METODOLOGÍA DE RESPUESTA A INCIDENTES

IRM #2 DETECCIÓN DE INTRUSIÓN EN WINDOWS

Análisis de un Sistema sospechoso en Windows

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 3
2. PASOS DE LA GESTIÓN DE INCIDENTES 4
2.1 PREPARACIÓN 5
2.2 IDENTIFICACIÓN 7
2.3 CONTENCIÓN 10
2.4 REMEDIACIÓN 11
2.5 RECUPERACIÓN 12
2.6 LECCIONES APRENDIDAS 13
3. DEFINICIONES 14

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 USAR LAS 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 contacte inmediatamente con el equipo de Respuesta a Incidentes de su línea de negocio o con el CERT si es necesario.

2. PASOS DE 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

El 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 de NIST.

2.1 PREPARACIÓN

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

- Despliegue una solución EDR en puntos finales y servidores.
    - Esta herramienta se convirtió en una de las piedras angulares de la respuesta a incidentes en caso de ransomware o compromiso a gran escala, facilitando las fases de identificación, contención y remediación.
    - Lance la Búsqueda EDR y el escaneo 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.

- En ausencia de EDR, se debe dar acceso físico al sistema sospechoso al investigador forense. Se prefiere el acceso físico al acceso remoto, ya que el hacker podría detectar las investigaciones realizadas en el sistema (utilizando un sniffer de red, por ejemplo).
- Podría ser necesaria una copia física del disco duro para fines forenses y de evidencia. Finalmente, si es necesario, podría requerirse un acceso físico para desconectar la máquina sospechosa de cualquier red.
- Se deben preparar perfiles de adquisición para EDR o herramientas como FastIR, DFIR Orc, KAPE.
- Se necesita un buen conocimiento de la actividad de red habitual de la máquina/servidor. Debe tener un archivo en un lugar seguro que describa la actividad de puertos habitual, para comparar eficientemente con el estado actual.
- Un buen conocimiento de los servicios habituales que se ejecutan en la máquina puede ser muy útil. No dude en pedir ayuda a un Experto en Windows, cuando corresponda.
- Una buena idea también es tener un mapa de todos los servicios/procesos en ejecución de la máquina.

Esté preparado para notificar a los equipos de abuso, a los servicios de aplicación de la ley y a los reguladores si es necesario durante un incidente (gestión de la célula de crisis).

Puede ser una verdadera ventaja trabajar en un entorno corporativo grande, donde todas las máquinas de los usuarios son iguales, instaladas desde una imagen maestra. Tenga un mapa de todos los procesos/servicios/aplicaciones. En dicho entorno donde los usuarios no están autorizados a instalar software, considere cualquier proceso/servicio/aplicación adicional como sospechoso.

Cuanto mejor conozca la máquina en su estado limpio, más posibilidades tendrá de detectar cualquier actividad fraudulenta que se ejecute desde ella.

ENDPOINTS

- Asegúrese de que las herramientas de monitoreo estén actualizadas.
- Establezca contactos con sus equipos de red y de operaciones de seguridad.
- Asegúrese de que se defina un proceso de notificación de alertas y que sea bien conocido por todos.
- Asegúrese de que todo el equipo esté configurado en el mismo NTP (Network Time Protocol).
- Seleccione qué tipo de archivos pueden perderse o ser robados y restrinja el acceso a archivos confidenciales.
- Asegúrese de que las herramientas de análisis estén activas, funcionales (Antivirus, EDR, IDS, analizadores de registros), no estén comprometidas y estén actualizadas.
- Instale desde la misma imagen maestra original.

2.2 IDENTIFICACIÓN

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

1. **Adquisición de evidencia.**

ADVERTENCIA (DATOS VOLÁTILES):

ANTES DE REALIZAR CUALQUIER OTRA ACCIÓN, ASEGÚRESE DE REALIZAR UNA CAPTURA DE MEMORIA VOLÁTIL DESCARGANDO Y EJECUTANDO FTK IMAGER, WINPMEM O OTRA UTILIDAD DESDE UNA UNIDAD EXTERNA. LOS DATOS VOLÁTILES PROPORCIONAN INFORMACIÓN FORENSE VALIOSA Y SON FÁCILES DE ADQUIRIR.

Datos volátiles.

- Los datos volátiles son útiles para realizar análisis en el historial de la línea de comandos, conexiones de red, etc. Utilice "Volatility" si es posible.

Tome una imagen de triaje.

- Utilice herramientas como EDR, FastIR, DFIR Orc, KAPE con perfiles pre configurado.

