Por lo general, cuando se habla de malware o virus, se está englobando una gran cantidad de tipos de archivos o software maliciosos, esto para evitar entrar en detalle cuando se brindan noticias al público en general sobre ataques cibernéticos.

El malware es aquel que tiene como finalidad acceder a equipos para obtener información sensible privada, ya sea sobre una persona o una organización. El uso de la información tiene muchos fines, ya sea para extorsión, venta o simplemente cobrar un rescate a cambio.

En el siguiente listado se mostrarán los tipos de malware que circulan por la red, que se pueden esparcir por medio de correos electrónicos, sitios web, aplicaciones de desarrolladores poco confiables, dispositivos flash, entre otros.

Virus

Los virus informáticos son programas maliciosos que infectan a otros archivos del sistema operativo con el fin de modificarlo o dañarlo. La infección consiste en incrustar su código malicioso en el interior del archivo de la víctima, que normalmente se trata de ejecutables, para que a partir de ese momento, el archivo ejecutable sea portador del virus y una nueva fuente de infección.

Adware

Este tipo de malware es el más común en Internet, despliega publicidad de distintos productos o servicios. Pueden incluir código adicional que muestra publicidad en ventanas emergentes, o por medio de una barra que aparece en la pantalla, simulando un banner que ofrece distintos servicios para el usuario.

Ejemplo de infección por Adware

Backdoor

Estos programas se diseñan para abrir una puerta trasera en el sistema, para permitir al atacante tener acceso al sistema y hacer lo que quiera dentro de él. El objetivo es lograr tener una gran cantidad de computadoras infectadas para disponer de los equipos libremente hasta poder formar redes como las botnet.

Botnet

Este malware está diseñado para la creación de botnets, que actualmente es una de las principales amenazas. Este tipo de ataques apareció en el 2004, aumentando cada año los casos de aparición.

Se trata de una red de equipos infectados por códigos maliciosos, que son controlados por un atacante, disponiendo de sus recursos para trabajar de forma conjunta y distribuida. Cuando una computadora ha sido infectada por un malware de este tipo, se dice que ahora es un robot o zombie.

Ejemplo gráfico de botnet

Gusanos

Son un sub conjunto de malware. Su diferencia con los virus es que no necesitan de un archivo anfitrión para estar activos. Los gusanos pueden reproducirse utilizando diferentes medios de comunicación como las redes locales, correo electrónico, programas de mensajería instantánea, redes P2P, dispositivos USB y redes sociales.

Ejemplo del gusano LoveLetter

Hoax

Se trata de un correo electrónico distribuido en formato de cadena, que tiene como objetivo hacer creer a los lectores que se trata de algo real, cuando en realidad es un correo falso. A diferencia de otras amenazas como el phishing, los hoax no tienen fines lucrativos.

Hijacker

Se encargan de secuestrar las funciones del navegador web, modificando la página de inicio y de búsqueda por alguna en la red de atacantes. Bloquea ajustes para impedir que el usuario pueda restaurarlos y por lo general, son parte de adwares y troyanos.

Keylogger

Son programas encargados de almacenar todo lo que el usuario ingrese por el teclado. Usualmente instalados por troyanos para el robo de contraseñas e información confidencial. Algunos keyloggers sofisticados incluyen opciones como capturar pantalla en imágenes o video, además de la captura de teclado, enviar los datos por correo electrónico, entre otros. Estos programas son más utilizados en su forma de software, pero también existe hardware dedicado.

PUP

Potentially Unwanted Program, o en español, Programa Potencialmente no Deseado, que se instala sin el consentimiento del usuario y realiza acciones que pueden hacer que el usuario pierda el control de su privacidad o recursos de la computadora.

Rogue

Se trata de un programa falso que se presenta como algo que no es. Este tipo de malware comenzó a surgir con la proliferación del spyware, como un gran negocio para los

ciberdelincuentes en formato de falso antispyware. Después, fueron evolucionando desde falsos optimizadores de Windows y falsos antivirus.

Al ejecutarlos, mostrarán alguna falsa infección o problema en el sistema, que para poder resolver, se tiene que adquirir la versión de pago, que realmente resulta ser un fraude.

Riskware

Son programas originales, como herramientas de administración remota (RAT), que contienen agujeros utilizados por crackers para realizar acciones dañinas en el equipo.

Rootkit

Es un tipo de malware muy peligroso, son capaces de colarse, establecer comunicaciones con la sede, realizar defensas de reconocimiento, entre otros.

Tratar de eliminarlos se vuelve un problema, incluso cada removedor de rootkit advierte que la eliminación podría causar problemas al sistema operativo, en algunos casos, imposibilitando el arranque.

Esto se debe a que se oculta sustituyendo archivos críticos que quedan bajo control del rootkit. Al ser reemplazados dichos archivos, el sistema operativo queda inutilizable.

Troyano

Aunque técnicamente no se trata de un virus, cuenta con características para considerarlo como malware. Se trata de un pequeño programa que se aloja dentro de otra aplicación. Tiene como objetivo pasar inadvertido e instalarse en el sistema cuando se ejecuta el archivo huésped. Después de instalarse, puede realizar muchas tareas, ocultas para el usuario. Su uso más común es para la instalación de otros malware, como backdoors, y permitir el acceso al sistema al creador de la amenaza.

Spyware

Se trata de software espía, recopila información acerca de una persona u organización sin su consentimiento ni conocimiento. El objetivo más común es distribuirlo a empresas publicitarias o cualquier otro tipo de organizaciones interesadas. Por lo general, este malware envía la información a sus servidores. También recogen datos sobre las páginas web donde navega la víctima y la información que se solicita en las mismas, así como direcciones IP y URL que se visitan.

Muchas veces la información recabada es explotada con propósitos de mercadotecnia, y otras veces es el origen del SPAM, ya que sirve para enviar publicidad personalizada al usuario.

Ransomware

Es un código malicioso que cifra la información del equipo de cómputo e ingresa en él una serie de instrucciones para que el usuario pueda recuperar sus archivos.

Por lo general, la víctima debe pagar al atacante para obtener una contraseña y así descifrar su información. Este tipo de ataques se ha extendido por todo el mundo muy rápido, el último ataque más popular fue el de WannaCry, que afectó a millones de computadoras en más de 150 países del mundo.

Ejemplo de Ransomware, captura de pantalla de WannaCry

Los piratas informáticos piden al usuario una recompensa que debe ser pagada, por lo general, con criptomonedas, específicamente Bitcoin, gracias al grado de anonimato que brinda a los atacantes.

La primera variante de este tipo de malware surgió en algunas páginas web, mostrando una ventana emergente con una imagen de la policía local, advirtiendo al usuario que está siendo

vigilado y que debe pagar una multa por haber visitado determinados sitios web.

Para evitar ser víctima de cualquier malware, es recomendable contar con algún antivirus, existen muchos software antivirus gratuitos muy buenos y otros de pago que ofrecen algunos complementos.