Resumen de la solución

Protección frente a amenazas esteganográficas

La esteganografía —arte y ciencia de la ocultación de información secreta— también puede emplearse para ocultar información en el mundo digital. Un mensaje puede esconderse en el interior de imágenes, pistas de audio, videoclips o archivos de texto. Puede utilizarse para fines legítimos, pero con frecuencia la esteganografía es utilizada por el malware.

Para evitar la detección, algunos tipos de malware emplean esteganografía digital para ocultar su contenido malicioso dentro de un archivo de portada aparentemente inocente. Esta técnica de evasión aprovecha el hecho de que la mayoría de las firmas antimalware detectan el contenido malicioso en el archivo de configuración del malware. Con la esteganografía, el archivo de configuración se incrusta en el archivo de portada. Además, es posible que el archivo de esteganografía resultante se descifre en la memoria principal, reduciendo aún más la posibilidad de detección. Por último, resulta extremadamente difícil detectar la presencia de información oculta, como un archivo de configuración, una actualización de archivos binarios o un comando de un bot, en el interior de los archivos de esteganografía. Desafortunadamente, el uso de la esteganografía en ciberataques es fácil de implementar y difícil de detectar.

Políticas y procedimientos recomendados para protegerse frente a los ataques que emplean esteganografía

McAfee recomienda a las organizaciones que tomen las siguientes medidas para protegerse frente a las amenazas que emplean esteganografía.

- **Refuerce los mecanismos de entrega y distribución de software para proteger frente a las amenazas internas.** Es siempre recomendable tener un repositorio centralizado de aplicaciones empresariales de confianza del que los usuarios pueden descargar el software aprobado, evitando de esta forma los riesgos de permitir a los usuarios descargar software de fuentes desconocidas que puede contener código esteganográfico.

McAfee
Together is power.

- **Analice las imágenes detenidamente.** Con la ayuda de software de edición de imágenes, busque marcadores de esteganografía, como un ligero color distinto en las imágenes. Un gran número de colores duplicados en una imagen podría ser un indicador de un ataque mediante esteganografía.
- **Controle el uso de software de esteganografía.** Debería prohibirse la presencia de software de esteganografía en todos los sistemas de la empresa, a menos que sea expresamente necesario para fines empresariales. Despliegue este tipo de software únicamente en un segmento de red confinado.
- **Permita solamente el empleo de firmas de confianza.** Instale únicamente aplicaciones con firmas de confianza procedente de proveedores de confianza.
- **Configure el antimalware para detectar enlazadores o *binders*.** El software antimalware debe configurarse para identificar la presencia de *binders* en los que podrían ocultarse imágenes esteganográficas.
- **Segmente las redes.** Si por desgracia se produjera un ataque con esteganografía, una arquitectura de sistemas virtualizada, combinada con una adecuada segmentación de red, puede ayudar a contener el brote, ya que el proceso de arranque seguro y verificable que utilizan los sistemas virtualizados, junto con la supervisión continua del tráfico de red facilitan el aislamiento de las aplicaciones.
- **Supervise el tráfico saliente.** Identifique la presencia de ataques mediante esteganografía a través de la supervisión del tráfico saliente.

Cómo pueden protegerle los productos de McAfee frente al código esteganográfico en los ataques de malware

McAfee Endpoint Security

Prevención de amenazas

Asegúrese de que McAfee Endpoint Security (ENS) esté configurado para evitar amenazas conocidas de malware que puedan contener código esteganográfico:

