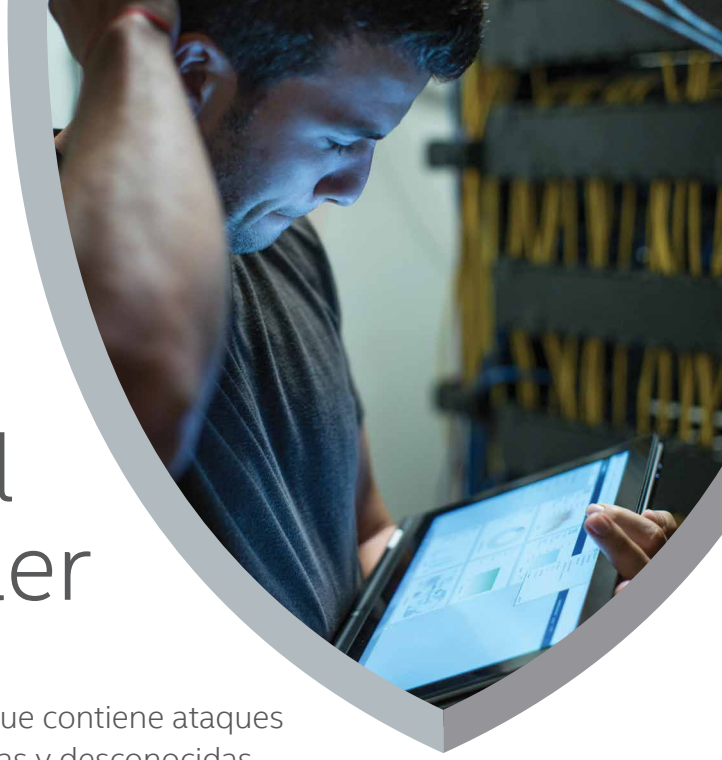
Resumen de la solución



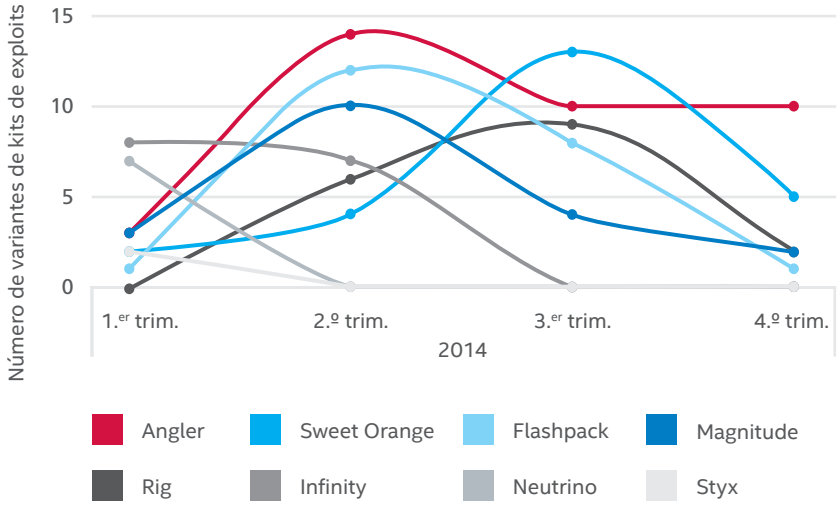
Luchando contra el kit de exploits Angler

Un kit de exploits es un paquete de software comercial que contiene ataques fáciles de usar que aprovechan vulnerabilidades conocidas y desconocidas (zero-day). Estos toolkits sacan partido de las vulnerabilidades del cliente y normalmente se centran en el navegador web y las aplicaciones a las que se puede acceder a través del mismo. Los kits de exploits también pueden conocer los niveles de infección y cuentan con sólidas funciones de control.

¿Qué es el kit de exploits Angler?

En el informe de **McAfee® sobre amenazas de febrero de 2015** se analiza el kit de exploits Angler en profundidad. En la segunda mitad de 2014, la presencia de Angler se hizo más notoria y predominante debido a sus funciones, como la capacidad de infectar sin necesidad de archivos (inyección en memoria), la detección de productos de seguridad y máquinas virtuales, y su capacidad de distribuir una amplia variedad de cargas útiles, incluidos troyanos bancarios, rootkits, ransomware, CryptoLocker y troyanos de puerta trasera. Además, Angler no exige grandes conocimientos técnicos para utilizarse de forma efectiva y gracias a su disponibilidad en los mercados virtuales clandestinos experimenta un gran crecimiento.

