COHESITY

DOCUMENTO TÉCNICO

Su hoja de ruta hacia la resiliencia frente al ransomware

ÍNDICE

Resiliencia cibernética frente a resiliencia de datos

La mayoría de las empresas tienen una estrategia de resiliencia de datos en forma de continuidad del negocio y recuperación después de un desastre (BC/DR), pero la tecnología y los procesos diseñados para la resiliencia de **datos** no siempre conducen a una verdadera resiliencia **cibernética** en la era del ransomware.

La creación de una empresa con resiliencia cibernética requiere comunicación, colaboración, herramientas de seguridad, sistemas de autenticación, plataformas de respaldo y una serie de otros sistemas para lo siguiente:

- Investigar cómo ocurrió el ataque
- Comunicarse con los titulares de los datos afectados, los reguladores y las fuerzas del orden público
- Mitigar la amenaza de recurrencia
- Recuperarse para reanudar la producción

Los ciberataques destructivos, también conocidos como ataques de wiper, cambian el flujo tradicional de detección, respuesta y recuperación para que sea más iterativo, con la necesidad de recuperar las capacidades de respuesta y comunicación antes de que incluso puedan comenzar los flujos de trabajo de investigación. En estos casos, la plataforma de copia de seguridad y recuperación se vuelve fundamental para servir como una fuente autorizada de análisis forense para los equipos de respuesta ante incidentes.

Para lograr la resiliencia cibernética y soportar los ciberataques modernos, las empresas deben considerar dos áreas que son fundamentales para el éxito:

1. La capacidad de recuperarse debe estar fuera del alcance de los adversarios.
2. La planificación de la respuesta debe tener disposiciones para la recuperación rápida no solo de los sistemas de producción, sino también de las plataformas de seguridad, autenticación y comunicaciones necesarias para responder con eficacia y eficiencia al incidente.

La naturaleza iterativa de recuperación-respuesta-recuperación en ataques de ransomware y wiper requiere que los equipos de Seguridad y Operaciones de TI trabajen estrechamente para minimizar el impacto de dichos ataques.

Creación de un programa de resiliencia cibernética

En escenarios tradicionales de BC/DR como inundaciones, incendios y desastres naturales, la causa fundamental del evento puede determinarse rápidamente. En el caso de un ataque de ransomware, un adversario está trabajando activamente para detener cualquier recuperación y garantizar que la única opción de la víctima sea pagar un rescate.

Estos atacantes se adaptan continuamente a las defensas del objetivo, lo que hace que una investigación prescriptiva y un programa de respuesta sean invaluables para establecer la naturaleza del ataque y comprender el proceso correcto para recuperarse. La investigación también permite a las organizaciones tener visibilidad de las vulnerabilidades que permitieron que el ataque tuviera éxito y reforzar las defensas para prevenir futuros incidentes. Esto contrasta con un desastre tradicional, en el que la respuesta puede ser casi instantánea.

Para ser resiliente ante un ciberataque, o sobrevivir a este, se requiere más que solo un plan para usar la tecnología. Los equipos de TI y seguridad deben entender a los atacantes y los tipos de ataques que están lanzando. Este tipo de inteligencia les permite crear defensas dirigidas, lo que les da una mejor oportunidad de bloquear los ataques o detectarlos con anticipación. Los marcos como MITRE ATT&CK permiten a las organizaciones cuantificar las amenazas y comunicar las correcciones de manera estandarizada.

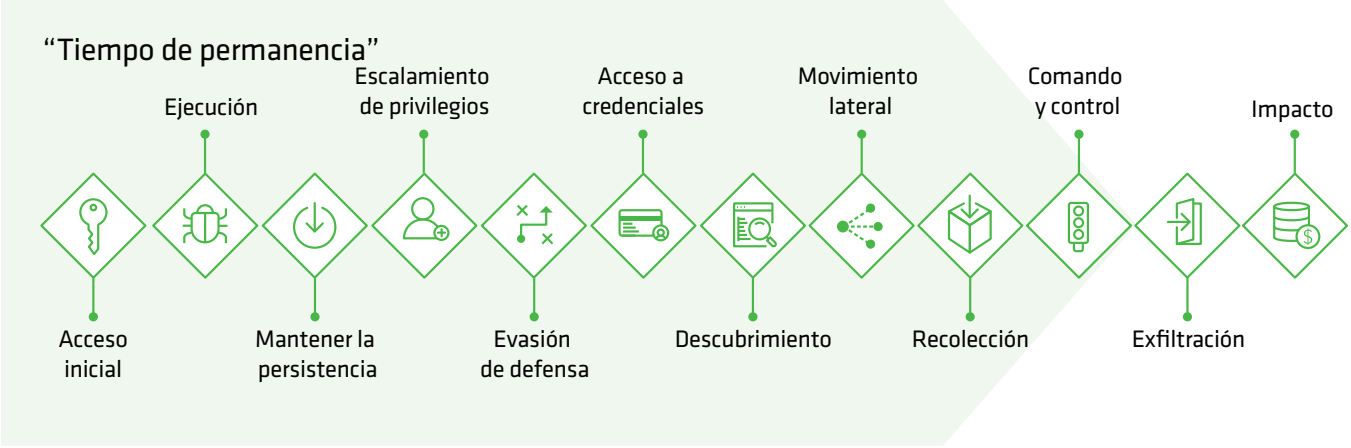
Por ejemplo, el siguiente diagrama muestra lo que los atacantes pueden hacer mientras permanecen en el entorno antes de que se active el ransomware. En algunos casos, estas podrían ser acciones necesarias para que la carga útil del ransomware tenga éxito, mientras que en otros, podría ayudar al atacante a permanecer persistente en la red y lanzar futuros ataques. El "tiempo de permanencia" puede ser de días a meses. Saber cómo opera un adversario en el entorno permite a los equipos de seguridad buscar indicadores de un ataque de manera proactiva.

> El tiempo de permanencia se refiere a la cantidad de tiempo que un actor malicioso tiene acceso a un sistema comprometido antes de que se detecte el ataque. El tiempo de permanencia más prolongado crea más oportunidades para que un atacante cause daños o robe información confidencial.

