METODOLOGÍA DE RESPUESTA A INCIDENTES

IRM #7: DETECCIÓN DE MALWARE EN WINDOWS

Análisis en vivo en un equipo sospechoso.

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.

- 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 en un 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.
    - Establezca sus políticas EDR en modo de prevención para evitar interrupciones comerciales innecesarias.
- 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).
- Una copia física del disco duro podría ser necesaria para fines forenses y de evidencia. Finalmente, si es necesario, se podría necesitar un acceso físico para desconectar la máquina sospechosa de cualquier red.
- Los perfiles de adquisición para EDR o herramientas como FastIR, DFIR Orc, KAPE, DumpIt, FTK Imager, WinPmem deben prepararse y probarse.
- 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 compararla 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 solicitar la asistencia de un experto en Windows, cuando corresponda. Una buena idea es también tener un mapa de todos los servicios/procesos en ejecución de la máquina.

Endpoints.

- Asegúrese de que las herramientas de monitoreo estén actualizadas.
- Despliegue Sysmon, SmartScreen y aplique líneas base de recomendación de ANSSI y CIS.
- Establezca contactos con sus equipos de red y operaciones de seguridad.
- Asegúrese de que se defina un proceso de notificación de alertas y sea bien conocido por todos.
- Asegúrese de que todos los equipos estén sincronizados con el mismo NTP.
- Seleccione qué tipo de archivos se pueden perder / robar y restrinja el acceso para archivos confidenciales.

- Asegúrese de que las herramientas de análisis estén activas, funcionales (Antivirus, EDR, IDS, analizadores de logs), no comprometidas y actualizadas.
- Instale desde el mismo master original.

2.2 IDENTIFICACIÓN

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

La familia del malware identificado impactará los siguientes pasos de la respuesta a incidentes. La investigación será más rápida para un Software Potencialmente No Deseado (Potentially Unwanted Software) o un Minero. Las familias Stealer, Dropper o Ransomware implicarán un análisis más profundo y pueden conducir a otro tipo de incidente (consulte Compromiso de malware a gran escala, Ransomware, Detección de Intrusiones en Windows o Infección por Worm si es necesario).

Señales generales de presencia en el escritorio.

Varias pistas pueden indicar que el sistema podría estar comprometido por malware:

- El software EDR, HIDS, Antivirus genera una alerta, no puede actualizar sus firmas, se apaga o no puede ejecutar escaneos manuales.
- Actividad inusual del disco duro: el disco duro realiza operaciones enormes en momentos inesperados.
- Computadora inusualmente lenta: desaceleraciones repentinas e inexplicables no relacionadas con el uso del sistema.
- Actividad de red inusual: conexión a Internet lenta / rendimiento deficiente de recursos compartidos de red a intervalos irregulares.
- La computadora se reinicia sin razón.
- Aplicaciones que fallan inesperadamente.
- Ventanas emergentes que aparecen mientras navega por la web (a veces incluso sin navegar).
- Su dirección IP (si es estática) está presente en una o más Listas de Bloqueo de Internet (Internet Blocklists).
- Las personas se quejan de que usted les envía correos electrónicos o se comunica con ellos por mensajería instantánea (IM), etc., mientras que usted no lo hizo.

Si el problema se considera estratégico (acceso a recursos sensibles), se debe activar una célula de gestión de crisis específica (por ejemplo, Compromiso a Gran Escala IRM-18).

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 U 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 sobre el historial de la línea de comandos, conexiones de red, etc. Use "Volatility" si es posible.

- Tome una imagen de triaje:
  Use herramientas como EDR, FastIR, DFIR Orc, KAPE con perfiles preconfigurados.

