Protección frente a WannaCry y Petya

En mayo de 2017 se lanzó un gran ciberataque, basado en la familia de malware WannaCry. WannaCry aprovechaba una vulnerabilidad en algunas versiones de Microsoft Windows. Se estima que durante el ataque principal se infectaron más de 300 000 ordenadores en 150 países, y para cada uno de ellos se exigía el pago de un rescate.

El vector de ataque inicial no está claro, pero un agresivo gusano facilita la propagación del malware. Microsoft distribuyó un parche crítico en marzo para eliminar la vulnerabilidad en las versiones compatibles de Windows, pero muchas empresas aún no lo han aplicado.

Los ordenadores que emplean versiones de Windows no compatibles (Windows XP, Windows Server 2003) no tenían un parche disponible. Microsoft distribuyó un parche de seguridad especial para Windows XP y Windows Server 2003 después del ataque de WannaCry.

Aproximadamente seis semanas más tarde, otro ciberataque aprovechó la misma vulnerabilidad. Petya no tuvo tanto impacto como WannaCry, pero estos dos ataques pusieron de manifiesto el uso continuado de sistemas operativos antiguos y no compatibles en áreas fundamentales y desvelaron los procesos de actualización de parches laxos que aplican algunas empresas. En el *Informe de McAfee Labs sobre amenazas: Septiembre de 2017* encontrará un exhaustivo análisis de estos ataques.

Prácticas y procedimientos recomendados para protegerse frente a WannaCry and Petya

- **Crear copias de seguridad de los archivos:** el procedimiento más eficaz contra el ransomware es realizar regularmente copias de seguridad de los archivos y verificar los procedimientos de restauración de la red.
- **Educar a los usuarios de la red:** como en el caso de otros tipos de malware, el ransomware a menudo infecta un sistema a través de ataques de phishing mediante adjuntos de correo electrónico, descargas o las secuencias de comandos entre sitios (*cross-scripting*) en páginas web.
- **Supervisar e inspeccionar el tráfico de red:** este paso ayudará a identificar tráfico anormal asociado a comportamientos de ransomware.
- **Utilizar flujos de datos de inteligencia sobre amenazas:** esta práctica puede ayudar a detectar más rápidamente las amenazas.
- **Limitar la ejecución de código:** el ransomware se diseña a menudo para ejecutarse en carpetas conocidas del sistema operativo. Si no consigue llegar a estas carpetas debido al control de acceso, se puede bloquear el cifrado de datos con fines delictivos.
- **Limitar el acceso administrativo y a sistemas:** algunos tipos de ransomware están diseñados para utilizar cuentas predeterminadas para llevar a cabo sus operaciones. Frente a este tipo de ransomware, cambiarle el nombre a las cuentas de usuario predeterminadas y desactivar las cuentas, con privilegios o sin ellos, que no sean necesarias ofrece protección adicional.
- **Retirar derechos administrativos locales:** impedir que el ransomware se ejecute en un sistema local y evitar que se propague con privilegios de administrador. La eliminación de los derechos administrativos locales también bloquea el acceso a todos los recursos y archivos de sistema críticos que intenta cifrar el ransomware.
- **Otras prácticas relacionadas con permisos:** plantéese limitar los derechos de escritura de los usuarios, para impedir la ejecución desde directorios de usuario, incluir aplicaciones en listas blancas y limitar el acceso al almacenamiento o los recursos compartidos de la red. Algunos tipos de ransomware requieren acceso de escritura a determinadas rutas de archivos para instalarse o ejecutarse. Limitar el permiso de escritura a un pequeño número de directorios (por ejemplo, Mis documentos y Mis descargas) puede frustrar la acción de las variantes del ransomware. Los ejecutables del ransomware también pueden neutralizarse mediante la eliminación del permiso de ejecución en esos directorios. Muchas empresas utilizan un número reducido de aplicaciones en su actividad comercial. Puede bloquearse la ejecución de aplicaciones no incluidas en la lista blanca, incluido el ransomware, mediante una directiva que determine el uso exclusivo de aplicaciones incluidas en la lista blanca. Otra práctica relacionada con los permisos es requerir un inicio de sesión en recursos compartidos, como las carpetas de red.
- **Mantener y actualizar el software:** otra regla básica importante para protegerse contra el ransomware es mantener y actualizar el software, en particular los parches del sistema operativo, así como el software antimalware y de seguridad.

