

Conceptos generales y tipos de malware

Generalmente, cuando un programa malicioso infecta un sistema, se suele hacer referencia a un “virus”, sin embargo, puede tratarse de cualquier otro tipo de malware. En su lugar, otros tipos de malware han proliferado para afectar a los usuarios con nuevas y variadas técnicas de propagación e infección, mismos que pueden ser clasificados en función de sus características, propósitos o funcionalidades.

Existen amenazas como los **gusanos** que, a diferencia del virus, no requieren un archivo anfitrión y tienen la capacidad de replicarse y propagarse por sí mismos; o los troyanos, que simulan ser una aplicación inofensiva, pero que en realidad realizan tareas maliciosas sin el consentimiento y muchas veces sin el conocimiento del usuario.

Los **rootkits** son otro tipo de programa malicioso que garantiza a los atacantes el acceso a un sistema, a la vez que ocultan su presencia. Luego de acceder, generalmente debido a una vulnerabilidad, utilizan funciones del sistema operativo para evitar ser detectados: ocultan procesos, archivos o registros, por lo que es difícil detectarlos por medio de técnicas convencionales de seguridad.

El **spyware**, que recopila información de las actividades de los usuarios y la envía a un atacante, o las **botnets**, redes de equipos infectados (conocidos como zombis o bots) que permiten a un cibercriminal utilizarlos, de forma remota, con diversos fines, como propagar más códigos maliciosos, emplearlos para ataques de Denegación de Servicio (DoS) o utilizarlos para enviar correos no deseados de forma masiva (spam).

Los **downloaders** (que permiten descargar otras amenazas desde Internet para instalarlas posteriormente), **droppers** (que instalan otros programas maliciosos incluidos en su código fuente), **clickers** (para generar tráfico hacia sitios o avisos publicitarios que generan ganancias a sus desarrolladores) o los que se incluyen en la categoría de bancarios, creados especialmente para obtener datos relacionados con entidades financieras.

Una tendencia creciente es el desarrollo **ransomware**, un tipo de malware que cifra la información o bloquea un sistema para impedir el acceso a los datos. Posteriormente, solicita un pago como rescate, para que el atacante pueda proporcionar la clave que permite al usuario acceder a los archivos “secuestrados”.

Como se puede observar, ahora no solamente es posible encontrar software malicioso para los equipos de cómputo tradicionales; los teléfonos inteligentes también se han visto afectados por programas y aplicaciones que tienen como propósito generar un daño patrimonial a los usuarios. También se han visto afectados otros dispositivos, como SmartWatch o SmartTV, que funcionan a partir de un sistema operativo, lo que apunta al desarrollo de amenazas hacia la Internet de las Cosas (IoT).

Aplicaciones potencialmente no deseadas

Además de los códigos maliciosos, es posible identificar otro tipo de programas que también pueden afectar a los usuarios y que por su naturaleza alcanzan otra clasificación.

Este tipo de **programas informáticos** presentan un comportamiento probablemente **indeseado** por el usuario, que por lo general no exhiben el comportamiento típico del malware y requieren del consentimiento del usuario antes de realizar la instalación.

Sin embargo, realizan otro tipo de acciones, como instalar aplicaciones adicionales, cambiar el comportamiento del entorno donde se ejecutó, instalar algún tipo de adware sin advertirlo para mostrar publicidad no solicitada, modificar configuraciones de los navegadores o instalar barras de herramientas (**toolbars**).

Aplicaciones Potencialmente Peligrosas

También existen otros programas cuya función es simplificar la administración de equipos en red, incluso algunos que se distribuyen como software comercial legítimo. Sin embargo, debido a sus funcionalidades y características pueden ser utilizados con propósitos maliciosos.

Pueden incluir programas como herramientas de acceso remoto, aplicaciones para adivinar contraseñas o registradores de pulsaciones en el teclado. En las soluciones de seguridad AV (**antivirus**) cuentan con herramienta para detección de **aplicaciones potencialmente no deseadas** y evitar así su instalación.

Síntomas comunes de una infección por malware

La ausencia de soluciones antivirus permite que haya altas posibilidades de padecer un incidente por malware, ya sea por falta de actualización del software, una configuración errónea o malas prácticas aplicadas a la Seguridad Informática.

Ante la falta de herramientas que permitan detectar de manera automática una infección por malware, existen distintos indicios que podrían mostrar que un sistema no está funcionando de la manera en la que debería. Esto representa una dificultad para saber de manera precisa si se está ante una infección, puesto que la mayoría de las amenazas buscan pasar inadvertidas.

