Preparación 1

Se le debe ofrecer al investigador forense un acceso físico al sistema sospechoso.

Se apreciará contar con un buen conocimiento de las actividades habituales de la red y locales de la computadora. Usted deberá tener un archivo con la descripción de la actividad usual de puertos, para así tener un punto de comparación con el estado actual.

Es necesario contar con un buen conocimiento de las aplicaciones comunes y de los servicios que se utilizan. Si es necesario no dude en pedir apoyo a un experto de Windows.

Identificación 2

Signos generales de la presencia de malware en el escritorio
Varios indicios pueden insinuar que el sistema estaría comprometido por malware:

- El antivirus levanta una alerta o no puede actualizar sus firmas o deja de correr o no corre ni siquiera manualmente
- Actividad inusual en el disco duro: El disco duro hace operaciones grandes momentos no esperados.
- Equipo inusualmente lento: si bien solía ofrecer una buena velocidad, últimamente es más lento.
- Actividad inusual de redl: conexión a Internet es muy lenta la mayor parte del tiempo de navegación.
- El equipo se reinicia sin motivo.
- Algunas aplicaciones se cierran o cuelgan de manera inesperada.
- Aparecen ventanas emergentes durante la navegación en la web. (a veces incluso sin estar navegando)
- Su dirección IP (si es estática) está consignada en una o más listas negras de Internet.
- Las personas se quejan de que han recibido un correo electrónico o mensaje instantáneo, mientras que usted no lo hizo.

Las acciones a continuación utilizan las herramientas de Windows por defecto. Los usuarios autorizados pueden utilizar las utilidades de ***sysinternals*** de “troubleshooting” para realizar estas tareas.

Identificación 2

Cuentas inusuales
Busque cuentas inusuales y desconocidas, especialmente en el grupo Administradores:
C:\> lusrmgr.msc

Archivos inusuales

- Busque archivos inusuales de gran tamaño en el soporte de almacenamiento, aquellos mayores a 10 MB.
- Busque archivos inusuales añadidos recientemente en carpetas del sistema, especialmente C:\WINDOWS\system32.
- Busque archivos con el atributo "oculto":
  C:\> dir /S /A:H

Entradas inusuales en el “Registry”
Busque en el Registry del Windows, la existencia de programas inusuales que arrancan el momento que se inicia el equipo, especialmente en:
HKLM\Software\Microsoft\Windows\CurrentVersion\Run
HKLM\Software\Microsoft\Windows\CurrentVersion\RunOnce
HKLM\Software\Microsoft\Windows\CurrentVersion\RunOnceEx
HKLM\Software\Microsoft\WindowsNT\CurrentVersion\Winlogon
Busque las mismas entradas en HKCU

Procesos inusuales y Servicios
Busque entradas inusuales/desconocidas entre los procesos en funcionamiento, especialmente entre los procesos con nombre de usuario "SYSTEM" y "administrador":
C:\> taskmgr.exe
(tlisk o tasklist, según la versión de Windows)
Busque servicios de red inusuales/inesperados instalado e iniciados:
C:\> services.msc
C:\> net start
Nota: Es necesario un buen conocimiento de los servicios habituales.

Actividad inusual de red

- Compruebe si hay recursos compartidos de archivos y verificar cada uno está vinculado a una actividad normal:
  C:\> net view | | 127.0.0.1
- Observe las sesiones abiertas en la máquina:
  C:\> net session
- Observe las acciones que la máquina ha abierto con otros sistemas:
  C:\> net use
- Verifique que no haya conexiones NetBIOS

Identificación 2

sospechosas:
C:\> nbtstat -S

- Busque cualquier actividad sospechosa en puertos TCP / IP del sistema:
  C:\> netstat -na 5 (-na 5 significa actualizar cada 5 seg.)
- Use -o en Windows XP/2003 para ver el dueño de cada proceso:
  C:\> netstat -nao 5
- Utilice un sniffer (Wireshark, tcpdump, etc) y vea si hay intentos de conexiones inusuales hacia o desde sistemas remotos. Si no se presencia actividad sospechosa, use un sniffer mientras navega por algunos sitios web sensibles (sitio web de bancos, por ejemplo) y vea si hay actividad particular en la red.

