Tipos de malware y herramientas para combatirlo

Un malware es un tipo de software malintencionado que tiene como objetivo infiltrarse o dañar un sistema informático o de información sin el consentimiento de su propietario. Dentro del malware podemos distinguir los siguientes tipo o variantes:

Adware: Programa que automáticamente muestra publicidad web al usuario durante su instalación o durante su uso para generar lucro a sus autores. 'Ad' en la palabra 'adware' se refiere a 'advertisement' (anuncios) en idioma inglés.

Spyware: Software que recopila información de un ordenador y después transmite esta información a una entidad externa sin el conocimiento o el consentimiento del propietario del ordenador. El término spyware también se utiliza más ampliamente para referirse a otros productos que no son estrictamente spyware. Estos productos, realizan diferentes funciones, como mostrar anuncios no solicitados (pop-up), recopilar información privada, redirigir solicitudes de páginas e instalar marcadores de teléfono.

Un spyware típico se autoinstala en el sistema afectado de forma que se ejecuta cada vez que se pone en marcha el ordenador (utilizando CPU y memoria RAM, reduciendo la estabilidad del ordenador), y funciona todo el tiempo, controlando el uso que se hace de Internet y mostrando anuncios relacionados. A diferencia de los virus, no se intenta replicar en otros ordenadores, por lo que funciona como un parásito.

Las consecuencias de una infección de spyware incluyen una pérdida considerable del rendimiento del sistema (hasta un 50 % en casos extremos), y problemas de estabilidad graves (el ordenador se queda "colgado"). También causan dificultad a la hora de conectar a Internet.

Virus: Un virus informático es un software malicioso que tiene por objeto alterar el normal funcionamiento del ordenador, sin el permiso o el conocimiento del usuario. Los virus, habitualmente, reemplazan archivos ejecutables por otros infectados con el código de este. Los virus pueden destruir, de manera intencionada, los datos almacenados en una computadora, aunque también existen otros más inofensivos, que solo se caracterizan por ser molestos.

Los virus informáticos tienen, básicamente, la función de propagarse a través de un software, son muy nocivos y algunos contienen además una carga dañina (payload) con distintos objetivos, desde una simple broma hasta realizar daños importantes en los sistemas, o bloquear las redes informáticas generando tráfico inútil.

Gusano informático (Worm): Software malicioso que tiene la propiedad de duplicarse a sí mismo. Los gusanos utilizan las partes automáticas de un sistema operativo que generalmente son invisibles al usuario. Los gusanos informáticos se propagan de ordenador a ordenador, pero a diferencia de un virus, tiene la capacidad a propagarse sin la ayuda de una persona. Lo más peligroso de los worms o gusanos informáticos es su capacidad para replicarse en tu sistema, por lo que tu ordenador podría enviar cientos o miles de copias de sí mismo, creando un efecto devastador a gran escala.

A diferencia de un virus, un gusano no necesita alterar los archivos de programas, sino que se encuentra en la memoria y se duplica a sí mismo. Los gusanos casi siempre causan problemas en la red (aunque sea simplemente consumiendo ancho de banda), mientras que los virus siempre infectan o corrompen los archivos de la computadora que atacan.

Troyano: Software malicioso que se presenta al usuario como un programa aparentemente legítimo

e inofensivo, pero que, al ejecutarlo, le brinda a un atacante acceso remoto al equipo infectado. Los troyanos pueden realizar diferentes tareas, pero, en la mayoría de los casos, crean una puerta trasera que permite la administración remota a un usuario no autorizado.

Un troyano no es de por sí, un virus informático, aun cuando teóricamente pueda ser distribuido y funcionar como tal. La diferencia fundamental entre un troyano y un virus consiste en su finalidad. Para que un programa sea un "troyano" solo tiene que acceder y controlar la máquina anfitriona sin ser advertido, normalmente bajo una apariencia inocua. Al contrario que un virus, que es un huésped destructivo, el troyano no necesariamente provoca daños, porque no es ese su objetivo.