O una imagen de copia de disco completo.

- Con herramientas como dd, FTKImager, etc.

Advertencia: puede necesitar privilegios de administrador en la máquina o un bloqueador de escritura (write-blocker) (físico o lógico) dependiendo del caso de uso.

2. **Análisis de memoria}**

- Busque procesos maliciosos (rogue processes)
- Revise las DLL y handles de los procesos
- Verifique los artefactos de red
- Busque inyección de código
- Verifique la presencia de rootkits
- Vuelque los procesos sospechosos para un análisis posterior

Si el problema se considera estratégico (acceso a recursos sensibles), se debe activar una célula de gestión de crisis específica p. ej., el IRM de Compromiso a Gran Escala.

3. Identificar mecanismos de persistencia

La persistencia puede estar permitida a través de diferentes técnicas, incluyendo:

- Tareas programadas (Scheduled tasks)
- Reemplazo de servicio (Service replacement)
- Creación de servicio (Service creation)
- Claves de registro de inicio automático y carpeta de inicio (Auto-start registry keys and startup folder)
- Secuestro del orden de búsqueda de Dll (Dll search order hijacking)
- Librerías del sistema legítimas con troyanos (Trojaned legitimate system libraries)
- Política de grupo local (Local Group Policy)
- Complemento de MS office (MS office add-in)
- Persistencia previa al arranque (alteración de BIOS/UEFI/MBR)

*Puede considerar usar Microsoft Autoruns para una victoria rápida.

4. Revisar Registros de Eventos (Event Logs)

- Registro de tareas programadas (creación y ejecución)
- Eventos de inicio de sesión de cuenta (verifique las conexiones fuera del horario de oficina)
- Cuenta local sospechosa
- Servicios maliciosos
- Borrado de Registros de Eventos
- Registros RDP/TSE
- Registros de Powershell
- Registros SMB

5. Súper-Línea de Tiempo (Super-Timeline)

- Procese la evidencia y genere una súper-línea de tiempo con herramientas como Log2timeline.
- Analice la línea de tiempo generada con Timeline Explorer o glogg, por ejemplo.

6. Para ir más allá

- Búsquedas de hash (Hash lookups)
- Anomalías y sellado de tiempo (timestamping) de MFT
- Análisis Antivirus/Yara/Sigma:

Monte la evidencia en modo de solo lectura. Ejecute un escaneo Antivirus o múltiples archivos Yara para una detección de "victoria rápida" (quick-win). Tenga en cuenta que el malware desconocido puede no ser detectado.

Si el problema se considera estratégico (acceso a recursos sensibles), se debe activar una célula de gestión de crisis específica, p. ej., el IRM de Compromiso a Gran Escala.

2.3 CONTENCIÓN

OBJETIVO: MITIGAR LOS EFECTOS DEL ATAQUE EN EL ENTORNO.

Asegúrese de que se hayan identificado todos los puntos de apoyo (footholds) de los atacantes antes de tomar medidas de contención. Sea discreto si es necesario y posible.

La adquisición de la memoria y de artefactos volátiles selectivos debe lograrse antes de los siguientes pasos:

- Si la máquina se considera crítica para la actividad comercial de su empresa y no se puede desconectar, haga una copia de seguridad de todos los datos importantes en caso de que el hacker note que está investigando y comience a eliminar archivos.
- Si es posible, aísle la máquina a través de EDR.
- Si la máquina no se considera crítica para su empresa y se puede desconectar, apague la máquina de la manera más drástica, quitando el cable de alimentación. Si es una computadora portátil con batería, simplemente presione el botón de "apagado" durante unos segundos hasta que la computadora se apague.

Las investigaciones offline deben comenzar de inmediato si el análisis en vivo no arrojó ningún resultado, pero el sistema debe seguir considerándose comprometido:

- Inspeccione los recursos compartidos de red o cualquier carpeta de acceso público compartida con otros usuarios para ver si el malware se ha propagado a través de ellos.
- De manera más general, intente descubrir cómo el atacante ingresó al sistema. Todas las pistas deben ser consideradas. Si no se encuentra ninguna prueba informática de la intrusión, nunca olvide que podría provenir de un acceso físico o de una complicidad/robo de información por parte de un empleado.
- Aplique correcciones cuando corresponda (sistema operativo y aplicaciones), en caso de que el atacante haya utilizado una vulnerabilidad conocida.

