Metodología de Respuesta a Incidentes Detección de Malware en Sistemas Operativos Windows

REPÚBLICA DOMINICANA
Con la gente y para la gente
MINISTERIO DE LA PRESIDENCIA
CNCS CENTRO NACIONAL DE CIBERSEGURIDAD REPÚBLICA DOMINICANA
CSIRT-RD
Equipo Nacional de Respuestas a Incidentes Cibernéticos del CNCS
REPÚBLICA DIGITAL

Metodología de Respuesta a Incidentes Detección de Malware

Este documento es un resumen dirigido a los responsables de manejar incidentes y/o investigadores de asuntos de seguridad informática, con el objetivo de orientarlos en el paso a paso ante un incidente de malware.

Preparación

El propósito de esta etapa es contar con los procedimientos organizados para poder manejar los incidentes de malware y tener la capacidad de determinar los eventos que deben ser escalados a incidentes.

Como punto inicial, el equipo de respuesta a incidentes debe contar y credenciales con permisos administrativos, así como también contar con cuentas administrativas de emergencia solo para casos de ocurrencia del incidente.

En esta primera fase de gestión de incidentes, el analista debe tener acceso físico al sistema y contar con toda la información necesaria lo más detallada posible, de las actividades que se realizan en el equipo y en la red a la cual se encuentra conectado.

Así como también deberá contar con una descripción de las aplicaciones comunes, de los servicios que se utilizan y del comportamiento de los puertos relacionados a este equipo, esto con la finalidad de brindar un escenario que sirva como punto de comparación.

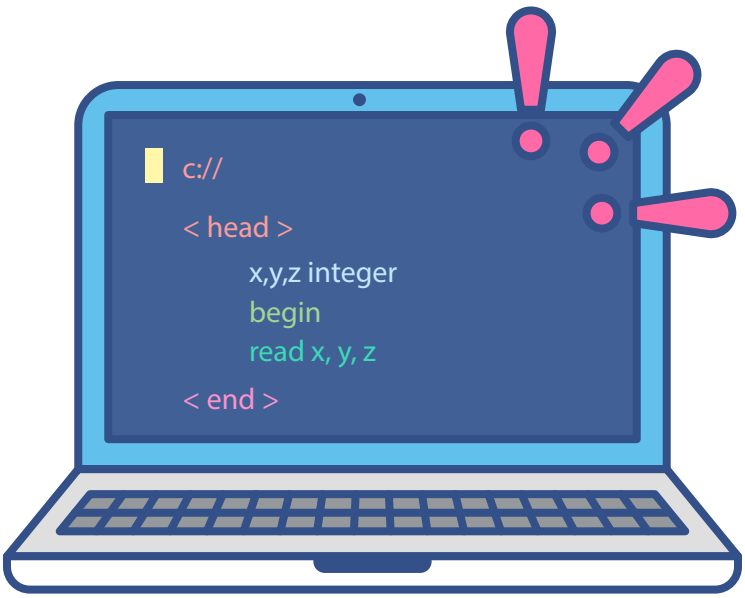
Es importante resaltar, contar con la correcta configuración de las aplicaciones y servicios relacionados a la prevención de malware en cuanto a alertas y otros métodos que permiten la respuesta oportuna ante el incidente.

La organización debe aplicar las buenas prácticas de políticas de backups periódicos tanto dentro como fuera de línea, que cumplan con el Punto Objetivo de Recuperación (RPO) o permitan el retorno al punto de tolerancia definido con anterioridad.

Identificación

Existen varios indicadores que pueden ser asociados a un equipo infectado por malware;

- **El antivirus levanta una alerta o no puede actualizar sus firmas, así como también presenta inconvenientes a la hora de realizar el análisis al equipo.**
- **Procesos inusuales en el disco duro y memoria.**
- **El equipo presenta una lentitud en el procesamiento que antes no solía presentar.**
- **Aparecen ventanas emergentes durante la navegación en la web.**
- **El equipo se reinicia sin motivo.**
- **Tus contactos reciben correos electrónicos de anuncios y temas relacionados que no fueron enviados por el usuario del dispositivo.**



Las siguientes acciones son realizadas utilizando las herramientas por defecto que dispone Windows, los usuarios autorizados pueden utilizar sysinternals de Troubleshooting para realizar las siguientes tareas:

- Identificación de cuentas inusuales especialmente en el grupo de administrador **C:\> lusrmgr.msc**

- Identificación de archivos inusuales o archivos añadidos recientemente en **system32** y con el atributo **“oculto” C:\> dir /S /A:H**

- Identificación de entradas inusuales al Registro de Windows especialmente en;