Variantes entre los kits de exploits en 2014



Fuente: McAfee Labs, 2015

intel Security

Resumen de la solución

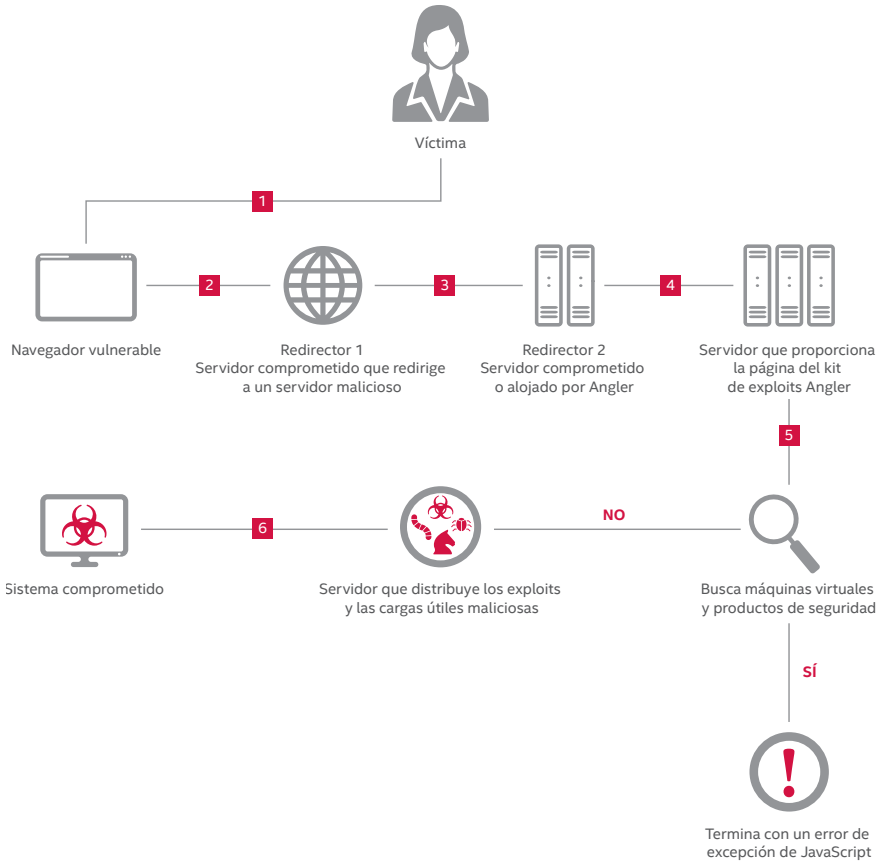
Angler cambia con frecuencia de patrones y cargas útiles para evitar ser detectado por los productos de seguridad. Para ello, lleva a cabo diversas operaciones de evasión:

- Utiliza dos niveles de redirectores antes de acceder a la página de destino.
- Los servidores web comprometidos que alojan la página de destino solo se pueden visitar una vez desde una dirección IP. Los agresores controlan los hosts de forma claramente activa.
- Es capaz de detectar la presencia de máquinas virtuales y productos de seguridad en el sistema.
- Realiza llamadas completamente inútiles, con el fin de dificultar la ingeniería inversa.
- Cifra todas las cargas en el momento de la descarga y las descifra en la máquina víctima del ataque.
- Utiliza infecciones sin necesidad de archivos (se implementan directamente en la memoria).

El kit de exploits Angler lleva a cabo varios pasos para conseguir infectar los sistemas:

- La víctima accede al servidor web comprometido a través de un navegador vulnerable.
- El servidor web comprometido redirige la conexión a un servidor intermedio.
- El servidor intermedio redirige a su vez la conexión a un servidor web malicioso que aloja la página de destino del kit de exploits.
- La página de destino comprueba la presencia de complementos vulnerables (Java, Flash y Silverlight) y la información relacionada con las versiones.
- Cuando detecta un navegador o complemento vulnerable, el kit de exploits distribuye la carga correspondiente e infecta la máquina.

Cadena de infección del kit de exploits Angler



Protección frente al kit de exploits Angler

A continuación, recomendamos varias formas de proteger los sistemas frente al kit de exploits Angler:

- Utilice un proveedor de servicios de Internet que tenga en cuenta la importancia de la seguridad y que implemente procedimientos eficaces antispam y antiphishing.
- 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. Instale los parches de los desarrolladores de software de terceros en cuanto se publiquen. Un equipo con todos los parches instalados y protegido mediante un firewall es la mejor defensa frente a ataques de spyware y troyanos.
- Tenga mucho cuidado cuando abra archivos adjuntos. Configure el software antivirus para que analice automáticamente los archivos adjuntos de todos los mensajes instantáneos y de correo electrónico. Asegúrese de que los programas de correo electrónico no abran automáticamente los archivos adjuntos ni procesen automáticamente los gráficos, así como de que el panel de vista previa esté desactivado. No abra nunca mensajes de correo electrónico no deseados ni archivos adjuntos que no espere recibir, incluso si provienen de personas que conoce.
- Tenga cuidado con el phishing basado en spam. No haga clic en enlaces de mensajes instantáneos o de correo electrónico.
- Utilice un complemento del navegador para bloquear la ejecución de secuencias de comandos y elementos iframe.

Cómo puede ayudarle Intel Security a protegerse frente al kit de exploits Angler

McAfee Web Gateway

Para distribuir el kit de exploits Angler 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 firma 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 VirusScan® Enterprise

Con **McAfee VirusScan Enterprise** detectar y eliminar malware como el que distribuye Angler es muy fácil. 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**: ofrece protección frente a amenazas como los rootkits y los troyanos con un análisis de comportamientos avanzado. 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 por medio de la integración con McAfee GTI**: ofrece protección frente a amenazas conocidas y emergentes en todos los vectores de entrada (archivos, Internet, correo electrónico y redes) con el respaldo de la plataforma de información sobre amenazas más completa del mercado.