Considere cada acción en el diagrama como una etapa del ataque. Puede resultar sorprendente que 10 de las 12 etapas se ejecuten incluso antes de que se active la carga útil. En el caso de un ataque de ransomware, los sistemas se ven completamente comprometidos antes de que comience cualquier cifrado o exfiltración de datos. Tener este punto de apoyo en la red permite a los atacantes frustrar los esfuerzos de recuperación y lanzar nuevos ataques para exigir múltiples rescates. Esto se denomina ransomware de "doble burbuja" o "doble extorsión" y es una forma cada vez más popular para que los atacantes creen un flujo de ingresos constante.

Para la víctima, un solo ataque puede ser devastador, ya que puede impedir que entregue bienes y servicios. Pero estar sujeto a múltiples ataques aumenta la probabilidad de pérdidas secundarias, que incluyen:

- Daño a la reputación
- Litigios de los socios y los titulares de los datos
- Multas regulatorias por no proteger adecuadamente la información del titular de los datos



Para complicar aún más la situación, mientras más tiempo se permita que un atacante permanezca en la red, mayor será la probabilidad de que los artefactos del ataque se almacenen en las copias de seguridad. Si estos artefactos se recuperan sin identificarse y eliminarse, el ataque puede reiniciarse. Los escenarios como este se desarrollan con frecuencia cuando las organizaciones que se han recuperado de los ataques de ransomware no garantizan que estén recuperando datos limpios.

Las organizaciones deben seguir los procesos de análisis forense digital y respuesta a incidentes (DFIR) para garantizar que se recuperen datos limpios dentro de los centros de operaciones de seguridad. Históricamente, el DFIR se ha basado en lo siguiente:

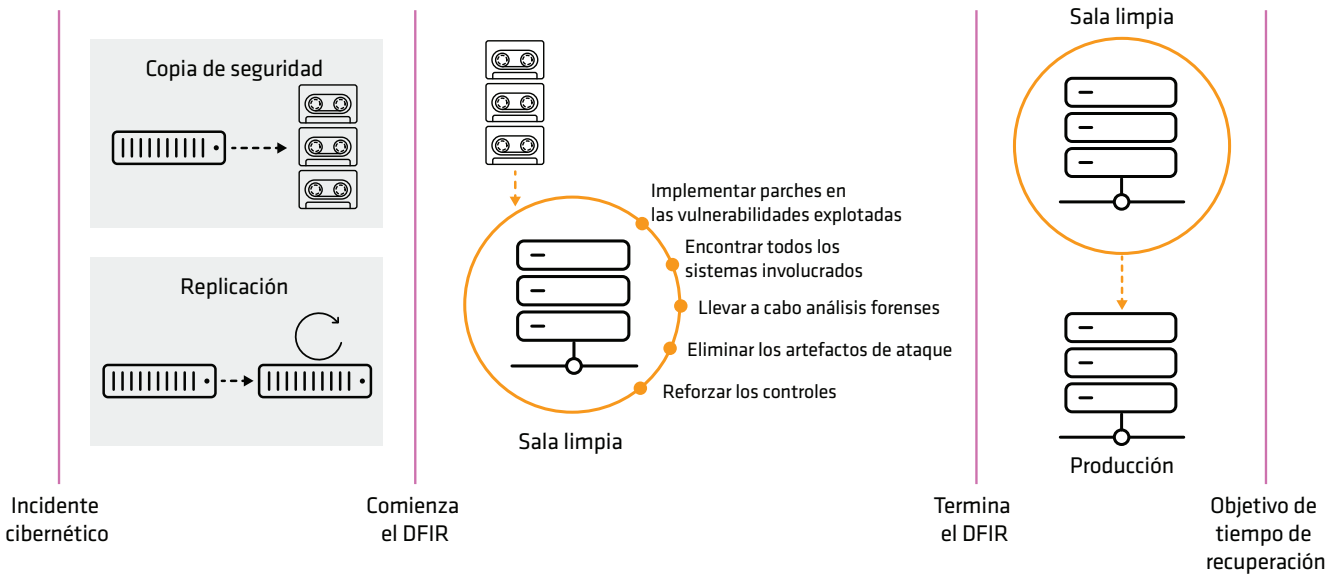
- obtener una imagen forense de un equipo host comprometido;
- aplicar procesos de investigación y herramientas para identificar la cronología del incidente;
- encontrar y analizar los artefactos binarios que se utilizaron en el ataque;
- descubrir los métodos de escalada de privilegios y persistencia utilizados;
- búsqueda de otros sistemas comprometidos para ampliar el alcance del incidente;
- búsqueda de vulnerabilidades que deben corregirse antes de que una plataforma se reintegre al entorno de producción, y
- averiguar por qué los controles preventivos y de detección no detuvieron ni detectaron el ataque.

Por lo general, estas tareas se llevan a cabo en un entorno de recuperación aislado (IRE) o en un entorno de "clean room".

Por supuesto, obtener imágenes forenses de un sistema que ha sido borrado o cifrado no proporcionará evidencia significativa, por lo que los equipos de respuesta ante incidentes han comenzado a confiar en repositorios de respaldo para sus investigaciones. El uso de datos de copia de seguridad les permite ver los cambios a lo largo del tiempo y hacer un seguimiento del ciclo de vida del ataque.

Cohesity proporciona una plataforma inmutable y sólida en términos de análisis forense para iniciar el proceso de DFIR. Los investigadores obtienen acceso a instantáneas históricas del sistema de archivos que pueden crearse y orquestarse rápidamente mediante una API, lo que proporciona no solo el contexto de los sistemas afectados, sino también información sobre el sistema de archivos durante toda la cronología del incidente. Es como darle al analista un superpoder para viajar en el tiempo. Los analistas pueden comparar los sistemas de archivos a lo largo del tiempo para identificar las tácticas del adversario, como modificar los archivos de configuración para mantener la persistencia, sobrescribir binarios y bibliotecas legítimos con copias maliciosas o identificar otros artefactos maliciosos utilizados en el ataque.

El objetivo de tiempo de recuperación (RTO) es la cantidad máxima aceptable de tiempo para restaurar una red o aplicación y recuperar el acceso a los datos después de una interrupción no planificada.