A pesar de ello, a continuación, se presentan algunos “síntomas” de una posible infección:

- Bajo desempeño en el procesamiento de tareas en el equipo.
- Aparición de ventanas y anuncios emergentes que no han sido solicitadas por el usuario.
- Aparición de programas instalados en el equipo sin el conocimiento y consentimiento del usuario.
- Comportamiento anormal del sistema operativo, como reinicio o apagado repentino.
- Fallas durante la descarga de actualizaciones del sistema operativo o de programas instalados.
- Funcionalidades deshabilitadas del sistema operativo o de programas.

- Lentitud al navegar por Internet o durante la descarga de archivos.
- Alertas de seguridad por parte del sistema operativo o de supuestas soluciones antivirus.
- Imposibilidad de iniciar el sistema operativo tanto en “modo normal” como en “modo seguro”.
- Cambio de página de inicio de Internet o redirección a sitios web desconocidos.
- Cambio del fondo de escritorio u otro aspecto del sistema.
- Mensajes intimidatorios para el usuario o solicitud de pagos para recuperar información.
- Conexiones de red entrantes y salientes por puertos y protocolos comúnmente no utilizados.

De manera general, este tipo de comportamientos podrían determinar que uno o más equipos se encuentran infectados. Ante las dudas, el método más fehaciente es el análisis y exploración que pueda realizar una solución de seguridad contra códigos maliciosos.

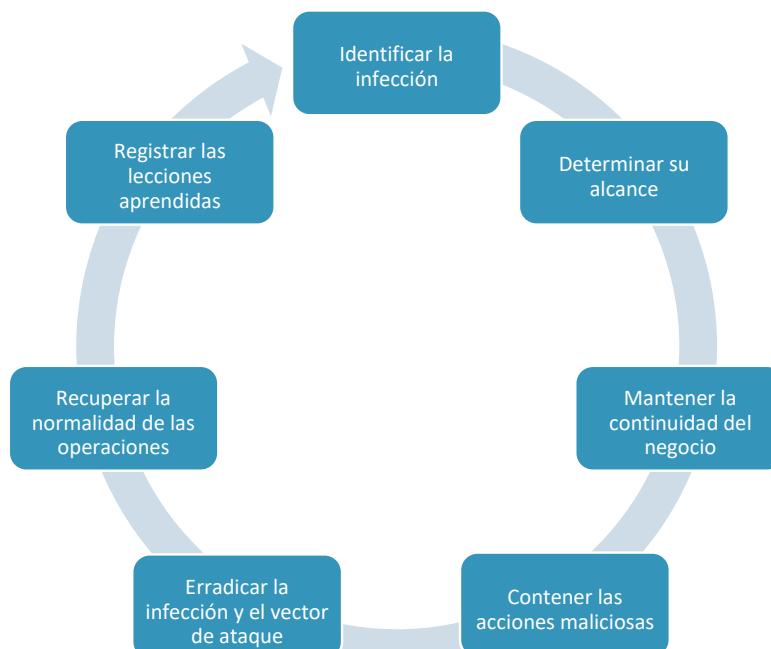
Acción ante una infección por malware

Resulta muy importante conocer las acciones a seguir si se ha determinado que uno o más equipos han sido afectados.

Los siguientes pasos permitirán definir fases y estimar recursos necesarios para atender una incidencia de esta naturaleza, pueden formar parte de un **Plan de Respuesta a Incidentes de Seguridad**.

Este explicativo, definen actividades y funciones básicas para hacer frente a algún incidente que comprometa la Seguridad de la Información, y sobre la manera de proceder ante los diferentes escenarios en los cuales podrían estar expuestos los activos de la organización si algún riesgo se materializa. Por tanto, estos planes **se consideran actividades preventivas y reactivas**, de manera que puedan evitarse las infecciones por malware o, en su defecto, que de presentarse sus consecuencias sean las mínimas aceptables.

El propósito primordial consiste en mantener el número de incidentes en un nivel razonablemente bajo para proteger los procesos de la organización. Cuando se trata de incidentes relacionados con malware, se pueden seguir actividades que contribuyen a una efectiva respuesta y rápida recuperación.



Identificar la infección

Un incidente de seguridad relacionado con malware puede ser detectado de diferentes maneras y con distintos niveles de detalle, y para hacerlo se pueden utilizar desde herramientas de detección automatizadas como consolas que centralizan la información relacionada con amenazas identificadas en los equipos administrados hasta medios manuales como un reporte de falla de un usuario que considere un comportamiento anormal en su sistema.

