www.eysglobal.com

TEMA:
ATAQUES INFORMATICOS FRECUENTES
PARTE 1

ATAQUE POR MALWARE

El malware o software malicioso es una categoría de software diseñado para infiltrarse y dañar un sistema de información sin ser detectado. Aunque el malware se utiliza para referirse de forma general a un software malicioso, existen diversos tipos de malware que responden a características propias y comportamientos diferentes. Entre los malwares más utilizados, destacan el virus, un código maligno que infecta los ficheros del dispositivo en forma de archivo ejecutable (o archivo .exe), y que se vale del desconocimiento de los usuarios para infectar un equipo u ordenador.

ATAQUE POR MALWARE

Otros malwares conocidos son los gusanos (software algo más sofisticado que el virus, que crea copias de sí mismo con el objetivo de afectar otros equipos), los troyanos (programas diseñados para ingresar en los sistemas de seguridad y permitir el acceso a otros archivos maliciosos), los spyware (programas que espían un dispositivo para obtener información privada y que pueden instalar otros softwares maliciosos) y los ya famosos ransomwares, que secuestran la información de valor de un dispositivo, con el fin de solicitar una transferencia en criptomoneda o monedas digitales a modo de rescate.

¿CÓMO FUNCIONA EL MALWARE?

Sea cual sea su tipo, todo malware sigue el mismo patrón básico: El usuario descarga o instala involuntariamente el malware, que infecta el dispositivo.

La mayoría de las infecciones se producen cuando realiza sin saberlo una acción que provoca la descarga del malware. Esta acción podría ser un clic en el vínculo de un correo electrónico o la visita a un sitio web malicioso. En otros casos, los hackers extienden el malware mediante servicios peer-to-peer de compartición de archivos y paquetes de descarga de software gratuito. Incrustar malware en un torrent o una descarga popular es una manera efectiva de extenderlo por una base de usuarios más amplia. Los dispositivos móviles también pueden infectarse mediante mensajes de texto.

TIPOS COMUNES DE MALWARE

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

Ransomware:

El ransomware es la versión malware de la nota de rescate de un secuestrador. Suele funcionar bloqueando o denegando el acceso a su dispositivo y sus archivos hasta que pague un rescate al hacker. Cualquier persona o grupo que guarde información esencial en sus dispositivos corre peligro frente a la amenaza del ransomware.

TIPOS COMUNES DE MALWARE

Spyware

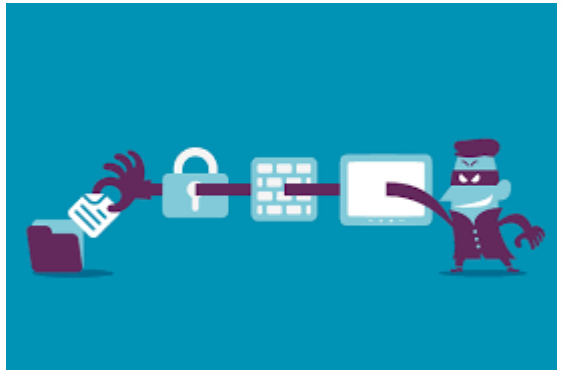
El spyware recaba información sobre un dispositivo o red para luego enviársela al atacante. Los hackers suelen utilizar spyware para supervisar la actividad en Internet de una persona y recopilar datos personales, incluidas credenciales de inicio de sesión, números de tarjeta de crédito o información financiera, con el propósito de cometer fraude o robo de identidad.

TIPOS COMUNES DE MALWARE

Gusanos

Los gusanos están diseñados con un objetivo en mente: proliferar. 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.

TIPOS COMUNES DE MALWARE



Adware

El trabajo del adware es crear ingresos para el desarrollador sometiendo 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.

TIPOS COMUNES DE MALWARE

Troyanos

Los antiguos poetas griegos hablaban de unos guerreros atenienses que se escondieron en un gigantesco caballo de madera para luego salir del interior, una vez que los troyanos lo arrastraron tras las murallas de la ciudad. Por tanto, un caballo de Troya es un vehículo que oculta atacantes. 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.

