Plan de respuesta a un incidente de malware en nuestra organización

Agudelo Salazar Alejandro
Universidad Piloto de Colombia
Alejandro.agudelo17@gmail.com

***Abstract* – At present the risk of seeing affected by an incident related to malware are higher each time, due to the ease of doing and the continuing development of the same, for which we have very well-defined policies in the company of prevention, and be prepared to respond appropriately to a situation in which jeopardize our information in any of its properties, availability, confidentiality or integrity.**

***Resumen* - En la actualidad los riesgos de vernos afectados por un incidente relacionado con malware cada vez son más altos, debido a la facilidad de conseguirlo y al continuo desarrollo de los mismos, para cual debemos tener muy bien definidas políticas en la compañía de prevención, y estar preparados para responder debidamente ante una situación en el que se ponga en peligro nuestra información en cualquiera de sus propiedades, disponibilidad, confidencialidad o integridad.**

***Palabras Clave* – Malware, prevención, recuperación, ataque, código malicioso, vector de ataque.**

I. INTRODUCCIÓN

Malware, también conocido como código malicioso, o software malicioso, es un programa que se introduce en nuestro sistema buscando comprometer la confidencialidad, la integridad o la disponibilidad de nuestra información. Esto lo convierte en el vector externo más común y a la vez más peligroso.

Pero para intentar gestionar un incidente de seguridad relacionado con malware con eficiencia, debemos como primer paso empezar por clasificarlo de la manera correcta, definir con claridad que pasos debemos seguir en el proceso de presentar el sistema y tener evidencias para estudiar los vectores de ataque y prevenir nuevas infecciones.

II. CATEGORÍAS DE MALWARE

En esta sección se busca clasificar los diferentes tipos de código malicioso como virus, worms, Trojan horses, y código malicioso para móviles, también sus combinaciones, esto explicando cómo cada uno entra e infecta el sistema, como trabaja en términos generales, cuál es su objetivo y cómo afecta el sistema.

a) *Virus:* Un está diseñado para reproducirse y distribuir copias en otras carpetas, o programas del sistema. Cada código tiene su propio mecanismo de reproducción, y también su objetivo que puede pasar desde anuncios molestos, como extraer información sensible como datos personales o acabando el sistema. Algunos deben ser ejecutados por el usuario para que la infección se haga efectiva, esta puede ser abriendo un archivo, ejecutando una aplicación, o dando click en un email malicioso, los virus se dividen principalmente en dos categorías, virus compilados y virus interpretados.

b) *Virus Compilados:* Son aquellos que su código fuente fue compilado para ser ejecutado en el sistema operativo.

c) *Virus Interpretados:* Estos no fueron compilados por tanto no puedes ser ejecutados en el sistema operativo por sí solo, ellos deben ser ejecutados por una aplicación en específico, o un servicio que sea vulnerable

Los virus se valen de diferentes métodos de ofuscación para evitar ser detectados algunas de estas técnicas son

- Self-Encryption and Self-Decryption, en la cual el virus por sí mismo se encripta y decripta para evitar ser detectado.
- Polymorfismo, este se auto encripta, alterando las técnicas comunes de encripción y así alterando la manera de decriptar el código, en esta técnica no se altera el contenido del código.
- Metamorfismo, la idea de esta técnica es encriptar el código y cambiar el código en si del virus, esto puede hacerse añadiéndole código que no es necesario, basura o cambiando las secuencias de código, este se compila y cambia la apariencia del ejecutable para no ser detectado.
- Sigiloso, en esta técnica se interfiere con la lista de los archivos de sistema operativo y no se refleja el cambio de tamaño en los archivos infectados.

d) *WORMS:* Estos se reproducen y son empaquetados en sí mismo, no necesitan un programa de la víctima para infectarla, y no necesitan intervención del usuario, por esto pueden infectar más víctimas en cortos espacios de tiempo que los virus. Se valen de vulnerabilidades conocidas instalando backdoors o dañando el sistema.

e) *Troyanos:* Parecen programas inofensivos que no se replican pero tienen propósitos maliciosos escondidos, modificando archivos de aplicaciones y archivos de sistema, modificando su función para ejecutar acciones maliciosas.