Rootkit: Permite un acceso de privilegio continuo a una computadora pero que mantiene su presencia activamente oculta al control de los administradores al corromper el funcionamiento normal del sistema operativo o de otras aplicaciones. El término proviene de una concatenación de la palabra inglesa root, que significa 'raíz' (nombre tradicional de la cuenta privilegiada en los sistemas operativos Unix) y de la palabra inglesa kit, que significa 'conjunto de herramientas' (en referencia a los componentes de software que implementan este programa). El término rootkit tiene connotaciones peyorativas ya que se lo asocia al malware.
En otras palabras, usualmente se lo asocia con malware, que se esconde a sí mismo y a otros programas, procesos, archivos, directorios, claves de registro, y puertos que permiten al intruso mantener el acceso a una amplia variedad de sistemas operativos como pueden ser GNU/Linux, Solaris o Microsoft Windows para remotamente comandar acciones o extraer información sensible.
La detección del rootkit es dificultosa pues es capaz de corromper al programa que debería detectarlo. La eliminación del rootkit también puede ser complicada o prácticamente imposible, especialmente en los casos en que el rootkit reside en el núcleo; siendo a veces la reinstalación del sistema operativo el único método posible que hay para solucionar el problema.

Backdoors: Método para eludir los procedimientos habituales de autenticación al conectarse a una computadora. Una vez que el sistema ha sido comprometido por uno de los anteriores métodos, puede instalarse una puerta trasera para permitir un acceso remoto más fácil en el futuro. Las puertas traseras también pueden instalarse previamente al software malicioso para permitir la entrada de los atacantes. Para instalar puertas traseras se suelen usar troyanos, gusanos u otros métodos.

Keyloggers: **S**oftware o dispositivo hardware específico que se encarga de registrar las entradas que se realizan en el teclado, para almacenarlas en un fichero o enviarlas a través de internet.
Suele usarse como malware del tipo daemon, permitiendo que otros usuarios tengan acceso a contraseñas importantes, como los números de una tarjeta de crédito, u otro tipo de información privada que se quiera obtener. El registro de lo que se teclea puede hacerse tanto con medios de hardware como de software.
Son ingresados por muchos troyanos para robar contraseñas e información de los equipos en los que están instalados.

Hoax: Un hoax (en español: bulo) es un correo electrónico distribuido en formato de cadena, cuyo objetivo es hacer creer a los lectores, que algo falso es real. A diferencia de otras amenazas, como el phishing o el scam; los hoax no poseen fines lucrativos, por lo menos como fin principal.

Hijacker: Los hijackers son los encargados de secuestrar las funciones de nuestro navegador web (browser) modificando la página de inicio y búsqueda por alguna de su red de afiliados maliciosos, entre otros ajustes que bloquea para impedir sean vueltos a restaurar por parte del usuario. Generalmente suelen ser parte de los Adwares y Troyanos.

Botnets: Una botnet es una red de equipos infectados por códigos maliciosos, que son controlados por un atacante, disponiendo de sus recursos para que trabajen de forma conjunta y distribuida. Cuando una computadora ha sido afectada por un malware de este tipo, se dice que es un equipo robot o zombi.

Phishing: El phishing consiste en el robo de información personal y/o financiera del usuario, a través de la falsificación de un ente de confianza. De esta forma, el usuario cree ingresar los datos en un sitio de confianza cuando, en realidad, estos son enviados directamente al atacante.

PUPS: Los Pups se instalan sin el consentimiento del usuario y realizan acciones o tienen características que pueden menoscabar el control del usuario sobre su privacidad, confidencialidad, uso de recursos del ordenador, etc.

Rogues: Los Rogues son programas falsos ya sea de seguridad (antivirus, anti-malware, anti-spyware..) u optimizacion, que lo único que hacen es mostrar resultados de problemas falsos, o bien ellos mismos provocarlos o infectar, con el único de fin de que para poder resolver dichos problemas, se adquiera las versiones de pago de estos. Las cuales en realidad no van a reparar ni desinfectar nada, pero nos va a mostrar que sí.

Riskwares: Programas originales, como las herramientas de administración remota, que contienen agujeros usados por los crackers para realizar acciones dañinas.

Ransomware: Programa informático malintencionado que restringe el acceso a determinadas partes o archivos del sistema infectado, y pide un rescate a cambio de quitar esta restricción. Normalmente se transmite como un troyano o un gusano, infectando el sistema operativo. En este punto el ransomware se iniciará y cifrara los archivos del usuario con una determinada clave, que sólo el creador del ransomware conoce y proveerá de ella al usuario que la reclame a cambio de un pago.

Spam: Se denomina spam al correo electrónico no solicitado enviado masivamente por parte de un tercero. El riesgo con esto, es que el spam se utiliza para hacer propuestas relacionadas con varias operaciones ilegales con dinero o participación en algún supernegocio. También hay emails dedicados a robo de contraseñas o números de tarjetas de crédito, cartas de cadena, etc. O bien tb para llevar acabo una infeccion, por medio de la descarga de algun archivo maliciosos que contenga, o algun enlace que lleve a alguna pagina o descarga maliciosa.

