Carrera: Tecnicatura en Ciberseguridad
Materia: FdCyPIC
JTP: Eduardo Winkler
Alumno: Alfredo Carini
Comisión: 2

UNIVERSIDAD NACIONAL RAÚL SCALABRINI ORTIZ SAN ISIDRO

Procedimiento para la gestión de incidentes de malware (gusano)

INTRODUCCION

Este documento tiene por objeto contemplar las acciones y procedimientos necesarios para la preparación, identificación, contención, remediación, recuperación y actividades post incidente resultantes de una infección por malware de tipo gusano informático.

Comportamiento

Este tipo de Malware se replica a sí mismo y luego se propaga a través de las interfaces de red sin necesidad de interacción por una aplicación del host o de parte del usuario.

Medio infección / propagación

La mayoría de los gusanos informáticos conocidos se propagan de una de las formas siguientes:

- Archivos enviados como adjuntos a correos electrónicos
- A través de un enlace a un recurso web o FTP
- A través de un enlace enviado en un mensaje ICQ o IRC
- A través de redes de uso compartido de archivos P2P
- A través de paquetes de red que se introducen directamente en la memoria del ordenador para, a continuación, activarse el código del gusano.

Objetivo

El objetivo de este malware suele ser colapsar los ordenadores y las redes informáticas, impidiendo así el trabajo a los usuarios.

También generar puertas traseras o backdoors y posteriormente usarla para tomar el control remoto del equipo.

Carrera: Tecnicatura en Ciberseguridad
Materia: FdCyPIC
JTP: Eduardo Winkler
Alumno: Alfredo Carini
Comisión: 2

UNIVERSIDAD NACIONAL RAÚL SCALABRINI ORTIZ SAN ISIDRO

GESTION DEL INCIDENTE

Durante el transcurso del incidente se debe:

- Clasificar el incidente: determinar tipo y alcance del incidente, vector de ataque
- Priorizar que recursos se asignan al incidente de acuerdo a la gravedad del mismo
- Gestionar el incidente:
    a) Darle un estado al incidente
        - abierto cuando se recibe el reporte del mismo
        - Pendiente cuando se están tomando acciones sobre el mismo
        - Cerrado una vez resuelto el incidente

    b) Darle seguimiento al incidente durante el transcurso del mismo y por un tiempo de 2 semanas una vez finalizado.
    c) Asignar a la resolución del incidente los recursos determinados en función de su magnitud y criticidad.
    d) Recolectar toda la evidencia digital forense del ataque

FORMULARIO DE REPORTE DE INCIDENTE

GESTIÓN DE INCIDENTES								CODIGO INCIDENTE:	
Fecha:			Hora:					Estado:	
QUIEN NOTIFICA	Apellido y Nombre:							Área:	
Email:			Tel interno:					Cargo:	
SOBRE EL INCIDENTE	Marque con **X** las opciones que considere se aplican al mismo								
Ingeniería social, fraude o phishing			Modificación, instalación o eliminación no autorizada de software.						
Destrucción no autorizada de información			Ataque o infección por código malicioso (virus, gusanos, troyanos, etc.						
Robo o pérdida de información.			Acceso o intento de acceso no autorizado a un sistema informático.						
Eliminación insegura de información			Modificación o eliminación no autorizada de datos.						
Anomalía o vulnerabilidad de software			Interrupción prolongada en un sistema o servicio de red						
Amenaza o acoso por medio electrónico			Divulgación no autorizada de información personal.						
Uso indebido de información crítica			Uso prohibido de un recurso informático o de red						
Otro no contemplado. Describa			Modificación no autorizada de un sitio o página web						
Descripción del incidente:									
El incidente esta aun en progreso?				SI		NO		NO LO SE	
¿Existe copia de respaldo de los datos o software afectado?				SI		NO		NO LO SE	
¿El recurso afectado tiene conexión con la red?				SI		NO		NO LO SE	
¿El recurso afectado tiene conexión a Internet?				SI		NO		NO LO SE	
Sistema, computadora o red afectada:									
Localización Física:									
Sistema operativo:									