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

3. **Identifique los mecanismos de persistencia:**
   La persistencia puede estar permitida a través de diferentes técnicas, incluyendo:
   - Tareas programadas
   - Reemplazo de servicio
   - Creación de servicio
   - Claves de registro de inicio automático y carpeta de inicio
   - Secuestro del orden de búsqueda de Dll (Dll search order hijacking)
   - Librerías legítimas del sistema troyanizadas
   - Política de grupo local (Local Group Policy)
   - Complemento (add-in) de MS office
   - Persistencia previa al arranque (alteración de BIOS/UEFI/MBR)

Puede considerar usar Microsoft autoruns para una victoria rápida (quick win).

4. **Verifique los Registros de Eventos**.
   - 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 Powershell
   - Registros SMB

5. Súper-Línea de Tiempo
   - Procese la evidencia y genere una súper-línea de tiempo con herramientas como Log2timeline.
   - Analice la línea de tiempo generada con TimelineExplorer o glogg por ejemplo.
6. Para ir más allá:
   - Búsquedas de Hash
   - Anomalías MFT y marcas de tiempo (timestamping)
   - Anti-virus/Yara análisis/Sigma:
     - Monte la evidencia en modo de solo lectura. Ejecute un escaneo Anti-virus o múltiples archivos Yara para una detección rápida (quick-win).
     - Tenga en cuenta que el malware desconocido puede no ser detectado.

2.3 CONTENCIÓN

OBJETIVO: MITIGAR LOS EFECTOS DEL ATAQUE EN EL ENTORNO.

ADVERTENCIA (DATOS VOLÁTILES):
LA ADQUISICIÓN DE LA MEMORIA Y DE ARTEFACTOS VOLÁTILES SELECTIVOS DEBE LLEVARSE A CABO ANTES DE QUE TENGAN LUGAR LOS SIGUIENTES PASOS.

Si la máquina se considera crítica para la actividad comercial de su empresa y no puede ser desconectada, respalde 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 puede ser desconectada, apáguela de la manera drástica, quitando el enchufe de alimentación. Si es una computadora portátil con batería, simplemente presione el botón de “apagado” durante unos segundos hasta que la computadora se apague.

Envíe los binarios sospechosos a su CERT, o solicite la ayuda del CERT si no está seguro sobre la naturaleza del malware. El CERT debería poder aislar el contenido malicioso y puede enviarlo a todas las empresas de AV, incluidos sus contratistas corporativos. (La mejor manera es crear un archivo comprimido y encriptado con contraseña del binario sospechoso).

Las investigaciones fuera de línea deben iniciarse de inmediato si el análisis en vivo no arrojó ningún resultado, pero el sistema aún debe considerarse 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.
- Más generalmente, intente encontrar cómo el atacante ingresó al sistema. Se deben considerar todas las pistas. Si no se encuentra ninguna prueba informática de la intrusión, nunca olvide que podría provenir de un acceso físico o una complicidad/robo de información por parte de un empleado.
- Aplique correcciones cuando sea aplicable (sistema operativo y aplicaciones) en caso de que el atacante haya utilizado una vulnerabilidad conocida.

2.4 REMEDIACIÓN

OBJETIVO: TOMAR ACCIONES PARA ELIMINAR LA AMENAZA Y EVITAR FUTURAS DESFIGURACIONES.

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

La forma más sencilla de deshacerse del malware es remasterizar la máquina.

- Elimine los binarios y las entradas de registro relacionadas.
- Encuentre las mejores prácticas para eliminar el malware. Por lo general, se pueden encontrar en los sitios web de las empresas de Antivirus.
- Elimine todos los archivos maliciosos instalados y los mecanismos de persistencia implementados por el atacante.
- Aplique el modo de prevención EDR para todos los IOCs identificados.

2.5 RECUPERACIÓN

OBJETIVO: RESTAURAR EL SISTEMA A SUS OPERACIONES NORMALES.

Si es posible, reinstale el SO y las aplicaciones y restaure los datos del usuario a partir de copias de seguridad limpias y confiables. Si lo considera necesario, puede pedir a su mesa de ayuda de TI local que re imagine el disco.