2.- Indica las funciones que tienen los siguientes tipos de aplicaciones:

Anti-Keylogger

Software para la detección de keyloggers. Este tipo de software graba una lista de todos los keyloggers conocidos. Los usuarios legítimos del PC pueden entonces hacer, periódicamente, una exploración de esta lista, y el software busca los artículos de la lista en el disco duro. Una desventaja de este procedimiento es que protege solamente contra los keyloggers listados, siendo vulnerable a los keyloggers desconocidos o relativamente nuevos.

Antiphising

Los filtros anti-phishing (correos electrónicos engañosos) comprueban las páginas web a las que

accede un usuario y las comparan con una base de datos de páginas legítimas y páginas de phishing. Estos filtros alertarán al usuario si la página que va a visitar es una página de phishing conocida o si la página entraña algún tipo de riesgo potencial para su seguridad. Muchas de las últimas versiones de los navegadores más habituales tienen un filtro de phishing incluido.

Antirootkit

Herramienta diseñada para detectar y eliminar las formas sofisticadas y sigilosas de malware llamado “Rootkits”. Los rootkits son formas ocultas de malware que los antivirus tradicionales normalmente no pueden detectar o eliminar.

Anti-spam

Aplicación o herramienta informática que se encarga de detectar y eliminar el spam y los correos no deseados. Algunos antivirus y cortafuegos poseen incorporadas herramientas antispam.

El principal objetivo de una herramienta antispam, es lograr un buen porcentaje de filtrado de correo no deseado. Pero tampoco deben identificar al correo deseado como no deseado, pues eso traería peores consecuencias que "olvidar" filtrar algún spam.

Las herramientas antispam utilizan múltiples técnicas para detectar el correo no deseado. Algunas utilizan técnicas locales. Por ejemplo, emplean un diccionario propio para detectar palabras que suelen aparecer en estos correos o usan de una lista de amigos y una lista de enemigos.
Una técnica no local, la utilizan las herramientas que se conectan a servidores remotos, que se encargan de analizar cada uno de los emails que llegan al usuario, para identificar si son o no spam. Esos servidores remotos utilizan grandes bases de datos para identificar el correo no deseado.

Antivirus

Programas cuyo objetivo es detectar o eliminar virus informáticos. No sólo buscan detectar virus informáticos, sino bloquearlos, desinfectar archivos y prevenir una infección de los mismos. Actualmente son capaces de reconocer otros tipos de malware, como spyware, gusanos, troyanos, rootkits, etc.

podemos clasificar los métodos para la protección antivirus que usan estos programas en activos o pasivos.

Activos:

- Sólo detección: son vacunas que sólo actualizan archivos infectados, sin embargo, no pueden eliminarlos o desinfectarlos.
- Detección y desinfección: son vacunas que detectan archivos infectados y que pueden desinfectarlos.
- Detección y aborto de la acción: son vacunas que detectan archivos infectados y detienen las acciones que causa el virus.
- Comparación por firmas: son vacunas que comparan las firmas de archivos sospechosos para saber si están infectados.
- Comparación de firmas de archivo: son vacunas que comparan las firmas de los atributos

guardados en tu equipo.

- Por métodos heurísticos: son vacunas que usan métodos heurísticos para comparar archivos.
- Invocado por el usuario: son vacunas que se activan instantáneamente con el usuario.
- Invocado por la actividad del sistema: son vacunas que se activan instantáneamente por la actividad del sistema operativo.

Pasivos:

Mantener una política de copias de seguridad garantiza la recuperación de los datos y la respuesta cuando nada de lo anterior ha funcionado.

Cortafuegos

Parte de un sistema o una red que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas.

Se trata de un dispositivo o conjunto de dispositivos configurados para permitir, limitar, cifrar, descifrar, el tráfico entre los diferentes ámbitos sobre la base de un conjunto de normas y otros criterios.

Los cortafuegos pueden ser implementados en hardware o software, o en una combinación de ambos. Los cortafuegos se utilizan con frecuencia para evitar que los usuarios de Internet no autorizados tengan acceso a redes privadas conectadas a Internet, especialmente intranets. Todos los mensajes que entren o salgan de la intranet pasan a través del cortafuegos, que examina cada mensaje y bloquea aquellos que no cumplen los criterios de seguridad especificados.

Control Parental

Método para impedir, o limitar el acceso a cierta información o contenido a menores de edad. Esto se realiza mediante una serie de sistemas de bloqueo, normalmente protegidos mediante claves, bien alfanuméricas, bien mediante una combinación de teclas, que realizan los responsables legales del menor, normalmente sus padres, o los adultos responsables del uso de la correspondiente máquina.