- Mantenga McAfee ENS totalmente actualizado con el último parche, versión de DAT y motor de análisis.
- Compruebe que todos los sistemas de su entorno están protegidos y actualizados.
- Configure el análisis en tiempo real para que analice todos los archivos en el momento de la lectura y de la escritura. No desactive nunca el análisis en el momento de lectura, excepto cuando se configuren procesos de bajo riesgo.
- Las reglas de exclusión de análisis deben minimizarse y utilizarse únicamente cuando sea necesario. Si se sospecha que hay malware, las exclusiones de análisis deben desactivarse temporalmente. Descubra cómo configurar las exclusiones en el artículo de Knowledge Base KB88595.
- Infórmese sobre las implicaciones para el rendimiento del uso de configuraciones de procesos de alto riesgo/predeterminadas/bajo riesgo para limitar la exposición a amenazas esteganográficas en entornos de uso intensivo o en los que la seguridad del hardware es mínima. Descubra cómo mejorar el rendimiento con el artículo KB88205 sobre McAfee Endpoint Security.
- Configure McAfee ENS para la función de reputación de archivos de McAfee Global Threat Intelligence (GTI). Esta tecnología cierra la brecha entre las amenazas de tipo zero-day y las detecciones basadas en firmas. Descubra las configuraciones de reputación de archivos recomendadas por McAfee GTI en KB74983, con más información en KB53735.

- Configure reglas de protección de acceso de McAfee ENS para impedir la creación de los archivos autorun.inf.
- Utilice reglas de protección de acceso para evitar que se instalen amenazas desconocidas.

Control de la Web

El módulo de control web de McAfee ENS se basa en los servicios de reputación web y clasificación web de McAfee GTI. El software infectado mediante técnicas esteganográficas se suele encontrar en sitios web de distribución de malware.

El módulo de control web de McAfee ENS identifica —antes de que los visite— los sitios que alojan o están infectados por malware, o bien que incluyen contenido inapropiado.

El módulo de control web de McAfee:

- Indica la seguridad relativa de los sitios web mediante un código de color:
  - Verde = seguro (riesgo bajo o ningún riesgo)
  - Amarillo = precaución (riesgo leve)
  - Rojo = advertencia (riesgo serio)
  - Gris = desconocido (no se ha calificado aún, utilizar con precaución)
  - McAfee Secure = indica la seguridad relativa de los sitios web mediante un esquema de colores
- Se despliega y configura fácilmente a través de McAfee ePolicy Orchestrator.
- Ofrece otra capa de protección de endpoints. Se puede utilizar con Internet Explorer, Firefox, y Chrome.
- Utiliza protección antispam eficaz para impedir que los mensajes maliciosos puedan acceder a las redes.

Más información: Guía del producto de McAfee Endpoint Security - Uso del módulo de control web de McAfee ENS

Protección contra amenazas adaptable

- Active McAfee Real Protect para aplicar técnicas de aprendizaje automático para identificar amenazas avanzadas en función de su aspecto y de lo que podrían hacer (análisis antes de la ejecución) y de lo que hacen (análisis dinámico de comportamientos) —todo ello sin firmas. Más información: Protección contra amenazas adaptable—Real Protect
- Implemente la Contención dinámica de aplicaciones de McAfee y siga las mejores prácticas recomendadas. Más información: KB87843.

McAfee VirusScan Enterprise

Los clientes que no hayan desplegado la última versión de McAfee ENS deben asegurarse de que McAfee VirusScan Enterprise (VSE) esté configurado para evitar amenazas conocidas de malware que puedan contener código esteganográfico:

- Mantenga McAfee VSE totalmente actualizado con el último parche, versión de DAT y motor de análisis.
- Compruebe que todos los sistemas de su entorno están protegidos y actualizados.
- Configure el análisis en tiempo real para que analice todos los archivos en el momento de la lectura y de la escritura. No desactive nunca el análisis en el momento de lectura, excepto cuando se configuren procesos de bajo riesgo.

