RANSOMWARE

Qué es y qué hacer al respecto

¿QUÉ ES EL RANSOMWARE?

El ransomware es un tipo de software malicioso que los delincuentes cibernéticos utilizan para negar el acceso a sistemas o datos. El actor cibernético malicioso retiene los sistemas o los datos como rehenes hasta que se paga el rescate. Después de la infección inicial, el ransomware intenta propagarse a unidades de almacenamiento compartidas y a otros sistemas accesibles. Si no se cumplen las demandas, el sistema o los datos encriptados no van a estar disponibles, o pueden ser eliminados.

¿CÓMO PROTEJO MIS REDES?

Un compromiso con la higiene cibernética y las mejores prácticas es fundamental para proteger sus redes. Aquí hay algunas preguntas que puede hacerle a su organización para ayudar a prevenir ataques de ransomware:

1. **Copias de seguridad**: ¿Hacemos copias de seguridad de toda la información crítica? ¿Las copias de seguridad se almacenan fuera de línea? ¿Hemos probado nuestra capacidad para volver a las copias de seguridad durante un incidente?
2. **Análisis de riesgo**: ¿Hemos realizado un análisis de riesgos de ciberseguridad de la organización?
3. **Entrenamiento del personal:** ¿Hemos capacitado al personal en las mejores prácticas de ciberseguridad?
4. **Parcheo de vulnerabilidades:**¿Hemos implementado parches apropiados para las vulnerabilidades ya conocidas en el sistema?
5. **Lista blanca de aplicaciones:** ¿Permitimos que solo se ejecuten programas aprobados en nuestras redes?
6. **Respuesta al incidente:** ¿Tenemos un plan de respuesta a incidentes y lo hemos ejercido?
7. **Continuidad de operaciones**: ¿Somos capaces de mantener las operaciones sin acceso a ciertos sistemas? ¿Por cuánto tiempo? ¿Hemos probado esto?
8. **Pruebas de penetración**: ¿Hemos intentado piratear nuestros propios sistemas para probar la seguridad de nuestros sistemas y nuestra capacidad para defendernos de los ataques?

¿CÓMO RESPONDO AL RANSOMWARE?

Implemente su respuesta a incidentes de seguridad y su plan de continuidad operacional. Los profesionales de IT de su organización pueden tardar un tiempo en aislar y eliminar la amenaza de ransomware de sus sistemas y restaurar los datos y las operaciones regulares. Mientras tanto, debe tomar medidas para mantener las funciones esenciales de su organización de acuerdo con su plan de continuidad operacional. Las organizaciones deben mantener y probar periódicamente los planes de copias de seguridad, los planes de recuperación ante desastres y los procedimientos de continuidad operacionales.

Comuníquese con la policía de inmediato. Le recomendamos que se ponga en contacto con una oficina local del FBI[1] o USSS[2] inmediatamente para reportar un evento de ransomware y solicitar ayuda.

Hay riesgos serios que debe considerar antes de pagar el rescate. No sugerimos pagar un rescate. Entendemos que cuando las empresas se enfrentan a la posibilidad de no poder funcionar, los ejecutivos evaluarán todas las opciones para proteger a sus accionistas, empleados y clientes. Al tomar su decisión, tenga en cuenta los siguientes riesgos:

- Pagar un rescate no garantiza que una organización recuperará el acceso a sus datos; de hecho, algunas personas u organizaciones nunca recibieron claves de descifrado después de haber pagado un rescate.
- Algunas víctimas que pagaron el rescate, informaron que fueron atacados nuevamente por actores cibernéticos.
- Después de pagar el rescate exigido originalmente, a algunas víctimas se les exigió pagar más para obtener la clave de descifrado previamente prometida.
- Pagar podría alentar este modelo de negocio delictivo de manera inadvertida.