En caso de que la computadora no haya sido reinstalada completamente:

- Restaure los archivos que podrían haber sido corrompidos por el malware, especialmente los archivos del sistema.
- Cambie todas las contraseñas de las cuentas del sistema y haga que sus usuarios hagan lo mismo de forma segura.
- Reinicie la máquina después de que se hayan eliminado todos los archivos sospechosos y confirme que la estación de trabajo no presenta ningún comportamiento inusual. Se recomienda un escaneo completo y actualizado con AV y EDR del disco duro y la memoria.

Si un usuario está en el origen del compromiso, debe reforzar las campañas de concienciación sobre seguridad.

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.

Los perfiles de las herramientas de adquisición pueden ajustarse 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
AV (Antivirus)	Software utilizado para el escaneo con reglas explícitas de IOC, y una herramienta de análisis que, junto con EDR y HIDS, puede generar alertas de compromiso.
IOC (Indicators of Compromise)	Reglas explícitas utilizadas para la búsqueda y el escaneo AV de EDR. También son los indicadores de compromiso que deben incluirse en el informe final.
Sniffer de red (Network Sniffer)	Herramienta que un hacker podría usar para detectar investigaciones remotas, por lo que se prefiere el acceso físico para el análisis forense.
Herramientas de Adquisición/Forenses	Herramientas como FastIR, DFIR Orc, KAPE, DumpIt, FTK Imager, y WinPmem. Se usan para tomar imágenes de triaje o capturar memoria volátil.
Sysmon	Herramienta que debe desplegarse en los puntos finales como parte de la preparación de seguridad.
SmartScreen	Herramienta que debe desplegarse en los puntos finales como parte de la preparación de seguridad.
ANSSI y CIS	Entidades que proporcionan líneas base de recomendación que deben aplicarse a los puntos finales.
NTP (Network Time Protocol)	Protocolo utilizado para asegurar que todos los equipos estén sincronizados.
HIDS (Host-based Intrusion Detection System)	Software de detección de intrusiones a nivel de host que puede generar alertas de compromiso.
Familias de Malware	Tipos de malware cuya identificación afecta los pasos de respuesta. Incluyen Software Potencialmente No Deseado (Potentially Unwanted Software), Miner, Stealer, Dropper, Ransomware y Worm.
Datos/Memoria Volátil	Información forense valiosa (historial de línea de comandos, conexiones de red) que debe capturarse

	inmediatamente antes de cualquier otra acción, utilizando herramientas como FTK Imager o WinPmem.
Volatility	Herramienta recomendada para realizar análisis en datos volátiles.
DLLs (Dynamic Link Libraries)	Librerías dinámicas que deben revisarse durante el análisis de memoria.
Rootkits	Software malicioso utilizado para ocultar la actividad de un atacante. Su presencia debe verificarse durante el análisis de memoria.
Mecanismos de Persistencia	Técnicas utilizadas por el malware para mantenerse activo en el sistema, incluyendo tareas programadas, reemplazo de servicios, claves de registro de inicio automático, y alteración de BIOS/UEFI/MBR.
Microsoft autoruns	Herramienta que se puede usar para la identificación rápida de mecanismos de persistencia.
RDP/TSE, Powershell, SMB	Registros de eventos que deben verificarse durante la identificación.
Log2timeline, TimelineExplorer, glogg	Herramientas utilizadas para procesar evidencia, generar y analizar una Súper-Línea de Tiempo (Super-Timeline) de eventos.
MFT anomalies	Anomalías en la Tabla Maestra de Archivos (Master File Table) de NTFS que deben verificarse en la fase de identificación.
Yara/Sigma	Herramientas o lenguajes de reglas utilizados para el análisis de binarios sospechosos y malware.
Remasterizar (Remaster)	La forma más sencilla de deshacerse del malware, lo que implica esencialmente una reinstalación limpia de la máquina.