- Las reglas de exclusión de análisis deben minimizarse y utilizarse únicamente cuando sea necesario. Si se sospecha que hay malware, las exclusiones de análisis deben desactivarse temporalmente. Descubra cómo configurar las exclusiones en el artículo de Knowledge Base KB50998.
- En entornos de uso intensivo o en los que la seguridad del hardware es mínima, utilice configuraciones de procesos de alto riesgo/predeterminadas/bajo riesgo para limitar la exposición a las amenazas esteganográficas. Puede informarse sobre esta función en KB55139 y descubrir cómo configurarla en KB58692.
- Configure McAfee VSE para la función de reputación de archivos de McAfee Global Threat Intelligence (GTI). Esta tecnología cierra la brecha entre las amenazas de tipo zero-day y las detecciones basadas en firmas. Descubra las configuraciones de reputación de archivos recomendadas por McAfee GTI en KB74983, con más información en KB53735.
- Configure reglas de protección de acceso de McAfee VSE para impedir la creación de los archivos autorun.inf.
- Utilice reglas de protección de acceso para evitar que se instalen amenazas desconocidas.

McAfee Application Control

McAfee Application Control ofrece un método eficaz para bloquear en los servidores, equipos de sobremesa de la empresa y dispositivos de función fija las aplicaciones y el código no autorizados que llegan en ataques esteganográficos. McAfee Application Control evita la infección de los archivos, así como su propagación por la red.

McAfee Application Control ayuda a proteger dos áreas principales:

- **Protección basada en archivos:** defiéndase frente a ataques basados en archivos, que son típicos en las amenazas esteganográficas. Estos ataques pueden intentar ejecutar nuevas aplicaciones o modificar las actuales.
- **Protección de la memoria:** protéjase frente a ataques basados en la memoria, que llegan a través de Internet o la red, o se producen de forma local al ejecutar archivos.

Protección basada en archivos

Las aplicaciones que no están incluidas en la lista blanca no están ni autorizadas ni protegidas. Por el contrario, las que forman parte de listas blancas están autorizadas y protegidas. Si se introduce un elemento no autorizado en un endpoint (por ejemplo, mediante una descarga, el acceso a través de la red o localmente en una unidad flash o un CD), es posible que se copie en el endpoint, o se cambie o mueva de una carpeta a otra del endpoint, pero en ningún caso se ejecutará. A continuación se incluyen ejemplos de estos casos.

Ejecución denegada	Se intenta ejecutar una aplicación que no está en la lista blanca, pero McAfee Application Control no lo permite.
Se impidió la instalación de ActiveX	McAfee Application Control bloquea los intentos de instalar controles de ActiveX no autorizados.

Si un proceso no autorizado (por ejemplo, iniciado al ejecutar un archivo malicioso en un endpoint remoto) o un usuario no autorizado intenta modificar, renombrar, mover o eliminar un archivo que pertenece a una lista blanca, y por tanto está protegido, McAfee Application Control bloqueará dicho cambio. A continuación se incluyen ejemplos de estos casos.

Escritura de archivo denegada	McAfee Application Control bloquea los intentos de procesos no autorizados de modificar aplicaciones incluidas en listas blancas.
Modificación de paquete evitada	McAfee Application Control impide que una aplicación que utilice un paquete de instalador basado en MSI pueda instalar, modificar o eliminar archivos mediante un mecanismo no autorizado.

Más información: Mejores prácticas de McAfee Application Control

McAfee Advanced Threat Defense

McAfee Advanced Threat Defense (ATD) detecta sofisticados compresores, cargas útiles cifradas y malware de tipo zero-day con un innovador enfoque por capas. Combina firmas antimalware que no requieren intervención, y sistemas de protección basados en la reputación y la emulación en tiempo real con un análisis de malware dinámico en entorno aislado (sandboxing), para analizar el comportamiento del malware.

Más información: Preguntas frecuentes sobre McAfee Advanced Threat Defense

Para ampliar la información

McAfee Security Advice Center: Protección contra phishing

Threat Landscape Dashboard: El kit de exploits Sundown se actualizó a finales de 2016 y se descubrió que utilizaba técnicas esteganográficas para ocultar el código de exploit

McAfee Ireland Ltd.
Building 2000, City Gate
Mahon, Cork, Ireland
www.mcafee.com/es