[1] https://www.fbi.gov/contact-us/field/listing_by_state
[2] http://www.secretservice.gov/contact/

Cómo proteger sus redes del

RANSOMWARE

Este documento es una guía de orientación técnica interinstitucional del gobierno de los EE. UU. destinado a informar a los Directores de Información y a los Directores de Seguridad Informática en entidades de infraestructura crítica, incluidas organizaciones pequeñas, medianas y grandes. Este documento proporciona un conjunto de las mejores prácticas y estrategias de mitigación ya existentes, del gobierno federal y de la industria privada, enfocadas en la prevención y la respuesta a incidentes de ransomware.

Protegiendo sus redes del ransomware

El ransomware es la amenaza de malware de más rápido crecimiento y tiene como objetivo a usuarios de todo tipo, desde el usuario doméstico hasta la red corporativa. En promedio, se han producido más de 4000 ataques diarios de ransomware desde el 1 de enero de 2016. Este es un aumento del 300 por ciento con respecto a los aproximadamente 1000 ataques diarios registrados en 2015. Existen acciones de prevención y de respuesta muy efectivas que pueden mitigar significativamente el riesgo que significa para su organización.

El ransomware es dirigido en contra de usuarios domésticos, empresas y redes gubernamentales y puede provocar la pérdida temporal o permanente de información confidencial o patentada, la interrupción de las operaciones regulares, las pérdidas financieras incurridas para restaurar los sistemas y archivos, y el daño potencial a la reputación de una organización.

El ransomware puede exigirle a un usuario que haga clic en un enlace con el fin pagar un rescate; sin embargo, dicho enlace puede ser malicioso y provocar infecciones de malware adicionales. Algunas variantes de ransomware contienen mensajes intimidantes, tales como:

> “Su computadora fue utilizada para visitar sitios web con contenido ilegal. Para desbloquear su computadora, debe pagar una multa de $100”.

> “Solo tiene 96 horas para enviar el pago. Si no envía el dinero dentro del plazo previsto, todos sus archivos se codificarán de forma permanente y nadie podrá recuperarlos”.

¿Qué es el Ransomware?

El ransomware es una forma de malware que selecciona como objetivo a sus datos y sistemas críticos con el fin de extorsionarlo.
El ransomware se instala con frecuencia a través de correos electrónicos de spearphishing. Una vez que el usuario ha sido bloqueado de los datos o del sistema, el actor cibernético malicioso exige el pago de un rescate. Después de recibir el pago, dicho actor cibernético está supuesto a proporcionar a la víctima un mecanismo para recuperar el acceso al sistema o los datos.
Las iteraciones recientes han sido dirigidas a los usuarios finales de productos empresariales, lo que hace que la concientización y la capacitación sean una medida preventiva crítica.

Protegiendo sus redes

Educar a su personal

Los atacantes a menudo ingresan a la organización engañando a un usuario para que revele una contraseña o haga clic en un archivo adjunto de correo electrónico infectado con virus.

Recuerde a los empleados que nunca deben clic en enlaces no solicitados, ni abrir archivos adjuntos no solicitados en correos electrónicos. Para mejorar la concientización de la fuerza laboral, el equipo de seguridad interna puede probar la capacitación de la fuerza laboral de una organización con correos electrónicos de phishing simulados[1]

La prevención proactiva es la mejor defensa

La prevención es la defensa más eficaz contra el ransomware y es fundamental tomar precauciones para protegerse. Las infecciones pueden ser devastadoras para una persona u organización, y la recuperación puede ser un proceso difícil que requiere los servicios de un especialista en recuperación de datos acreditado.

