PlayBook

Acciones de respuesta ante ransomware y extorsión de datos

Acciones a realizar en caso de haber sufrido un incidente de ransomware

Detección y análisis

☐ Determinar qué sistemas fueron afectados y aislarlos inmediatamente

☐ Apagar los dispositivos o desconectarlos de la red para evitar una mayor propagación de la infección de ransomware

☐ Clasificar los sistemas afectados para la restauración y recuperación.

☐ Examinar los registros y los sistemas existentes de detección o prevención de la entidad (p. ej., antivirus, EDR, IDS, sistema de prevención de intrusiones)

☐ Consultar con su equipo para desarrollar y documentar una comprensión inicial de lo que ocurrió basándose en el análisis inicial.

Iniciar actividades de búsqueda de amenazas.

En caso de que la entidad cuente con infraestructura física, verifique:

☐ Cuentas de AD recién creadas o cuentas con privilegios elevados y actividad reciente relacionada con cuentas privilegiadas, como administradores de dominio

☐ Inicios de sesión anómalos en dispositivos de VPN u otros inicios de sesión sospechosos.

☐ Modificaciones de puntos de conexión que puedan deteriorar las copias de seguridad, las instantáneas, el registro en diario de los discos o las configuraciones de arranque. Busque un uso anómalo de las herramientas integradas de Windows, como bcdedit.exe, fsutil.exe (deletejournal), vssadmin.exe, wbadmin.exe y wmic.exe (shadowcopy o shadowstorage). El uso indebido de estas herramientas es una técnica de ransomware común para inhibir la recuperación del sistema.

☐ Indicios de la presencia de la señal/cliente de Cobalt Strike. Cobalt Strike es un paquete de software comercial de pruebas de penetración. Los agentes maliciosos suelen nombrar los procesos de Windows de Cobalt Strike con los mismos nombres que los procesos de Windows legítimos para ofuscar su presencia y complicar las investigaciones.

☐ Señales de cualquier uso inesperado de software de supervisión y administración remota (RMM) (incluidos los ejecutables portátiles que no están instalados). Los agentes maliciosos suelen utilizar el software de RMM para mantener la persistencia

☐ Cualquier ejecución inesperada de PowerShell o uso del conjunto PsTools.

☐ Signos de enumeración de credenciales de AD o LSASS que se vuelcan (p. ej., Mimikatz, Sysinternals ProcDump o NTDSutil.exe).

☐ Señales de comunicaciones inesperadas entre puntos de conexión (incluidos los servidores), por ejemplo, el envenenamiento del protocolo de resolución de direcciones (ARP, por sus siglas en inglés) de un punto de conexión o el tráfico de comando y control retransmitido entre puntos de conexión.

☐ Cantidad anormal de datos salientes a través de cualquier puerto. El software de código abierto puede canalizar datos a través de varios puertos y protocolos. Por ejemplo, los agentes de ransomware han utilizado Chisel para canalizar el shell seguro (SSH, por sus siglas en inglés) a través del puerto 443 del protocolo de transferencia de hipertexto seguro (HTTPS, por sus siglas en inglés). Los agentes de ransomware también han utilizado Cloudflared para hacer mal uso de los túneles de Cloudflare a fin de canalizar las comunicaciones a través del HTTPS.

☐ La presencia de Rclone, Rsync y diversos servicios de almacenamiento de archivos basados en la web, y del protocolo de transferencia de archivos (FTP, por sus siglas en inglés) y del protocolo de transferencia segura de archivos (SFTP, por sus siglas en inglés), que son herramientas comunes para la exfiltración de datos (y también las utilizan los agentes de amenazas para implantar malware o herramientas en las redes afectadas)

☐ Servicios recién creados, tareas programadas inesperadas, software instalado imprevisto, archivos inusuales creados, procesos legítimos con procesos secundarios inesperados, etc.

En caso de que la entidad utilice entorno en la nube, verifique:

☐ Habilite herramientas para detectar y evitar las modificaciones en recursos de IAM, seguridad de la red y protección de datos

☐ Utilice la automatización para detectar problemas comunes (p. ej., deshabilitación de características, introducción de nuevas reglas del cortafuegos) y tomar medidas automatizadas apenas ocurran. Por ejemplo, si se crea una nueva regla del cortafuegos que permite el tráfico abierto (0.0.0.0/0), se puede tomar una medida automatizada para deshabilitar o eliminar esta regla y enviar notificaciones al usuario que la creó, así como al equipo de seguridad para que esté al tanto. Esto ayudará a evitar la fatiga de alertas y permitirá que el personal de seguridad se concentre en cuestiones fundamentales.