f) *Código Malicioso Móvil:* Este tipo de malware se ejecuta desde un sistema remoto hacia el host víctima, y no necesita interacción del usuario, se vale de las vulnerabilidades conocidas en los sistemas para ganar privilegios por configuraciones por default, es escrito por lo general en lenguajes como Java, ActiveX, JavaScript, y VBScript.

g) *Ataques combinados:* Es una instancia donde se usan diferentes vectores de infección como pueden ser por email, un usuario vulnerable abre un correo infectado, luego se ejecuta un adjunto, un archivo compartido de Windows vulnerable, se escanean y por mensajes de netbios se propaga la infección, se comprometen archivos del web server y se infectan los usuarios que usen este servicio.

h) *Rastreo de cookies:* Una cookie es una pequeña porción de información del uso de una página web, las *session cookies* son temporales y válidas para una sola sesión de un sitio web. Por otro lado las cookies persistentes tienen tiempo de duración alta o indefinida y sirven para mejorar el desempeño de la página, identificación del usuario y customización de sus necesidades y gustos.

Para el caso de estudio el malware roba estas *session cookies* y las modifica para que cuando el usuario visita páginas web los anuncios lo dirijan a sitios web maliciosos y así infectarlo mediante otros ataques descritos.

i) *Herramientas de atacante:* Son herramientas descargadas para abrir puertas traseras, estas también pueden tener puertas trasera e infectar a un atacante inexperto.

j) *Backdoors:* Término genérico para un programa malicioso que está escuchando comando remotos. Por lo general se componen de usuario y servidor.

El usuario es el atacante que está enviando comandos y manipulando el sistema comprometido.

El servidor es el sistema infectado y quien está escuchando los comandos enviados por el usuario, estos comandos son aceptados según el nivel de compromiso del sistema afectado, su nivel de privilegios y funcionalidades instaladas, ya sea permisos de root, administrador o permisos de lectura y ejecución limitados.

k) *Key Loggers:* Monitorean y guardan todas las teclas usadas en el server, luego son enviadas al cliente según la configuración aplicada en la herramienta, ya sea por email o enviados a un ftp del atacante.

l) *RootKits:* Son un conjunto de archivos que se instala en el host infectado reemplazando los archivos originales de sistema o documentos personales del host infectado para alterar su normal funcionamiento.

m) *Plug-ins de explorador WEB:* Estos se instalan en el browser para actuar como spyware y así monitorear las actividades del host infectado. Algunas de las acciones maliciosas que se ejecutan son convertir el equipo comprometido en elemento para hacer llamadas de alto costo, sin que la cuenta llegue al atacante, por el contrario, el usuario infectado tendrá que asumir estos cargos.

n) *Generadores de email:* Se usan para enviar gran cantidad de email ya sea de publicidad o una campaña de malware con contenido malicioso, esto sin permitir que la IP del atacante sea catalogada en las lista de anti-spam como una IP peligrosa, y así poder seguir actuando libremente.

o) *Packet Sniffer:* Monitorean el tráfico de una red y lo guardan para posteriormente analizarlos y verificar datos que se trasmiten en texto plano, esto con el fin de recolectar la mayor cantidad de información posible de la infraestructura a atacar.

p) *Scanner de Puertos:* Esta herramienta se usan para verificar los puertos que están disponibles en la infraestructura a atacar, con el fin de verificar que servicios están publicando e identificar los posibles objetivos, la más usada es nmap, la cual con la configuración correcta provee gran cantidad de información acerca de los servicios publicados lo que facilita la búsqueda de vulnerabilidades conocidas y la aplicación de exploits existentes para su explotación.

q) *Scanner de Vulnerabilidades:* Identifica las vulnerabilidades en los servicios escaneados lanzando una lista de scripts almacenados en su base de datos esto con el fin de testear a cual son vulnerables, también dentro del proceso de crawling identifican archivos disponibles con información sensible que puede ser usada para ejecutar ataques más avanzados.

r) *Programas de Login Remoto:* Una vez comprometido un servicio, este puede ser el puente para acceder a otro dentro de la infraestructura según la configuración de la red, en este caso el atacante instala agentes que le permiten intentar conexiones hacia otros objetivos.

s) *Amenazas no-malware:* Esta se compone de phishing y falsas amenazas de virus, las dos con la intención de engañar al usuario y motivarlo a realizar acciones, consultar paginas maliciosas o instalar software con malware.

