METODOLOGÍA DE RESPUESTA A INCIDENTES

IRM #9: MALWARE EN SMARTPHONE

Cómo manejar un Smartphone 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.

El soporte técnico móvil (helpdesk) debe tener un proceso definido: reemplazar el Smartphone del usuario por uno nuevo e aislar el dispositivo sospechoso para su análisis forense.

Se recomienda un buen conocimiento de la actividad habitual del Smartphone (herramientas por defecto y extras instaladas). Un experto en soporte de Smartphone puede ayudar al investigador forense.

Recomendaciones:

- Habilitar el registro de logs (MDM, lista de aplicaciones u otros).
- Instalar antivirus/aplicaciones de seguridad en el smartphone.
- Configurar una VPN para analizar la actividad de red.

Para Forense

- Android:
  - Activar las Opciones de desarrollador con Depuración USB (con precaución por riesgos como estaciones de carga USB públicas).
  - Desbloquear las opciones OEM si es posible.
- Probar las rutinas de extracción con antelación para asegurar la compatibilidad con las evidencias

2.2 IDENTIFICACIÓN

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

Puntos principales de notificación para un smartphone sospechoso:

- Alertas de antivirus o aplicaciones de seguridad.
- Permisos anómalos otorgados a aplicaciones.
- Actividad del sistema anómala o funcionamiento inusualmente lento.
- Actividad de red anómala o conexión lenta a Internet.
- El sistema se reinicia o se apaga sin motivo.
- Las aplicaciones se cierran inesperadamente.
- El usuario recibe mensajes con caracteres inusuales (SMS, MMS, Bluetooth, etc.).
- Aumento en la factura telefónica o actividad web.
- Llamadas a números desconocidos o en horarios/días inusuales.
- Se debe monitorizar la factura del usuario o la actividad de red inusual.

Preguntar al usuario sobre su actividad habitual: qué sitios visita y qué aplicaciones externas instaló.

2.3 CONTENCIÓN

OBJETIVO: MITIGAR LOS EFECTOS DEL ATAQUE EN EL ENTORNO.

Solicitar al usuario sus credenciales de acceso:

- PIN de la tarjeta SIM
- Contraseña del smartphone
- Credenciales de iCloud
- Google Play
- Contraseñas de copias de seguridad

- Asegurarse de que el usuario reciba un dispositivo de reemplazo durante la investigación.
- Respaldar los datos creando un sistema de archivos físico, copia de seguridad lógica o adquisición manual.
- Colocar el teléfono en una bolsa de Faraday si está disponible.

Después de la adquisición, quitar la batería (si es factible) o poner el teléfono en modo avión para bloquear toda actividad (WiFi, Bluetooth, etc.)

Acciones Adicionales:

- Retirar la SIM para análisis adicional fuera del smartphone.
- Realizar un escaneo de seguridad o antivirus a los archivos adquiridos en una estación forense dedicada.
- Realice la rutina forense aplicable según su caso de uso.

Su equipo de respuesta a incidentes debe usar herramientas específicas para liderar la investigación forense en el teléfono inteligente.
Usar soluciones forenses dedicadas como Cellebrite, XRY, Oxygen, Axiom, Andriller, etc..

2.4 REMEDIACIÓN

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

- Eliminar la amenaza identificada del smartphone.
- O bien, limpiar el smartphone infectado y realizar un restablecimiento de fábrica (Hard/Soft reset) con un firmware original.
- Reinsertar la tarjeta SIM en el smartphone.

Reportar todas las aplicaciones maliciosas identificadas que sigan disponibles en las tiendas de aplicaciones para su eliminación.

2.5 RECUPERACIÓN

OBJETIVO: RESTAURAR EL SISTEMA A SUS OPERACIONES NORMALES.

- Reinstalar selectivamente los datos y aplicaciones guardados desde la copia de seguridad.

Se puede considerar mantener el dispositivo en un periodo de cuarentena adicional para controles de seguridad apropiados.

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.
Debatir el incidente con el usuario para mejorar su concienciación.

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
Adquisición de Datos	Proceso de respaldar la información del smartphone mediante la creación de un sistema de archivos físico, una copia de seguridad lógica o una adquisición manual.
Bolsa de Faraday	Herramienta utilizada para aislar físicamente el teléfono y bloquear señales externas.
Modo Avión	Estado del dispositivo para bloquear toda actividad inalámbrica como WiFi y Bluetooth tras la adquisición de datos.
Opciones de Desarrollador / Depuración USB	Configuración necesaria en dispositivos Android para permitir la comunicación y extracción de datos por parte de investigadores forenses.
Restablecimiento de Fábrica (Hard/Soft Reset)	Procedimiento de limpieza del dispositivo para devolverlo a su estado original con un firmware íntegro.
Indicadores de Compromiso (IoC)	Elementos técnicos descritos en el informe final que evidencian la presencia de la intrusión o malware.
Herramientas Forenses mencionadas	Cellebrite XRY Oxygen Axiom Andriller