**Tipos de malware y otras amenazas informáticas**

**Malware**

Malware es el acrónimo, en inglés, de las palabras "malicious" y "software", es decir software malicioso. Dentro de este grupo se encuentran los virus clásicos (los que ya se conocen desde hace años) y otras nuevas amenazas, que surgieron y evolucionaron, desde el nacimiento de las amenazas informáticas. Como malware, se encuentran diferentes tipos de amenazas, cada una con características particulares. Incluso existe malware que combina diferentes características de cada amenaza. Se puede considerar como malware todo programa con algún fin dañino.

**Clasificación del Malware**

* Adware
* Botnets
* Gusanos
* Hoax
* PayLoad
* Phishing
* Ransomware
* Rogue
* Rootkit
* Scam
* Spam
* Spyware
* Troyanos
* Virus

**Virus**

Un virus es un programa informático creado para producir algún daño en el ordenador y que posee, además, dos características particulares: pretende actuar de forma transparente al usuario y tiene la capacidad de reproducirse a sí mismo.

Todas las cualidades mencionadas pueden compararse con los virus biológicos, que producen enfermedades (y un daño) en las personas, actúan por sí solos y se reproducen (contagian).

Como cualquier virus, los virus informáticos necesitan de un anfitrión o huésped donde alojarse, y este puede ser muy variable: un archivo ejecutable, el sector de arranque o incluso la memoria del ordenador.

El daño que un virus puede causar también es extremadamente variable: desde un simple mensaje en pantalla para molestar al usuario o la eliminación de archivos del sistema, hasta inhabilitar completamente el acceso al sistema operativo son algunas de las alternativas conocidas. Los virus pueden infectar de dos maneras diferentes. La tradicional consiste en “inyectar” una porción de código en un archivo normal. Es decir, el virus reside dentro del archivo ya existente. De esta forma, cuando el usuario ejecute el archivo, además de las acciones normales del archivo en cuestión, se ejecutan las instrucciones del virus. La segunda forma de infectar consiste en “ocupar el lugar” del archivo original y renombrar este por un nombre conocido solo por el virus. En este caso, al ejecutar el archivo primero se ejecuta el malicioso y, al finalizar las instrucciones, este llama al archivo original, ahora renombrado.

Cuando un virus es ejecutado se producen dos acciones en paralelo: el daño en cuestión y la propagación para seguir infectando. Esta es la característica primordial de los virus, su capacidad de reproducirse por sí mismos: el mismo virus es el que causa el daño y continúa infectando nuevos ordenadores o archivos.

A pesar de que hoy en día la principal vía de contagio es a través de Internet, los canales de entrada de un virus informático pueden ser variables y se incluyen también los medios de almacenamiento (un disco rígido, un diskette, un pen drive, etc.) o una red local (por ejemplo, a través de las carpetas compartidas).

El surgimiento de los virus informáticos se puede localizar de forma aproximada a comienzos de los años ’80. Sin embargo, los virus de hoy en día no son los mismos que los de aquel entonces. Estos han evolucionado en muchos aspectos y uno de los principales es la capacidad de infectar archivos no ejecutables (los programas como .exe, .bat o .com) como por ejemplo los .mp3 o .pdf, entre otros. Se llama archivos ejecutables, a aquellos que alojan una aplicación en su extensión.

Los archivos no ejecutables como los mencionados, también se ejecutan pero utilizando una aplicación ajena al archivo en sí mismo. Otra de las características principales que ha evolucionado es la velocidad de reproducción. Los nuevos virus aprovechan las conexiones de alta velocidad de Internet para contagiar la mayor cantidad de computadoras en el menor tiempo posible.

**Troyanos**

El nombre de esta amenaza proviene de la leyenda del caballo de Troya, ya que el objetivo es el de engañar al usuario. Son archivos que simulan ser normales e indefensos, como pueden ser juegos o programas, de forma tal de "tentar" al usuario a ejecutar el archivo. De esta forma, logran instalarse en los sistemas. Una vez ejecutados, parecen realizar tareas inofensivas pero paralelamente realizan otras tareas ocultas en el ordenador.

