TLP:BLANCO

La información conlleva un riesgo mínimo o inexistente aplicables para publicación pública. Sujeto a las normas de protección intelectual, puede distribuirse sin restricciones.

GUÍA PARA LA DETECCIÓN DE MALWARE

1. INTRODUCCIÓN

La palabra malware proviene de la abreviación de malicious software, y puede ser utilizado para comprometer funciones del sistema, robo de información, saltear controles de acceso, o cualquier otra forma de causar daño al host sobre el cual se está ejecutando.

Existen diferentes tipos de malware y cada uno busca objetivos de un modo diferente. Como ejemplos de malware se tiene: Adware, spyware, virus, redes de robots (botnets), troyanos, gusanos, rootkits y ransomware.

El malware presenta un patrón básico de infección, independientemente del tipo que se tenga, y consiste en que el usuario descarga o instala involuntariamente el malware, que infecta el dispositivo.

2. TIPOS DE MALWARE

La inmensa mayoría del malware entra en las siguientes categorías básicas, dependiendo de su funcionamiento.

Ransomware.- Suele funcionar bloqueando o denegando el acceso a su dispositivo y sus archivos hasta que pague un rescate. Cualquier persona o grupo que guarde información esencial en sus dispositivos corre peligro frente a la amenaza del ransomware.

Spyware.- Recaba información sobre un dispositivo o red para luego enviársela al atacante. Se suele utilizar para supervisar la actividad en Internet de una persona y recopilar datos personales, incluidas credenciales de inicio de sesión, números de tarjeta de crédito o información financiera, con el propósito de cometer fraude o robo de identidad.

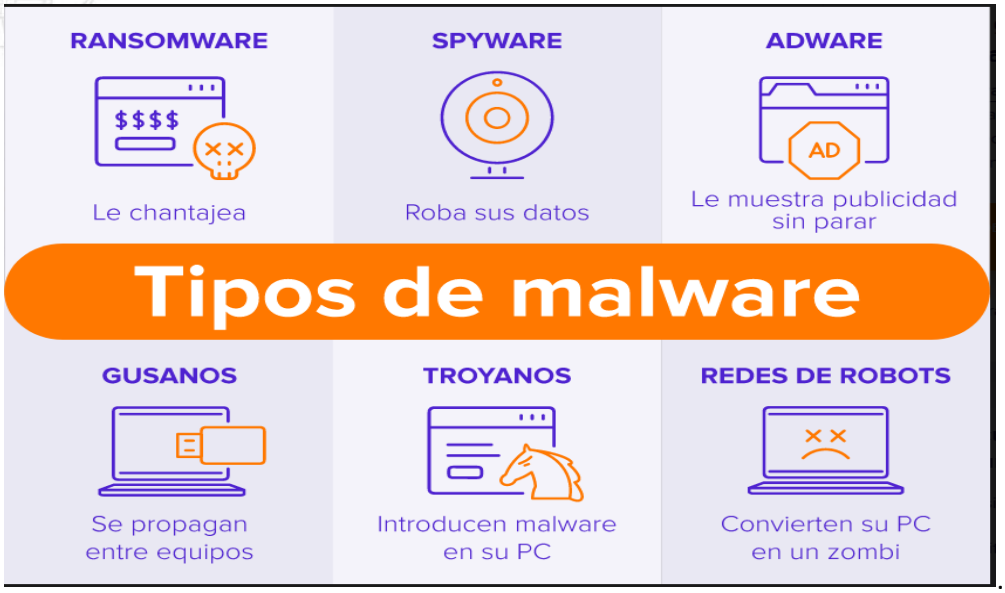
Gusanos.- Están diseñados con un objetivo en mente: expandirse. Un gusano infecta un equipo y después se replica y se extiende a dispositivos adicionales, permaneciendo activo en todas las máquinas afectadas. Algunos gusanos actúan como mensajeros para instalar malware adicional.

Otros están diseñados solo para extenderse y no causan daño intencionadamente a las máquinas anfitrionas, aunque siguen atestando las redes con sus demandas de ancho de banda.

Adware.- Somete a la víctima a publicidad no deseada. Algunos tipos comunes de adware son los juegos gratuitos y las barras de herramientas para el navegador. Recaban datos personales acerca de la víctima y después los emplean para personalizar los anuncios que muestran. Aunque la mayoría del adware se instala de forma legal, no por ello es menos molesto que otros tipos de malware.

Troyanos.- El malware troyano se infiltra en el dispositivo de una víctima presentándose como software legítimo. Una vez instalado, el troyano se activa y, en ocasiones, llega incluso a descargar malware adicional.

Redes de robots (botnets).- Una red de robots no es un tipo de malware, sino una red de equipos o de código informático que puede desarrollar o ejecutar malware. Los atacantes infectan un grupo de equipos con software malicioso conocido como "robots" (o "bots"), capaz de recibir órdenes desde su controlador. A continuación, estos equipos forman una red que proporciona al controlador acceso a una capacidad de procesamiento sustancial. Dicha capacidad puede emplearse para coordinar ataques, enviar spam, robar datos y crear anuncios falsos en su navegador.



Fuente: https://www.avast.com/es-es/c-malware

El ransomware es la forma de malware más hostil y directa. Mientras que los demás tipos operan invisibles, el ransomware anuncia su presencia de inmediato y exige un pago a cambio de devolver el acceso a sus dispositivos o archivos

3. FORMAS DE INFECCIÓN DE MALWARE

La mayoría de las infecciones se producen cuando un usuario, realiza sin saberlo una acción que provoca la descarga del malware. Entre las principales vías de infección de malware se puede destacar:

- Al instalar cualquier programa gratuito, sin leer sus opciones (PUPs/Adware)
- Al insertar en el equipo un dispositivo USB infectado. (Gusanos)
- Al visitar algún sitio web legítimo que haya sido infectado -drive-by-download- o malvertising (Troyano/Ransomware)
- Al descargar una supuesta actualización de algún programa instalado, si la actualización no se realiza de fuentes oficiales el equipo podría verse comprometido. (Troyano/Botnet)
- Al abrir un archivo adjunto o seguir un enlace de un correo no solicitado. (Spam/Phishing)
- Al seguir un enlace infectado de un contacto o muro en las redes sociales.
- Mediante servicios peer-to-peer de compartición de archivos y paquetes de descarga de software gratuito.