Resulta extremadamente importante reducir la superficie de ataque, especialmente del phishing, una de las técnicas más populares utilizadas por el ransomware. En lo que respecta al correo electrónico, pueden aplicarse las siguientes prácticas:

- **Filtrar el contenido del correo electrónico:** la protección de las comunicaciones por correo electrónico es fundamental. La posibilidad de éxito de un ataque disminuirá si los usuarios de la red reciben menos mensajes de spam que puedan tener contenido potencialmente malicioso e inseguro.
- **Bloquear datos adjuntos:** la inspección de adjuntos es una medida importante para reducir la superficie de ataque. El ransomware se distribuyen a menudo en un archivo adjunto ejecutable. Apruebe una directiva que especifique que algunas extensiones de archivos no puedan enviarse por correo electrónico. Estos adjuntos podrían analizarse mediante una solución de entorno aislado y podrían ser eliminados por un dispositivo de seguridad para el correo electrónico.

Cómo pueden proteger los productos de McAfee frente a WannaCry

McAfee Network Security Platform (NSP)

McAfee NSP responde rápidamente para prevenir exploits y proteger los activos de las redes. El equipo de McAfee NSP trabaja con diligencia para desarrollar y desplegar firmas definidas por el usuario para problemas críticos. En un período de 24 horas durante el ataque de WannaCry, McAfee creó y cargó varias firmas de usuario para que los clientes las desplegaran en sus sensores de red. En este caso, la firma afectaba concretamente a las herramientas EternalBlue, Eternal Romance SMB Remote Code Execution y DoublePulsar. McAfee también distribuyó indicadores de peligro relacionados que podían agregarse a una lista negra para bloquear posibles amenazas asociadas con el troyano original.

Encontrará más información sobre las firmas de NSP aquí.

McAfee Host Intrusion Prevention (HIPS)

McAfee HIPS 8.0 con la firma de NIPS 6095 ofrece protección frente a las cuatro variantes conocidas de WannaCry. Consulte en KB89335 la última información sobre estas configuraciones.

Firma personalizada 1: Regla de bloqueo del registro de WannaCry
Utilizar subregla estándar
Tipo de regla = Registro
Operaciones = Crear, Modificar, Cambiar permisos, incluir la clave del Registro
Clave del Registro = \REGISTRY\MACHINE\SOFTWARE\WanaCrypt0r
Ejecutable = *

Firma personalizada 2: Regla de bloqueo de archivos/carpetas de WannaCry
Utilizar subregla estándar
Tipo de regla = Archivos
Operaciones = Crear, Escribir, Cambiar nombre, Modificar atributos de solo lectura/oculto, los parámetros incluyen archivos
Archivos = *.wnry
Ejecutable = *

Configuraciones del módulo Protección frente a amenazas adaptable de McAfee Endpoint Protection (ENS) y McAfee VirusScan Enterprise (VSE)

McAfee Endpoint Security 10.5—Protección frente a amenazas adaptable

McAfee Endpoint Security 10.5 con Real Protect con Protección frente a amenazas adaptable y Contención dinámica de aplicaciones (DAC) ofrece protección frente a exploits conocidos y desconocidos relacionados con WannaCry.

- Configure lo siguiente en la directiva Protección frente a amenazas adaptable—Opciones:
  - Asignación de regla = Seguridad. (El valor predeterminado es Equilibrado).
- Configure las reglas siguientes en la directiva Protección frente a amenazas adaptable—Contención dinámica de aplicaciones:
  - Contención dinámica de aplicaciones—Reglas de contención

Consulte KB87843: Lista de reglas de contención dinámica de aplicaciones para ENS y prácticas recomendadas y configure las reglas de DAC recomendadas como "Bloquear", como se indica.

McAfee Endpoint Security 10.1, 10.2 y 10.5—Prevención de amenazas

Prevención de amenazas de McAfee Endpoint Security 10.x con contenido de AMCore versión 2978 o posterior ofrece protección frente a las cuatro variantes de WannaCry conocidas en la actualidad.

