Preparación 1

- Al Investigador forense se le deberá de proporcionar acceso físico al sistema sospechoso. Se prefiere acceso físico sobre el acceso remoto pues el atacante podría detectar las investigaciones que se hacen en el sistema (empleando por ejemplo un sniffer)

- Puede ser necesario contar con una copia física del disco duro con propósitos de forensia y de evidencia. Finalmente, puede ser necesario un acceso físico para desconectar la máquina sospechosa de cualquier red.

- Se precisa de un buen conocimiento de la actividad usual de la máquina/servidor en la red. Usted debe de tener un archivo en lugar seguro donde se describa la actividad usual de puertos para poder comparar eficientemente con el estado actual.

- Puede ser de gran ayuda tener un buen conocimiento de los servicios que corren usualmente en la máquina. No dude en pedir ayuda a un experto en Windows si lo considera necesario.. Es una buena idea tener un mapa de los servicios y procesos que se ejecutan en la máquina.

Puede ser una verdadera ventaja trabajar en un medio corporativo muy grande donde todas las máquinas son iguales e instaladas con un CD/DVD maestro. Tenga un mapa de todos los procesos/servicios/aplicaciones. En semejante entorno donde a los usuarios no se les permite instalar software, considere todo proceso/ servicio/aplicación como sospechoso.

Mientras más conozca la máquina en su estado "limpio", más oportunidades tendrá de detectar cualquier actividad fraudulenta ejecutándose en ella.

Identificación 2

Tenga en cuenta que se pueden usar los Utilitarios Sysinternals para troubleshooting para realizar gran parte de estas tareas.

Cuentas inusuales
Busque cuentas inusuales creadas, especialmente dentro del grupo Administadores:
```
c:\> lusrmgr.msc
```
o
```
c:\> net localgroup administrators o net localgroup administradores
```

Archivos inusuales
Busque archivos inusualmente grandes en los medios de almacenamiento, mayores a 5MB. (Puede ser la indicación de un sistema comprometido para almacenamiento de contenido ilegal)
Busque archivos inusuales recientemente añadidos en las carpetas de sistema, especialmente en
```
c:\WINDOWS\system32
```

Entradas inusuales al Registro
Busque en el registro de Windows si hay programas inusuales lanzados al momento de inicializar (boot), específicamente:
HKLM\Software\Microsoft\CurrentVersion\Run
HKLM\Software\Microsoft\CurrentVersion\Runonce
HKLM\Software\Microsoft\CurrentVersion\RunonceEx
Si es posible, use "HiJackThis". Vea también su carpeta Startup

Procesos y Servicios inusuales
Revise todos los procesos ejecutándose en busca de entradas inusuales o desconocidas, en particular aquellas con nombre de usuario "SYSTEM" o "ADMINISTRATOR".
```
c:\> taskmgr.exe
```
(o tlisk, tasklist dependiendo de la versión de Windows)
Utilice **psexplorer** si está disponible

Revise las carpetas "Inicio" de los usuarios
```
c:\Documents ans Settings\user\Start Menu\Programs\Startup
c:\WinNT\Profiles\user\Start Menu\Programs
```

Busque servicios de red inusuales/inesperados instalados e iniciados
```
c:\> services.msc
c:\> net start
```

Identificación 2

Actividad inusual en la red
- Revise los archivos compartidos y verifique que cada uno esté enlazado a una actividad normal:
  `c:\> net view \\127.0.0.1`
  Use "tcpview si está disponible.
- Revise las sesiones abiertas en la máquina:
  `c:\> net session`
- Mire las sesiones que la máquina ha abierto con otros sistemas:
  `c:\> net use`
- Revise si hay conexiones Netbios sospechosas:
  c:\> nbtstat -S
- Busque actividad sospechosa en los puertos del sistema:
  c:\> netstat -na 5
  (el "5" hace que se refresque cada 5 segundos)
  Use la opción -o de Windows XP/2003 para ver el dueño (owner) de cada proceso:
  c:\> netstat -nao 5
  Use fport si es posible.