III. HISTORIA DEL MALWARE

La importancia de diferenciar los tipos de malware en una respuesta a incidente es crítica para determinar qué dirección tomar en las medidas implementadas durante la contención, para esto es recomendable conocer la historia del mismo, los primeros virus desarrollados no se trataba de software malicioso, en los años 70 se desarrollaron WORMS para hacer mantenimiento del sistema en organizaciones extensas. El malware se volvió común en los años 80, en forma de virus compilados que atacaban la secuencia de inicio del sistema para provocar un mal funcionamiento, también desarrollaron ofuscación para no ser detectados.

Hasta la segunda mitad de los 90, los virus no cambiaron demasiado, en ese momento se volvieron más económicos los computadores personales, con lo que hubo una explosión de objetivos para atacar y así oportunidades nuevas, este incremento impulso el uso del e-mail desde el hogar y otras aplicaciones basadas en macro-lenguajes dando la ventaja a los virus en atacar sus vulnerabilidades encontradas y llegar a mayor cantidad de estaciones de trabajo. Se volvieron comunes virus tipo RAT (Remote Administration Tools), y troyanos infectando millones de computadoras en pocos días.

A partir del 2000 se empiezan a identificar virus más sofisticados con diferentes vectores de ataque, principalmente con características de WORM con posibilidades de propagación rápida.

IV. PREVENCIÓN DE UN INCIDENTE DE MALWARE

Principalmente un plan de acción frente a incidente de malware reside en 4 pilares los cuales son: políticas, concientización, mitigación de vulnerabilidades y mitigación de amenazas.

Manteniendo las correctas políticas, el correcto mantenimiento de las campañas de concientización se va a reducir el riesgo de verse comprometido por un incidente de malware causado por un error humano, mantener las aplicaciones actualizadas, los sistemas operativos constantemente parchados y mitigando la mayor cantidad de vulnerabilidades posibles, se van a reducir los vectores de ataque, esto combinado con una fuerte infraestructura de seguridad perimetral, y correcta configuración en los equipos de CORE. A continuación se va a profundizar en cada uno de estos aspectos.

En el momento de crear las políticas anti-malware se debe ser los más general posible, esto para implementar controles según se va avanzando en la complejidad de las amenazas, sin tener que cambiar la política constantemente. En la elaboración de estas políticas también es muy importante tener en cuenta el teletrabajo, pues son puestos de trabajo fuera de sitio y su control tiene una alta complejidad en la organización.

Los principales ítems a tener en cuenta en una política anti-malware son:

- Scan de dispositivos externos antes de que puedan ser usados.
- Adjuntos de correo deben ser primero almacenados y escaneados por el antivirus, definido por el modelo de seguridad, también en los casos que los archivos se encuentren comprimidos.
- Prohibir el envío o llegada por e-mail de archivo .exe, y bloquearlos.
- Prohibir el uso de software innecesario como mensajería instantánea o programas para compartir archivos del tipo peer to peer, esto va a agregar nuevos vectores de ataque y vulnerabilidades que pueden ser explotadas.
- Restringir permisos para los usuarios usando una estricta política del menor nivel de privilegios posible para ejecutar sus actividades a cabalidad.
- Mantener aplicaciones y sistemas operativos actualizados y parchados.
- Restringir el uso de medios de almacenamiento removible.
- Especificar qué tipo de software de prevención se va usar para prevenir las infecciones en nuestra organización, como antivirus y configuraciones de firewall de host.
- Permitir el acceso a internet solo mediante un Gateway controlado y con las suficientes restricciones para brindar seguridad a la infraestructura de la organización.
- Implementar un proceso de control de cambios para configuraciones en el firewall donde se validen los riesgos asociados.
- Restringir el acceso por móviles a redes internas.

V. CONCIENTIZACIÓN

Un programa de concientización debe explicar claramente cómo prevenir incidentes de malware, describiendo los vectores de infección más comunes y como se debe manejar adecuadamente.

Indicar a todos los usuarios de la organización como los controles en la infraestructura no son suficientes para bloquear todas las posibles fuentes de infección, esto alineado a las políticas de seguridad de la empresa.

Indicar como se deben prevenir incidentes de malware cuando se está navegando a través de la infraestructura de la organización esto recalcando el cumplimiento de las políticas y controles de la empresa.

También es importante guiar al usuario en los procedimientos definidos que se deben seguir en caso de una sospecha de infección en sus estaciones de trabajo.