Incluir la infraestructura de respaldo en el proceso de DFIR permite que las investigaciones se completen antes de que los datos se reintegren al entorno de producción. El desafío, en este caso: esto puede tener un impacto negativo en el objetivo de tiempo de recuperación (RTO) establecido por la organización. Después de todo, la mayoría de los RTO no se calcularon teniendo en cuenta las investigaciones requeridas durante un ciberataque.

Utilizar las copias de seguridad para crear un entorno de sala limpia reducirá el tiempo de inactividad general y garantizará que los datos restaurados estén limpios, eliminando así la necesidad de pasar nuevamente por el proceso durante una reinfección. Esto ayuda a las organizaciones a cumplir con sus RTO y evitar el tiempo de inactividad continuo.

Resiliencia cibernética desde la planificación hasta la ejecución

Esté preparado

Establezca un equipo de resiliencia multidisciplinaria al ransomware con todas las partes interesadas.

Los incidentes de ransomware son diferentes de otros ciberataques. Afectan a toda la organización y su capacidad para entregar productos y prestar servicios a los clientes. Cada segundo que toma una respuesta y una recuperación es una pérdida primaria. El personal no se puede comunicar ni hacer su trabajo. La prensa estará ansiosa por publicar informes sobre el incidente. Y los clientes se sentirán frustrados. Es fundamental garantizar que todos en una organización conozcan su función durante un ciberataque.

Esto incluye determinar:

- Cómo se llevará a cabo la comunicación si los métodos principales, como el correo electrónico, no funcionan.
- Quién tomará la iniciativa para cada función y etapa de la respuesta.
- Qué proceso seguir si un miembro del equipo no está disponible y quién será el contacto secundario.

Los empleados que no estén directamente involucrados en la respuesta y recuperación también deben saber lo que se espera de ellos. ¿Por qué? Porque ante la ausencia de información confiable, los rumores y las conjeturas pueden impedir la respuesta y retrasar la recuperación.

Lleve a cabo una simulación práctica y realista de ransomware con todas las partes interesadas.

Una de las mejores maneras de reunir a la organización es una simulación práctica y realista de ransomware que se centre en los detalles específicos de su organización. Obtendrá información sobre algunas de las amenazas y desafíos para la respuesta al ransomware que probablemente enfrentará durante un ataque real de ransomware.

Considere todos los impactos en el cálculo del riesgo de ransomware. Los impactos incluyen:

- Impacto principal:
  - La incapacidad de la organización para entregar sus productos y prestar servicios.
- Impactos secundarios:
  - costos operativos de investigación y respuesta a incidentes, lo que incluye servicios profesionales y cualquier pago al operador del ransomware;
  - daño a la reputación de la organización;
  - multas regulatorias relacionadas con el incidente de ransomware o el pago a entidades sancionadas;
  - pérdida de capital intelectual, y
  - litigios de socios o clientes relacionados con violaciones de datos.

Integre el riesgo de ransomware en la gestión de riesgos empresariales.

Aunque parece obvio hacerlo, muchas empresas no consideran el impacto del ransomware como un riesgo operativo significativo. Garantizar que el riesgo de ransomware se integre en la gestión de riesgos empresariales de la organización ayuda a establecer niveles adecuados de gobernanza para obtener un respaldo adecuado para las políticas de ciberseguridad y ayuda a mantener niveles adecuados de gestión de riesgos.

Cree una política de ransomware en toda la organización. Debe hacer lo siguiente:

- **Establecer criterios claros para que un incidente se declare como un ataque de ransomware.** Los flujos de trabajo para responder a un ransomware y recuperarse del mismo difieren de los que abordan el malware tradicional y la exfiltración de datos. Se deben establecer los criterios que permiten a un analista del SOC declarar un incidente para que pueda tomar las medidas de investigación, contención y erradicación adecuadas. Sin esta claridad, un ataque de ransomware puede propagarse dentro de una organización mientras el SOC busca autorización para tomar estas medidas.

- **Defina su estrategia de copia de seguridad cibernética.** La estrategia de copia de seguridad para escenarios de resiliencia cibernética puede diferir de la estrategia de resiliencia de datos para eventos tradicionales de recuperación ante desastres y continuidad del negocio. Está impulsada por la estructura y la madurez de la capacidad de respuesta y recuperación.
  - Hacer copia de seguridad únicamente de los datos: poner en marcha los servidores necesarios para investigar el incidente y reconstruir la infraestructura desde cero, para luego recuperar los datos. Esta política debe establecer cómo se mantienen las imágenes maestras de referencia utilizadas para la recuperación, incluido el escaneo de vulnerabilidades y configuraciones erróneas.
  - Hacer copia de seguridad de la infraestructura: recuperar toda la infraestructura, luego limpiarla mediante la restauración de distintas partes a diferentes puntos impulsada por la respuesta al incidente.
- **Defina las categorías de resiliencia operativa.** Base estas categorías en su análisis de impacto comercial de resiliencia de datos ya establecido e incluya la capacidad de poner en marcha nuestras herramientas de respuesta dentro de una sala limpia y sus estrategias de respaldo de resiliencia cibernética.
  - **Incluya la capacidad de recuperar las comunicaciones y la infraestructura de seguridad necesarias para responder al incidente y recuperarse del mismo.** Considere:
    - control de acceso físico
    - servicios de nombres de dominio
    - comunicaciones de voz
    - correo electrónico
    - plataformas de colaboración utilizadas para coordinar la respuesta
    - administración de casos
    - herramientas forenses y de respuesta a incidentes
    - escaneo y gestión de vulnerabilidades
    - gestión de identidades y acceso
- **Defina en qué condiciones la organización consideraría pagar el rescate.**
  - ¿Cómo obtendría la organización los fondos para pagar el rescate?
  - ¿La póliza de seguro de la organización incluye el pago de rescates?
  - ¿El proveedor de seguros trata las acciones de los actores partidistas de ransomware como combatientes?
  - ¿El proveedor de seguros cubre pagos a entidades sancionadas?
  - ¿Cuál es el enfoque de la organización para negociar con un operador de ransomware?
  - ¿Cuáles son las implicaciones reputacionales, regulatorias y penales si, por ejemplo, el grupo que recibe el pago es sancionado?
  - ¿Cómo obtendría su organización la criptomoneda para pagar el rescate? Tome en cuenta el tiempo para la confirmación, en concordancia con los plazos de la política Conozca a su cliente.
- **Asegúrese de que la política de ransomware se actualice periódicamente:** hacerlo reflejará mejor la naturaleza cambiante de los ataques de ransomware.