El gobierno de los EE. UU. (USG, por sus siglas en inglés) recomienda que los usuarios y administradores tomen las siguientes medidas preventivas para evitar que sus redes informáticas sean víctimas de una infección de ransomware:

Medidas preventivas

- Implementar un programa de concientización y capacitación. Debido a que los usuarios finales son seleccionados como objetivos, los empleados y las personas deben conocer la amenaza del ransomware y cómo se puede infiltrar.
- Habilitar sólidos filtros de correo no deseado para evitar que los correos electrónicos de phishing lleguen a los usuarios finales y autentiquen el correo electrónico entrante utilizando tecnologías como el marco de políticas del remitente (SPF), el informe y conformidad de autenticación de mensajes de dominio (DMARC) y el correo identificado con claves de dominio (DKIM) para evitar la suplantación de correo electrónico.
- Analizar todos los correos electrónicos entrantes y salientes para detectar amenazas y filtrar los archivos ejecutables para que no lleguen a los usuarios finales.
- Configurar firewalls para bloquear el acceso a direcciones IP maliciosas conocidas.
- Hacer uso de parches para sistemas operativos, software y firmware en los dispositivos. Considere usar un sistema de administración de parches centralizado.
- Configurar los programas antivirus y anti-malware para realizar análisis regulares automáticamente.
- Administrar el uso de cuentas privilegiadas según el principio de privilegio mínimo: No se debe asignar acceso administrativo a ningún usuario a menos que sea absolutamente necesario; y aquellos que necesiten cuentas de administrador solo deben usarlas cuando sea necesario.

[1] Para obtener información adicional sobre cómo evitar ataques de ingeniería social y phishing, consulte la sugerencia de seguridad de US-CERT (ST04-014), disponible en: https://www.us-cert.gov/ncas/tips/ST04-014

- Configurar los controles de acceso, incluidos los permisos para compartir archivos, directorios y redes, teniendo en cuenta los privilegios mínimos. Si un usuario solo necesita leer archivos específicos, el usuario no debe tener acceso para escribir sobre esos archivos, directorios o recursos compartidos.
- Deshabilitar los scripts de macros de los archivos de Office enviados por correo electrónico. Considere usar el software Office Viewer para abrir archivos de Microsoft Office enviados por correo electrónico en lugar de aplicaciones completas de la suite informática.
- Implementar políticas de restricción de software (SRP) u otros controles para evitar que los programas se ejecuten desde ubicaciones comunes de ransomware, como carpetas temporales compatibles con navegadores de Internet populares o programas de compresión/ descompresión, incluyendo la carpeta AppData/LocalAppData.
- Considerar deshabilitar el protocolo de escritorio remoto (RDP) si no se está utilizando.
- Usar la lista blanca de aplicaciones, que solo permite que los sistemas ejecuten programas conocidos y permitidos por la política de seguridad.
- Ejecutar entornos de sistemas operativos o programas específicos en un entorno virtualizado.
- Clasificar los datos según el valor organizacional e implemente la separación física y lógica de redes y datos para diferentes unidades organizacionales.

Consideraciones para la continuidad operacional

- Generar regularmente copias de seguridad de los datos. Verifique la integridad de esas copias de seguridad y pruebe el proceso de restauración para asegurarse de que funciona.
- Realizar una prueba anual de penetración y una evaluación de vulnerabilidad.
- Asegurar sus copias de seguridad. Este seguro de que las copias de seguridad no estén conectadas permanentemente a las computadoras y redes de las que están haciendo copias de seguridad. Algunos ejemplos son la protección de copias de seguridad en la cloud o el almacenamiento físico de copias de seguridad fuera de línea. Algunas instancias de ransomware tienen la capacidad de bloquear las copias de seguridad ubicadas en la nube cuando los sistemas realizan copias de seguridad continuas en tiempo real, lo que también se conoce como sincronización persistente. Las copias de seguridad son críticas en la recuperación y respuesta de ransomware; si su sistema está infectado, una copia de seguridad puede ser la mejor manera de recuperar sus datos críticos.

Qué hacer si está infectado con ransomware

Si las medidas preventivas fallan, el USG recomienda que las organizaciones consideren tomar los siguientes pasos ante una infección con ransomware:

- **Aislar la computadora infectada inmediatamente.** Los sistemas infectados deben eliminarse de la red lo antes posible para evitar que el ransomware ataque la red o las unidades compartidas.
- **Aislar o apagar los dispositivos afectados que aún no se hayan dañado por completo.** Esto puede dar más tiempo para limpiar y recuperar datos, contener daños y evitar el empeoramiento de las condiciones.