Algunos incidentes muestran signos que facilitan la detección, no obstante, se pueden presentar ocasiones en donde es casi imposible detectarlos si no se cuenta con herramientas adecuadas. Por lo tanto, reconocer los indicios de infección es fundamental para conocer los equipos infectados y la información que puede estar en riesgo.

Las actividades de detección de malware pueden aplicarse a distintos niveles dentro de la organización: a **nivel de host** (en los sistemas operativos de servidores y estaciones de trabajo), a **nivel de aplicaciones de servidor** (correo electrónico o proxies web) y a **nivel de aplicaciones de cliente** (mensajería instantánea o correo electrónico de clientes).

Determinar el alcance de la infección

Luego de la identificación de una infección por malware, es necesario determinar la cantidad de sistemas que han sido comprometidos y de qué manera, con el propósito de conocer el alcance de la infección y el impacto que puede representar. Por ejemplo, si está limitada a un único equipo, un conjunto de ellos, una subred o, en casos más graves, a toda la red corporativa.

Conocer el alcance de una infección permite calcular los recursos que serán necesarios para solucionar los inconvenientes que haya generado. Además, permite saber los sistemas que han sido comprometidos, junto con la criticidad de la información que almacenan, procesan o transmiten. Por otro lado, a partir del tipo de malware y su comportamiento, también es posible determinar saber si se ha filtrado información sensible, si se han visto comprometidos datos corporativos o privados de los empleados y/o de clientes.

Mantener la continuidad del negocio

Durante un incidente, resulta fundamental mantener la continuidad de las operaciones críticas de las organizaciones.

En el caso de incidentes por malware, luego de conocer el alcance de la infección, se podrá determinar si información sensible o equipos críticos se han visto afectados. En función de este resultado, se podrán tomar decisiones para continuar correctamente con las operaciones de la compañía.

Por otro lado, **si la infección derivara en una fuga de información** que puede comprometer datos de empleados, usuarios o clientes, será necesario contactarlos para avisar sobre la posible brecha; de esta manera, se podrá mantener el registro de cualquier movimiento de datos vinculados a los servicios proporcionados por la empresa.

En el caso de que algún **equipo físico haya resultado comprometido**, se deberán poner en marcha procesos de restauración de información y de los equipos de cómputo necesarios, a fin de mantener los servicios ofrecidos a clientes y usuarios.

Contener las acciones maliciosas

Las estrategias de contención pueden variar en función del incidente y de los lineamientos establecidos por los equipos de respuesta, lo que a su vez depende del tipo de malware que afecte a la organización. Por ejemplo, si un equipo se ve afectado por un caso de ransomware, se deberá seguir una estrategia distinta a si se está ante un caso de una botnet o un spyware. A partir del comportamiento del código malicioso se pueden determinar los pasos a seguir para la contención.

Una manera de **iniciar esta fase está relacionada con el aislamiento de los equipos** que se sabe que están comprometidos. La **suspensión de los segmentos de red** de los cuales forman parte evita que la infección pueda propagarse a través de la red corporativa e interrumpe cualquier conexión que pueda establecerse con el atacante para el robo de información. **La segmentación de las redes es una práctica que contribuye a mitigar la propagación.**

Por otro lado, la **identificación del vector de ataque** resulta fundamental para contener los estragos generados por un código malicioso y evitar su propagación. En este sentido, es importante la previsión para manejar incidentes que utilizan los vectores más comunes: propagación e infección a través de medios externos y removibles, explotación de vulnerabilidades en el software y sitios web, archivos adjuntos a correos electrónicos y enlaces a sitios que alojan malware.

Los **ataques por malware** pueden deberse a una campaña masiva de propagación, por malas prácticas de los usuarios, o bien puede tratarse de un ataque dirigido y con un propósito específico.

En todos estos casos, una vez que se haya identificado el vector de ataque, se podrán aplicar distintas acciones en función de las características de la muestra de malware.

Por ejemplo, si se trata de un **programa malicioso que realiza conexiones a Internet**, con el monitoreo de los canales de comunicación de los atacantes se puede obtener el tráfico generado por el agente malicioso. En cambio, **si la comunicación se realiza sobre protocolos no cifrados** (como HTTP). Asimismo, **la creación de reglas de firewall** para generar una primera barrera de defensa permite bloquear las acciones que intente realizar cualquier agente malicioso que haya logrado saltar los mecanismos de seguridad.