McAfee VirusScan Enterprise 8.8

McAfee VirusScan Enterprise 8.8 con contenido del DAT 8527 o posterior ofrece protección frente a las cuatro variantes de WannaCry conocidas en la actualidad.

Medidas proactivas de protección de McAfee Endpoint Security (ENS) y de protección de acceso de McAfee VirusScan Enterprise (VSE)

Las reglas de protección de McAfee ENS y de protección de acceso de McAfee VSE evitarán la creación del archivo .wnry. Esta regla detiene la rutina de cifrado, que crea archivos cifrados que contienen una extensión .wncryt, .wncry o .wcry. Al implementar el bloqueo de los archivos .wnry, no son necesarios otros bloqueos de tipos de archivos cifrados.

Más información sobre la configuración de reglas de protección de acceso de McAfee VSE.

Configure el sistema de seguridad de endpoints para protegerse frente al cifrado de archivos que lleva a cabo WannaCry (y variantes desconocidas futuras)

Los clientes que no utilicen seguridad de Protección frente a amenazas adaptable de McAfee ENS no pueden contar con protección de contenido definida por McAfee contra variantes que aún no se ha distribuido. Recomendamos que se configuren tareas de actualización de repositorios con un intervalo de actualización mínimo para garantizar que el nuevo contenido se aplique cuando lo distribuya McAfee.

Se pueden configurar otras medidas de protección frente a la rutina de cifrado con las reglas de protección de acceso de McAfee VSE/ENS, o las reglas personalizas de McAfee HIPS. Consulte en KB89335 la última información sobre estas configuraciones.

Las reglas de protección de acceso de McAfee VSE y McAfee ENS, y las firmas de cliente de McAfee HIPS impedirán la creación del archivo .wnry.

Las reglas evitan la rutina de cifrado, que crea archivos cifrados que contienen una extensión .wncryt, .wncry o .wcry.

Al implementar el bloqueo de los archivos .wnry, no son necesarios otros de archivos cifrados.

Consulte en KB89335 (accesible para los clientes registrados de McAfee) la última información sobre estas configuraciones.

McAfee Advanced Threat Defense (ATD)

El aprendizaje automático de McAfee ATD permite detectar una muestra en análisis de "gravedad media".

McAfee ATD ha observado lo siguiente:

Clasificación de comportamientos:

- Ocultación de archivos
- Propagación
- Exploit a través de código shell
- Propagación por la red

Análisis dinámico:

- Comportamiento provocado por el ransomware
- Cifrado de archivos
- Creación y ejecución de contenido de scripting sospechoso
- Comportamiento como un troyano dropper de macros

Al mismo tiempo que WannaCry, McAfee ATD ha observado 22 operaciones de procesos, incluidas cinco DLL de tiempo de ejecución, 58 operaciones con archivos, modificaciones del registro, creaciones de archivos (dll.exe), inyecciones de DLL, y 34 operaciones de red.

McAfee Web Gateway (MWG)

McAfee Web Gateway (MWG) es una familia de productos (dispositivo, nube e híbrido) de proxies web que proporciona protección inmediata contra las variantes de WannaCry que llegan a través de la Web (HTTP/HTTPS) mediante varios motores de análisis en tiempo real.

Las variantes conocidas serán bloqueadas por el análisis antimalware y de reputación de McAfee Global Threat Intelligence (GTI) cuando se procese el tráfico web a través del proxy.

El motor Gateway Anti-Malware (GAM) Engine de MWG proporciona prevención eficaz de variantes que no han sido aún identificadas con una firma (las amenazas "zero-day") mediante su proceso de emulación de comportamientos —efectuado en archivos, HTML y JavaScript. Los emuladores reciben con regularidad inteligencia de los modelos de aprendizaje automático. GAM funciona junto a los análisis antimalware y de reputación de GTI, cuando se procesa el tráfico.

La combinación de MWG y ATD permite realizar más inspecciones y facilita una estrategia de prevención y detección.

McAfee Threat Intelligence Exchange (TIE)

McAfee Threat Intelligence Exchange (TIE) amplía aún más la seguridad del cliente. Gracias a la posibilidad de combinar los resultados de reputación de ENS, VSE, MWG y NSP, TIE puede compartir rápidamente información de reputación relativa a WannaCry con cualquier vector integrado. Con la posibilidad de utilizar GTI para las consultas de reputación globales, TIE también permite a los productos integrados tomar una decisión inmediata antes de la ejecución de la carga útil del ransomware, aprovechando la reputación almacenada en la base de datos de TIE.