Sea proactivo

- **Comprenda a los operadores de ransomware y sus herramientas, técnicas y procedimientos** (TTP).
  - Obtenga inteligencia gubernamental, comercial o de código abierto sobre pandillas, campañas y técnicas de ransomware.
  - Priorice la recopilación y el análisis de inteligencia sobre los operadores de ransomware y aquellos que llevan a cabo ataques de wiper con operaciones en su mercado vertical o zona geográfica.
  - Determine las técnicas que están utilizando en comparación con el marco MITRE ATT&CK.
  - Planifique pruebas regulares de phishing al incorporar las técnicas más recientes que utilizan las pandillas de ransomware.

- Asegúrese de que las vulnerabilidades explotadas por los operadores de ransomware se prioricen en la implementación de parches en su programa de gestión de vulnerabilidades.
- Comprenda cómo los operadores de ransomware explotan las relaciones entre terceros y proveedores de servicios administrados para dirigirse a organizaciones similares a la suya. Tenga esto en cuenta en sus evaluaciones y controles de riesgos de terceros.

- **Documente y mantenga la información de contacto.** Incluya a todos los miembros y personas de respaldo de su equipo de respuesta, personal clave y partes interesadas clave, idealmente mediante un canal de comunicaciones fuera de banda que no se vería afectado por un incidente de ransomware.
- **Cree canales de informes.** Incluya a terceros como clientes, empresas homólogas y socios de la cadena de suministro para informar sobre incidentes de ransomware.
- **Cree un canal de informes para que los usuarios internos informen sobre comportamientos similares al ransomware.** Capture lo siguiente:
  - nombre y función de la persona informante;
  - cuándo sucedió;
  - lo que notaron;
  - por qué pensaron que se trataba de ransomware;
  - lo que estaban haciendo en ese momento;
  - dónde estaban físicamente ubicados y a qué redes estaban conectados;
  - qué cuenta estaban usando;
  - qué sistema(s) estaba(n) usando (sistema operativo, nombre de host, dirección IP);
  - en qué cuenta iniciaron sesión;
  - con quién se comunicaron y qué le dijeron, y
  - a qué tienen acceso generalmente en su función.
- **Cree un canal de informes para que las agencias de cumplimiento de la ley y de ciberseguridad informen sobre incidentes de ransomware o wiper que involucren a su organización.**
- **Reúna un equipo de respuesta a crisis cibernéticas.** Incluya lo siguiente:
  - líderes de la empresa
  - TI (incluida la gestión de recuperación y vulnerabilidad)
  - tecnología operativa (si es relevante)
  - operaciones de seguridad (incluido el gerente de respuesta a incidentes, análisis forense digital y, si la organización los tiene, ingeniería inversa de malware, equipo de búsqueda e inteligencia sobre amenazas)
  - asesor legal
  - relaciones públicas
  - recursos humanos
- **Si es necesario, conserve los servicios de una organización de respuesta a incidentes.**
  - Obtenga la autorización previa para contratar a la organización de respuesta a incidentes.
  - Si depende de un proveedor de seguros para la respuesta a incidentes, tenga en cuenta que también puede buscar evidencia de incumplimiento de las certificaciones de control efectuadas cuando se tomó la póliza, así como lidiar con el incidente de ransomware real.
- **Redacte declaraciones de reserva y plantillas para anuncios de violaciones de seguridad.** Tener previamente redactada la mayor parte de una declaración facilitará la respuesta rápida y evitará la especulación, incluso si necesita agregar detalles más adelante.
  - Nombre a un vocero y un respaldo para la organización que esté capacitado en los medios y en la narrativa de la respuesta a violaciones de seguridad.
  - Prepare un canal de comunicaciones (que no se vea afectado por un incidente) para las reuniones informativas y entrevistas con los medios.
- **Establezca previamente relaciones con las fuerzas del orden público y los equipos nacionales de respuesta a emergencias informáticas.**
- **Pida al asesor legal que revise los acuerdos que tenga con las fuerzas del orden público.**
- **Haga que el asesor legal revise los planes y las declaraciones de respuesta propuestos, y la posibilidad de responsabilidad civil, regulatoria y penal.**

Reduzca la superficie de ataque

- **Priorice la implementación de parches en sistemas con vulnerabilidades que a menudo aprovechan las pandillas de ransomware.** Identifique las vulnerabilidades críticas de los activos e implemente parches.
- **Endurezca los sistemas.** Priorice los sistemas críticos y los vectores de ataque que utilizan las pandillas de ransomware y que se descubran mediante su inteligencia sobre amenazas. Configure correctamente los dispositivos con puertos y protocolos y desactive aquellos que no se utilizan para fines comerciales. Los operadores de ransomware utilizan herramientas legítimas en los ataques de "Living off the Land", por lo que restringir el acceso a estas herramientas disminuye la probabilidad de un ataque.
- **Siga las mejores prácticas para usar el protocolo de escritorio remoto y otros servicios de escritorio remoto.** Los servicios de acceso remoto son un vector de acceso inicial principal para los operadores de ransomware. Aplique bloqueos de cuentas después de una cantidad específica de intentos, autenticación multifactor y registro de todos los intentos de inicio de sesión de escritorio remoto. Asegúrese de que el acceso remoto se justifique con un motivo comercial válido para tener servicios de escritorio remoto. Audite su red para detectar el uso no autorizado de servicios de escritorio remoto.
- **Desactive o bloquee los protocolos de uso compartido de archivos.** Estos incluyen el protocolo de bloque de mensajes del servidor (SMB) saliente y la eliminación o desactivación de versiones obsoletas de protocolos de uso compartido de archivos. Los actores de amenazas utilizan protocolos de uso compartido de archivos para propagar malware entre organizaciones.
- **Asegúrese de que las credenciales y los derechos de acceso en todos los sistemas se gestionen siguiendo el principio de menor privilegio, y limite la cantidad de cuentas privilegiadas.**
- **Evite que las cuentas privilegiadas se utilicen para las actividades diarias.**
- **Implemente la segmentación de red.** La segmentación de red sigue siendo una de las formas más efectivas de limitar la propagación del ransomware y aumentar la probabilidad de detectar el movimiento lateral.
- **Use configuraciones de referencia y control de cambios de implementación.** El uso de configuraciones de referencia y el conocimiento de los cambios significa que las imágenes de respaldo se pueden comparar con las que se sabe que se encuentran en buen estado durante las investigaciones.
- **Identifique repositorios de datos mal protegidos dentro de su organización.** La clasificación de datos de Cohesity DataHawk escanea las copias de seguridad para identificar datos confidenciales sin afectar los sistemas de producción. Esta visión integral de dónde residen los datos confidenciales permite a las organizaciones evaluar sus riesgos.