- **Asegurar inmediatamente los datos o sistemas de copia de seguridad colocándolos fuera de línea.** Asegúrese de que las copias de seguridad estén libres de malware.

- **Comunicarse con la policía de inmediato.**Le recomendamos encarecidamente que se ponga en contacto con una oficina local de el Bureau Federal de Investigaciones (FBI) o del Servicio Secreto de los EE. UU. inmediatamente después de haber descubierto un evento de ransomware con el fin de reportarlo y de solicitar asistencia.

- **De estar disponible, recopilar y asegurar partes parciales de los datos rescatados que puedan existir.**

- **De ser posible, cambiar todas las contraseñas de cuentas en línea y contraseñas de red después de quitar el sistema de la red.** Además, cambie todas las contraseñas del sistema una vez que se elimine el malware del sistema.

- **Borrar los valores y archivos en el registro para evitar que el programa cargue.**

Implemente su respuesta a incidentes de seguridad y su plan de continuidad operacional. Idealmente, las organizaciones se han de asegurar de tener copias de seguridad adecuadas, por lo que su respuesta a un ataque será simplemente restaurar los datos de una copia de seguridad no infectada y conocida. Tener una copia de seguridad de datos puede eliminar la necesidad de pagar un rescate para recuperar los datos.

Hay riesgos serios a considerar antes de pagar el rescate. El USG no sugiere el pago de un rescate a los actores criminales. Sin embargo, después de que los sistemas se han visto comprometidos, pagar un rescate es una decisión seria que requiere la evaluación de todas las opciones para proteger a los accionistas, empleados y clientes. Las víctimas querrán evaluar la viabilidad técnica, la oportunidad y el costo de reiniciar los sistemas desde la copia de seguridad. Las víctimas de ransomware también pueden considerar los siguientes factores:

- Pagar un rescate no garantiza que una organización recuperará el acceso a sus datos; de hecho, algunas personas u organizaciones nunca recibieron claves de descifrado después de haber pagado un rescate.
- Algunas víctimas que pagaron la demanda fueron atacadas nuevamente por ciberactore maliciosos.
- Después de pagar el rescate exigido originalmente, se le pidió a algunas víctimas que pagaran más para obtener la clave de descifrado previamente prometida.
- Pagar podría alentar este modelo de negocio delictivo de manera inadvertida.

Cómo pueden ayudar las fuerzas del orden

Cualquier entidad infectada con ransomware debe comunicarse con las autoridades de inmediato. Las fuerzas del orden pueden hacer uso de autoridades y herramientas legales que no están disponibles para la mayoría de las organizaciones. Las fuerzas del orden pueden solicitar la asistencia de socios internacionales encargados de hacer cumplir la ley para localizar los datos robados o encriptados o identificar al perpetrador. Estas herramientas y relaciones pueden aumentar en gran medida las probabilidades de detener con éxito al criminal, evitando así futuras pérdidas.

La policía federal da prioridad a la realización de investigaciones cibernéticas de modo que cause una interrupción menor en las operaciones normales de la entidad víctima, al tiempo que busca trabajar de manera cooperativa y discreta con esa entidad. La policía federal utiliza medidas de investigación que evitan el tiempo de inactividad innecesario o el desplazamiento de los empleados de una empresa. La policía federal coordina estrechamente sus actividades con la organización afectada para evitar la divulgación injustificada de información.

A medida que una entidad afectada se recupera de un incidente de seguridad cibernética, la entidad debe iniciar medidas para prevenir incidentes similares. Los organismos encargados de hacer cumplir la ley y el Centro Nacional de Integración de Comunicaciones y Ciberseguridad del Departamento de Seguridad Nacional pueden ayudar a las organizaciones a implementar medidas en contra y proporcionar información y mejores prácticas para evitar incidentes similares en el futuro. Además, la organización afectada debe realizar una revisión posterior de su respuesta al incidente y evaluar las fortalezas y debilidades de su plan de respuesta al incidente.

