Resumen de la solución

Protección contra la manipulación del firmware y la BIOS

En el ***Informe de McAfee Labs sobre amenazas: Mayo de 2015***, analizamos en profundidad un grupo de hackers conocido como el Equation Group y sus ataques contra el firmware de los discos duros y las unidades en estado sólido. El "Equation Group", que recibe su nombre por su predilección por esquemas de cifrado y malware asociado extremadamente sofisticados, se encuentra en la actualidad entre los ejemplos más palpables y avanzados de ataques al firmware jamás observados.

Uno de los descubrimientos más importantes de esta investigación se refiere a los módulos de reprogramación del firmware de los discos duros (HDD) y de las unidades en estado sólido (SSD). Las unidades HDD/SSD cuyo firmware ha sido reprogramado pueden recargar el malware asociado cada vez que se reinician los sistemas infectados, y el malware persiste incluso tras reformatear las unidades o reinstalar el sistema operativo. Además, una vez que la unidad ha sido infectada, tanto el firmware reprogramado como el malware asociado son indetectables para el software de seguridad.

Durante los últimos siete años, Intel Security ha observado muchos ejemplos de malware con capacidades de manipulación del firmware o la BIOS. Hemos visto tanto pruebas de concepto académicas como casos reales, como **CIH/Chernobyl**, Mebromi y **BIOSkit**. También habíamos previsto este tipo de ataque específico en el informe *Predicciones de amenazas de McAfee Labs para 2012*. Con el descubrimiento de las muestras "específicas del Equation Group" ahora las consideramos uno de los ejemplos más visibles y avanzados de ataque al firmware jamás observado.

Cómo protegerse de los ataques del Equation Group

A continuación incluimos las prácticas y procedimientos recomendados para protegerse contra los ataques del estilo de los llevados a cabo por el Equation Group:

- Instale software de protección para endpoints en todos los endpoints.
- Active las actualizaciones automáticas del sistema operativo o descargue con regularidad las actualizaciones para que los sistemas operativos 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.
- Cifre los datos y las unidades de disco duro importantes.
- Elimine las campañas masivas de phishing con filtrado del correo electrónico a nivel de una gateway segura.

intel Security

- Implemente la verificación de la identidad de los remitentes para reducir el riesgo de que los ciberdelincuentes sean confundidos con personas en las que se confía.
- Detecte y elimine los adjuntos maliciosos con antimalware avanzado.
- Analice las URL incluidas en los mensajes de correo electrónico y una vez más al hacer clic en ellas.
- Analice el tráfico web en busca de malware cuando el phishing incite al usuario hacer clic varias veces para quedar infectado.
- Eduque a los usuarios sobre las mejores prácticas en la detección y modo de proceder frente a mensajes de correo electrónico sospechosos.
- Implemente una solución de prevención de la pérdida de datos para evitar la filtración en caso de que se produzca un ataque.

Cómo puede ayudarle Intel Security a protegerse contra este tipo de ataques

La protección contra ataques de manipulación del firmware o de la BIOS debe formar parte del enfoque de seguridad de todas las empresas. Los esfuerzos deben concentrarse en dos áreas:

- Establecer formas de detectar la distribución inicial del malware del Equation Group. Los vectores de ataque conocidos son el phishing, los CD y las unidades USB, por lo que es preciso prestar atención especial a estas áreas.
- Proteger los sistemas de la filtración de datos. Aunque en la actualidad no puede detectarse el módulo de reprogramación de firmware, el objetivo general del ataque es muy probable que sea el reconocimiento. Como el reconocimiento depende de la comunicación sistemática y la filtración de datos con un servidor de control, resulta extremadamente importante detener esta fase.

McAfee Advanced Threat Defense

McAfee Advanced Threat Defense es una solución de detección de malware multicapa que combina 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 le protegerá del malware avanzado que ha recibido la orden del firmware reprogramado del Equation Group de volver a cargarse.

- **Detección basada en firmas:** detecta virus, gusanos, spyware, bots, troyanos, ataques por desbordamiento del búfer y ataques combinados. McAfee Labs ha creado y mantiene su completa base de conocimientos, 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 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 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 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.

Resumen de la solución

McAfee Threat Intelligence Exchange
Es importante disponer de una plataforma inteligente que pueda adaptarse 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 para impedir la ejecución de aplicaciones desconocidas en el entorno. Si una aplicación cuya ejecución estaba autorizada se califica posteriormente como 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):** 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.

McAfee VirusScan Enterprise
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 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 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.

Resumen de la solución

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.
- **Uso de técnicas de inspección avanzadas:** entre ellas, se incluyen el análisis de todos los protocolos, la reputación de amenazas y los comportamientos para detectar y prevenir tanto los ataques de red conocidos como los desconocidos (zero-day).
- **Integración con McAfee Global Threat Intelligence:** 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 DLP Monitor

McAfee Data Loss Prevention (DLP) Monitor permite recopilar, rastrear e informar sobre los datos en uso en toda la red. Descubre fácilmente las amenazas desconocidas para sus datos y le permite adoptar las medidas para protegerlos y garantizar que su empresa no sufre la próxima gran fuga de datos.

- **Examen del tráfico de red:** las funciones de análisis de datos, líderes del sector, de McAfee DLP Monitor examinan en profundidad el tráfico de red.
- **Identificación rápida de los datos:** la detección en tiempo real detalla rápidamente cómo se están utilizando los datos, quién los usa y a dónde van, lo que proporciona al usuario la información que necesita para tomar las medidas adecuadas. McAfee DLP Monitor puede identificar rápidamente más de 300 tipos de contenido que transita por cualquier puerto o protocolo, lo que garantiza la visibilidad para su empresa.
- **Análisis forenses detallados:** realice análisis forenses para correlacionar los eventos de riesgo actuales y pasados, detectar tendencias de riesgos e identificar amenazas. Esto le permite comprender rápidamente la situación y desarrollar las reglas y directivas para corregir las posibles anomalías.

McAfee DLP Prevent

McAfee Data Loss Prevention (DLP) Prevent protege frente a la pérdida de información garantizando que solo salga de la red cuando proceda, ya sea mediante correo electrónico, correo web, mensajería instantánea, wikis, blogs, portales, HTTP/HTTPS o transferencias FTP. La capacidad para identificar y mitigar rápidamente los intentos de filtración marca la diferencia entre mantener a salvo sus datos valiosos o aparecer en los siguientes titulares.

- **Visibilidad de los incidentes de seguridad:** las vistas personalizadas y los informes de incidentes proporcionan vistas resumidas y detalladas de los incidentes de seguridad y de las medidas de corrección adoptadas.
- **Implementación de directivas de forma proactiva para todos los tipos de información:** permite implementar directivas para la información que sabe que es confidencial, así como para la que no es tan obvia. Gracias a una amplia variedad de directivas, que van desde el cumplimiento de normativas al uso aceptable y la propiedad intelectual, puede comparar documentos completos o parciales con un conjunto de reglas completo para que pueda proteger toda su información confidencial.

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