Al igual que los gusanos, no siempre son malignos o dañinos. Sin embargo, a diferencia de los gusanos y los virus, estos no pueden replicarse por sí mismos.

Los troyanos pueden ser utilizados para muchos propósitos, entre los que se encuentran, por ejemplo:

* Acceso remoto (o Puertas Traseras): permiten que el atacante pueda conectarse remotamente al equipo infectado.
* Registro de tipeo y robo de contraseñas.
* Robo de información del sistema.

Los "disfraces" que utiliza un troyano son de lo más variados. En todos los casos intentan aprovechar la ingenuidad del usuario explotando diferentes técnicas de Ingeniería Social. Uno de los casos más comunes es el envío de archivos por correo electrónico simulando ser una imagen, un archivo de música o algún archivo similar, legitimo e inofensivo. Además del correo electrónico, otras fuentes de ataque pueden ser las mensajerías instantáneas o las descargas directas desde un sitio web.

Al igual que los gusanos, se pueden encontrar los primeros troyanos a finales de los años ’80, principios de los años ’90, de la mano del surgimiento de la Internet.

**Tipos de troyanos**

* **Backdoors:** Otros nombres para estos tipos son troyanos de acceso remoto o puertas traseras. Un troyano de estas características, le permite al atacante conectarse remotamente al equipo infectado. Las conexiones remotas son comunmente utilizadas en informática y la única diferencia entre estas y un backdoor es que en el segundo caso, la herramienta es instalada sin el consentimiento del usuario. La tecnología aplicada para acceder remotamente al equipo no posee ninguna innovación en particular ni diferente a los usos inofensivos con que son utilizadas estas mismas aplicaciones. Una vez que el atacante accede al ordenador del usuario, los usos que puede hacer del mismo son variados, según las herramientas que utilice: enviar correos masivos, eliminar o modificar archivos, ejecución de archivos, reiniciar el equipo o usos más complejos como instalar aplicaciones para uso malicioso (por ejemplo: alojamiento de sitios web de violencia o pedofilia).
* **Keyloggers:** Los keyloggers (del inglés Key = Tecla y Log = Registro) son uno de los tipos más utilizados para obtener información sensible de los usuarios. Los troyanos de este tipo, instalan una herramienta para detectar y registrar las pulsasiones del teclado en un sistema. Pueden capturar información como contraseñas de correos, cuentas bancarias o sitios web, entre otras, y por lo tanto atentar contra información sensible del usuario. La información capturada es enviada al atacante generalmente, en archivos de texto con la información. Estos troyanos, no son una amenaza para el sistema sino para el usuario y su privacidad. Los datos recolectados, pueden ser utilizados para realizar todo tipo de ataques, con fines económicos o simplemente malignos como modificar las contraseñas de las cuentas de acceso a algún servicio.
* **Banker:** Los troyanos bancarios tienen como principal objetivo robar datos privados de las cuentas bancarias de los usuarios. Utilizan diferentes técnicas para obtener los datos de acceso a todo tipo de entidades financieras, algunas de ellas son: reemplazar parcial o totalmente el sitio web de la entidad, enviar capturas de pantalla de la página bancaria (útiles cuando el usuarios utiliza teclados virtuales) o incluso la grabación en formato de video de las acciones del usuario mientras accede al sitio web. Los datos son enviados al atacante, por lo general, por correo electrónico o alojándolos en sitios FTP.
* **Downloader:** Este tipo de troyanos tiene como principal función la de descargar otros archivos maliciosos. Esta clase de amenazas no hace algún daño en sí, sino que descarga otros archivos maliciosos para el ordenador. El troyano se encarga, no solo de descargar el/los archivos, sino también de ejecutarlos o preparar la máquina para su ejecución automática al inicio.
* **Botnets:** Los troyanos botnets, son utilizados para crear redes de equipos zombis (botnets). El atacante utiliza el troyano (generalmente combinado con herramientas de backdoors) para controlar una cantidad importante de ordenadores y así poder utilizarlos para cualquier fin maligno. Pueden ser utilizados para enviar spam o para realizar ataques de denegación de servicio (DoS); estos consisten en saturar un sitio web generando más accesos y requerimientos de los que puede soportar y provocando la baja del servicio. De forma simple: el atacante dispone de miles de ordenadores para utilizarlos como él quiera y para los fines que él desee. Utilizar un troyano no es la única forma de crear y controlar una red botnet, sino simplemente una de ellas.
* **Proxy:** Este tipo de troyanos instalan herramientas en el ordenador que le permiten al atacante utilizar la Pc infectada como un servidor proxy. Un proxy es un servidor que da acceso a otros ordenadores a Internet a través de él. En este caso, el atacante utiliza el ordenador infectado para acceder a la web a través de él, enmascarando su identidad. En resumen, el atacante utiliza el troyano para cometer delitos por Internet (envío de spam, robo de información o de dinero) y, si se rastreara el origen del ataque, se encontraría la Pc infectada con el troyano.
* **Password Stealer:** Los password Stealer se encargan de robar información introducida en los formularios en las páginas web. Pueden robar información de todo tipo, como direcciones de correo electrónico, logins, passwords, PINs, números de cuentas bancarias y de tarjetas de crédito. Estos datos pueden ser enviados por correo electrónico o almacenados en un servidor al que el delincuente accede para recoger la información robada. En la mayoría de sus versiones, utilizan técnicas keyloggers para su ejecución y son similares a estos.
* **Dialer:** Los troyanos "Dialer" crean conexiones telefónicas en el ordenador del usuario, utilizando las funcionalidades del módem. Estas conexiones son creadas y ejecutadas de forma transparente a la víctima. Generalmente, se trata de llamados de alto costo a sitios relacionados con contenido adulto en Internet. Este tipo de troyanos crean un daño económico al usuario, el ordenador no se ve afectado por hacer una llamada telefónica.