Variantes de ransomware[2]

El ransomware es una actividad delictiva en crecimiento que involucra numerosas variantes. Desde 2012, cuando surgieron por primera vez variantes de ransomware de casilleros policiales, las variantes de ransomware se han vuelto más sofisticadas y destructivas. Algunas variantes encriptan no solo los archivos en el dispositivo infectado, sino también el contenido de las unidades compartidas o en red, los dispositivos de medios de almacenamiento conectados externamente y los servicios de almacenamiento en la nube que están asignados a las computadoras infectadas. Estas variantes se consideran destructivas porque encriptan los archivos de los usuarios y las organizaciones y los inutilizan hasta que se paga un rescate.

Recientes investigaciones federales realizadas por el FBI revelan que los autores de ransomware continúan mejorando el código de ransomware mediante el uso de servicios de anonimización como “Tor3” para la comunicación de extremo a extremo con los sistemas infectados y la moneda virtual Bitcoin para cobrar los pagos de rescate. Actualmente, las cinco principales variantes de ransomware dirigidas a empresas e individuos estadounidenses son CryptoWall, CTB-Locker, TeslaCrypt, MSIL/ Samas y Locky. Continuamente surgen nuevas variantes de ransomware.

CryptoWall

El CryptoWall y sus variantes se han utilizado activamente para atacar a las víctimas estadounidenses desde abril de 2014. CryptoWall fue la primera variante de ransomware que solo aceptaba pagos de rescate en Bitcoin. Los montos de rescate asociados con CryptoWall suelen oscilar entre $ 200 y $ 10,000.
Tras el desmantelamiento de la botnet CryptoLocker, CryptoWall se ha convertido en la variante de ransomware más exitosa con víctimas en todo el mundo. Entre abril de 2014 y junio de 2015, IC3

2 Para obtener más información sobre las variantes de Ransomware y otros recursos, visite https://www.us- cert.gov/ncas/alerts/TA16-091A
3 Tor es un software gratuito que permite la comunicación anónima. Tor dirige el tráfico de Internet a través de una red de voluntarios mundial y gratuita que consta de más de 7000 repetidores para ocultar la ubicación y el uso de un usuario de cualquier persona que haga vigilancia en la red o análisis de tráfico. (El nombre deriva del nombre del proyecto de software original, The Onion Router.)

recibió 992 quejas relacionadas con CryptoWall, y las víctimas reportaron pérdidas por un total de más de $18 millones.[4] CryptoWall se propaga principalmente a través de correo electrónico no deseado, pero también infecta a las víctimas a través de descargas ocultas[5] y publicidad maliciosa[6].

Casillero CTB

CTB-Locker surgió en junio de 2014 y es una de las primeras variantes de ransomware en usar Tor para su infraestructura C2. CTB-Locker usa Tor exclusivamente para sus servidores C2 y solo se conecta a C2 después de encriptar los archivos de las víctimas. Además, a diferencia de otras variantes de ransomware que utilizan la red Tor para algunas comunicaciones, los componentes Tor están integrados en el malware CTB-Locker, lo que lo hace más eficiente y más difícil de detectar. CTB-Locker se propaga a través de descargas ocultas y correos electrónicos no deseados.

TeslaCrypt

TeslaCrypt surgió en febrero de 2015, inicialmente dirigido a la comunidad de videojuegos mediante la encriptación de archivos de juegos. Estos archivos fueron atacados además de los archivos típicamente atacados por ransomware (documentos, imágenes y archivos de bases de datos). Una vez que se cifraron los datos, TeslaCrypt intentó eliminar todas las instantáneas de volumen y los puntos de restauración del sistema para evitar la recuperación de archivos. TeslaCrypt se distribuyó a través de los kits de explotación Angler, Sweet Orange y Nuclear.

