Solution Brief

Protección frente al malware sin archivos

En el ***Informe sobre amenazas de McAfee® Labs de noviembre de 2015***, analizamos en profundidad el malware sin archivos y los detalles técnicos de Kovter, que elude la detección reduciendo o eliminando el almacenamiento de archivos binarios en el disco y ocultando su código en el Registro del host afectado. Los creadores de este malware han dificultado su detección con técnicas como el polimorfismo, la implantación de órganos de vigilancia, la revocación de permisos y otros métodos. En 2015 también hemos visto que los agresores aprovechan funciones como el Instrumental de administración de Microsoft Windows (WMI - Windows Management Instrumentation) y Windows PowerShell para atacar endpoints sin guardar ningún archivo binario en disco, lo que les garantiza que el ataque sea difícil de localizar.

Las infecciones sin archivos basadas en la memoria se conocen en el sector de la seguridad desde hace muchos años. 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 host afectado. Sin embargo, las nuevas técnicas de evasión del malware sin archivos —por ejemplo, Kovter, Powelike y XswKit— no dejan rastro en el disco, por lo que su detección, que en general se basa precisamente en buscar archivos estáticos en el disco, resulta más difícil.

Los tres tipos de malware sin archivos 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. Por consiguiente, este tipo de malware no funciona del todo sin archivos.
- **Rootkits**: en este caso el malware sin archivos 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 nuevos de malware sin archivos residen en el Registro del sistema operativo Windows. Los creadores del malware se aprovechan de funciones como la caché de vistas en miniatura de Windows, que almacena imágenes para las miniaturas que se muestran en el Explorador de Windows. La caché de vistas en miniatura actúa como mecanismo de persistencia para el malware. 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 vía de entrada. 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.

intel Security

Los creadores de malware sin archivos han diseñado ingeniosamente las familias Kovter, Powelike y XswKit 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 autodestruye una vez que el sistema está listo para la operación maliciosa.

Cómo puede ayudarle Intel Security a protegerse frente al malware sin archivos

La detección directa del malware 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 Advanced Threat Defense

McAfee Advanced Threat Defense 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 Advanced Threat Defense ofrece protección frente al malware que deposita un archivo binario en el sistema de la víctima durante el inicio del ataque.

- **Detección basada 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.
- **Detección basada en la reputación**: consulta la reputación de los archivos utilizando McAfee Global Threat Intelligence (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 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 de aplicaciones en entornos aislados**: con los archivos cuya seguridad no puede determinarse mediante los motores de inspección mencionados antes, McAfee Advanced Threat Defense 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 Advanced Threat Defense admite imágenes personalizadas de los sistemas operativos (SO) Windows XP SP2 y SP3, Windows 7 (de 32 y 64 bits), Windows 8 (de 32 y 64 bits), Windows Server 2003, Windows Server 2008 (de 64 bits) y Android.

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** 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 Threat Intelligence Exchange 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 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**: 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 Threat Intelligence Exchange puede eliminar todos los procesos y las aplicaciones asociados a él.

McAfee Web Gateway

Los principales métodos para distribuir malware sin archivos son las descargas secundarias y las URL maliciosas incorporadas en mensajes de correo electrónico de phishing. **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 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.

Además de estos productos de Intel Security, recomendamos otras dos clases de tecnologías de seguridad.

- **Seguridad del gateway de correo electrónico**: la mayor parte del malware sin archivos 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. Part of Intel Security.
Avenida de Bruselas n.º 22
Edificio Sauce
28108 Alcobendas
Madrid, España
Teléfono: +34 91 347 8500
www.intelsecurity.com