4. CONSECUENCIAS DE LA INFECCIÓN DE MALWARE

Cuando un dispositivo está infectado de malware se podría presentar lo siguiente:

- La **velocidad de Internet es más lenta** de lo normal (debido a un elevado tráfico de datos).

- **Nota que le falta espacio de almacenamiento.** Una reducción repentina en la cantidad de almacenamiento libre podría indicar que está infectado con algún malware.

- **En su dispositivo aparecen ventanas emergentes y programas no deseados.** Si le bombardean los anuncios emergentes o encuentra nuevos y extraños programas en el dispositivo, es probable que sea cosa del malware.

- El equipo **se apaga de manera espontánea**, no se puede volver a encender o el sistema se bloquea de repente.

- El **equipo funciona más lento de lo normal** (debido a un aumento en la carga del procesador).

- Aumenta la asiduidad con la que aparecen **contenidos indeseados de Internet**, tales como ventanas emergentes, reenvío automático a ciertas direcciones de Internet o acceso repentino a una nueva página web, buscador o nuevas barras de herramientas en el navegador.

- Los **programas se desinstalan o bloquean de repente**. Algunos elementos dañinos pueden, incluso, desactivar programas antivirus y cortafuegos, lo que se convierte en otro indicio de que el sistema ha sido infectado con un malware.

- Se instalan programas **no deseados** y algunos se abren solos.

5. MEDIDAS DE PROTECCIÓN PARA PREVENIR INFECCIÓN DE MALWARE

Hay diversos tipos de software diseñados para proteger a los sistemas informáticos de las amenazas externas, pero no toda la responsabilidad recae en ellos. Esto hace referencia, por un lado, a las **medidas preventivas basadas en software** y, por otro, a las **directrices sobre el uso de Internet**.

Dentro de las medidas preventivas basadas en software se tiene:

- Un **programa antivirus actual** y **eficaz**: un antivirus es un programa que se ejecuta de manera permanente y protege al equipo de las amenazas de software maligno, para lo cual es imprescindible que se encuentre actualizado. Los programas antivirus **no solo**

protegen contra virus informáticos, sino también **contra otros tipos de programas malintencionados** y ayudan, también, a eliminar malware.

- Un **firewall activo**: para proteger el ordenador de accesos no autorizados.
- Una **versión actual** del **sistema operativo**: las actualizaciones ayudan a eliminar los vacíos de seguridad ocasionados por la presencia de malware en los equipos, por lo que es recomendable mantener los equipos actualizados.
- **Versiones actuales** de los **programas**: también es recomendable actualizar el software que se utiliza, sobre todo aquel que posibilita la conexión a Internet. Las versiones anticuadas de los navegadores, de Java, de Flash y de otras aplicaciones, contienen a menudo fallos de seguridad y permiten que el malware tenga acceso al sistema.

En relación a las directrices sobre el uso de Internet se puede considerar:

- Instalar programas y archivos que procedan de **fuentes fiables**. El software y las actualizaciones deben descargarse siempre desde la página web del proveedor original y, en caso de freeware o shareware, la descarga debe realizarse desde portales confiables.
- No abrir ningún archivo o enlace proveniente de correos electrónicos cuyos **remitentes se desconozcan** o que contengan mensajes con **asuntos dudosos**.
- Prestar atención a los **anuncios**, banners o ventanas emergentes en los que se hace clic y evitar, sobre todo, los enlaces que contienen promociones, vales o cualquier otro tipo de oferta dudosa.
- Manejar con cautela datos sensibles como la información sobre la cuenta bancaria, los datos de registro y las contraseñas.
- Realizar un respaldo externo periódico de la información que sea importante para la empresa.
- Realizar pruebas periódicas de restauración de los respaldos externos.

- En situaciones extremas, es necesario el formateo del o los equipos sobre el que se albergue el malware.

- Gestión de vulnerabilidades en la infraestructura empresarial.

- Información a los usuarios, para lo cual es necesario crear un programa de concientización que los incentive a aprender a sospechar de los enlaces y los archivos adjuntos en los correos electrónicos, incluso de aquellos que parecen auténticos.

- Reducción de la superficie de ataque, para lo cual es necesario reducir la cantidad de sistemas, aplicaciones y puertos que están expuestos a internet

6. BIBLIOGRAFÍA

- Forospyware (6 de enero de 2021). Guía de detección y eliminación de malware. Recuperado 22 de abril de 2021. Obtenido de: https://forospyware.com/t/gu%C3%ADa-de-detecci%C3%B3n-y-eliminaci%C3%B3n-de-malwares-2021/23
- Ivan Belcic (actualizado al 2 de diciembre de 2020). Que es el malware. Recuperado 22 de abril de 2021. Obtenido de https://www.avast.com/es-es/c-malware
- Ionos (22 de agosto 2019). Software malicioso: cómo prevenir, identificar y eliminar el malware. Recuperado 22 de abril de 2021. Obtenido de: https://www.ionos.es/digitalguide/servidores/seguridad/como-identificar-y-eliminar-malware/.
- Red Hat, Qué es el malware. Recuperado 22 de abril de 2021. Obtenido de: https://www.redhat.com/es/topics/security/what-is-malware