TIPOS COMUNES DE MALWARE

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.

TIPOS COMUNES DE MALWARE

Tipos de malware

RANSOMWARE

Le chantajea

SPYWARE

Roba sus datos

ADWARE

Le muestra publicidad sin parar

GUSANOS

Se propagan entre equipos

TROYANOS

Introducen malware en su PC

REDES DE ROBOTS

Convierten su PC en un zombi

COMO SABRE SI MI DISPOSITIVO ESTA AFECTADO

- **El dispositivo empieza a funcionar más lento de lo normal**. Si ha notado una ralentización repentina sin causa aparente, puede deberse a una infección de malware. Como el malware se adueña de los recursos de procesamiento del dispositivo, queda menos capacidad para todo lo demás.

- **Nota que le falta espacio de almacenamiento**. Muchos tipos de malware descargan e instalan archivos y contenido adicional en el dispositivo. Una reducción repentina en la cantidad de almacenamiento libre podría indicar que está infectado con algún malware.

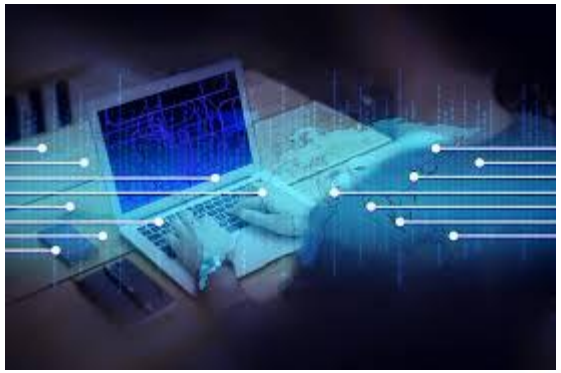
COMO SABRE SI MI DISPOSITIVO ESTA AFECTADO

- **En su dispositivo aparecen ventanas emergentes y programas no deseados**. Esta es una de las señales más claras de que sufre una infección de malware. Si le bombardean los anuncios emergentes o encuentra nuevos y extraños programas en el dispositivo, es probable que sea cosa del malware.

El funcionamiento lento y la reducción en el espacio de almacenamiento no siempre significan que haya malware. Con el tiempo, los dispositivos se van cargando de forma natural con archivos innecesarios. Siempre es buena idea limpiar de vez en cuando, y si al hacerlo el funcionamiento vuelve a ser el normal, es probable que no sufra una infección de malware.

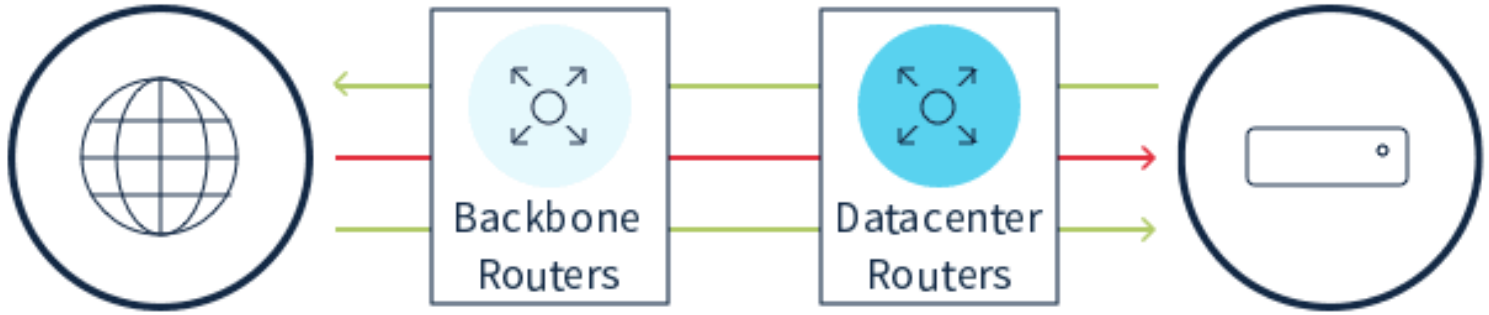
Ataque DDoS

Es uno de los ataques más frecuentes en Internet. También conocido como “denegación del servicio distribuida” (que proviene del inglés “distributed denial of service”), consiste en el bloqueo al acceso de un sitio web y, en simultáneo, el ataque al servidor mediante el ingreso de un gran volumen de información basura (por ejemplo, el rellenado de formularios con datos falsos o envío de solicitudes). Esto origina una saturación en el flujo del servidor, colpasa el sitio web o determina la pérdida de conectividad en este espacio. Normalmente, estos ataques se hacen a través de ordenadores infectados con troyanos.