**Gusanos**

En términos informáticos, los gusanos son en realidad un sub-conjunto de malware. Su principal diferencia con los virus radica en que no necesitan de un archivo anfitrión para seguir vivos. Los gusanos pueden reproducirse utilizando diferentes medios de comunicación como las redes locales o el correo electrónico. El archivo malicioso puede, por ejemplo, copiarse de una carpeta a otra o enviarse a toda la lista de contactos del correo electrónico.

El archivo malicioso puede copiarse de una carpeta a otra o enviarse a toda la lista de contactos del correo electrónico, citando solo algunos ejemplos.

La segunda diferencia con los virus tradicionales es que los gusanos no deben necesariamente provocar un daño al sistema. El principal objetivo de un gusano es copiarse a la mayor cantidad de equipos como sea posible. En algunos casos los gusanos transportan otros tipos de malware, como troyanos o rootkits; en otros, simplemente intentan agotar los recursos del sistema como memoria o ancho de banda mientras intenta distribuirse e infectar más ordenadores.

Los gusanos aprovechan las vulnerabilidades del sistema para propagarse; tanto de un sistema operativo como vulnerabilidades de las aplicaciones.

Para infectar por primera vez el equipo, estos programas generalmente aprovechan la ingeniería social mostrando temas o mensajes atractivos, principalmente si se trata de un mensaje de correo electrónico con el gusano adjunto. Una vez que se realizó esta acción, el gusano ya se propaga por los diferentes archivos del sistema o por la red a la que está conectado el mismo, siguiendo su propagación por sí solo.

El surgimiento de estas amenazas puede ubicarse a finales de los años ’80, más precisamente en el año 1988, cuando apareció el gusano Morris, considerado el primero de su especie. Este, logró colapsar cientos de sistemas pertenecientes a ArpaNet (la predecesora de Internet).

En general, los gusanos son mucho más fáciles de eliminar de un sistema que los virus, dado que no infectan archivos. Los gusanos muy a menudo se añaden al inicio del sistema o modifican las claves de registro, para asegurarse que serán cargados cada vez que el mismo se inicie.

