Preparación 1

Objetivo: Establecer contactos, definir procedimientos y recopilar información para ahorrar tiempo durante un ataque.

- El escritorio de ayuda de móviles debe tener un proceso definido en caso de una infección de malware: sustituir el teléfono inteligente del usuario con uno nuevo y aislar el dispositivo sospechoso para su análisis por el investigador forense.
- Se apreciará contar con un buen conocimiento de la actividad habitual de los teléfonos inteligentes (herramientas por defecto y adicionales que se ejecuten en él). Puede ser útil contar con un experto de apoyo smartphone para ayudar al investigador forense.
- Debe hacerse un seguimiento para comprobar el consumo del usuario o actividad inusual de la red.

Identificación 2

Objetivo: Detectar el incidente, determinar su alcance, e involucrar a las partes apropiadas.

Principales puntos de notificación para smartphone sospechosas:

- El antivirus presenta alertas;
- Actividad inusual del sistema, sistema inusualmente lento;
- Actividad inusual de red, conexión a Internet muy lenta;
- El sistema se reinicia o apaga sin motivo;
- Algunas aplicaciones se bloquean inesperadamente;
- El usuario recibe uno o múltiples mensajes, algunos de ellos podrían tener caracteres especiales (SMS, MMS, Bluetooth, etc);
- Gran incremento en la facturación de teléfono o de la actividad web.
- Llamadas a los números telefónicos inusuales o poco comunes en horas/días inusuales .

Se necesita recoger las evidencias tales como direcciones de Internet.
Pregunte al usuario sobre su actividad habitual en el smartphone: los sitios web que navega, qué aplicaciones externas ha instalado. Esta información puede ser opcionalmente cotejada con la política de la empresa.

Contención 3

Objetivo: Mitigar los efectos del ataque sobre el medio ambiente apuntado.

- Asegúrese de usuario tiene un dispositivo provisional o permanente nuevo para evitar cualquier restricción de tiempo en la investigación.
- Realice una copia de seguridad de los datos del smartphone.
- Retire la batería para bloquear toda la actividad (wifi, Bluetooth, etc).
- Inicie una comprobación antivirus en los equipos que estén o hayan sincronizado con el smartphone comprometido.
- Envíe el smartphone sospechoso y componentes adecuados (SIM, batería, cable de alimentación, tarjetas de memoria) a su equipo de seguridad de respuesta a incidentes. Este equipo le ayudará a aislar el contenido malicioso y enviarlo a las compañías antivirus.

Remedio 4

Objetivo: Emprender acciones para eliminar la amenaza y evitar futuros incidentes.

Si está establecido algún acceso encriptado con contraseña, encuentre una manera de tener acceso a los datos almacenados. Si esto no es posible, la investigación se verá altamente limitada.

Su equipo de respuesta a incidentes deberá de utilizar herramientas específicas para realizar la investigación forense en el smartphone.

Sólo para su información, aquí hay una breve lista de las herramientas que pueden ser útiles:

Herramientas gratuitas: Utilidades de XDA (Windows Mobile), MIAT (herramienta de Adquisición Mobile Interna - Symbian, Windows Mobile), TULP2G, Blackberry Desktop Manager

Herramientas comerciales: XRY, Cellebrite, Paraben ...

Acciones:

- Retire SIM del teléfono inteligente si no lo ha hecho;
- Recupere la historia de teléfono, historial web y todos los "logs" disponibles;
- Recupere el "log" de conexiones a servidor si está disponible;
- Identifique y elimine la amenaza en el smartphone.
- Si la amenaza se relaciona con una aplicación instalada, identifique su ubicación en Internet y retírela.

Recuperación 5

Objetivo: Restaurar el sistema a las operación normal.

Si el usuario necesita recuperar del medio infectado, defina un período de cuarentena y haga la verificación correspondiente con un anti-virus, si es posible, para asegurar que nada podría hacerle daño al usuario o a los sistemas de la organización.

Restaure al dispositivo de destino los datos respaldados previamente desde una fuente confiable.

Una vez que las investigaciones hayan terminado, limpie el smartphone infectado (si es posible) y la restablezca la configuración de fábrica con el firmware original y el sistema de archivos, con el fin de ser utilizado de nuevo.

Repercusiones 6

Informe
Deberá de escribirse un informe de incidente y ponerlo a disposición de todos los interesados. Deberán de describirse los siguientes temas:

- La detección inicial.
- Las acciones y línea de tiempo.
- Lo que sí funcionó.
- ¿Qué salió mal?
- Costo del incidente

Capitalice
Deberán de definirse acciones para mejorar los procesos de detección de malware de Windows para sacar provecho de esta experiencia.

Un aporte para:

Organización de los Estados Americanos

CICTE

IRM #9

Malware en Smartphones

Cómo manejar un smartphone sospechoso

Autor IRM: CERT SG / Julien Touche
Versión IRM: 1.1
email: cert.sg@socgen.com
web: http://cert.societegenerale.com
Traducción: Francisco Neira
email: neira.francisco@gmail.com
Twitter: @neirafrancisco

Extracto

Esta "Metodología de Respuesta a Incidentes" (IRM, por sus siglas en inglés) es una hoja resumen dedicada a los manejadores de incidentes que investigan un asunto de seguridad específico. Quién debe de usar estas hojas IRM?

- Administradores
- Centro de Operaciones de Seguridad (SOC)
- CISOs y sus delegados
- CSIRT (equipos de respuesta a incidentes informáticos)

Recuerde: Si usted afronta un incidente, siga el IRM, tome notas y no pierda el control. Contacte su CSIRT inmediamente si es necesario.

Pasos del manejo de incidentes

Se definen 6 pasos para manejar los incidentes de seguridad:

- Preparación: Alistarse para manejar el incidente
- Identificación: Detectar el incidente
- Contención: Limitar el impacto del incidente
- Remedio: Remover la amenaza
- Recuperación: Recobrar a una etapa normal
- Repercusiones: Delinear y mejorar el proceso