Cuando se protege un endpoint, se detectan variantes relacionadas y se actualiza la calificación de la reputación en TIE, este procedimiento totalmente integrado amplía la protección distribuyendo esta información a todos los endpoints con TIE. Esta posibilidad bidireccional de compartir inteligencia de amenazas se duplica con MWG y NSP. Así, cuando una amenaza potencial intente filtrarse en la red o la Web, MWG y NSP proporcionarán protección y detección, y compartirán esta inteligencia con TIE para inocular a los endpoints —protegiendo inmediatamente a la empresa sin necesidad de ejecutar la variante detectada en un "paciente cero" potencial en el entorno.

Cómo pueden proteger los productos de McAfee frente a Petya

McAfee ofrece protección frente al ataque inicial de Petya a través de análisis de comportamiento de malware avanzados con las técnicas de Real Protect Cloud y Dynamic Neural Network (DNN) disponibles en McAfee Advanced Threat Defense.

ATD 4.0 introdujo una nueva función de detección mediante una red neuronal con retropropagación, de varias capas (DNN) que emplea el aprendizaje semisupervisado. DNN busca determinadas funciones que realiza el malware para obtener un veredicto positivo o negativo que permita determinar si el código es malicioso.

Ya se use en modo autónomo o conectado a sensores de McAfee para endpoints o redes, ATD combina inteligencia de amenazas con análisis de comportamientos en entornos aislados y aprendizaje automático para proporcionar protección adaptable de tipo zero-day. Real Protect, parte de la solución Dynamic Endpoint, utiliza también aprendizaje automático y análisis de enlaces para proteger frente al malware sin firmas, y proporcionar inteligencia detallada a Dynamic Endpoint y al resto del ecosistema de McAfee. Real Protect combinado con contención dinámica de aplicaciones proporcionaba protección anticipada frente a Petya.

Varios productos de McAfee ofrecen protección adicional para contener el ataque o prevenir su ejecución posterior.

