Informe técnico

Cómo protegerse frente al ransomware

Evite las amenazas actuales de ransomware con los productos de Intel® Security.

El ransomware es malware que emplea cifrado asimétrico para secuestrar la información de la víctima y solicitar un rescate. El cifrado asimétrico (clave pública-privada) es una técnica criptográfica que utiliza un par de claves para cifrar y descifrar un archivo. El agresor genera un par de claves pública-privada especial 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 secuestrados por los que se exige un rescate.

Existen distintas variantes de ransomware. El ransomware (y otro malware) se distribuye a menudo a través de campañas de spam por correo electrónico o mediante ataques selectivos. Los productos de Intel® Security utilizan varias tecnologías que ayudan a prevenir el ransomware. Los siguientes productos de McAfee® y sus correspondientes configuraciones están diseñadas para evitar muchos tipos diferentes de ransomware.

McAfee VirusScan® Enterprise 8.8 o McAfee Endpoint Security 10

- Mantenga actualizados los archivos DAT.
- Asegúrese de utilizar McAfee Global Threat Intelligence (McAfee GTI); contiene más de 8 millones de firmas de ransomware diferentes.
- Elabore reglas de protección de acceso para impedir la instalación y las cargas útiles del ransomware. Consulte los siguientes artículos sobre reglas de protección de acceso en la base de conocimientos: KB81095 y KB54812.

McAfee Host Intrusion Prevention

- Vea el vídeo sobre cómo configurar McAfee Host Intrusion Prevention para evitar la carga útil de CryptoLocker.
- Active la firma de Host Intrusion Prevention 3894, Access Protection—Prevent svchost.exe executing non-Windows executables (Protección de acceso: impedir que svchost.exe ejecute archivos ejecutables que no son de Windows).
- Active las firmas de Host Intrusion Prevention 6010 y 6011 para bloquear la inyección de forma inmediata.

intel Security

Reglas de McAfee Host Intrusion Prevention
McAfee Host Intrusion Prevention permite supervisar la creación de archivos y su lectura, escritura, ejecución, eliminación, cambio de nombre, modificación de atributos y creación de enlaces físicos. Defina sobre qué ruta/tipo de archivos desea o no activar alertas y qué ejecutables desea incluir (fuentes maliciosas conocidas) o excluir (generadores conocidos de falsos positivos). Esta regla puede llegar a ser invasiva, por lo que quizá deba utilizarla en modo de información/registro durante un periodo de prueba. Tenga en cuenta que las reglas de protección de archivos requieren la creación de una base de datos de aplicaciones de confianza.

Rule: Cryptolocker—block EXE in AppData

Rule type: files

Operations: create, execute, write

Parameters:
- Include: Files: **\AppData*.exe
- Include: Files: **\AppData\Local*.exe
- Include: Files: **\AppData\Roaming*.exe

Executables: Include *.*

En el ejemplo siguiente se han omitido muchas extensiones de archivo por limitaciones de espacio. Compruebe todas las extensiones de archivo que correspondan a sus aplicaciones.

Rule {

tag “Blocking a Non-Trusted program attempt to write to protected data file extensions”

Class Files

Id 4001

level 4

files {Include “**.3DS” “**.7Z” “**.AB4” “**.AC2” “**.ACCDB” “**.ACCDE” “**.ACCDR” “***.ACCDT” “**.ACR” “**.ADB” “**.AI” “**.AIT” “**.al” “**.APJ” “**.ARW” “**.ASM” “**.ASP” “**.BACKUP” “**.BAK” “**.BDB” “**.BGT” “**.BIK” “**.BKP” “**.BLEND” “**.BPW” “**.C” “**.CDF” “**. CDR” “**.CDX” “**.CE1” “**.CE2” “**.CER” “**.CFP” “**.SRF” “**.SRW” “**.ST4” “**.ST5” “**.ST6” “**.ST7” “**.ST8” “**.STC” “**.STD” “**. STI” “**.STW” “**.STX” “**.SXC” “**.SXD” “**.SXG” “**.SXI” “**.SXM” “**.SXW” “**.TXT” “**.WB2” “**.X3F” “**.XLA” “**.XLAM” “**.XLL” “**. XLM” “**.XLS” “**.XLSB” “**.XLSM” “**.XLSX” “**.XLT” “**.XLTM” “**. XLTX” “**.XLW” “**.XML” “**.ZIP”}