MSIL o Samas (SAMSAM)

MSIL o Samas (SAMSAM) se utilizó para comprometer las redes de múltiples víctimas de EE. UU., incluidos los ataques de 2016 a instalaciones de atención médica que ejecutaban versiones obsoletas de la aplicación de administración de contenido JBoss. SAMSAM explota servidores web vulnerables basados en Java. SAMSAM utiliza herramientas de código abierto para identificar y compilar una lista de hosts que informan al directorio activo de la víctima. Luego, los actores usan psexec.exe para distribuir el malware a cada host en la red y encriptar la mayoría de los archivos en el sistema. Los actores cobran cantidades variables en Bitcoin para proporcionar las claves de descifrado a la víctima.

Bloqueado

A principios del 2016, se observó que una variante de ransomware destructiva, Locky, infectaba computadoras pertenecientes a empresas de todo el mundo, incluidas las de Estados Unidos, Nueva Zelanda, Australia, Alemania y el Reino Unido. Locky se propaga a través de correos electrónicos no deseados que incluyen documentos maliciosos de Microsoft Office o archivos adjuntos comprimidos (por ejemplo, .rar, .zip) que anteriormente estaban asociados con troyanos bancarios como Dridex y Pony. Los archivos adjuntos maliciosos contienen macros o archivos JavaScript para descargar los archivos de Locky.
Recientemente, este ransomware también se distribuyó utilizando el Nuclear Exploit Kit.

---

[4] Este número incluye los costos adicionales incurridos por la víctima. Los gastos pueden estar asociados con la mitigación de la red, las contramedidas de la red, la pérdida de productividad, los honorarios legales, los servicios de TI y la compra de servicios de monitoreo de crédito para empleados o clientes.

[5] Drive by download" es la transferencia de software malicioso a la computadora de la víctima sin el conocimiento o ninguna acción por parte de la víctima.

[6] "Malvertizing" es el uso de anuncios maliciosos en sitios web legítimos. Estos anuncios maliciosos contienen un código que infectará la computadora de un usuario sin ninguna acción por parte del usuario (es decir, el usuario no tiene que hacer clic en el anuncio para infectarse).

Enlaces a otros tipos de malware

Los sistemas infectados con ransomware también suelen estar infectados con otro malware. En el caso de CryptoLocker, un usuario generalmente se infectaba al abrir un archivo adjunto malicioso de un correo electrónico. Este archivo adjunto malicioso contenía Upatre, un descargador que infectaba al usuario con GameOver Zeus. GameOver Zeus era una variante del troyano Zeus que se utilizaba para robar información bancaria y otros tipos de datos. Después de que un sistema se infectara con GameOver Zeus, Upatre también descargaría CryptoLocker. Finalmente, CryptoLocker encriptó archivos en el sistema infectado y exigió el pago de un rescate.

La operación de interrupción contra la botnet GameOver Zeus también afectó a CryptoLocker, lo que demuestra los estrechos vínculos entre el ransomware y otros tipos de malware. En junio de 2014, una operación policial internacional debilitó con éxito la infraestructura de GameOverZeus y CryptoLocker.

Recursos del Gobierno Federal

Informes

Federal Bureau of Investigation

Grupos operativos de actividad cibernética
www.fbi.gov/contact-us/field
Centro de denuncias de delitos en internet
www.ic3.gov

United States Secret Service

Grupos operativos de delitos electrónicos
www.secretservice.gov/investigation/#field

Oficinas Locales
www.secretservice.gov/contact/

Mitigación

Department of Homeland Security
United States Computer Emergency Readiness Team (US-CERT)

www.us-cert.gov

Marco de Seguridad Cibernética NIST:
http://www.nist.gov/cyberframework/

Estrategias Top 10 de Mitigación de Aseguramiento de la Información NSA/IAD :
https://www.iad.gov/iad/library/ia-guidance/iads-top-10-information-assurance-mitigation-strategies.cfm