En cambio, **si se trata de ransomware que cifra archivos**, será necesario aplicar algún método de restauración de información con la intención de evitar el pago de la información secuestrada y mantener las actividades críticas.

La mayor parte de los procedimientos nombrados implican el análisis no automatizado de la información, por lo que se torna evidente que la prevención y detección proactiva de amenazas son la piedra angular de la Seguridad de la Información y evitarán que haya que recurrir a los Planes de Respuesta a Incidentes.

Erradicar la infección y eliminar el vector de ataque

La remoción de la amenaza es un procedimiento complejo que implica, inicialmente, **un análisis minucioso del comportamiento del malware para comprender su funcionamiento y, en condiciones ideales, un análisis del código fuente del mismo**. Las soluciones de AV, permiten la automatización de la desinfección y el ahorro de tiempo en el proceso de respuesta.

- **Si los medios empleados no son erradicados completamente**, existe una enorme posibilidad de que puedan retomar sus actividades maliciosas sobre los equipos infectados a través de otro vector de ataque. Por ello, **es de vital importancia aislar la falla que les permitió el ingreso, para luego eliminarla del sistema**.
- **Si los equipos comprometidos han sido desinfectados, continúa presente el riesgo de mantener en funcionamiento otros equipos infectados no descubiertos**. Para evitar que esto ocurra, se pueden poner en práctica otras acciones como **el análisis de los paquetes de red para identificar tráfico anormal**, con la ventaja de que ahora se conocen los protocolos, puertos y comandos utilizados en el análisis previo.
- Luego de conocer el comportamiento, **es necesario comenzar a aplicar medidas de protección**. Por ejemplo, junto con la revisión de las **reglas de firewall**, el **cambio de las contraseñas** es otra medida preventiva a tomar luego de detectar recursos comprometidos, ya que éste es uno de los objetivos en los ataques corporativos.
- Existen otras herramientas de seguridad, como los **sistemas de Información de seguridad y administración de eventos** (SIEM) o **Sistemas de prevención y detección de intrusos** (IPS/IDS), que permiten contar con alertas tempranas sobre actividades anormales en la red y sistemas, y pueden ser configuradas para evitar nuevas infecciones que utilizan vías conocidas.
- A partir de la identificación del método de propagación, **es obligatorio llevar a cabo acciones que mitiquen de manera específica el vector**, por ejemplo **el filtrado de correo electrónico y análisis de los mensajes y adjuntos**, la modificación de los sistemas operativos para **evitar la ejecución de programas de manera automática cuando se introduce un dispositivo removable**, la **actualización de software** necesario **para evitar la explotación de alguna vulnerabilidad** que permita el ingreso de malware a la red corporativa, entre otras acciones.

Llegada esta instancia, es necesario definir si la infección fue el simple resultado de un descuido en la Web o si, por el contrario, constituye el eslabón exitoso dentro de una cadena de ataques persistentes y dirigidos. Si se determina que la infección tuvo como objetivo específico a la organización, entonces se debe tener en mente que un nuevo ataque puede ser inminente.

Recuperar la normalidad en las operaciones

La fase de recuperación se presenta luego de que un incidente por malware ha sido contenido y de que se han identificado y mitigado las vulnerabilidades que fueron explotadas.

Llegado este punto, se confirma que los sistemas se encuentran funcionando de manera normal y que el malware ha sido removido para evitar incidentes similares. **La recuperación puede incluir acciones como la restauración de sistemas operativos y respaldos, el reemplazo de archivos infectados, la instalación de parches de seguridad y actualizaciones, el cambio de contraseñas en los sistemas, el refuerzo de la seguridad perimetral a través de nuevas reglas de firewall, la creación de listas de control de acceso o el desarrollo de nuevas firmas de malware.**

A partir de los patrones identificados, es posible determinar que si un ataque cumplió su cometido malicioso y si se intentarán nuevos casos de una manera similar. Por este motivo, es fundamental eliminar de raíz los problemas para mantener la seguridad; cabe destacar que esto logra con el conocimiento pleno del código malicioso.

El tiempo de recuperación dependerá en gran medida de las consecuencias generadas por la infección, por lo que no se puede establecer un periodo para alcanzarla, aunque siempre se busca que sea en el menor tiempo posible.

Documentar y adjuntar evidencia

Finalmente, otro elemento de importancia en el **proceso de documentación respecto al incidente, como la detección, la identificación y su alcance, pasando por su contención hasta su erradicación y normalización de los servicios.** La acción de documentar el hecho se basa en la mejora continua de los procesos y el aprendizaje de la misma.

