METODOLOGÍA DE RESPUESTA A INCIDENTES

IRM #17: INCIDENTE RANSOMWARE

Directrices para manejar y responder a una infección de Ransomware

Autor IRM: CERT SG
Contribución: CERT a Dvens / Paloma Vargas
Versión del IRM: 2.0
E-Mail: cert.sg@socgen.com
Web: https://cert.societegenerale.com
Twitter: @CertSG

Traducción al Español

Paloma Amilene Vargas Alvarado
E-Mail: amilenhalvarado@gmail.com
Twitter / X: @AmileneVargas

CONTENIDO

1. ABSTRACTO

Esta metodología de respuesta a incidentes, es una hoja de referencia dedicada a los analistas que investigan un problema preciso de seguridad.

¿QUIÉN DEBE UTILIZAR HOJAS IRM?

- Administradores.
- Centro de Operaciones de Seguridad.
- CISO y adjuntos.
- CERT (Equipo de respuesta ante emergencias informáticas).

Recuerde: Si se enfrenta a un incidente, siga el IRM y tome notas. Mantenga la calma y, si es necesario, contacte inmediatamente con el equipo de Respuesta a Incidentes o el CERT de su línea de negocio.

2. PASOS PARA LA GESTIÓN DE INCIDENTES

SE DEFINEN 6 PASOS PARA GESTIONAR INCIDENTES DE SEGURIDAD

1. Preparación: prepárese para manejar el incidente
2. Identificación: detectar el incidente
3. Contención: limitar el impacto del incidente
4. Remediación: eliminar la amenaza
5. Recuperación: recuperarse a una etapa normal
6. Lecciones aprendidas: elaborar y mejorar el proceso

IRM proporciona información detallada para cada paso del proceso de respuesta a incidentes. Los pasos provienen de la Guía de Gestión de Incidentes de Seguridad Informática del NIST.

2.1. PREPARACIÓN

OBJETIVO: ESTABLECER CONTACTOS, DEFINIR PROCEDIMIENTOS, REUNIR INFORMACIÓN PARA AHORRAR TIEMPO DURANTE UN INCIDENTE.

Se necesita un buen conocimiento de:

- Las políticas de seguridad habituales de los sistemas operativos.
- Las políticas de perfil de usuario habituales.
- Arquitectura, segmentación de VLAN e interconexiones:
    - Tenga la capacidad de aislar entidades, regiones, socios o Internet.

Asegúrese de que los productos de seguridad del endpoint y perimétricos (pasarela de correo electrónico, cachés proxy) estén actualizados.

Despliegue una solución EDR (Endpoint Detection and Response) en endpoints y servidores:

- Esta herramienta se ha convertido en una de las piedras angulares de la respuesta a incidentes en caso de ransomware o en compromiso a gran escala, facilitando las fases de identificación, contención y remediación.
- Ejecute una Búsqueda EDR y un análisis AV con reglas explícitas de IOC y obtenga los primeros indicadores para el seguimiento del progreso de la remediación.
- Configure sus políticas de EDR en modo de prevención.

Dado que esta amenaza a menudo es detectada por los usuarios finales, concientice a su soporte de TI sobre la amenaza del ransomware.

Bloquee los IOCs (Indicadores de Compromiso) vinculados a actividades de ransomware recopilados por Inteligencia de Amenazas (Threat Intelligence).

Despliegue y opere soluciones de seguridad que permitan la detección y faciliten la respuesta:

- Recopilación de logs en un SIEM.
- Tenga la capacidad de ejecutar herramientas como YARA o DFIR-ORC (ANSSI).
- Tenga una buena retención y verbosidad de logs.
- Defina una postura estricta frente al atacante.
- Prepare una estrategia de comunicación interna y externa.

Si se identifica una máquina con ransomware, desconéctela de la red y manténgala encendida para una investigación forense de la memoria.

PREPARACIÓN DE LAS COPIAS DE SEGURIDAD (BACKUPS):

Asegúrese de tener copias de seguridad exhaustiva, reciente y fiable de los datos de los usuarios locales y de la red.

Puede seguir las reglas de copia de seguridad **3-2-1: cada una de estas reglas** está destinada a asegurar que sus datos se almacenen de múltiples maneras.

Si está haciendo una copia de seguridad, debería tener:

- Al menos tres copias: tres copias diferentes significan tres copias diferentes en lugares distintos. Al mantenerlas en lugares diferentes, se reduce el riesgo de que un solo evento destruya múltiples copias.

