Resumen de la solución

Protección de los sistemas de centros sanitarios frente al ransomware

El ransomware es malware que emplea normalmente cifrado asimétrico para secuestrar la información de la víctima a cambio de 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 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.

En los últimos años, el ransomware ha sido una de las mayores preocupaciones para todos los profesionales de la seguridad. Lamentablemente, el ransomware es una herramienta de ciberataque sencilla y eficaz que permite ganar dinero fácil. Durante el pasado año observamos que sus objetivos han cambiado: ya no son personas, sino empresas, porque estas pagan rescates más elevados. En los últimos tiempos los hospitales se han convertido en un blanco muy atractivo para los autores de ransomware. En el *Informe de McAfee Labs sobre amenazas: septiembre de 2016*, investigamos los ataques de ransomware que tuvieron lugar durante el primer y el segundo trimestre de 2016 en varios hospitales y concluimos que se trata de ataques selectivos relacionados entre sí que tuvieron éxito a pesar de ser relativamente poco sofisticados. Examinamos las dificultades que plantea el ransomware, específicamente en el ámbito hospitalario, debido a la escasez de seguridad de sistemas anticuados y dispositivos médicos, y a la necesidad de acceso inmediato a la información por cuestiones de vida o muerte.

intel Security

Recomendaciones y procedimientos para protegerse frente al ransomware

El paso más importante a la hora de proteger los sistemas contra el ransomware es ser consciente del problema y de cómo se propaga. Existen varias directivas y procedimientos que los hospitales pueden llevar a cabo para minimizar el éxito de los ataques de ransomware:

- Tener un plan de acción en caso de sufrir un ataque. Saber dónde se encuentran los datos importantes y saber si hay un método para filtrarlos. Realizar simulacros de recuperación frente a desastres y de continuidad del negocio con el equipo de gestión ante urgencias del hospital para validar el punto de recuperación y los objetivos de tiempo. Estos ejercicios pueden revelar consecuencias ocultas en las operaciones del hospital que de otra forma no se conocerían durante las pruebas de copia de seguridad habituales. La mayoría de los hospitales pagaron el rescate porque no contaban con un plan de contingencias.
- Mantener 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 compruebe que los parches se han aplicado correctamente.
- Para los sistemas y los dispositivos médicos más antiguos de los hospitales, a los que no se les pueden aplicar parches, limite el riesgo mediante el uso de tecnología de listas blancas de aplicaciones, que bloquea los sistemas e impide la ejecución de programas no autorizados. Separe estos sistemas y dispositivos de otras partes de la red mediante un firewall o un sistema de prevención de intrusiones. Desactive los servicios o puertos no necesarios en estos sistemas para reducir la exposición a posibles puntos de entrada de infecciones.
- Proteger los endpoints. Utilice protección para endpoints y sus funciones avanzadas. En muchos casos, el cliente se instala solamente con las funciones predeterminadas activadas. El uso de algunas funciones avanzadas —por ejemplo, "evitar que se ejecuten archivos .exe desde la carpeta Temp"— permitirá detectar y bloquear más malware.
- Si es posible, evitar el almacenamiento de datos confidenciales en discos locales. Pida a los usuarios que almacenen los datos en unidades de red seguras. De esta manera se limitará el tiempo de inactividad, ya que se puede volver a crear una imagen de los sistemas infectados fácilmente.
- Emplear soluciones antispam. La mayoría de las campañas de ransomware empiezan por un mensaje de correo electrónico de phishing que contiene un enlace o algún tipo de adjunto. En las campañas de phishing que incluyen el ransomware en un archivo .scr o algún otro formato de archivo poco común, resulta fácil definir una regla de spam que bloquee estos adjuntos. Si se autorizan los archivos .zip, analice al menos dos niveles del archivo .zip en busca de contenido malicioso.
- Bloquear los programas y el tráfico no deseado o innecesario. Si no necesita Tor, bloquee la aplicación y su tráfico en la red. A menudo el bloqueo de Tor impedirá que el ransomware obtenga la clave RSA pública desde el servidor de control, lo que a su vez impedirá el proceso de cifrado del ransomware.
- Añadir segmentación de red en los dispositivos importantes necesarios para proporcionar atención al paciente.
- Aislar las copias de seguridad en entornos protegidos. Asegúrese de que los sistemas de copias de seguridad, almacenamiento y cintas se encuentren en un lugar no accesible por los sistemas de las redes de producción. Si las cargas útiles recibidas como consecuencia de los ataques de ransomware se propagan lateralmente, podrían afectar a los datos de copias de seguridad.
- Utilizar una infraestructura virtual para registros médicos electrónicos importantes que esté aislada del resto de la red de producción.
- Llevar a cabo campañas continuas de concienciación de los usuarios. La mayoría de los ataques de ransomware empiezan por mensajes de correo electrónico de phishing, por lo que es extremadamente importante que los usuarios sean conscientes del peligro. 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.