UNIVERSIDAD NACIONAL RAÚL SCALABRINI ORTIZ SAN ISIDRO

Ciclo de vida del incidente

1. PREPARACION

   Todas aquellas actividades que por la naturaleza de este tipo de malware tiendan a impedir / prevenir la infección.

   a) Se debe formar / implementar un equipo de respuesta a incidentes (CIRT) o similar y definir roles y actividades de sus integrantes.
   b) Se debe configurar la menor cantidad de servicios (principio de menor privilegio) con el fin de proveer únicamente aquellos servicios necesarios tanto a usuarios como a otros equipos.
   c) Se deben revisar configuraciones por default (passwords y archivos compartidos).
   d) Utilizar, mantener actualizado y monitoreado un SIEM.
   e) Se debe tener en todo momento activados los escudos antivirus de correo electrónico para escanear los archivos adjuntos ANTES de abrirlos.
   f) Se debe tener la vista previa de los mensajes de correo electrónico desactivada ya que el solo hecho de hacer un preview del archivo adjunto de un correo puede activar el script de un gusano y originar la infección.
   g) Evitar abrir y eliminar cualquier archivo recibido con las siguientes extensiones:

      exe, com, bat, pif, vbs, scr, doc, xls, msi, eml

   h) Solo se podrán usar enlaces y recursos FTP que sean previamente securizados, No se deben abrir enlaces que vengan de cualquier remitente externo a la red. Los recursos FTP que vengan desde fuera de la red deben abrirse SIEMPRE en una sandbox o similar.
   i) Los programas P2P deben estar restringidos en el firewall mediante el cierre de los puertos asociados o el uso de WAP.
   j) Mantener los sistemas operativos totalmente actualizados para evitar vulnerabilidades usadas por los gusanos para replicarse.
   k) Mantener los antivirus actualizados.
   l) Actualizar de forma constante las aplicaciones de terceros, no usar y eliminar aplicaciones inseguras u obsoletas (adobe flash, java, etc.).
   m) NO usar cracks ni generadores de claves descargados desde internet.
   n) Usar y tener activos SIEMPRE (si se tienen) los balanceadores de carga de la red.
   o) Es recomendable utilizar segmentación de la red para poder aislar el tráfico en el / los segmentos comprometidos.

UNIVERSIDAD NACIONAL RAÚL SCALABRINI ORTIZ SAN ISIDRO

2. IDENTIFICACION

En esta fase se debe identificar el tipo de infección, el vector de ataque y determinar su alcance, para ello se debe tener en cuenta los siguientes indicios para identificar posibles infecciones por gusano:

a. Rendimiento inferior a lo normal en el equipo debido al alto consumo de memoria RAM por parte del malware.
b. Conexión a internet o a la red excesivamente lenta debido al incremento de tráfico producido por el malware.
c. Ventanas emergentes o mensajes en el escritorio, NUNCA hacerles click ni aceptarlos ni cerrarlos.
d. Programas que se abren y se ejecutan automáticamente.
e. Caídas de dispositivos de red por sobrecarga o alertas de trafico de los mismos.
f. El espacio libre de almacenamiento de un equipo disminuye de forma anormal debido a la alta replicación del malware.
g. Fallas durante la descarga de actualizaciones del sistema operativo o de programas instalados.
h. Funcionalidades deshabilitadas del sistema operativo o de programas.
i. Trafico por conexiones de red entrantes y salientes por puertos y protocolos comúnmente no utilizados.