Nota: Se necesita tener un buen conocimiento de la actividad legítima de la red.

Tareas automáticas inusuales

- Busque entradas inusuales en la lista de las tareas programadas:
  C:\> at
  En Windows 2003/XP: ***C:\> schtasks***
- También puede ver los directorios de usuario de inicio automático:
  C:\Documents and Settings*usuario*\Start Menu\Programs\Startup
  C:\WINNT\Profiles*usuario*\Start Menu\Programs\Startup

Las entradas de registro inusuales

- Busque entradas inusuales en archivos de registro:
  C:\> eventvwr.msc
- Busque eventos como los siguientes:
  “Event log service was stopped”
  “Windows File Protection is not active”
  “The protected System file <nombre> was not restored to its original”
  “Telnet Service has started successfully”
- Busque actividad sospechosa en los archivos de registro de su firewall, si lo hay. También puede utilizar un antivirus actualizado para identificar malware en el sistema, pero tenga en cuenta que podría destruir evidencia.
- En caso de no encontrar nada sospechoso, no significa que el sistema no esté infectado. Por ejemplo un rootkit puede estar activo, evitando que sus herramientas den buenos resultados.
- Si el sistema es aún sospechoso, se puede hacer

• Identificación 2

investigación forense adicional en el sistema mientras está apagado. El caso ideal es hacer una copia bit a bit del disco duro que contiene el sistema, y luego analizar la copia utilizando herramientas forenses como EnCase o X-Ways.

Contención 3

Desconecte físicamente el cable de la red para prevenir más infecciones en la red y para detener la probable acción ilegal que se podría estar realizando desde la computadora (el software malicioso podría por ejemplo, enviar spam de forma masiva, participar a un ataque DDoS o almacenar archivos ilegales en el sistema).
Envíe los archivos binarios sospechosos a su CSIRT o solicite ayuda al CSIRT si no está seguro(a) sobre el malware. En el CSIRT deben ser capaces de aislar el contenido malicioso y lo pueden enviar a las empresas antivirus, particularmente con los proveedores del antivirus que usa su organización. (La mejor manera es creando un archivo comprimido del binario sospechoso, encriptándolo con una contraseña).

Remedio 4

Reinicie desde un CD "Live" y haga una copia de seguridad de todos los datos importantes en un medio de almacenamiento externo. Si no está seguro, lleve su disco duro a la mesa de ayuda y pida que le hagan una copia de todo el contenido importante.

Borre los binarios y las entradas relacionadas en el "Registry"

- Busque las mejores prácticas para eliminar el malware. Por lo general, se pueden encontrar en sitios web de compañías antivirus.
- Ejecute una búsqueda con antivirus en línea.
- Reinicie con un CD live basado en Bart-PE que contenga herramientas de desinfección (se pueden descargar de las páginas web de antivirus), o un CD live dedicado de antivirus.

(***BART CD:*** **B**ootable **A**ntivirus & **R**ecovery **T**ools CD, CD booteable con antivirus y herramientas de recuperación) (***PE***: **P**reinstalled **E**nvironment, Entorno Preinstalado)

Recuperación 5

Si es posible reinstale el sistema operativo y las aplicaciones y restaure los datos del usuario desde una copia de respaldo confiable.

En caso de que el equipo no se haya reinstalado completamente:

Restaure los archivos que podrían haber sido dañados por el malware, especialmente los archivos de sistema.

Reinicie el equipo después de hacer toda la limpieza y revise la salud el sistema, haciendo un análisis con antivirus de todo el sistema, los discos duros y la memoria.

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 #7

Detección de malware en Windows

Análisis en vivo a una computadora sospechosa

Autor IRM: CERT SG / Cédric Pernet
Versión IRM: 1.2
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