Proteja sus copias de seguridad

- **Asegúrese de que los sistemas de respaldo estén suficientemente aislados.** Esto debería evitar que los adversarios los eliminen o dañen. Cohesity FortKnox mejora la resiliencia cibernética con una copia inmutable de datos en una bóveda en la nube administrada por Cohesity mediante un aislamiento virtual.
- **Asegúrese de que los sistemas de respaldo utilicen almacenes de datos inmutables que eviten que los adversarios los dañen o eliminen.** Por ejemplo, Cohesity Data Cloud se basa en una plataforma de almacenamiento inmutable con capacidad de bloqueo de datos para evitar que incluso aquellos con privilegios escalados eliminen copias de seguridad.
- **Utilice la autenticación multifactor en las cuentas de administrador de respaldo.** Implemente múltiples opciones en caso de que su servidor de gestión de acceso e identidad principal se vean afectados por ransomware. Cohesity admite enfoques multifactor tanto SSO como TOTP.
- **Utilice el control de acceso basado en roles (RBAC) para asignar el menor privilegio.** Los usuarios de su sistema de copia de seguridad deben recibir solo los privilegios mínimos necesarios para efectuar tareas relacionadas con su función. Cohesity tiene un RBAC granular para respaldar el principio de privilegio mínimo.
- **Asegúrese de que los sistemas de copia de seguridad tengan una separación de funciones para evitar que una cuenta de administrador comprometida lleve a cabo cambios maliciosos.** La capacidad de Quorum de Cohesity permite a las organizaciones definir múltiples niveles de autorización para tareas relacionadas con la copia de seguridad y la recuperación.
- **Adopte una estrategia de copia de seguridad 3-2-1.** Tenga tres copias de sus datos en dos medios diferentes con al menos una copia fuera del sitio.
- **Pruebe las copias de seguridad periódicamente.** Las pruebas de copias de seguridad deben ser periódicas y automatizadas.

Informe los resultados de las pruebas para que se puedan tomar medidas correctivas cuando sea necesario. Cohesity DataProtect admite las pruebas automatizadas.

- **Recopile e informe métricas sobre la cobertura de copias de seguridad completadas/fallidas/probadas de los sistemas críticos.**
- **Garantice la capacidad adecuada en la infraestructura de copias de seguridad para el crecimiento.**
- **Asegúrese de que el sistema de copias de seguridad pueda admitir las funciones de ciberseguridad necesarias para responder a un incidente de ransomware.** Durante un incidente, el equipo de seguridad no puede crear imágenes forenses del sistema víctima, ya que está cifrado. Deberán confiar en el sistema de copia de seguridad para poder investigar el incidente. Cohesity ha incorporado capacidades de respuesta (como clasificación de datos, fuentes de inteligencia sobre amenazas y búsqueda) en su propia plataforma de gestión de datos. También ofrece soluciones previamente integradas con proveedores de seguridad líderes como Splunk, Cisco, Palo Alto, Tenable, Qualys, Crowdstrike y ServiceNow mediante la Alianza de Seguridad de Datos.
- **Cree y mantenga imágenes maestras de referencia de sistemas críticos para acelerar la reconstrucción después de un incidente.** Mantenga plantillas de imágenes que incluyan un sistema operativo preconfigurado y software de aplicación asociado que pueda implementarse rápidamente para reconstruir un sistema dentro de la sala limpia.

Refuerce su protección contra el ransomware

- **Identifique brechas en su cobertura de control preventivo y de detección existente contra las técnicas de ATT&CK que utilizan las pandillas de ransomware.** Hágalo de forma continua para maximizar sus posibilidades de prevención o detección a medida que los adversarios adaptan su comportamiento.
  - Los indicadores de compromiso (IOC) típicos que pueden utilizarse en las etapas de prevención, detección y respuesta incluyen:
    - transacciones de archivos anómalas (desviaciones de volumen de cifrado y eliminación);
    - tiempo de arranque sospechoso de servicios y aplicaciones;
    - presencia de servicios y aplicaciones desconocidos e inesperados;
    - presencia de software no autorizado de acceso remoto/VPN;
    - disminución del rendimiento del sistema (aumento de la utilización de CPU/RAM);
    - rendimiento degradado o deshabilitado de la instrumentación de seguridad del host con agentes de seguridad deshabilitados;
    - conexiones desconocidas/inesperadas de nombre de dominio y dirección IP;
    - discrepancias de protocolo;
    - hashes de archivos maliciosos conocidos;
    - cambios sospechosos en los archivos de configuración;
    - tráfico o fuente/destino entrantes y salientes anómalos;
    - procesos y texto sospechosos en volcados de memoria;
    - cuentas sospechosas en usuarios conectados (históricas y actuales);
    - recursos compartidos de red sospechosos y recursos compartidos de red montados;
    - cuentas de usuario sospechosas;
    - certificados instalados sospechosos;
    - entradas sospechosas en cachés de ARP y DNS;
    - anomalías en la fecha/hora en los sistemas, o en archivos de registro o servidores NTP;
    - entradas o arrendamientos sospechosos en registros de DHCP;
    - cadenas de agentes de usuario anómalas;
    - balizas y actualizaciones de aplicaciones no estándar, y
    - binarios dentro de la captura completa de paquetes.
- **Pruebe el contenido preventivo y de detección.** Pruebe cualquier regla creada con los IOC de ransomware.
- **Implemente la detección de anomalías del sistema de archivos en el endpoint que correspondan a ataques de ransomware y de wiper, como el cifrado o la eliminación de archivos.** Cohesity utiliza el aprendizaje automático para identificar estos patrones.
- **Implemente filtros de puerta de enlace de correo electrónico para bloquear correos electrónicos con indicadores maliciosos conocidos.**
- **Implemente un mecanismo para eliminar correos electrónicos identificados como portadores de**

contenido relacionado con ransomware de los buzones de los usuarios.