Tareas automáticas inusuales
Busque si hay entradas inusuales en la lista de tareas programadas:
```
c:\> at
```
En Windows 2003/XP c:\> schtasks

Entradas inusuales en el log
- Revise sus log buscando entradas inusuales:
  c:\> eventvwr.msc
  Si es posible, use "Event Log Viewer" o herramienta similar
- Busque eventos que afecten al firewall, al antivirus, la protección de archivos o cualquier servicio nuevo sospechoso.

- Busque si hay una gran cantidad de intentos fallidos de login o cuentas bloqueadas.
- Revise los archivos de log de su firewall en busca de actividad sospechosa.

Busque la existencia de rootkits
Ejecute "GMER", "TDSSkiller", o similares

Busque malware
Ejecute al menos un antivirus sobre todo el disco. Si es posible use varios antivirus. Éstos deben de estar absolutamente actualizados.

Contención 3

- Si la máquina es considerada crítica para la actividad de su organización y no puede ser desconectada, respalde todos los datos importantes en caso que el atacante note que usted está investigando y empiece a borrar archivos. Haga también una copia de la memoria del sistema para análisis posterior. Puede emplear herramientas como Win32dd, Memoryze, etc.
- Si la máquina no es considerada crítica para su organización y puede ser desconectada, apáguela súbitamente desenchufándola. Si es una laptop con su batería, sólo presione por unos segundos el botón de apagado hasta que se apague.
- Si el análisis en vivo no arrojó un resultado se deben de iniciar inmediatamente las investigaciones "off line" y el sistema aún se debe de considerar como comprometido.

Haga una copia física (bit a bit) de todo el disco duro en un soporte externo de almacenamiento empleando una herramienta forense como EnCase, X-Ways, dd, ddrescue, etc.

Trate de hallar evidencia de cada acción del atacante:

- Busque todos los archivos usados por el atacante, incluyendo archivos borrados y vea que se hizo con ellos o al menos su funcionalidad, con la finalidad de evaluar la amenaza.
- Revise todos los archivos accedidos recientemente.
- Inspeccione los compartidos de red para ver si el malware se ha propagado por ella.
- Mas generalmente, trate de encontrar cómo entró el atacante al sistema. Deben de considerarse todas las pistas. Si no hay prueba computacional de la intrusión, nunca olvide que pudo haber llegado por acceso físico, en complicidad o robo de información por un empleado.
- Aplique todos los "fixes" disponibles al sistema operativo y a aplicaciones en caso el atacante haya usado una vulnerabilidad.

Remedio 4

En caso el sistema haya sido comprometido:

- Remueva temporalmente todos los accesos a las cuentas involucradas en el incidente.
- Borre todos los archivos maliciosos que instaló el atacante.

Recuperación 5

Sin importar cómo entró el atacante al sistema y el conocimiento que usted obtenga del ataque, en medida que el sistema ha sido penetrado, la mejor práctica es reinstalar íntegramente el sistema desde medios originales y aplicarle todos los parches al sistema recién instalado.

Si no se puediese aplicar esta solución, Ud. deberá:

- **Cambiar todas las contraseñas** de cuenta del sistema, y hacer que sus usuarios lo hagan de manera segura: deberán de usar combinaciones de mayúsculas/minúsculas, caracteres especiales y números, 8 caracteres mínimo.

- **Restaure todos los archivos** que pudieran haber sido cambiados por el atacante. p.ej. svchost.exe

Repercusiones 6

Informe
Deberá de redactarse un informe de crisis que será distribuído entre todos los actores de la célula de manejo de crisis.

Deben de describirse los siguientes temas:
Causa inicial de la infección
Acciones y líneas de tiempo de cada evento importante
Qué salió bien
Qué salió mal
Costo del incidente

Capitalice
Deberán de definirse las acciones para mejorar los procesos de manejo de infecciones de gusanos para capitalizar esta experiencia.

Un aporte para:

Organización de los Estados Americanos

CICTE

IRM #2

Detección de Intrusión en Windows

Análisis en vivo sobre un sistema sospechoso en Windows

Autor IRM: CERT SG / Cedric 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