Resumen de la solución

Protección frente al malware que ataca la GPU

En el **Informe de McAfee® Labs sobre amenazas de agosto de 2015**, examinamos detenidamente el malware que se aparta de la norma y no aprovecha la memoria del sistema o la CPU del endpoint, sino que ataca la unidad de procesamiento gráfico (GPU).

El malware que ataca o aprovecha la GPU del endpoint no es una novedad. Los troyanos que hacen uso de la GPU para incrementar la carga útil potencial desde los equipos atacados llevan al menos cuatro años en circulación. Sin embargo, la publicación de código de prueba de concepto que supuestamente aprovecha funciones de la GPU de formas totalmente nuevas ha puesto de nuevo el malware basado en la GPU en el punto de mira. Las afirmaciones, que se describen en detalle en el informe, se pueden agrupar en cuatro puntos:

- Acceso a la memoria del host de la CPU desde la GPU
- Eliminación posterior de los archivos del host de la CPU
- Persistencia tras los reinicios en caliente
- Ausencia de herramientas de análisis de la GPU

Aunque el malware que ejecuta este tipo de ataque es por el momento solamente una prueba de concepto, las amenazas a la GPU son muy preocupantes. Nosotros no hemos observado una proliferación de infecciones. Debido a la ausencia de herramientas que lleven a cabo el análisis forense en las GPU, revertir la ingeniería y obtener un análisis forense de estas unidades es mucho más complicado que analizar los ataques contra la memoria o las CPU. Para reducir la superficie de detección, los agresores eliminan el código malicioso de la CPU y la memoria, aunque no por completo, ya que suelen quedar elementos que permiten rastrear su actividad en el endpoint.

No hay duda de que asistiremos a nuevos avances en el malware basado en la GPU y solo el tiempo dirá si este tipo de ataques serán muy prolíficos.

Protección frente al malware que ataca la GPU

McAfee Labs recomienda varias formas de protección de los sistemas contra ataques a la GPU:

- Active las actualizaciones automáticas del sistema operativo o descargue con regularidad las actualizaciones para que los sistemas cuenten con los parches necesarios para estar protegidos frente a las vulnerabilidades conocidas.
- Instale los parches de otros fabricantes de software en cuanto se publiquen.
- Instale software de seguridad en todos los endpoints y mantenga actualizadas las firmas antimalware.

intel Security

- Considere utilizar listas blancas de aplicaciones para impedir la ejecución de aplicaciones no autorizadas.
- Evite ejecutar aplicaciones en modo de administrador siempre que sea posible.

Cómo puede ayudarle Intel Security a protegerse frente al malware para GPU

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 el malware avanzado.

- **Detección basada en firmas:** detecta virus, gusanos, spyware, bots, troyanos, ataques por desbordamiento del búfer y ataques combinados. McAfee Advanced Threat Defense incluye una completa base de conocimientos, creada y mantenida por McAfee Labs, que actualmente incluye más de 150 millones de firmas.
- **Detección basada en la reputación:** consulta la reputación de los archivos utilizando el servicio McAfee Global Threat Intelligence (McAfee 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 estático completo del código:** revierte la ingeniería del código de los archivos con el fin de evaluar todos sus 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 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:** 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 VirusScan Enterprise

McAfee VirusScan® Enterprise emplea el galardonado motor de análisis de Intel Security 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 ataques 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 diversas 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 Threat Intelligence Exchange

Es importante disponer de una plataforma inteligente con capacidad de adaptación 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.

- **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 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 (del inglés, IoC):** suelen importar hashes de archivos maliciosos conocidos. McAfee Threat Intelligence Exchange puede inmunizar 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 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, garantizando su protección contra las aplicaciones vulnerables o maliciosas conocidas.

- **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.
- **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 facilitar la creación de la lista blanca y asegurarse de que su empresa esté al tanto de las 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.

Intel y los logotipos de Intel y de McAfee, así como VirusScan, son marcas comerciales de Intel Corporation o de McAfee, Inc. en EE. UU. y/o en otros países. Los demás nombres y marcas pueden ser reclamados como propiedad de otros. Copyright © 2015 McAfee, Inc.
62072brf_protect-against-gpu-malware_0815

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