Executable {Include “*”}

user_name{Include “*”}

directives files:writefiles:renamefiles:delete

}

- Reglas de protección de acceso: también puede utilizar las reglas de protección de acceso para reforzar la regla de Host Intrusion Prevention utilizando la flexibilidad de los caracteres comodín: **\Users**\AppData***.exe

Nota: con las últimas versiones de SYSCore que se suministran con las versiones actualizadas de McAfee VirusScan Enterprise, McAfee Agent, Host Intrusion Prevention y Data Loss Prevention, al principio del campo "File or folder name to block" (Nombre de archivo o carpeta que bloquear) ya no funcionan los caracteres **. Con las últimas versiones, debe utilizarse el siguiente formato:

```
C:\**\AppData\**.exe
```

Está diseñado para bloquear todos los archivos .exe aleatorios en el directorio raíz y en todos los subdirectorios de la carpeta denominada AppData en cualquier lugar de la unidad C:.

Las posibles iteraciones de una regla de este tipo son casi ilimitadas, por lo que se deben considerar detenidamente todos los aspectos de la misma. Deberá analizar todos los aspectos de la regla, todas las entradas posibles para su función prevista y también cómo configurar las reglas en conjunto (vea el ejemplo siguiente):

```
Process to include: *

Process to exclude: [Dejar vacío]

File or folder name to block: <ruta o directorio>

File actions to prevent: [Las acciones que desee (se recomienda comenzar
por las menos agresivas para minimizar los posibles daños al endpoint)]
```

McAfee SiteAdvisor® Enterprise o Endpoint Security/Web Protection

- Utilice las reputaciones de sitios web para impedir el uso o advertir a los usuarios de sitios web en los que se distribuye ransomware.

McAfee Threat Intelligence Exchange y Advanced Threat Defense

- Configuración de directivas de Threat Intelligence Exchange:
  - Empiece en el modo de observación: a medida que se descubran procesos sospechosos en los endpoints, utilice etiquetas del sistema para aplicar las directivas de implementación de Threat Intelligence Exchange.
  - **Clean at: Known Malicious** (Limpiar si el nivel es Malicioso conocido).
  - **Block at: most likely malicious** (Bloquear si el nivel es probablemente malicioso) (bloquear si el nivel es **Unknown** [Desconocido] aumentaría la protección, pero quizá también añadiría más carga de trabajo administrativo).
  - **Submit files to McAfee Advanced Threat Defense** (Enviar archivos a McAfee Advanced Threat Defense) si el nivel es **Unknown** (Desconocido) e inferiores.
  - Directiva de Threat Intelligence Exchange: aceptar reputaciones de Advanced Threat Defense de archivos que McAfee Threat Intelligence Exchange aún no haya visto.
- Intervención manual de Threat Intelligence Exchange:
  - Implementación de la reputación de archivos (según el modo operativo): **Most Likely Malicious** (Probablemente malicioso): limpiar/eliminar.
  - **Might be Malicious** (Posiblemente malicioso): bloquear.
- La reputación de la empresa (organización) puede reemplazar la de McAfee GTI:
  - Puede optar por bloquear procesos no deseados, por ejemplo, una aplicación no admitida o vulnerable.
  - Marque el archivo como **Might be Malicious** (Posiblemente malicioso).
- O bien, puede autorizar un proceso no deseado para probar:
  - Marque el archivo como **Might be Trusted** (Posiblemente de confianza).

McAfee Advanced Threat Protection

- Funciones de detección incluidas en los productos:
  - Detección basada en firmas: McAfee Labs mantiene más de 8 millones de firmas de ransomware, incluidas las de CTB-Locker, CryptoWall y sus variantes.
  - Detección basada en la reputación: McAfee GTI.
  - Emulación y análisis estático en tiempo real: utilizados para la detección sin firmas.
  - Reglas YARA personalizadas.
  - Análisis de código estático completo: revierte la ingeniería del código de los archivos con el fin de evaluar todos los atributos y conjuntos de funciones, y analizar íntegramente el código fuente sin ejecutarlo.
  - Análisis dinámico en entornos aislados.
- Creación de perfiles de analizador donde es probable que se ejecute el ransomware:
  - Sistemas operativos habituales, Windows 7, Windows 8, Windows XP.
  - Instalación de aplicaciones Windows (Word, Excel) y activación de macros.
- Concesión de acceso a Internet al perfil de analizador:
  - Numerosas muestras ejecutan una secuencia de comandos de un documento de Microsoft que establece una conexión saliente y activa el malware. Al darle conexión a Internet al perfil de analizador aumentan las tasas de detección.