- **Implemente una política y verificación de Autenticación de mensajes basada en dominios, informes y conformidad (DMARC).** Será menos probable que reciba correos electrónicos falsificados o modificados de dominios válidos.
- **Deshabilite las macros para archivos de Microsoft Office transmitidos por correo electrónico, a menos que exista un requisito empresarial específico.**
- **Utilice aplicaciones que permitan listas o listas blancas de activos críticos para garantizar que solo se pueda ejecutar el software autorizado.** En plataformas Windows, utilice la Política de restricción de software de Microsoft o AppLocker. Use listados de directorios permitidos en lugar de tratar de enumerar todas las aplicaciones posibles. Un valor predeterminado para restringir la ejecución de muchos vectores de ataque de ransomware permite que las aplicaciones se ejecuten desde PROGRAMFILES, PROGRAMFILES(X86) y SYSTEM32, aunque esto no detendrá los ataques de "Living off the Land". Impida la ejecución desde todas las demás ubicaciones a menos que se otorgue una excepción para una aplicación específica.
- **Comprenda las prácticas de gestión de riesgos e higiene cibernética de la cadena de suministro, los socios externos y los proveedores de servicios administrados (MSP).** Muchos ataques de ransomware se facilitan mediante terceros.
  - Comprenda la función de la empresa y del socio en la gestión y los controles de riesgos cibernéticos. Asegúrese de que las funciones y responsabilidades estén claramente definidas y medidas, y que los mecanismos para las medidas correctivas estén incluidos en los acuerdos contractuales.
- **Emplee la autenticación multifactor para la mayor cantidad posible de servicios, particularmente para el acceso remoto y las cuentas privilegiadas.**
- **Implemente segmentación de red lógica o física para separar unidades de negocio o categorías de recursos de TI, y cualquier entorno de tecnología operativa (TO).** Esto limitará la propagación del ransomware en caso de un ataque.
- **Reduzca la oportunidad de que PowerShell se utilice en ataques de "Living off the Land".**
  - Restrinja el uso de PowerShell a usuarios específicos caso por caso.
  - Actualice PowerShell a la versión 5.0 o posterior, desinstale todas las versiones anteriores de PowerShell.
  - Asegúrese de que el registro de módulos, bloques de script y transcripción esté habilitado.
  - Asegúrese de que el registro de eventos de Windows "PowerShell" y el registro "PowerShell operativo" tengan un período de retención de al menos 180 días en sistemas con PowerShell habilitado.
- **Analice el tráfico de red histórico para detectar patrones de tráfico anómalos de este a oeste y de norte a sur.** Utilice metadatos de tráfico de red (NetFlow/sFlow) o, si está disponible, captura completa de paquetes o un sistema de detección/prevención de intrusiones de red.
- **Proteja los controladores de dominio.**
  - **Asegúrese de que no se instale software adicional en los controladores de dominio que no sean agentes de gestión de datos y seguridad.** El acceso a los controladores de dominio debe limitarse al grupo de administradores. Todo usuario dentro de este grupo debe usar una cuenta restringida separada para las actividades diarias.
  - **Configure el firewall del host en los controladores de dominio para evitar el acceso a internet.**
  - **Habilite Kerberos para la autenticación y habilite la auditoría de NTLM para garantizar que solo se envíen respuestas de NTLM v2 mediante la red, si es posible.**
  - **Audite LSASS.EXE para comprender qué aplicaciones se verían afectadas si se habilitaran las protecciones de autenticación de seguridad local.** Esto evitará que la inyección de código adquiera credenciales y habilitará estas protecciones si el impacto es aceptable.
  - **Asegúrese de que se requiera la firma SMB entre los hosts y los controladores de dominio.** Esto evita el uso de ataques de repetición en la red.

Refuerce su detección de ransomware

- **Busque proactivamente utilizando datos históricos para encontrar riesgos.** Utilice nueva inteligencia sobre amenazas y los IOC relacionados con las pandillas de ransomware para los que no hay una regla de prevención o detección. Cohesity incluye una fuente integrada de inteligencia sobre amenazas que proporciona más de 110 000 IOC utilizados por las pandillas de ransomware y ofrece la capacidad de buscar si están presentes mediante comparación con las copias de seguridad. Al buscar pasivamente y comparar con las copias de seguridad en lugar de sistemas en vivo, los atacantes no pueden detectar esta actividad, por lo que no está sujeta a las técnicas de evasión de defensa que los adversarios utilizan contra las soluciones de endpoint. Además, los períodos de retención en las copias de seguridad tienden a ser más largos que los de las soluciones de seguridad, lo que permite un horizonte de detección extendido.
- **Implemente un mecanismo para cambios inusuales en la utilización de CPU y discos.** Generalmente, las plataformas de operaciones de TI recopilan estas métricas, pero pueden canalizarse adicionalmente al equipo de seguridad como señales adicionales para mejorar la detección.
- **Identifique protocolos de red inusuales.** Estos incluyen I2P o TOR, que se sabe que los utilizan las pandillas de ransomware.
- **Identifique conexiones de red que utilizan puertos o destinos que se sabe que se usan para el comando y control de ransomware y wiper.**

Responda al incidente

- **Identifique y agrupe alertas similares relacionadas con los activos afectados.**
- **Cree una expectativa de pérdida inicial (radio de explosión) del incidente, que incluya:**
  - cantidad estimada de endpoints cifrados/borrados;
  - cadenas de valor comerciales afectadas por sistemas cifrados/borrados;
  - obligaciones regulatorias de los datos afectados (cantidad de registros, tipos de datos), y
  - cualquier evidencia de exfiltración.

Cohesity busca automáticamente la copia de seguridad de los sistemas afectados para identificar el posible impacto regulatorio de los incidentes de ransomware. Los sistemas que se están respaldando también pueden clasificarse bajo demanda, tanto antes de un incidente como en respuesta al mismo.