3. CONTENCION

Debido al comportamiento altamente replicativo del gusano se deben tomar las siguientes medidas en cuanto se ha confirmado la infección para evitar o limitar su propagación:

a. No apagar el /los equipos infectados para evitar la posible pérdida de información volátil.
b. Desconectar inmediatamente el / los equipos afectados de la red / internet.
c. No usar credenciales de autenticación de ningún tipo hasta no resolver el incidente.
d. No borrar ningún archivo sospechoso, en su lugar confinarlo o contenerlo.
e. Identificar el vector de ataque utilizado para desactivarlo o aislarlo transitoriamente en el resto de los equipos no comprometidos.
f. Analizar los paquetes de red para identificar tráfico anormal.
g. Suspender o aislar los segmentos de red que puedan estar comprometidos hasta definir el alcance de la infección.
h. Realizar una búsqueda en el sistema afectado de archivos con doble extensión por ejemplo.mp4.exe o .avi.exe o similares y aislarlos inmediatamente.
i. Activar (si es factible) la protección contra escritura de las unidades de almacenamiento.
j. Deshabilitar las herramientas de backup automáticas o recuperación de sistema para que no hagan copias del sistema infectado hasta que se elimine la amenaza.

4. REMEDIACION
    a. Recolectar toda evidencia forense del ataque (archivos infectados, logs del sistema, logs del trafico de red de SIEM, copias de volcado de memoria RAM.
    b. Correr un análisis completo de sistema con el antivirus a todos los equipos afectados para que este elimine los archivos infectados.
    c. Si en antivirus no logra eliminar la infección, se debe tomar nota de que malware se trata y se debe usar un medio de arranque seguro y correr una herramienta de escaneo de malware para hallar los archivos infectados y eliminarlos.
    d. Si no se puede eliminar el gusano automáticamente con herramientas de software, se debe buscar en knowledge bases el malware encontrado y aplicar manualmente los pasos para su remoción.
    e. Se debe eliminar asimismo cualquier copia de seguridad o de recuperación de sistema que se encuentre comprometida.
    f. Si no es posible la remoción de los archivos infectados se debe reconstruir / reinstalar el sistema desde cero en la fase de recuperación.

5. RECUPERACION

    En este punto se deben llevar a cabo el conjunto de acciones para restaurar los sistemas afectados a un funcionamiento correcto para asegurar la continuidad de las operaciones y servicios críticos de la organización:

    a. Restaurar o reinstalar el software de los equipos infectados.
    b. Restaurar copias de seguridad no comprometidas para recuperar los archivos eliminados durante la fase de remediación.
    c. Volver a activar las copias de seguridad automáticas y las copias de restauración de sistema.
    d. Volver a activar cualquier otro servicio que haya sido desactivado durante la fase de contención.
    e. Volver a conectar los equipos a la red / internet.
    f. Volver a habilitar el trafico de los segmentos de red que hayan sido desconectados o aislados durante la contención.

6. ACTIVIDADES POST INCIDENTES

En este momento se deben aplicar aquellas medidas tendientes a subsanar, mejorar y fortalecer todo aquello que se identificó como débil o vulnerable en los pasos anteriores, así como restituir las operaciones a su funcionamiento optimo.

a. Aplicar todos los parches de seguridad faltantes sobre las vulnerabilidades encontradas
b. Revisar y optimizar las reglas de firewalls
c. Cambiar las credenciales de acceso de manera preventiva.
d. Revisar las listas de control de acceso y reemplazarlas de ser necesario
e. Implementar mejoras sobre correo electrónico como filtrado de correo y análisis heurístico de correos y archivos adjuntos.
f. Modificar los sistemas operativos de los hosts para prohibir la ejecución automática de programas mediante un script o la inserción de dispositivos removibles.
g. Documentar todas las cuentas, máquinas, etc. comprometidas para que se pueda realizar un registro, posteriores mediciones y análisis futuros sobre incidencias en ellos.
h. Establecer capacitaciones a usuarios sobre links maliciosos en la web y manejo de links y archivos adjuntos en correo electrónico.
i. Crear si es que no existe un registro de incidentes.
j. Verificar si los roles y actividades definidos previamente se cumplieron durante el incidente.
k. Una vez cerrado el incidente realizar el seguimiento del mismo y luego archivar en el registro de incidentes.