McAfee Network Security Platform

- Network Security Platform incluye firmas en sus directivas predeterminadas para detectar lo siguiente:
  - Verificar que cuenta con la firma id=0x4880f900 (específica de ransomware).
  - Network Security Platform también tiene firmas para identificar TOR, que puede utilizarse para transferir archivos relacionados con malware.
- Integración con Advanced Threat Defense para nuevas variantes de ataques:
  - Configure la integración con Advanced Threat Defense en una directiva de malware avanzado.
  - Configure Network Security Platform para enviar archivos .exe, de Microsoft Office, Java Archive y PDF a Advanced Threat Protection para su inspección.
  - Verifique que la configuración de Advanced Threat Protection se aplica a nivel de sensor.
- Actualice las reglas de detección de devoluciones de llamadas (redes de bots).

McAfee Web Gateway

- Active la inspección de McAfee Gateway Anti-Malware.
- Active McAfee GTI para conocer la reputación de URL y archivos.
- Integración con McAfee Advanced Threat Defense para la detección de amenazas de tipo zero-day y el uso de entornos aislados.

VirusTotal Convicter: intervención automatizada

- Convicter es una secuencia de comandos Python que activa el sistema de respuesta automática de McAfee ePolicy Orchestrator® (McAfee ePO™) para contrastar con VirusTotal los archivos que generan eventos de amenazas en McAfee Threat Intelligence Exchange.
- Tenga en cuenta que puede modificar la secuencia de comandos para incluir otros sistemas de intercambio de información sobre amenazas, como GetSusp.
- Si se alcanza el umbral de confianza de la comunidad, la secuencia de comandos establece automáticamente la reputación de la empresa.

- Umbral recomendado de identificación como malicioso: deben estar de acuerdo el 30 % de los proveedores y dos grandes compañías.
- Filtro: Target File Name Does Not Contain (El nombre de archivo seleccionado no contiene): McAfeeTestSample.exe.
- Esta es una herramienta gratuita que financia la comunidad (no McAfee/Intel Security).

McAfee Active Response
Active Response es una solución que busca y responde a las amenazas avanzadas. Cuando se utiliza junto a la información sobre amenazas que suministran McAfee GTI, Dell SecureWorks o ThreatConnect, es posible buscar y eliminar amenazas nuevas —incluidas las de ransomware— antes de que tengan oportunidad de extenderse.

- Los recopiladores personalizados permiten crear herramientas específicas para buscar e identificar indicadores de peligro asociados al ransomware.
- El usuario crea desencadenadores y reacciones para definir acciones cuando se cumplen determinadas condiciones. Por ejemplo, cuando se encuentran hashes o nombres de archivo, puede emprenderse automáticamente una acción de eliminación.

Para ampliar la información

Protecting Against Ransomware (Protección frente a ransomware)
Este artículo de la base de conocimientos ofrece a los clientes información detallada y actualizada para protegerse frente al ransomware en un entorno de Intel Security.

Para obtener información sobre las distintas variantes del ransomware CryptoLocker, así como sobre los síntomas, vectores de ataque y técnicas de prevención, vea los siguientes vídeos:

- CrytpoLocker Malware Session (Sesión sobre el malware CrytpoLocker)
- CryptoLocker Update (Actualización de CryptoLocker)

Notificación de amenazas de McAfee Labs: X97M/Downloader
Este artículo proporciona a los clientes un análisis detallado de la última versión de este ransomware.

Cómo derrotar al ransomware: evite el secuestro de sus datos
En las cinco páginas de este resumen de la solución se explica qué es el ransomware y cómo algunas de las soluciones de Intel Security (no todas) pueden ayudarle a protegerse de él.

Advice for Unfastening CryptoLocker Ransomware (Consejo para desbloquear el ransomware CryptoLocker)
Artículo detallado del blog sobre lo que debe hacer un cliente después de un ataque de este ransomware.

El ransomware está de vuelta: emergen nuevas familias con ansias de venganza
Artículo del informe de McAfee Labs sobre amenazas (página 14) que habla del nuevo ransomware y de su evolución.

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