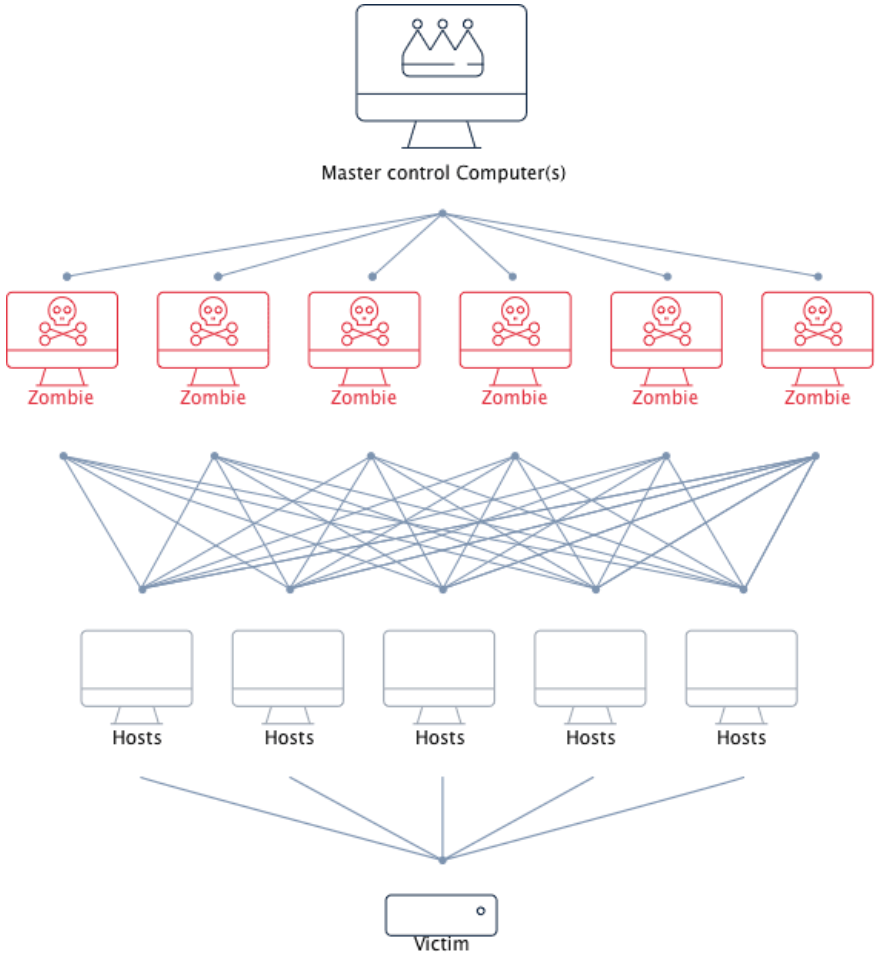


Ataque DDoS

Con el crecimiento exponencial del volumen de datos en la red, los ataques por denegación de servicio distribuidos (DDoS) son cada vez más frecuentes.



Ataque DDoS



Durante un ataque DDoS, se envían simultáneamente múltiples solicitudes desde distintos puntos de la red. La intensidad de este «fuego cruzado» compromete la estabilidad, y, en ocasiones, la disponibilidad del servicio.

Ataque DDoS

Desarrollo de un ataque DDoS

- El servidor está operativo enviando y recibiendo paquetes normalmente.
- El ataque DDoS se produce por la sobrecarga del ancho de banda o por el agotamiento de los recursos del sistema.
- La red se satura, por lo que el servidor no puede procesar los paquetes legítimos entre la masa de información entrante.