

METODOLOGÍA DE RESPUESTA A INCIDENTES

IRM #18 COMPROMISO A GRAN ESCALA

Directrices para manejar y responder a un compromiso a gran escala.

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 PARA LA GESTIÓN DE INCIDENTES	4
2.1 PREPARACIÓN	5
2.2 IDENTIFICACIÓN	6
2.3 CONTENCIÓN	7
2.4 REMEDIACIÓN	8
2.5 RECUPERACIÓN	9
2.6 LECCIONES APRENDIDAS	10
3. DEFINICIONES	11

1. ABSTRACTO

Esta metodología de respuesta a incidentes, es una hoja de consulta dedicada a los encargados 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 (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.
- Bloquee los IOCs (Indicadores de Compromiso) vinculados a actividades de malware 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) (<https://github.com/dfir-orc>).
- Tenga una buena retención de los logs y nivel de detalle.
- Defina una postura estricta frente al atacante.
- Prepare una estrategia de comunicación interna y externa.
- Tenga un proceso para definir una postura tan pronto como se detecte el compromiso: reacción discreta o rápida.

2.2 IDENTIFICACIÓN

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

Detectar la infección

Se debe recopilar y analizar información procedente de varias fuentes:

- Registros de antivirus
- Sistemas de identificación y sistemas de información geográfica (IDS/IPS)
- EDR (Detección y Respuesta de puntos de conexión)
- Intentos de conexión sospechosos en servidores
- Gran cantidad de cuentas bloqueadas
- Tráfico de red sospechoso
- Intentos de conexión sospechosos en firewalls
- Alto aumento de llamadas de soporte
- Carga alta o congelamiento del sistema
- Grandes volúmenes de correo electrónico enviados

Identificar la infección

Analizar los síntomas para identificar el malware, sus vectores de propagación y contramedidas.

Se pueden encontrar clientes potenciales en:

- Boletines del CERT
- Contactos de soporte externo (empresas de antivirus, etc.)
- Sitios web de seguridad
- Capacidades y proveedores de inteligencia de amenazas

Notificar al Director de Seguridad de la Información.

Comuníquese con su CERT nacional y con los reguladores si es necesario.

Evaluar el perímetro de la infección

Defina los límites de la infección (p. ej.: infección global, limitada a una subsidiaria, etc.). Si es posible, identifique el impacto empresarial de la infección.

2.3 CONTENCIÓN

OBJETIVO: MITIGAR LOS EFECTOS DEL ATAQUE EN EL ENTORNO.

OBJETIVO: La célula de gestión de crisis deberá realizar y supervisar las siguientes acciones:

Desconecte el área infectada de Internet.

1. Aísle el área infectada. Desconéctela de cualquier red.
2. Si no se puede desconectar el tráfico crítico para el negocio, permítalo después de asegurarse de que no pueda ser un vector de infección o encontrar técnicas de elusión validadas.
3. Neutralizar los vectores de propagación. Un vector de propagación puede ser cualquier cosa, desde tráfico de red hasta fallos de software. Se deben aplicar las contramedidas pertinentes (parche, bloqueo de tráfico, desactivación de dispositivos, etc.).

Por ejemplo, se pueden utilizar las siguientes herramientas/técnicas:

- Herramientas de EDR (Sirven para dar visibilidad y responder a las amenazas avanzadas).
 - Herramientas de implementación de parches (WSUS).
 - GPO de Windows
 - Reglas del firewall
 - Procedimientos operativos
4. Repita los pasos 2 a 4 en cada subárea del área infectada hasta que el gusano deje de propagarse. Si es posible, monitoree la infección con herramientas de análisis (consola antivirus, registros del servidor, llamadas de soporte).

Es necesario monitorear la propagación del malware.

Dispositivos móviles

- Asegúrese de que el malware no pueda usar su portátil, Smartphone ni dispositivo de almacenamiento móvil como vector de propagación. Si es posible, bloquee todas sus conexiones.
- Pedir a los usuarios finales que sigan las instrucciones con precisión.

2.4 REMEDIACIÓN

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

Identificar

Identificar herramientas y métodos de remediación. Se deben considerar los siguientes recursos:

- Base de datos de firmas de antivirus
- Contactos de soporte externo
- Sitios web de seguridad
- Escaneo de Yara, Loki, DFIR-ORC, ThorLite
- Búsqueda de EDR

Defina un proceso de desinfección. El proceso debe ser validado por una estructura externa, como el CERT, el SOC o el equipo de respuesta a incidentes.

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

Prueba

Pruebe el proceso de desinfección y asegúrese de que funciona correctamente sin dañar ningún servicio.

Desplegar

Implemente las herramientas de desinfección. Se pueden utilizar varias opciones:

- EDR
- Windows WSUS y GPO
- Implementación de firmas de antivirus
- Desinfección manual
- Parches de vulnerabilidades

Advertencia: Algunos gusanos pueden bloquear algunos métodos de implementación de remediación. En tal caso, se debe buscar una solución alternativa.

El progreso de la remediación debe ser supervisado por la equipo de crisis o incidentes.

2.5 RECUPERACIÓN

OBJETIVO: RESTAURAR EL SISTEMA A SUS OPERACIONES NORMALES.

Verifique que todos los pasos anteriores se hayan realizado correctamente y obtenga la aprobación de la gerencia antes de seguir los siguientes pasos:

1. Reabrir el tráfico de red que fue utilizado como método de propagación por el malware.
2. Reconectar las subáreas entre sí.
3. Vuelva a conectar las computadoras portátiles móviles al área
4. Vuelva a conectar el área a su red local
5. Vuelva a conectar el área a Internet

Todos estos pasos se realizarán de forma gradual y el equipo de crisis aplicará una supervisión técnica.

Para obtener más detalles sobre la autenticación y la recuperación de la infraestructura, consulte el IRM-18 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 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 (ANSSI)	Digital Forensics and Incident Response, es una metodología integral que las organizaciones implementan para abordar los incidentes de ciberseguridad
WSUS	Permite a los administradores de tecnologías de la información implementar las actualizaciones de productos de Microsoft más recientes.
ThorLite	Es un escáner de respuesta a incidentes gratuito basado en firmas que utiliza YARA, Sigma y IOCs conocidos para detectar amenazas y anomalías en sistemas Windows, Linux y macOS.
SOC	Un SOC (Centro de Operaciones de Seguridad) es un equipo o función centralizada que se encarga de monitorear, prevenir y responder a incidentes de ciberseguridad en una organización.