Protección frente al malware basado en scripts

Los creadores de malware han dificultado su detección con técnicas como el polimorfismo, la implantación de órganos de vigilancia, la revocación de permisos y otros métodos.

Durante esta década, también hemos visto que los agresores aprovechan funciones como el Instrumental de administración de Microsoft Windows (WMI) y Windows PowerShell para atacar endpoints sin guardar ningún archivo binario en disco, lo que les garantiza que el ataque sea difícil de localizar, ya que el código malicioso se puede implantar directamente en el registro de un host comprometido.

Las infecciones basadas en scripts llevan años produciéndose. Aunque se denominaban "sin archivos", las familias de malware depositaban en el disco un pequeño archivo binario durante el ataque inicial antes de desplazarse a la memoria principal del sistema.

Sin embargo, las últimas técnicas de evasión utilizadas por el malware basado en scripts no dejan rastro en el disco, lo que complica su detección, que por lo general depende de la búsqueda de archivos estáticos. Lea nuestro exhaustivo análisis del malware basado en macros en el *informe de McAfee Labs sobre amenazas de septiembre de 2017*.

Los tres tipos de malware basado en scripts más comunes son:

- **Residente en memoria:** este tipo de malware utiliza el espacio en memoria de un archivo de Windows legítimo. Carga el código en ese espacio y permanece latente hasta que se reactiva o se accede a él. Aunque la ejecución tiene lugar dentro del espacio legítimo del archivo en la memoria, la inicia o reinicia un archivo físico inactivo.
- **Rootkits:** en este caso el malware oculta su presencia detrás de una interfaz de programación de aplicaciones (API) de nivel de usuario o kernel. Hay un archivo presente en el disco, pero está en modo oculto.
- **Registro de Windows:** algunos tipos de malware basado en scripts avanzado residen en el Registro de Windows. En el pasado, los creadores del malware se aprovechaban de funciones como la caché de vistas en miniatura de Windows, que almacena imágenes para las miniaturas que se muestran en el Explorador. La caché de vistas en miniatura actúa como mecanismo de persistencia para el ataque. Este tipo de malware sigue necesitando entrar en el sistema de la víctima a través de un archivo binario estático. La mayoría emplea el correo electrónico como vector de entrada en el sistema. En cuanto el usuario hace clic en el archivo adjunto, el malware escribe la carga útil completa, una vez cifrada, en un subárbol del Registro de Windows. Después desaparece del sistema autodestruyéndose.

En la actualidad, los creadores de malware han diseñado ingeniosamente malware basado en scripts para ejecutar ataques desde el Registro de Windows sin utilizar ningún archivo ni dejar ningún rastro en el sistema de archivos. Aunque el entorno que debe llevar a cabo estos ataques se prepara ejecutando código de un archivo, este se autoelimina una vez que el sistema está listo para la operación maliciosa.

Recomendaciones y procedimientos para protegerse frente al malware basado en scripts

Las últimas mejores prácticas de ciberdefensa de McAfee recomiendan la adopción de determinadas estrategias de mitigación de amenazas generales para redes y endpoints:

- La mejor forma de proteger su sistema frente a las infecciones de malware basado en scripts es frenarlas antes de que ocurran. La prevención es la clave. El factor más importante a la hora de evitar cualquier tipo de ataque de malware a un sistema es el usuario. Los usuarios deben ser conscientes de los riesgos que implican las descargas e instalaciones de aplicaciones que no conocen o que no son de confianza. Además, deben saber que se puede descargar malware mientras se navega.
- Es importante aplicar las actualizaciones y parches de seguridad para las aplicaciones y el sistema operativo.
- Tenga siempre actualizados los navegadores web y los complementos, así como el antimalware en los endpoints, y los gateways de la red con las últimas versiones.

- No utilice nunca sistemas que no hayan sido distribuidos y certificados por el grupo de seguridad de TI de la empresa. El malware basado en scripts se propaga fácilmente por activos no protegidos conectados a la red de la empresa.
- En los casos en los que los usuarios tienen privilegios de administrador para instalar aplicaciones por sí solos, se les debe informar de que únicamente deben instalar aplicaciones con firmas de confianza procedentes de proveedores conocidos. Es muy habitual que aplicaciones que se ofrecen online supuestamente "inofensivas" tengan incrustados rootkits y otros tipos de malware basado en scripts.
- Evite descargas de aplicaciones de fuentes distintas de la Web. Son muy elevadas las probabilidades de descargar malware de grupos Usenet, canales IRC, clientes de mensajería instantánea o redes P2P. Los enlaces a sitios web vistos en IRC y mensajes instantáneos suelen llevar a descargas infectadas.
- Ponga en práctica programas educativos para prevenir los ataques de phishing. El malware se suele distribuir a través de ataques de correo electrónico selectivos.
- Utilice la inteligencia sobre amenazas en combinación con la tecnología antimalware. Esta combinación le ayudará a mejorar el tiempo de detección para las amenazas de malware nuevas y para las conocidas.

Cómo puede ayudarle McAfee a protegerse contra el malware basado en scripts

La detección directa del malware basado en scripts que no utiliza archivos binarios iniciales puede ser complicada y a menudo depende de la investigación de las organizaciones de seguridad. Sin embargo, para detenerlo es fundamental asegurar la implantación de los controles adecuados que impidan a los agresores todo punto de entrada.