**Tipos de gusanos**

* **De correo electrónico.** Los gusanos que se envían por correo electrónico son los más antiguos y los más populares también hasta el momento. Las técnicas utilizadas son similares a las explicadas en el ítem anterior: mensajes atractivos utilizando ingeniería social, envío automático a la libreta de contactos si el usuario está infectado y archivos adjuntos por lo general ejecutables. Una de las características relevantes es la de suplantar la identidad de un usuario con fines maliciosos, conocida como spoofing. De esta forma, el correo llega a través de un remitente conocido por el usuario, solo que este no ha enviado el correo de forma voluntaria. Este detalle puede hacer que el usuario confíe en el correo solo por los datos de quién lo envía
* **De P2P.** Los gusanos también utilizan las redes P2P como medio de transmisión para infectar ordenadores. En este tipo de redes (como el Emule o el Kazaa) utilizan nombres atractivos, teniendo en cuenta cuáles son las palabras más buscadas en estos servicios. Entre los disfraces más comunes, aparentan ser generalmente cracks de programas, fotos o videos de mujeres famosas o películas taquilleras.
* **De páginas web.** También es posible descargar un gusano a través de páginas web. Las técnicas utilizadas son similares al resto de los tipos de gusanos, utilizando nombres atractivos y creando páginas web falsas. Estos gusanos se combinan muchas veces con técnicas de phishing para lograr que la víctima ingrese a la página web y descargue el archivo malicioso.
* **De aplicaciones web.** Otra metodología de propagación web, utilizada por los gusanos, es a través de vulnerabilidades en las aplicaciones utilizadas. A través de la ejecución de scripts (porciones de código), es posible generar una descarga y ejecución del código malicioso, sin necesidad de intervención del usuario. Esta técnica se denomina Drive-By-Download, siendo el único paso que realiza el usuario para infectarse, el ingreso a una URL con el código malicioso. Estos scripts, se encuentran por lo general ofuscados, de forma tal de evitar su detección.
* **De mensajería instantánea.** Estos gusanos aprovechan el envío de archivos en el cliente de mensajería instantánea. Por lo general, solo afectan a los más populares: el MSN y el Windows Messenger. De esta forma, el usuario recibe la opción para transferir un archivo que en realidad es malware. Por lo general, estos archivos utilizan nombres atractivos para asegurarse que más usuarios lo descargarán, combinando el malware con técnicas de ingeniería social. Por lo general, una Pc que está infectada con este tipo de malware, al iniciar sesión en Messenger, automáticamente el código malicioso envía el archivo (la invitación para descargar el archivo específicamente) a todos los contactos que tenga el usuario conectados. Otra característica es que comúnmente estos archivos son ejecutables (extensión .exe o .bat) a pesar de que en el texto de envío figuran como fotos o videos.

**Spyware**

Los spyware o (programas espías) son aplicaciones que recopilan información del usuario, sin el consentimiento de este. El uso más común de estos aplicativos es la obtención de información respecto a los accesos del usuario a Internet y el posterior envío de la información recabada a entes externos.

Al igual que el adware, no es una amenaza que dañe al ordenador, sino que afecta el rendimiento de este y, en este caso, atenta contra la privacidad de los usuarios. Sin embargo, en algunos casos se producen pequeñas alteraciones en la configuración del sistema, especialmente en las configuraciones de Internet o en la página de inicio.

Puede instalarse combinado con otras amenazas (gusanos, troyanos) o automáticamente. Esto ocurre mientras el usuario navega por ciertas páginas web que aprovechan vulnerabilidades del navegador o del sistema operativo, que permiten al spyware instalarse en el sistema sin el consentimiento del usuario.

No es el objetivo de este tipo de malware, robar archivos del ordenador, sino obtener información sobre los hábitos de navegación o comportamiento en la web del usuario atacado. Entre la información recabada se puede encontrar: qué páginas web se visitan, cada cuánto se visitan, cuánto tiempo permanece el usuario en el sitio, qué aplicaciones se ejecutan, qué compras se realizan o qué archivos se descargan.

Ciertos spyware poseen características adicionales para conseguir información e intentan interactuar con el usuario simulando ser buscadores o barras de herramientas. Con estas técnicas, los datos obtenidos son más legítimos y confiables que con otros métodos espías utilizados.