McAfee Endpoint Security

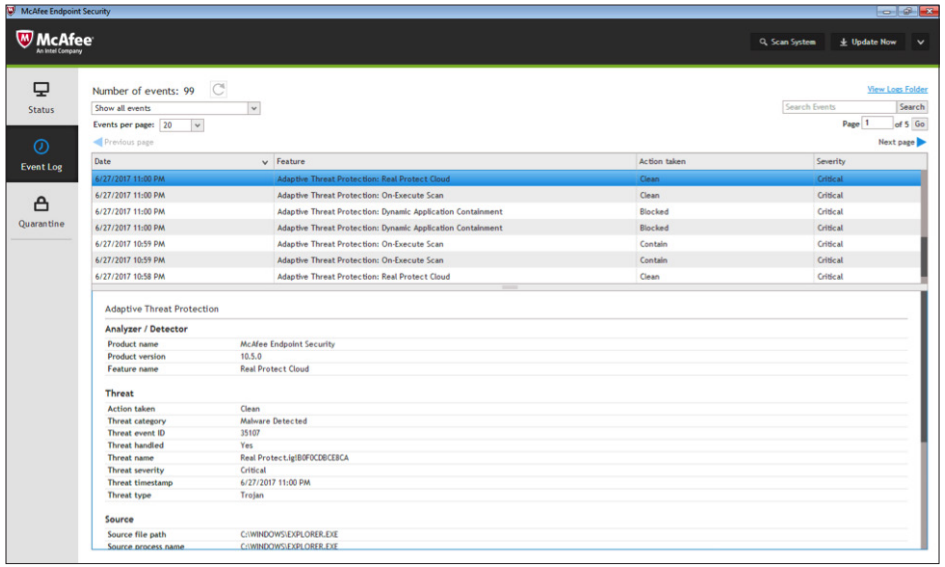
Prevención de amenazas

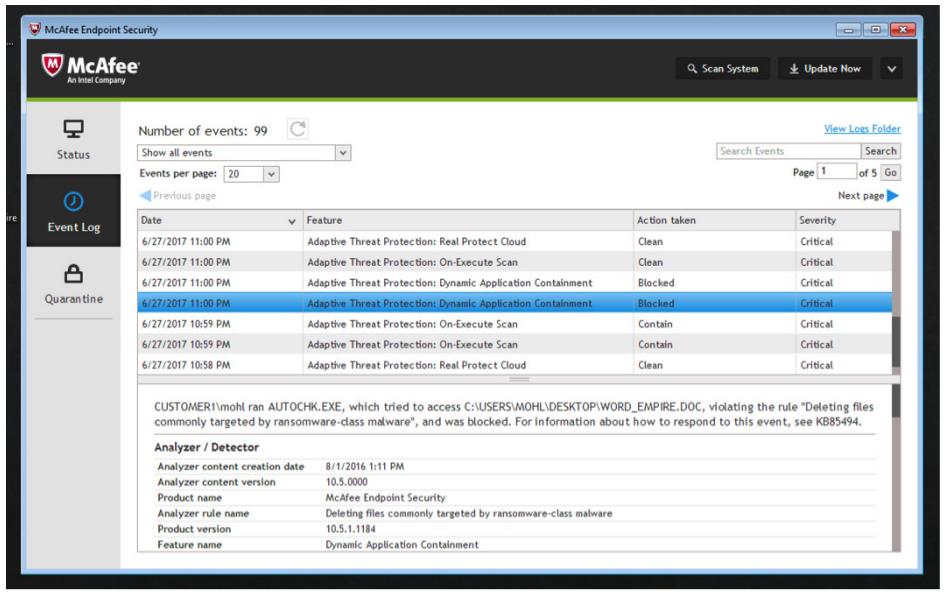
- McAfee Endpoint Security con McAfee Global Threat Intelligence y la directiva de análisis en tiempo real con el nivel de confidencialidad "Bajo" protege frente a muestras y variantes conocidas.
- Amplíe la información sobre las configuraciones de reputación de archivos recomendadas por McAfee GTI en KB74983, con más información en KB53735.
- McAfee Threat Intelligence Exchange con GTI protege frente a muestras y variantes conocidas.

Los sistemas que utilizan McAfee ENS 10 están protegidos frente a muestras y variantes conocidas con firmas e inteligencia de amenazas.

Protección frente a amenazas adaptable

- El módulo Protección frente a amenazas adaptable (ATP), con asignación de reglas configurada en "modo equilibrado" (el valor predeterminado en ATP\ Opciones\Asignación de reglas), protegerá frente a variantes conocidas y desconocidas del ransomware Petya.
- El módulo ATP protege frente a esta amenaza desconocida con varias capas de protección y contención avanzadas:
  - ATP - Real Protect Static utiliza análisis de comportamientos preejecución del lado del cliente para supervisar las amenazas maliciosas desconocidas antes de que se lancen.
  - ATP - Real Protect Cloud emplea aprendizaje automático asistido por la nube para identificar y limpiar la amenaza, como se muestra arriba.
- ATP - Contención dinámica de aplicaciones (DAC) detiene la amenaza y previene daños potenciales (eventos de DAC mostrados abajo).