  - o HKLM\Software\Microsoft\Windows\CurrentVersion\Run
  - o HKLM\Software\Microsoft\Windows\CurrentVersion\RunOnce
  - o HKLM\Software\Microsoft\Windows\CurrentVersion\RunOnceEx

- Identificar procesos inusuales y servicios con nombre de Usuario SYSTEM y ADMINISTRADOR

- Identificar servicios inusuales de red **C:\> services.msc & C:\> net start**

- Identificar actividades inusuales en la red como recursos compartidos **C:\> net view \ \ 127.0.0.1,** sesiones abiertas en máquinas **C:\> net session**, conexiones NetBios **C:\> nbtstat -S**, actividad sospechosa de TCP/IP **C:\> netstat -nao.**

- Identificar entradas inusuales en la lista de tareas programadas **C:\> SCHTASKS /Query**

- Identificar entradas de registros inusuales **C:\> eventvwr.msc** buscar eventos como los siguientes;

  - o “Event log service was stopped”
  - o “Windows File Protection is not active”
  - o “The protected System file <nombre> was not restored to its original”
  - o “Telnet Service has started successfully”
  - o Así como también identificar registros en su firewall y antivirus.

En caso de que se realicen estas indagaciones y el sistema aún continúe con un procesamiento sospechoso se debe realizar una investigación forense al sistema, para lo cual sería ideal una copia bit a bit del disco duro para fines de análisis y así evitar comprometer la evidencia.

Contención

Para contener este tipo de incidentes se debe desconectar físicamente el cable de la red para prevenir más infecciones y para detener la posibilidad de acciones ilegales por los ciberatacantes.
De igual forma se pueden realizar las siguientes acciones:

- Bloquear dirección de correo electrónico que envía (Exchange, Postfix, Barracuda, etc).
- Bloquear direcciones IP fuente de servidor correo (Firewall, IDS/IPS, etc)
- Identificar los Indicadores de Compromiso (IoC) para detectar otros hosts que pudieran estar infectados.
- En caso de que el correo de phishing contenga alguna URL realizar el bloqueo. Así como también identificar otras URL relacionadas para su bloqueo.
- Borrar el correo de la bandeja de entrada del usuario para evitar vuelva acceder al correo.
- Envíe los archivos sospechosos al CSIRT-RD o solicite ayuda si no tiene seguridad sobre el malware enviando la muestra a Incidentes@csirt.gob.do

Remediación

Una de las medidas de remediación para este tipo de incidentes es la siguiente:

- Con la utilización de un CD “Live” reinicie el equipo y realice una copia en un disco externo de toda la información importante.
- Una vez con acceso a los registros identificados como malicioso utilice herramientas para desinfección, esto puede hacerlo utilizando un CD de inicio con antivirus y herramientas de recuperación en un entorno preinstalado.

Recuperación

EL proceso de recuperación, de ser posible, deberá reinstalar el sistema operativo y las aplicaciones, restaurando los datos del usuario desde la última copia actualizada de respaldo confiable.

En caso de que no se cuente con un respaldo confiable o no sea posible la restauración completa del equipo, se podrían tomar las siguientes acciones:

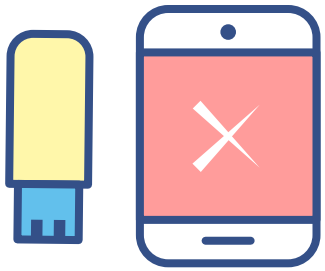
- Restaure los archivos del sistema que pudiesen haber sido afectados por el malware.
- Reiniciar el equipo después de realizar una limpieza.
- Realizar las pruebas del correcto funcionamiento fuera de línea o desconectado de la red.
- Revisar que no exista persistencia en la ejecución de archivos y procesos del sistema.

Documentación e Informe

Se deberá realizar un informe del incidente y distribuirlo a todos los interesados donde inicialmente se describen los siguientes puntos:

- Detección inicial
- Acciones y línea de tiempo
- Base de conocimiento (lecciones aprendidas)
- Impacto del incidente
- Indicadores de Compromiso (IoC)

Así como también será necesario mejorar los procesos relacionados a la detección de malware y los controles relacionados a la causa de la infección.



REPÚBLICA DOMINICANA
Con la gente y para la gente

MINISTERIO DE LA PRESIDENCIA

CNCS
CENTRO NACIONAL DE CIBERSEGURIDAD
REPÚBLICA DOMINICANA

CSIRT-RD
Equipo Nacional de Respuestas a Incidentes Cibernéticos del CNCS

REPÚBLICA DIGITAL

Metodología de Respuesta a Incidentes Detección de Malware Sistemas Operativos Windows