Resumen de la solución

Cómo derrotar al ransomware: evite el secuestro de sus datos

El ransomware es malware que emplea cifrado asimétrico para secuestrar la información de la víctima y solicitar un rescate. El cifrado asimétrico (clave pública) es una técnica criptográfica en la que se utilizan un par de claves para cifrar y descifrar un archivo. El agresor genera de manera exclusiva el par de claves pública-privada para la víctima y almacena la clave privada para descifrar los archivos en su servidor. La víctima solamente podrá acceder a la clave privada tras el pago de un rescate al agresor, aunque tal y como se ha podido comprobar en campañas recientes de ransomware, esto no siempre sucede así. Sin acceso a la clave privada, resulta prácticamente imposible descifrar los archivos por los que se exige un rescate.

Análisis del ransomware

Para obtener un análisis técnico en profundidad del ransomware, consulte el ***Informe de McAfee Labs sobre amenazas: Mayo de 2015***. En el *Informe de McAfee Labs sobre amenazas de noviembre de 2014* fuimos capaces de predecir nuevas amenazas importantes que aparecerían en 2015. En concreto, en McAfee Labs afirmábamos: "En cuanto al ransomware, prevemos una evolución de sus métodos de propagación, cifrado y los objetivos a los que apunta". Casi de manera inmediata, comenzamos a observar un enorme repunte en la prevalencia del ransomware, así como la aparición de nuevas familias, como Teslacrypt, y más cambios en las familias actuales, como CTB-Locker, CryptoWall y TorrentLocker.

La mayoría de las campañas de ransomware empiezan por un mensaje de correo electrónico de phishing. Con el paso del tiempo, han ganado en sofisticación, y ahora muchas están específica y meticulosamente diseñadas en el idioma local de las víctimas a las que van dirigidas.

intel Security

Además, se han adaptado a las nuevas tecnologías para hacer el ransomware más potente:

- **Moneda virtual:** mediante el uso de **moneda virtual** como método de pago de los rescates, los agresores evitan la exposición a la banca tradicional y a la posibilidad de rastrear las transferencias de dinero.
- **Red Tor:** gracias al uso de la **red Tor**, los agresores puede ocultar más fácilmente la ubicación de sus servidores de control, que almacenan las claves privadas de las víctimas. Tor permite mantener la infraestructura criminal durante mucho tiempo e incluso alquilarla a otros agresores para que puedan lanzar campañas de afiliados.
- **Desplazamiento hacia los dispositivos móviles:** en junio de 2014, los investigadores descubrieron la primera familia de ransomware para cifrar datos en dispositivos Android[1]. Pletor utiliza cifrado AES, bloquea los datos de la tarjeta de memoria del teléfono y utiliza Tor, SMS o HTTP para conectarse con los agresores.
- **Dispositivos de almacenamiento masivo como objetivo:** en agosto de 2014, Synolocker comenzó a atacar discos y servidores en bastidor NAS (dispositivos de almacenamiento conectados a la red) de Synology[2]. El malware aprovecha una vulnerabilidad en versiones sin parche de los servidores NAS para cifrar de forma remota todos sus datos mediante claves RSA de 2048 o 256 bits.

Cómo protegerse contra el ransomware

A continuación incluimos algunas buenas prácticas y procedimientos para estar mejor protegido tanto usted como su empresa frente a la amenaza del ransomware.