- **Encuentre los entornos de almacenamiento temporal utilizados para la exfiltración de datos.** Identifique sistemas en su red que tengan aumentos inesperadamente grandes en los datos, u otros tipos de datos que no esperaría encontrar en ese equipo host. Cohesity busca automáticamente la copia de seguridad de los sistemas afectados para identificar el posible impacto regulatorio de los incidentes de ransomware.
- **Aísle los equipos host infectados de las redes cableadas e inalámbricas.**
- **Si se conoce la variante del ransomware y se propaga por sí misma, bloquee las comunicaciones conocidas y los canales de infección (firewalls de host o de red, puertas de enlace de correo electrónico, control de acceso a la red).**
- **Active el clean room.** Si las herramientas de seguridad, la comunicación, la colaboración o los sistemas de control de acceso se han visto afectados, cree rápidamente instancias conocidas en buen estado para permitir que comiencen las actividades de respuesta.
- **Restaure la última copia de seguridad de los sistemas afectados en un entorno de sala limpia.** Esto actúa como una imagen forense para comenzar su investigación. El estado del sistema en otros puntos cronológicos puede ayudar a establecer tendencias históricas e identificar cambios en el sistema de archivos a lo largo del tiempo.
- **Vuelva a implementar herramientas forenses/de respuesta/de detección confiables en los sistemas dentro de la sala limpia.** Los atacantes apuntarán a herramientas de endpoint para garantizar que puedan evadir la detección. Esto reduce la confianza de que las herramientas de endpoint funcionan correctamente. La reinstalación de las herramientas de endpoint

garantiza un funcionamiento adecuado y puede generar confianza en que las herramientas están informando correctamente.

- **Si no se conoce la variante de ransomware, determínela haciendo lo siguiente:**
  - Recopile mensajes de rescate (ventanas emergentes gráficas, texto o archivos html, que pueden abrirse automáticamente después del cifrado; archivos de imagen como fondo de pantalla en sistemas infectados que contienen correos electrónicos de contacto; archivos de sonido con demandas de rescate).
  - Analice los mensajes de rescate para identificar la pandilla y variante de ransomware (nombre de ransomware, idioma utilizado, sintaxis, estructura, frases, material gráfico, dirección de correo electrónico de contacto, nombres de usuario, tipo de pago de demanda de rescate [es decir, tipo de criptomoneda, tarjetas de regalo], dirección de pago en caso de criptomoneda; dirección de chat de soporte o URL de soporte).
  - Analice los archivos cifrados y otros artefactos creados (esquema y extensión de cambio de nombre de archivos cifrados; tipos de archivos objetivo; ubicaciones de archivos objetivo; propiedad de archivos y grupo de archivos afectados; cambios en metadatos de archivos como cambios masivos en los tiempos de creación/modificación de archivos; visualización de entropía y gráficos de bytes; icono utilizado para archivos cifrados; indicadores de archivos; archivo que contiene el manifiesto de archivos cifrados o material clave; otros archivos de datos).
  - Investigue el vector de infección con mayor detenimiento, si es necesario.
  - Extraiga binarios sospechosos de sistemas de archivos instantáneos para efectuar ingeniería inversa si no es una variante conocida.
  - Verifique los artefactos recopilados para identificar la pandilla y las variantes de ransomware mediante su análisis en sitios como:
    - Censo de ransomware (https://goo.gl/b9R8DE)
    - CryptoSheriff (https://www.nomoreransom.org/crypto-sheriff.php)
    - ID Ransomware
- **Busque evidencia de la persistencia.** Se pueden crear instancias de las instantáneas históricas tomadas por Cohesity para permitir que los analistas examinen los sistemas de archivos y busquen evidencia de persistencia. Esto incluye:
  - Mecanismos de persistencia "de afuera hacia adentro", que pueden incluir acceso autenticado a sistemas externos mediante cuentas no autorizadas; puertas traseras en sistemas perimetrales; y explotación de vulnerabilidades en sistemas perimetrales.
  - Persistencia "de adentro hacia afuera", que puede incluir implantes de malware en los sistemas internos o una variedad de modificaciones de tipo "Living off the Land" (incluida la implementación de marcos de pruebas de penetración comerciales como Cobalt Strike; el uso de PsTools, especialmente PsExec, para instalar y controlar malware de forma remota y recopilar información; y el uso de scripts de PowerShell).
- **Capture una imagen del contenido de la memoria para detectar procesos o artefactos de texto sospechosos.**
- **Identifique las claves de registro modificadas.**
- **Identifique archivos comprimidos creados recientemente.**
- **Examine los procesos y trabajos programados.**
- **Audite los servicios de red activos/en ejecución y compárelos con lo que debería estar funcionando.**
- **Ejecute el manual de estrategias de pérdida de datos si se enfrenta a evidencia de preparación o exfiltración.** Cohesity DataHawk puede identificar qué datos estaban en esos sistemas en el momento del ataque, lo que permite a los equipos de respuesta ante incidentes identificar las obligaciones de cumplimiento y notificar a los titulares de los datos y a los entes reguladores.
- **Identificar las vulnerabilidades en los sistemas explotados en el ataque.** Cohesity CyberScan permite a los equipos de respuesta ante incidentes ejecutar el escáner de vulnerabilidades Tenable Nessus y comparar con la instantánea próxima al punto del ataque, para que pueda crear un manifiesto de parches que se aplicarán antes de que el sistema se reintegre al entorno de producción y cualquier vulnerabilidad que los atacantes puedan haber explotado desde el último escaneo de vulnerabilidades programado.
- **Identifique los activos utilizados para la preparación mediante el análisis de propiedad intelectual, información financiera o información de identificación personal sobre activos no autorizados.** Los datos confidenciales pueden identificarse en entornos de preparación utilizando la clasificación de datos Cohesity DataHawk.