McAfee Endpoint Security

McAfee Endpoint Security (ENS) proporciona una plataforma de seguridad colaborativa para reducir la complejidad de los entornos de seguridad de los endpoints, y ofrece visibilidad de las amenazas avanzadas, como el malware basado en scripts, que agiliza la detección y respuesta. Su arquitectura ampliable proporciona un marco a los equipos de seguridad, enfrentados a la dificultad que implica gestionar varias soluciones, que les permite ver, responder y administrar el ciclo de defensa de amenazas de manera más fácil.

McAfee ENS presenta una serie de nuevas tecnologías y mejoras:

- **Real Protect.** Aplica técnicas de aprendizaje automático para identificar código malicioso en función de su aspecto, de lo que podría hacer (análisis antes de la ejecución) y de lo que hace (análisis dinámico de comportamientos) —todo ello sin firmas. Real Protect es parte de una estrategia de defensa contra el malware basado en scripts.

- **Contención dinámica de aplicaciones.** Incluye la capacidad para contener una única instancia de un proceso.
- **Integración con McAfee Client Proxy.** McAfee Endpoint Security puede combinarse con seguridad del gateway de la Web multicapa, que proporciona protección integral dondequiera que viaje el usuario, eliminando la protección el vacío de protección fuera de la red al conectar los endpoints al servicio en la nube Web Gateway.
- **Módulo Firewall.** La siguiente capa de protección que garantiza una estrategia de seguridad proactiva se utiliza para bloquear las comunicaciones entre su ordenador y los servidores controlados por los ciberdelincuentes.
- **Módulo de prevención de amenazas.** Los análisis bajo demanda incluyen ahora una opción de análisis del Registro, que resulta muy útil en la protección frente a malware basado en scripts. Los administradores pueden crear reglas de protección de acceso, que ahora incluyen servicios de Windows. La prevención de exploits de aplicaciones personalizada está disponible junto a firmas para el sistema de prevención de intrusiones (IPS) facilitadas por McAfee. Por último, se ha añadido la protección de aplicaciones de Windows a las reglas de prevención de exploits.

McAfee Advanced Threat Defense

McAfee Advanced Threat Defense (ATD) es un producto de detección de malware multicapa que combina varios motores de inspección. Al utilizar varios motores de inspección que aplican análisis basado en firmas y reputación, emulación en tiempo real, análisis del código completamente estático y entornos aislados dinámicos, McAfee ATD ofrece protección frente al malware que deposita un archivo binario en el sistema de la víctima durante el inicio del ataque.

- **Detecciones basadas en firmas:** detecta virus, gusanos, spyware, bots, troyanos, ataques por desbordamiento del búfer y ataques combinados. Su exhaustiva base de conocimientos ha sido creada por McAfee Labs, que también se ocupa de su mantenimiento.
- **Detecciones basadas en reputación:** consulta la reputación de los archivos utilizando McAfee Global Threat Intelligence (GTI) para detectar las amenazas de nueva aparición.
- **Análisis y emulación estáticos en tiempo real:** 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 completo del código estático:** revierte la ingeniería del código de los archivos con el fin de evaluar todos sus atributos y conjuntos de instrucciones, y analiza íntegramente el código fuente sin ejecutarlo. Sus completas funciones de descompresión abren todo tipo de archivos empaquetados y comprimidos para facilitar su análisis total y la clasificación del malware, de manera que su empresa pueda entender la amenaza que supone dicho malware.
- **Análisis dinámico en entornos aislados:** con los archivos cuya seguridad no puede determinarse mediante los motores de inspección mencionados, McAfee ATD puede ejecutar el código en un entorno virtual de tiempo de ejecución y observar cómo se comporta. Los entornos virtuales pueden configurarse como los entornos de host.

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 del entorno. McAfee Threat Intelligence Exchange (TIE) reduce significativamente la exposición a los ataques del malware sin archivos 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 de ejecución y medidas correctivas:** McAfee TIE puede intervenir para impedir la ejecución de aplicaciones desconocidas en el entorno. Si se descubre que una aplicación cuya ejecución estaba autorizada es maliciosa, McAfee TIE 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 TIE 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:** importe hashes de archivos maliciosos conocidos e inmunice su entorno contra estos archivos mediante la implementación de las directivas adecuadas. Si se activa alguno de los indicadores en el entorno, McAfee TIE puede eliminar todos los procesos y las aplicaciones asociados a él.

McAfee Web Gateway

Los principales métodos para distribuir malware basado en scripts son las descargas desapercibidas y las URL maliciosas incorporadas en mensajes de correo electrónico de phishing. McAfee Web Gateway (MWG) es un producto robusto que mejorará significativamente la protección de su empresa frente a este tipo de amenazas.

- **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 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 MWG deniega los intentos de conexión a sitios web maliciosos o sitios web que hacen uso de redes de publicidad engañosa. Además de estos productos de McAfee, recomendamos otras dos clases de tecnologías de seguridad.
  - **Seguridad del gateway de correo electrónico:** la mayor parte del malware basado en scripts entra en el sistema a través de los adjuntos a mensajes de correo electrónico, por lo que cualquier defensa sólida frente a este tipo de ataque debe contar con un producto robusto de seguridad del gateway de correo electrónico.
  - **Firewall:** en todo sistema de seguridad es básica la tecnología del firewall. Un firewall puede detectar muchas amenazas en el perímetro antes de que entren en la red de confianza. Teniendo en cuenta que el malware sin archivos entra en el sistema mediante archivos binarios estáticos, muchos de estos ataques pueden detenerse antes de que entren en los sistemas del interior de la red de confianza.

McAfee
Together is power.

Avenida de Bruselas nº 22
Edificio Sauce
28108 Alcobendas, Madrid, España
+34 91 347 85 00
www.mcafee.com/es