2.4 REMEDIACIÓN

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

ADVERTENCIA: SOLO COMIENCE A REMEDIAR UNA VEZ QUE ESTÉ 100% SEGURO DE HABER DELIMITADO Y CONTENIDO BIEN EL PERÍMETRO, PARA EVITAR QUE EL ATACANTE LANCE ACCIONES DE REPRESALIA.

En caso de que el sistema haya sido comprometido:

- La forma más sencilla de deshacerse del malware es remasterizar la máquina.
- Elimine temporalmente todos los accesos a las cuentas involucradas en el incidente.
- Elimine todos los archivos maliciosos instalados y los mecanismos de persistencia implementados por el atacante.
- Aplique el modo de prevención de EDR para todos los IOCs identificados.

2.5 RECUPERACIÓN

OBJETIVO: RESTAURAR EL SISTEMA A LAS OPERACIONES NORMALES.

No importa cuán avanzado haya estado el hacker en el sistema y el conocimiento que haya podido obtener sobre el compromiso, mientras el sistema haya sido violado, la mejor práctica es **reinstalar el sistema completamente desde el medio original y aplicar todas las actualizaciones de seguridad al sistema recién instalado.**

En caso de que esta solución no se pueda aplicar, usted debe:

- **Cambiar todas las contraseñas de las cuentas del sistema** y hacer que sus usuarios hagan lo mismo de forma segura.
- **Restaurar todos los archivos** que podrían haber sido alterados (Ejemplo: svchost.exe) por el atacante.

Para obtener más detalles sobre la autenticación y la recuperación de la infraestructura, consulte el IRMXXX de compromiso de malware a gran escala.

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 incidentes y ponerlo a disposición de todos los actores aplicables.
Los siguientes temas deben ser cubiertos:

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

Lecciones aprendidas.

Se deben definir acciones para mejorar los procesos de gestión de detección de intrusiones en Windows para capitalizar esta experiencia. Los perfiles de las herramientas de adquisición se pueden ajustar para que coincidan mejor con los artefactos detectados durante la investigación.

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.
FastIR	FastIR es un proyecto de código abierto desarrollado para la gestión de incidentes de seguridad. Esta herramienta permite extraer datos de archivos de memoria, realizar recolecciones forenses rápidas y guardar los resultados en archivos CSV.
DFIR - ORC	Digital Forensics and Incident Response, es una metodología integral que las organizaciones implementan para abordar los incidentes de ciberseguridad.
KAPE	KAPE, que significa Kroll Artifact Parser and Extractor, es un conjunto de herramientas de análisis forense digital de código abierto utilizado para adquirir, analizar y presentar pruebas digitales en investigaciones forenses.
ENDPOINTS	Un endpoint se refiere a un punto final o interfaz que permite la comunicación entre diferentes sistemas o componentes de software a través de la red.
Volatility	Es código abierto que permite a los analistas extraer información crucial de sistemas en funcionamiento, como procesos, conexiones de red, etc.
DLL	Los archivos DLL son archivos de biblioteca de vínculos dinámicos que contienen recursos necesarios para que una aplicación funcione correctamente.
handles	Se refiere a un identificador que permite gestionar y acceder a recursos digitales, así como a la identidad de usuarios en plataformas digitales.

BIOS	Firmware que reside en un chip de la placa base y se ejecuta al encender la computadora.
UEFI	Interfaz de firmware que conecta el firmware de un ordenador con su sistema operativo.
MBR	Master Boot Record es un disco que aplica un sector de arranque de la tabla MBR al principio.
Registros RDP	Son archivos de configuración utilizados por el Protocolo de Escritorio Remoto (RDP) para establecer conexiones remotas a otros ordenadores.
Registros TSE	Se refieren a la generación y almacenamiento de registros cronológicos de actividades y eventos del sistema.
Registros SMB	Permiten la comunicación y el intercambio de datos entre dispositivos en una red.
glogg	Es una herramienta de software de código abierto multiplataforma utilizada como un explorador o visor de archivos de registro (logs) rápido e inteligente
Timestamping	Es un mecanismo digital que certifica de manera segura e inalterable que un conjunto de datos o un documento electrónico existieron en un momento preciso y específico del tiempo.
MFT	Managed File Transfer, o Transferencia Gestionada de Archivos.
Sigma	Es un formato de firma de código abierto para detectar amenazas en sistemas SIEM (Security Information and Event Management)
footholds	Se refiere a la fase en la que un atacante o hacker ético, tras comprometer un sistema inicial, logra mantener y asegurar su acceso persistente a dicho sistema o red.