- En **dos formatos diferentes**: esto significa que debe utilizar al menos dos métodos diferentes para almacenar sus datos. Por ejemplo, DVD, disco duro, servicios en la nube son formatos diferentes. Pero si almacena dos copias en dos discos duros, solo estará utilizando un formato.

- Con **una de esas copias fuera del sitio (off-site):** Mantener una copia fuera del sitio asegura que, pase lo que pase donde estén sus datos (incendio, robo, desastre natural...), al menos una copia esté segura en otro lugar. En esta regla, los servicios en la nube tienen sentido.

Intente usar un formato de copia de seguridad almacenado fuera de su red: incluso si hay movimiento lateral por parte de la amenaza que daña su red con cifrado, una copia estará fuera de su alcance.

2.2. IDENTIFICACIÓN

OBJETIVO: DETECTAR EL INCIDENTE, DETERMINAR SU ALCANCE E INVOLUCRAR A LAS PARTES APROPIADAS.

SEÑALES GENERALES DE LA PRESENCIA DE RANSOMWARE
Varias pistas pueden indicar que el sistema podría estar comprometido por ransomware:

- Monitoreo de los IOCs de ransomware por un SOC.
- Supervisión de las alertas de EDR.
- Se reciben correos electrónicos profesionales extraños (a menudo disfrazados de facturas) que contienen archivos adjuntos.
- Aparece en el escritorio del usuario un mensaje de rescate que explica que los documentos han sido cifrados y pide dinero.
- Las personas se quejan de que sus archivos no están disponibles o están corruptos en sus ordenadores o en sus recursos compartidos de red con extensiones inusuales (.abc, .xyz, .aaa, etc.).
- Numerosos archivos están siendo modificados en un período de tiempo muy corto en los recursos compartidos de red.
- Publicación de información en los sitios web o foros del operador de ransomware.
- El movimiento lateral se realiza habitualmente; verifique todas las conexiones al servidor AD y ShareFile con cuentas privilegiadas en horarios diurnos anormales.
- Busque actividades de red o navegación web inusuales; especialmente conexiones a IP Tor I2P, pasarelas Tor (tor2web, etc.) o sitios web de pago con Bitcoin.
- Busque conexiones poco comunes.

Determinación del alcance del incidente:

- EDR o herramientas de búsqueda a gran escala como YARA o DFIR-ORC permiten determinar el alcance de las máquinas infectadas con ransomware.
- La prioridad es la identificación del acceso inicial y el pivote utilizado por los atacantes, como en el compromiso por malware a gran escala. Esto permite establecer las acciones de las siguientes fases.

La identificación del Actor de Amenaza que originó el ataque de ransomware podría ayudar en las siguientes fases basándose en las TTPs (Tactics, Techniques and Procedures) conocidas.

La identificación de un compromiso de red por ransomware tiene muchas similitudes con el compromiso por malware a gran escala. La mayoría de las veces, la decisión de reaccionar debe tomarse más rápido en casos de ransomware.

2.3. CONTENCIÓN

OBJETIVO: MITIGAR LOS EFECTOS DEL ATAQUE EN EL ENTORNO OBJETIVO.

- Haga una declaración pública tan pronto como sea posible basándose en la plantilla de comunicación elaborada en la fase de preparación.
- Siga la postura definida en la fase de preparación.
- Envíe las muestras no detectadas a su proveedor de seguridad de endpoints y/o sandboxes privadas.
- Envíe la URL maliciosa, los nombres de dominio y la IP no categorizados a su proveedor de seguridad perimétrica.
- Bloquee el tráfico a los C2 (Command and Control).
- Bloquee cualquier IP detectada como utilizada por los atacantes.
- Aísle la VLAN, interconexión, entidades, regiones, socios o Internet comprometidos.
- Deshabilite las cuentas comprometidas/creadas por los atacantes.
- Desconecte de la red todos los ordenadores que hayan sido detectados como comprometidos.
- Puede aislar con su EDR y cerrar Internet manteniendo solo sus conexiones EDR activas.
- Si no puede aislar los ordenadores, desconecte/cancele las unidades compartidas. (NET USE x: \unc\path /DELETE)

Monitoree los sitios web y el Internet del actor de amenazas de ransomware para buscar si hay alguna publicación de fuga de datos relacionada con el compromiso por ransomware.

2.4. REMEDIACIÓN

OBJETIVO: TOMAR ACCIONES PARA ELIMINAR LA AMENAZA Y EVITAR FUTUROS INCIDENTES.