- **Lleve a cabo campañas continuas de concienciación de los usuarios:** puesto que la mayoría de los ataques de ransomware empiezan por mensajes de correo electrónico de phishing, la concienciación de los usuarios es extremadamente importante y necesaria. Las estadísticas demuestran que de cada diez mensajes de correo electrónico enviados por los agresores, al menos uno conseguirá su objetivo. No abra mensajes de correo electrónico ni adjuntos procedentes de remitentes no verificados o desconocidos.
- **Mantenga actualizados los parches de los sistemas:** hay parches disponibles que corrigen muchas de las vulnerabilidades que aprovecha el ransomware. Actualice los parches de los sistemas operativos, Java, Adobe Reader, Flash y las aplicaciones. Establezca un procedimiento de aplicación de parches y verifique que los parches se aplicaron correctamente.
- **Tenga mucho cuidado cuando abra archivos adjuntos:** configure el software antivirus para que analice automáticamente los archivos adjuntos de todos los mensajes instantáneos y de correo electrónico. Asegúrese de que los programas de correo electrónico no abran automáticamente los archivos adjuntos ni procesen automáticamente los gráficos, así como de que el panel de vista previa esté desactivado. No abra nunca mensajes de correo electrónico no deseados ni archivos adjuntos que no espere recibir, incluso aunque provengan de personas que conoce.
- **Tenga cuidado con el phishing basado en spam:** no haga clic en enlaces de mensajes instantáneos o de correo electrónico.

Cómo puede ayudarle Intel Security a protegerse frente al ransomware

McAfee Web Gateway

Para distribuir ransomware se utilizan métodos como la publicidad engañosa, las descargas inadvertidas y las URL maliciosas incrustadas en sitios web de confianza. **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 Global Threat Intelligence (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.

McAfee Email Gateway

A las empresas les preocupa enormemente saber si un mensaje de correo electrónico recibido en la bandeja de entrada de un usuario es inofensivo o por el contrario malicioso y con intención de distribuir ransomware. **McAfee Email Gateway** ofrece protección gracias a varias funciones contra este tipo de ataques de phishing cada vez más sofisticados.

- **ClickProtect:** elimine las amenazas asociadas a las direcciones URL incrustadas en mensajes de correo electrónico analizando dichas direcciones URL en el mismo momento en que se hace clic en ellas. Esta inspección incluye la comprobación de la reputación de la dirección URL y la emulación proactiva del motor McAfee Gateway Anti-Malware Engine.
- **Integración con McAfee Advanced Threat Defense:** detecte malware sofisticado y evasivo con análisis de código estático en profundidad y análisis dinámicos de archivos sospechosos adjuntos a mensajes de correo electrónico, de manera que los archivos maliciosos no lleguen nunca a la bandeja de entrada.
- **Integración con McAfee GTI:** combina información de la red local con datos de reputación de McAfee GTI a fin de proporcionar el modelo más completo de protección frente a malware, spam y amenazas entrantes.

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 contra el ransomware, como CTB-Locker, CryptoWall, etc.

- **Detección basada en firmas:** detecta virus, gusanos, spyware, bots, troyanos, ataques por desbordamiento del búfer y ataques combinados. McAfee Labs ha creado y mantiene la completa base de conocimientos de esta solución, que actualmente incluye más de 150 millones de firmas, incluidas las de CTB-Locker, CryptoWall y sus variantes.
- **Detección basada en la reputación:** consulta la reputación de los archivos utilizando el servicio 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 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.

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 que intentan ejecutarse en el entorno. El bloqueo de los ejecutables nuevos o desconocidos garantiza una protección proactiva contra el ransomware.

- **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

Con **McAfee VirusScan® Enterprise** detectar y proteger contra el ransomware es muy fácil. 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 exploits 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.

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 e impedir las comunicaciones del ransomware a través de protocolos de red como Tor, IRC y otros.

- **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 GTI:** 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.

Garantizar la invulnerabilidad de los datos más valiosos de su empresa es una tarea ardua, sobre todo si tenemos en cuenta el crecimiento estable del ransomware como vector de ataque. La tecnología de Intel Security puede contribuir a que su empresa se proteja de forma proactiva frente a amenazas como el ransomware tanto en endpoints como en redes.

1. **https://threatpost.com/android-ransomware-first-to-encrypt-data-on-mobile-devices/106535**
2. **http://forum.synology.com/enu/viewtopic.php?f=108&t=88770**

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