Cómo puede ayudarle la tecnología de Intel Security a protegerse frente al ransomware

McAfee VirusScan Enterprise y McAfee Endpoint Security 10

- Con McAfee VirusScan Enterprise (VSE) o McAfee Endpoint Security (ENS), siga estas recomendaciones:
  - Utilice McAfee ePolicy Orchestrator (ePO) a diario para desplegar DAT actualizados.
  - Asegúrese de utilizar McAfee Global Threat Intelligence (McAfee GTI); contiene más de 7 millones de firmas de ransomware diferentes.
  - Defina reglas de protección de acceso para detener 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.
  - Utilice Contención dinámica de aplicaciones para evitar que las aplicaciones desconocidas realicen actividades maliciosas.

McAfee Threat Intelligence Exchange

- Con McAfee Threat Intelligence Exchange (TIE) siga estas recomendaciones:
  - Comience en modo de observación.
  - A medida que se descubran procesos sospechosos en los endpoints, utilice etiquetas del sistema para aplicar las directivas de implementación de McAfee TIE.
  - Aplique **Clean at Reputation: Known Malicious** (Limpiar si la reputación es Malicioso conocido).
  - Aplique **Block at Reputation: Most Likely Malicious** (Bloquear si la reputación 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 (ATD)** (Enviar archivos a McAfee Advanced Threat Defense) si el nivel es **Unknown** (Desconocido) e inferiores.
  - Directiva de servidor de TIE: aceptar reputaciones de McAfee ATD de archivos que McAfee TIE aún no haya visto.
- Intervención manual de McAfee 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) tiene prioridad sobre 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).
  - Introduzca los datos de reputación externos en McAfee TIE mediante indicadores de riesgo.

McAfee Advanced Threat Defense

- McAfee Advanced Threat Defense ofrece las siguientes funciones de detección en bandeja de entrada:
  - Detección basada en firmas: McAfee Labs mantiene más de 150 millones de firmas, incluidas las de CTB-Locker, CryptoWall y sus variantes.
  - Detección basada en la reputación: McAfee GTI.
  - Análisis y emulación estáticos en tiempo real: utilizados para la detección sin firmas.
  - Reglas YARA personalizadas.
  - Análisis del código completamente estático: 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:
  - SO habituales, Windows 7, Windows 8, Windows XP.
  - Instalación de aplicaciones Windows (Word, Excel) y activación de macros.

- Definición de distintos perfiles del analizador exclusivos para distintos sistemas operativos con acceso a Internet:
  - Numerosas muestras ejecutan una secuencia de comandos de un documento de Microsoft Office que establece una conexión saliente y activa el malware. Al darle conexión a Internet al perfil de analizador, aumentan las tasas de detección.

McAfee Application Control

- McAfee Application Control proporciona protección con una lista blanca de aplicaciones. Es ideal para proteger todo tipo de dispositivos, en particular:
  - Dispositivos estáticos, como los dispositivos médicos.
  - Sistemas con sistemas operativos antiguos que ya no reciben actualizaciones.
  - Servidores de aplicaciones que proporcionan servicios limitados.
  - Sistemas que no se cambian con frecuencia.
- Instalación inicial
  - McAfee Application Control analizará completamente un sistema durante la instalación, creará el inventario de endpoints y definirá las aplicaciones de la lista blanca.
- Modo de observación
  - Permite a los administradores controlar las aplicaciones nuevas que se instalan o ejecutan, con la opción de incluirlas en una lista blanca centralizada si se decide que están autorizadas.
  - Facilita el proceso de creación de la lista blanca mediante la identificación de las nuevas actualizaciones de confianza para las aplicaciones del entorno.
  - Identifica métodos para actualizar la lista blanca, como procesos, certificados, directorios o usuarios aprobados.
- Modo de autoaprobación
  - Los usuarios podrán aprobar las aplicaciones que no estén en la lista blanca. De esta forma se aumenta la flexibilidad y se reduce el impacto en la empresa.
  - Los administradores podrán supervisar de manera centralizada el contenido aprobado por el usuario y aceptar o revocar la autorización de la aplicación, según su reputación y las directivas de la empresa.
- Implementación de la lista blanca
  - El sistema está totalmente protegido frente a aplicaciones desconocidas, incluidas las maliciosas como el ransomware.
  - Proporciona un aviso al usuario final para el procedimiento de aprobación de los nuevos ejecutables.

Más información

Comunidad Intel Security Expert Center

- McAfee VirusScan Enterprise
- McAfee Endpoint Security
- McAfee Threat Intelligence Exchange
- McAfee Advanced Threat Defense
- McAfee Application Control

916_0816_brf_protecting-health-care-systems-ransomware

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