- Elimine el acceso inicial utilizado por el atacante.
- Elimine los binarios utilizados por el atacante para moverse lateralmente en la red.
- Elimine cualquier cuenta creada por los atacantes.
- Revierta los cambios de configuración.
- Opere un endurecimiento de la configuración de los sistemas y la red.

2.5. RECUPERACIÓN

OBJETIVO: RESTAURAR EL SISTEMA A LAS OPERACIONES NORMALES.

1. Actualice las firmas de antivirus para que los binarios maliciosos identificados sean bloqueados.
2. Asegúrese de que no haya binarios maliciosos presentes en los sistemas antes de reconectarlos.
3. Asegúrese de que el tráfico de red vuelva a la normalidad.
4. Restaure los documentos del usuario a partir de las copias de seguridad.

Priorice su plan de recuperación basándose en su DRP (Plan de Recuperación ante Desastres).

Todos estos pasos deben hacerse de forma gradual y con seguimiento técnico.

- Verifique que las copias de seguridad no estén comprometidas: solo restaure desde una copia de seguridad si está muy seguro de que la copia de seguridad y el dispositivo al que la está conectando están limpios. O
- Reinstale el sistema operativo en el ordenador con una instalación limpia (reimage).
- Restablezca las credenciales, incluidas las contraseñas (especialmente para el administrador y otras cuentas del sistema).

Monitoree el tráfico de red para identificar si queda alguna infección.

Si es posible, aplique geofiltros en los firewalls para bloquear el tráfico ilegítimo de países extranjeros.

Mantenga el monitoreo de los sitios web y el Internet del actor de amenazas de ransomware para buscar si hay alguna publicación de fuga de datos relacionada con el compromiso por ransomware.

2.6. LECCIONES APRENDIDAS

OBJETIVO: DOCUMENTAR LOS DETALLES DEL INCIDENTE, DISCUTIR LAS LECCIONES APRENDIDAS Y AJUSTAR LOS PLANES Y LAS DEFENSAS.

Informe

Se debe redactar un informe de crisis y ponerlo a disposición de todos los actores de la célula de gestión de crisis.

Se deberán describir los siguientes temas:

- Causa inicial de la infección
- Acciones y cronogramas de cada evento importante
- ¿Qué salió bien?
- ¿Qué salió mal?
- Costo del incidente
- Indicadores de compromiso

Capitalizar

Se deben definir acciones para mejorar los procesos de gestión de infecciones por gusanos, para aprovechar esta experiencia.

3. DEFINICIONES

CONCEPTO	DESCRIPCIÓN
IRM	Metodología de Respuesta a Incidentes
CISO	Chief Information Security Officer (ejecutivo responsable de la seguridad de la información)
CERT	Equipo de Respuesta a Incidentes Informáticos
NIST	Instituto Nacional de Estándares y Tecnología
EDR	Detección y Respuesta de Puntos de Acceso
IDS	Sistema de Detección de Intrusiones
IPS	Sistema de Prevención de Intrusiones
IOC	Un IoC (Indicador de Compromiso) es cualquier evidencia forense que indica que un sistema o red ha sido atacado por una amenaza de seguridad.
SIEM	(Gestión de Eventos e Información de Seguridad) es una solución de ciberseguridad que recopila, analiza y correlaciona datos de seguridad para detectar y responder a amenazas en tiempo real.
YARA	Es una herramienta de código abierto utilizada para identificar y clasificar malware mediante la creación de reglas que describen patrones específicos en archivos y procesos.
DFIR - ORC	Digital Forensics and Incident Response, es una metodología integral que las organizaciones implementan para abordar los incidentes de ciberseguridad.
Servidor AD	Un servidor AD (Active Directory) es un servicio de directorio desarrollado por Microsoft que se utiliza para gestionar y almacenar información sobre los recursos de red en un entorno corporativo.
ShareFile	ShareFile es una solución de almacenamiento y uso compartido de archivos que permite a las empresas optimizar los flujos de trabajo y mejorar la seguridad de los datos.
I2P	I2P (Invisible Internet Project) es un proyecto de red anónima que permite la comunicación segura y privada entre usuarios.
tor2web	Tor2Web es una solución de navegador que actúa como una puerta de entrada a la web oscura, permitiendo a los

	usuarios acceder a sitios cebolla utilizando un navegador web normal como Chrome o Firefox.
Sandboxes	Es un entorno virtual aislado que permite ejecutar programas o archivos sospechosos sin afectar el sistema operativo principal, protegiendo así los recursos del sistema de posibles amenazas.
C2	Command and Control, se refiere a la infraestructura utilizada por los atacantes para comunicarse y controlar sistemas comprometidos en una red.