- **Extraiga los binarios sospechosos de los sistemas de archivos históricos instanciados.** Analícelos, efectúe ingeniería inversa en ellos o cárguelos en servicios como VirusTotal. La creación de instancias de sistemas de archivos históricos se puede orquestar en Cohesity mediante herramientas de orquestación de seguridad y respuesta automatizada (SOAR), como ServiceNow Security Incident Response, Splunk Phantom y Palo Alto XSOAR.
- **Extraiga los binarios sospechosos de sistemas de archivos instanciados y actívelos en un espacio aislado (sandbox) de análisis de malware.**
- **Verifique sistemas similares dentro de la organización para detectar infecciones.** Investigue equipos host con usuarios y grupos similares. Si los sistemas no están cifrados, compare las instancias de estos equipos host con el sistema infectado para identificar el impacto potencial. Cohesity tiene capacidades de indexación y búsqueda que pueden consultar rápidamente la infraestructura de respaldo de una organización.
- **Consulte las cuentas locales, las herramientas de gestión de identidad y acceso, y los servicios de directorio para conocer nuevas cuentas o cambios en permisos/derechos de acceso.**
- **Identifique otros sistemas que intentan conectarse al comando y control de ransomware.**
- **Continúe siguiendo la cadena de investigación utilizando MITRE ATT&CK para encontrar el paciente cero, el vector de infección inicial y cada endpoint infectado.**
- **Identifique cualquier control de prevención o detección que se haya eludido y el mecanismo utilizado.** Agréguelos a su plan de mitigación para reforzar los controles antes de recuperarse en producción.

Comuníquese

- **Comuníquese con la prensa.** Mantenga actualizada a la prensa para ayudar a evitar especulaciones perjudiciales.
- **Comuníquese con los titulares de los datos afectados.** Asegúrese de que cualquier notificación cumpla con las obligaciones reglamentarias y legales.
- **Comuníquese con las partes interesadas internas.** Mantenga informado a su personal interno sobre la situación y lo que se espera de ellos, especialmente porque la prensa puede usar plataformas como LinkedIn para identificar a los empleados y comunicarse con ellos directamente.
- **Comuníquese con los entes reguladores para cumplir con las obligaciones de cumplimiento normativo para la presentación de informes.**
- **Informe a su compañía de seguros.**
- **Informe a las fuerzas del orden público y al CERT nacional/industrial.**

Recupérese del incidente

El mejor escenario sería encontrar y eliminar la infección y restaurar los sistemas a la producción utilizando herramientas como la restauración masiva instantánea (IMR). En realidad, es probable que tenga una combinación de sistemas que se restauran y de sistemas que se deberán reconstruir desde cero. Para llevar a cabo restauraciones desde cero, necesitará acceso a "imágenes maestras" de sistemas críticos, que sean seguras y se mantengan al día con los últimos parches probados. Estas plantillas se pueden implementar rápidamente para reconstruir sistemas que ya no se pueden recuperar. También se pueden proteger utilizando herramientas que se encuentran en Cohesity Data Cloud, para que no se dañen durante un ciberataque. Luego puede restaurar el sistema operativo base y las aplicaciones, así como los datos asociados de otras copias de seguridad. Esto optimiza el RTO y, al mismo tiempo, crea copias de seguridad históricas de los sistemas afectados para efectuar análisis forenses.

A medida que se recuperen los datos y las aplicaciones, deberá documentar el incidente y tomar medidas para evitar que este último vuelva a ocurrir.

Las organizaciones deben:

- utilizar el conocimiento del vector de infección inicial, las vulnerabilidades explotadas y los mecanismos de persistencia para actualizar sus planes de recuperación a fin de protegerse contra futuros ataques y garantizar que cada componente pueda volver a un estado seguro y estable;
- recuperar los sistemas restantes de vuelta a la sala limpia y repetir los pasos anteriores, poniendo en cuarentena todo indicador de compromiso;
- implementar parches en las vulnerabilidades encontradas;
- emitir restablecimientos de contraseñas para todos los sistemas y cuentas afectados;
- eliminar correos electrónicos históricos que contengan artefactos de explotación de las bandejas de entrada de correo electrónico eliminadas, y
- aumentar el monitoreo enfocado de los sistemas previamente infectados.

Establezca conclusiones clave y acciones de seguimiento

Después de experimentar un ataque de ransomware, haga las siguientes preguntas para recopilar las lecciones aprendidas:

- ¿Qué productos y servicios se vieron afectados?
- ¿Cuáles fueron los impactos en la empresa?
- ¿Qué partes interesadas se vieron afectadas?
- ¿Quiénes fueron los perpetradores involucrados?
- ¿Qué salió mal en el proceso de respuesta?
- ¿Qué salió bien en el proceso de respuesta?
- ¿Cuándo detectamos el ataque?
  - ¿Cuál fue el retraso entre la infección inicial y la detección?
  - ¿Por qué no se detectó antes?
  - ¿Qué controles no pudieron detectar/prevenir el ataque?
- ¿Qué controles se evadieron y cómo?
- ¿Qué se debe ajustar dentro de las operaciones comerciales para evitar incidentes futuros?
- ¿Cómo puede evitarse esto en el futuro?
- ¿Pudimos recuperar el funcionamiento de la producción dentro del RTO/RPO requerido?

Envíe los IOC recién descubiertos a cualquier socio y proveedor autorizado.

- Actualice la documentación y los manuales de estrategias.
- Comunique el informe final del incidente y las lecciones aprendidas a las partes interesadas y los entes reguladores.

Acerca de Cohesity

Cohesity es el líder en seguridad de datos impulsada por IA. Más de 13 600 clientes empresariales, incluidos más de 85 de las empresas Fortune 100 y casi el 70 % de las empresas Global 500, confían en Cohesity para fortalecer su resiliencia y, al mismo tiempo, proporcionar información sobre la inteligencia artificial generativa en sus vastas cantidades de datos. Formadas a partir de la combinación de Cohesity con el negocio de protección de datos empresariales de Veritas, las soluciones de la empresa aseguran y protegen los datos en las instalaciones, en la nube y en el borde. Con el respaldo de NVIDIA, IBM, HPE, Cisco, AWS, Google Cloud y otros, Cohesity tiene sede en Santa Clara, CA, con oficinas en todo el mundo. Para obtener más información, siga a Cohesity en **LinkedIn**, **X** y **Facebook**.

Obtenga más información en cohesity.com/es-es

COHESITY

cohesity.com/es-es
1-855-926-4374
2625 Augustine Drive, Santa Clara, CA 95054

2000048-002 EN 4-2025