McAfee Advanced Threat Defense

McAfee Advanced Threat Defense es una solución de detección de malware multicapa que combina varios motores de inspección. Al utilizar varios motores de inspección que aplican un análisis basado en firmas y en la reputación, una emulación en tiempo real, un análisis del código completamente estático y entornos aislados dinámicos, McAfee Advanced Threat Defense ofrece protección frente a los kits de exploits más frecuentes, como Angler y el malware que este despliega.

- **Detección basada en firmas**: detecta virus, gusanos, spyware, bots, troyanos, ataques por desbordamiento del búfer y ataques combinados. McAfee Labs ha creado y mantiene la completa base de conocimientos de esta solución, que actualmente incluye más de 150 millones de firmas, incluidas las de Angler y sus variantes.
- **Detección basada en la reputación**: consulta la reputación de los archivos utilizando la red de McAfee GTI para detectar las amenazas de nueva aparición.
- **Análisis estático en tiempo real y emulación**: proporciona emulación y análisis estático en tiempo real para localizar rápidamente las amenazas de malware y de tipo zero-day no identificadas, mediante técnicas basadas en firmas o en la reputación.
- **Análisis del código completamente estático**: revierte la ingeniería del código de los archivos con el fin de evaluar todos los atributos y conjuntos de instrucciones, y analizar íntegramente el código fuente sin ejecutarlo. Sus completas funciones de descompresión abren todo tipo de archivos empaquetados y comprimidos con el fin de facilitar su análisis total y la clasificación del malware, de manera que su empresa pueda entender la amenaza que supone dicho malware.
- **Análisis de aplicaciones en entornos aislados**: ejecuta el código de los archivos en un entorno virtual de tiempo de ejecución y observa cómo se comporta. Los entornos virtuales se pueden configurar como los entornos de host de su empresa, y admiten imágenes personalizadas de los sistemas operativos Windows 7 (de 32 y 64 bits), Windows XP, Windows Server 2003, Windows Server 2008 (de 64 bits) y Android.

McAfee Network Security Platform

McAfee Network Security Platform se ha diseñado para llevar a cabo inspecciones exhaustivas del tráfico de red. McAfee Network Security Platform utiliza una combinación de técnicas de inspección avanzadas, como el análisis de todos los protocolos, la reputación de amenazas, el análisis de comportamientos y el análisis de malware avanzado, para detectar y prevenir tanto los ataques de red conocidos como los desconocidos (zero-day).

- **Protección antimalware completa**: combina la información de reputación de archivos de McAfee GTI, el análisis de archivos en profundidad con inspección de JavaScript y el análisis de malware avanzado para detectar y combatir las amenazas de tipo zero-day, el malware personalizado y otros ataques que pueden pasar desapercibidos.
- **Emplea técnicas de inspección avanzadas**: entre ellas, se incluyen el análisis de todos los protocolos, la reputación de amenazas y el análisis de comportamientos para detectar y prevenir tanto los ataques de red conocidos como los desconocidos (zero-day).

- **Integración con McAfee GTI**: combina la reputación de archivos en tiempo real, la reputación de direcciones IP y la información de geolocalización con datos contextuales completos sobre usuarios, dispositivos y aplicaciones, con el fin de responder de manera rápida y precisa a los ataques que se propagan por la red.
- **Security Connected**: la integración práctica con McAfee Advanced Threat Defense permite que McAfee Network Security Platform pueda enviar los archivos sospechosos detectados en el tráfico supervisado a McAfee Advanced Threat Defense, así como denegarlos o autorizarlos en función de los resultados de McAfee Advanced Threat Defense.

McAfee Threat Intelligence Exchange

Es importante contar con una plataforma de información que sea capaz de adaptarse con el tiempo a las necesidades de su entorno. **McAfee Threat Intelligence Exchange** reduce de forma significativa la exposición a este tipo de ataques gracias a la visibilidad que ofrece de las amenazas inmediatas, como las aplicaciones y los archivos desconocidos que se ejecutan en el entorno.

- **Información integral sobre amenazas**: combine fácilmente la información exhaustiva sobre amenazas que recibe de las fuentes de datos globales, como aportaciones de McAfee GTI o de terceros, con la información local sobre amenazas 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 se permite la ejecución de una aplicación y posteriormente se confirma que es maliciosa, McAfee Threat Intelligence Exchange puede desactivar los procesos de ejecución asociados a dicha aplicación en el entorno gracias a sus sólidas 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 (en 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.

La creciente prevalencia de kits de exploits fáciles de usar, como Angler, es una clara muestra de que el panorama de las amenazas cambia constantemente. La tecnología de Intel Security puede contribuir a que su empresa se proteja de forma proactiva frente a amenazas como el kit de exploits Angler tanto en endpoints como en redes.

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