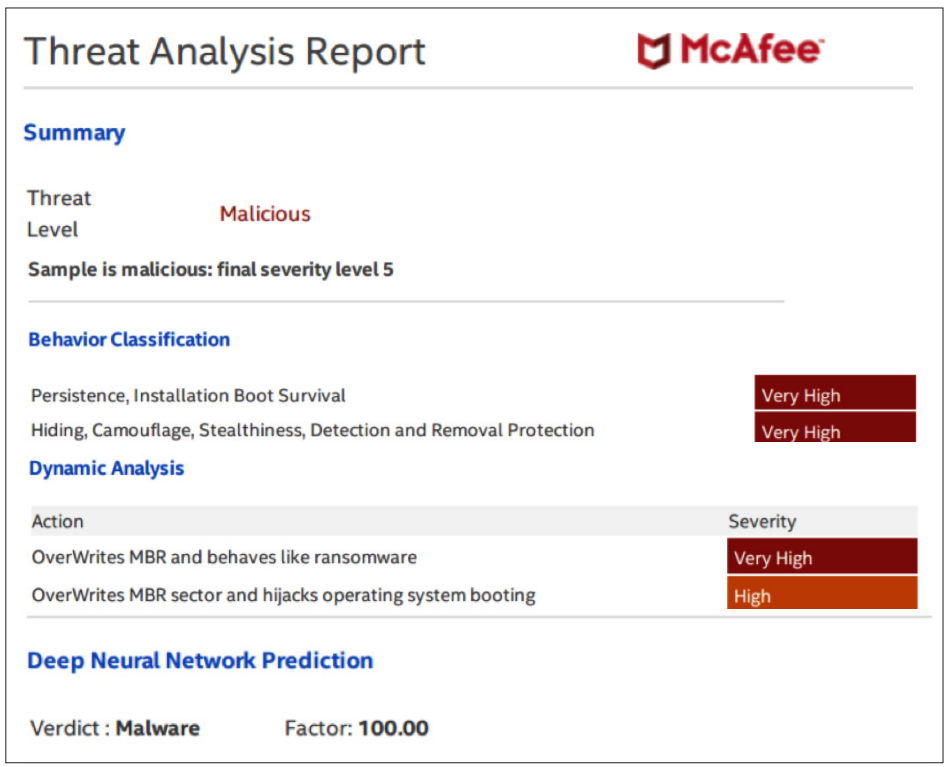
McAfee Advanced Threat Defense

- McAfee Advanced Threat Defense 4.0 con Red neuronal profunda y Análisis dinámico en entornos aislados identificó la amenaza y actualizó de forma proactiva el ecosistema de ciberdefensa. (Véase abajo).

McAfee Enterprise Security Manager

McAfee Enterprise Security Manager (ESM) es una solución de administración de información y eventos de seguridad que ofrece inteligencia práctica e integraciones para priorizar, investigar y responder a las amenazas. Los paquetes Suspicious Activity Content Pack y Exploit Content Pack para McAfee ESM han sido actualizados con reglas, alarmas y listas de vigilancia específicas para WannaCry, para que pueda localizar e identificar posibles infecciones. Estas actualizaciones también protegerán frente a Petya. Los dos paquetes están disponibles para descargarse en la consola de McAfee ESM de forma gratuita. Las reglas de correlación predeterminadas de McAfee ESM pueden alertar también a los usuarios sobre el aumento de los niveles análisis SMB horizontales.

Al igual que WannaCry, el ataque de Petya ofrece una oportunidad a los analistas de los centros de operaciones de seguridad de aprender. Conocer y automatizar estas mejores prácticas ayudará a los responsables de la seguridad a gestionar el próximo ataque que avance rápido.



McAfee Web Gateway

McAfee Web Gateway (MWG) es una familia de productos (dispositivo, nube e híbrido) de proxies web que proporciona otra capa de protección contra las variantes de Petya que llegan a través de la Web (HTTP/HTTPS) mediante varios motores de análisis en tiempo real. Las variantes conocidas serán bloqueadas por el análisis antimalware y de reputación de McAfee Global Threat Intelligence (GTI) cuando se procese el tráfico web a través del proxy.

El motor Gateway Anti-Malware Engine de MWG proporciona prevención eficaz de variantes que no han sido aún identificadas con una firma mediante su proceso de emulación de comportamientos —efectuado en archivos, HTML y JavaScript. Los emuladores reciben con regularidad inteligencia de los modelos de aprendizaje automático. GAM funciona junto a los análisis antimalware y de reputación de GTI, cuando se procesa el tráfico.

La combinación de MWG y ATD permite realizar más inspecciones y facilita una estrategia de prevención y detección.

Productos de McAfee que utilizan archivos DAT

McAfee distribuyó un Extra.DAT para incluir cobertura para Petya. También McAfee distribuyó un DAT de emergencia para incluir protección para esta amenaza. Los DAT posteriores incluirán cobertura. Los últimos archivos DAT están disponibles en el artículo del Centro de conocimiento KB89540.

Para ampliar la información

Encontrará detalles técnicos actualizados con frecuencia en los artículos del Centro de conocimiento de McAfee KB89335, KB87843, KB74983, KB53735 y KB89540.

McAfee
Together is power.

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