Contención y erradicación

☐ Identifique los sistemas y las cuentas involucrados en la vulneración inicial. Esto puede incluir cuentas de correo electrónico.

☐ Deshabilite las redes privadas virtuales, los servidores de acceso remoto, los recursos de inicio de sesión único y los activos públicos basados en la nube o de otro tipo.

Si una estación de trabajo infectada está cifrando datos del lado del servidor, siga los pasos de identificación rápida del cifrado de datos del lado del servidor

☐ Revise Administración de equipos > Sesiones y las listas de Archivos abiertos en los servidores asociados para determinar el usuario o el sistema que accede a esos archivos.

☐ Revise las propiedades de los archivos cifrados o las notas de rescate para identificar usuarios específicos que puedan estar asociados a la propiedad de los archivos.

☐ Revise el registro de eventos de TerminalServices-RemoteConnectionManager para verificar si hay conexiones de red del RDP satisfactorias.

☐ Revise el registro de seguridad de Windows, los registros de eventos de SMB y los registros relacionados que puedan identificar eventos importantes de autenticación o acceso

☐ Ejecute un software de captura de paquetes, como Wireshark, en el servidor afectado con un filtro para identificar las direcciones IP involucradas en la escritura activa o el cambio de nombre de archivos (p. ej., smb2.filename contains cryptxxx).

Realice un análisis extendido para identificar los mecanismos de persistencia de interacción indirecta y de interacción directa.

☐ La persistencia de interacción indirecta puede incluir el acceso autenticado a los sistemas externos a través de cuentas no autorizadas, las puertas traseras en los sistemas perimetrales, la
explotación de las vulnerabilidades externas, etc.

☐ La persistencia de interacción directa puede incluir implantes de malware en la red interna o una variedad de modificaciones al estilo “living-off-the-land” (p. ej., el uso de herramientas comerciales de pruebas de penetración, como Cobalt Strike; el uso del conjunto PsTools, incluido PsExec, para instalar y controlar malware de forma remota, y recopilar información relativa a los sistemas Windows o realizar su administración remota; el uso de scripts de PowerShell).

☐ La identificación puede implicar la implementación de soluciones de EDR, auditorías de cuentas locales y de dominio, la revisión de los datos encontrados en los sistemas de registro centralizados o un análisis forense más profundo de sistemas específicos una vez que se ha trazado el movimiento dentro del entorno.

☐ Reconstruya los sistemas con base en la priorización de los servicios fundamentales mediante el uso de imágenes estándar preconfiguradas si es posible. Utilice la infraestructura como plantillas de código para reconstruir los recursos en la nube.

☐ Emita restablecimientos de contraseña para todos los sistemas afectados y aborde cualquier vulnerabilidad asociada y deficiencia en la seguridad o visibilidad una vez que el

entorno se haya limpiado y reconstruido completamente, lo que incluye cualquier cuenta afectada asociada y la eliminación o la corrección de los mecanismos de persistencia maliciosos. Esto puede incluir aplicar correcciones, actualizar el software y tomar otras precauciones de seguridad que no se hayan adoptado previamente. Actualice las claves de cifrado administradas por el cliente según sea necesario.

☐ La autoridad de tecnologías de la información o de seguridad de la información designada de la entidad declara finalizado el incidente de ransomware según criterios establecidos, que pueden incluir seguir los pasos anteriores o buscar asistencia externa.

Recuperación y actividad posterior al incidente

☐ Reconecte los sistemas y restaure los datos a partir de copias de seguridad cifradas sin conexión, con base en una priorización de los servicios fundamentales. Tenga cuidado de no reinfectar los sistemas limpios durante la recuperación. Por ejemplo, si se ha creado una nueva red de área local virtual (VLAN, por sus siglas en inglés) con fines de recuperación, asegúrese de que solo se agreguen sistemas limpios.

☐ Documente las conclusiones obtenidas a partir del incidente y las actividades de respuesta asociadas para actualizar y perfeccionar las políticas, los planes y los procedimientos de la organización, y orientar futuros ejercicios relacionados con ellos.

☐ Considere compartir las conclusiones y los indicadores de riesgo relevantes con el Centro de Gestión de Incidentes Informáticos para ayudar a otras entidades públicas que pudieran sufrir incidentes similares.

Revision #4
Created 23 junio 2025 14:02:15 by Rodrigo Alexis
Updated 24 junio 2025 12:46:12 by Rodrigo Alexis