Esto va a reducir la probabilidad de presentarse un incidente de malware, atacando y concientizando el eslabón más débil en nuestro modelo de seguridad en profundidad, que es el usuario.

VI. MITIGACIÓN DE VULNERABILIDADES

Como se describía anteriormente un incidente de malware por lo general se va a generar explotando una vulnerabilidad del sistema operativo o de las aplicaciones instaladas en cada uno de las estaciones de trabajo, sistemas de información y demás servicios proporcionados, por tanto se debe tener un proceso juicioso de mitigación de cada una de las vulnerabilidades encontradas que representen una amenaza alta, por tanto no sea recomendable asumir este riesgo.

Dentro de este procedimiento de mitigación de vulnerabilidades se tienen en cuenta reconfiguraciones para el endurecimiento de sistemas operativos, aplicaciones o infraestructura crítica, también se debe tener un plan de actualizaciones periódicas y minimizando así el riesgo de que una vulnerabilidad sea explotada.

Dentro de la organización es importante tener un grupo dedicado al continuo descubrimiento y evaluación de nuevas vulnerabilidades encontradas, verificando como podrían afectar su infraestructura.

Este grupo también debe revisar constantemente tendencias de nuevo malware, sus vectores de infección e indicar que acciones se deben tomar como plan de acción para reducir los riesgos de sufrir un incidente de malware.

Se debe implementar una política de menores privilegios posibles para los usuarios, según sus competencias y necesidades para ejecutar normalmente sus actividades diarias.

Tener plantillas definidas y suficientes de endurecimiento de sistemas operativos y aplicaciones instaladas, según las recomendaciones de los fabricantes, y entes de investigación en buenas prácticas, no mantener servicios innecesarios disponibles ya que se convierten en un adicional que cuidar sin recibir beneficios del mismo.

Es recomendable tener instalada una consola de antivirus centralizada con las directivas correctamente configuradas según las buenas prácticas del fabricante, esto con el fin de responder a amenazas nuevas, el continuo escaneo de la infraestructura de la organización, y el constante mantenimiento de los agentes.

Configurar políticas de escaneo de todos los dispositivos de almacenamiento periódicamente, esto con el fin de desinfectar o eliminar, según sea el caso, archivos comprometidos.

Al tener una consola centralizada de antivirus se tiene mayor visibilidad sobre la infraestructura de la organización, esto por sus reportes, donde se indica cuantos agentes están online, cuantos están offline, estadísticas de amenazas detectadas y tratadas, top de host infectados, lo cual nos indicará que plan de acción se debe tomar hacia equipos que se evidencie que están comprometidos.

También se deben tener en cuenta dentro de nuestro modelo de seguridad en profundidad elementos que van a reducir el riesgo por tratarse de dispositivos de control, como lo son IPS, host firewall, firewall, correctas configuraciones en los dispositivos de red como routers, switches, filtradores de contenido de navegación, y proxy con restricciones de navegación.

VII. RESPUESTA A INCIDENTE DE MALWARE

En un incidente de malware se tienen definidas 4 fases principalmente, las cuales son:

- Preparación
- Detección y análisis.
- Contención – erradicación.
- Recuperación y actividades post-infección.

El principal objetivo de la fase de preparación es tener un equipo interdisciplinario para la respuesta al incidente, este grupo debe tener el conocimiento suficiente de la infraestructura de la organización, entendimiento de los riesgos asociados a cada uno de los activos, roles según su experiencia y perfiles.

Se deben ejecutar constantes ejercicios en ambientes controlados, simulando un ataque de malware y ver cómo responde el equipo, esto va a hacer que cada vez trabajen más unidos y eficientemente.

Es importante desarrollar habilidades en métodos de infección de malware, herramientas de detección, procedimientos forenses y programación.

En la fase de detección y análisis se debe tener un plan de detección eficiente, ya que un incidente de malware se puede propagar rápidamente dentro de la infraestructura de la organización.

El equipo de respuesta a incidentes como parte de su preparación debe estar al tanto de las nuevas amenazas existentes informándose, esto afiliándose a listas de correos con información especializada de tendencias y nuevas amenazas presentadas, grupos especializados de detección y análisis de muestras de malware, y demás medios que puedan tener a la mano.

También monitorizar el comportamiento de la red, las detecciones y mitigaciones ejecutas por el IPS.

Algunos signos de un incidente de malware pueden ser:

- Servidores Web colapsados.
- Lentitud en la navegación.
- El administrador del correo detecta gran cantidad de emails sospechosos.
- Alertas en la consola de anti-virus.
- Aumento anormal del tráfico en la red.

Para una correcta respuesta a un incidente de malware se debe tener clara la fuente, y el tipo de malware, esto basándose en la alarmas del antivirus, logs de routers, logs de firewall, capturas de paquetes para verificar su contenido.

Una vez clara esta información se procede a clasificar el incidente y así definir servicios afectados, sistemas operativos y aplicaciones vulnerables, medios de propagación y como se debe contener el incidente.

VIII. CONTENCIÓN

Al tener clara cuál es la fuente de infección, se debe proceder a evaluar qué servicios deshabilitar, segmentos de red que deben ser ser aislados, que configuraciones se deben aplicar en los firewall, IPS, y demás dispositivos de control que se tengan a mano para así proteger la parte de la infraestructura que no ha sido infectada por el incidente.

IX. ERRADICACIÓN

El objetivo de esta fase es la eliminación del malware en los sistemas infectados, si se hace un proceso de reversing dinámico con herramientas disponibles en la web como ANUBIS, se puede generar un script deshabilitando y eliminando las configuraciones que el malware haya ejecutado en el sistema, esto dependiendo del nivel de compromiso de las maquinas afectadas.

La eliminación total de la información es otra alternativa que se debe evaluar, aplicación de parches, eliminación de archivos compartidos, ejecución de scan con antivirus actualizado, anti-spyware recomendado para la infección especifica.

Para minimizar la pérdida de información es recomendable tener una política de backup activa y con aceptación de cada área de una perdida aceptable de información para así definir la periodicidad y rutas a guardar.

X. RECUPERACIÓN – ACTIVIDADES POST INFECCIÓN

Los objetivos de esta fase son restaurar las funcionalidades de los servicios afectados y desactivar las medidas tomadas durante la erradicación.

En el proceso de recuperación se deben tener definidas las prioridades de los activos a normalizar para así tomar decisiones de cuales se deben recuperar primero, según ANS contratados, costo de multas, costo de activos, criticidad de la información por afectación al CORE del negocio.

En cada respuesta a incidente se debe documentar el proceso de cómo se comportó el equipo y las actividades desarrolladas, para al final hacer una reunión de lecciones aprendidas y tomar medidas en las fallas que se hayan presentado, esto con el fin de minimizar cada vez el impacto de incidentes de esta naturaleza.

XI. CONCLUSIONES

1. Para atacar un incidente de malware primero se deben entender los diferentes tipos de malware, formas de propagación e historia de desarrollo durante el avanzar de las tecnologías.
2. Un correcto diseño de políticas de seguridad de la información, de la mano del objetivo del negocio y con los controles adecuados va a minimizar el riesgo de sufrir un incidente.
3. Mantener un proceso de concientización constante, con mantenimientos en la metodología y la correcta información nos va a ayudar a endurecer nuestro nivel más débil en el modelo de seguridad en profundidad, que es el usuario.
4. El éxito de una correcta respuesta a incidente reside en la planeación, correcta distribución de cargos, diseño correcto de plan de comunicaciones y constantes ejercicios que van a entrenar nuestro equipo en la respuesta correcta a incidentes de malware.
5. Luego de cada incidente el proceso va a ser cada vez más efectivo luego de tomar en cuenta las lecciones aprendidas en cada uno de ellos.
6. Establecer un modelo de seguridad en profundidad va a ayudarnos a asegurar cada uno de los niveles de nuestra infraestructura, esto minimizando los riesgos de sufrir un incidente de malware.

XII. REFERENCIAS

[1] Guide to Malware Incident Prevention and Handling - [en línea] - http://csrc.nist.gov/publications/nistpubs/800-83/SP800-83.pdf

[2] http://www.sans.org/reading-room/whitepapers/detection/early-malware-detection-correlation-incident-response-system-case-studies-34485 [En línea].

[3] Guide to Malware Incident Prevention and Handling for Desktops and Laptops, http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-83r1.pdf [en línea].

[4] Malware Response, https://msdn.microsoft.com/en-us/library/cc162838.aspx, [En línea].

Autor

Alejandro Agudelo Salazar
Ingeniero Electrónico
Aspirante a Especialista en Seguridad Informática
2015