Otro modo de difusión es a través de los programas que, legítimamente incluyen adware en sus versiones gratuitas y ofrecen e informan al usuario de la existencia de esta. Es habitual, aunque no se informe al usuario, que también se incluya algún tipo de spyware en estas aplicaciones para complementar con los anuncios publicitarios aceptados legítimamente por el usuario.

Tanto el spyware como el adware forman parte de una etapa posterior en la historia del malware, respecto a otros tipos de amenazas como virus, gusanos o troyanos. Los primeros ejemplares de esta amenaza se remontan a mediados de los años '90, con la popularización de Internet. Tanto el spyware como el adware, no tienen las capacidades de auto-propagación que poseen los virus.

**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.

El phishing es una de las técnicas y tipos de Password Harvesting, forma en que se denominan los ataques que recolectan contraseñas de los usuarios. En su forma clásica, el ataque comienza con el envío de un correo electrónico simulando la identidad de una organización de confianza, como por ejemplo un banco o una reconocida empresa. Las características de un correo de phishing son las siguientes:

* Uso de nombres de reconocidas organizaciones.
* El correo electrónico del remitente simula ser de la compañía en cuestión.
* El cuerpo del correo, presenta el logotipo de la compañía u organización que firma el mensaje.
* El mensaje insta al usuario a reingresar algún tipo de información que, en realidad, el supuesto remitente ya posee.
* El mensaje incluye un enlace.

El enlace, es un componente importante del ataque. Cuando el usuario hace clic sobre él es direccionado a un sitio web, donde podrá ingresar la información solicitada en el correo electrónico. A pesar de que el texto sobre el que usuario haga clic, indique una dirección web válida, el mismo puede direccionar a cualquier otro sitio web, en este caso, el sitio falsificado. De esta forma, el correo induce al usuario a clickear sobre los vínculos del mensaje.

Como técnica de Ingeniería Social, el phishing utiliza el factor miedo, para inducir al usuario a ingresar la información en el sitio del atacante. Un aviso legítimo de caducidad de información (como contraseñas, cuentas de correo o registros personales), nunca alertará al usuario sin el suficiente tiempo para que este, gestione las operaciones necesarias en tiempos prudenciales. Mensajes del tipo "su cuenta caducará en 24hs." o "si no ingresa la información en las próximas horas..." son frecuentemente utilizados en este tipo de ataques.

El sitio web falso es creado utilizando, no solo el logotipo, sino también la estructura, las imágenes, las tipografías y los colores de la página original. El atacante intenta crear la página web de forma idéntica a la original, para aumentar la eficacia del engaño.

Prácticamente todos los componentes, del mensaje enviado al usuario, son idénticos a un mensaje legítimo del mismo tipo. Reconocer un mensaje de phishing no es una tarea simple para el usuario. Cualquier usuario de correo, es una potencial víctima de estos ataques. Entre las principales formas de prevención se encuentran:

* Nunca hacer clic en los enlaces incluidos en los correos electrónicos. Ingresar siempre a la web tipeando o copiando la dirección web mencionada en el mail.
* A pesar de no ser garantía absoluta, verificar la seguridad del sitio, observando el protocolo utilizado (debe ser https) y el certificado de seguridad.
* Corroborar la legitimidad de un correo que solicite información confidencial, estableciendo contacto con la entidad, a través de información previamente conocida, como números de teléfono o personal de la organización.
* Revisar periódicamente los sitios web donde se aloja información financiera.

Este tipo de ataques, comenzaron a suceder a mediados de la década del '90. A partir del año 2000, y con el auge de la conectividad, el phishing fue popularizado y comenzaron a surgir nuevos tipos y variantes de este fraude.

Otros ataques, derivados del phishing y de características similares, son:

* **Pharming:** Consiste en atacar los servidores DNS de un sitio y direccionar el tráfico legítimo a un sitio web falsificado. En este caso, cualquier usuario que intente ingresar en el sitio web original, a pesar de ingresar correctamente la dirección del sitio web, es direccionado a otro servidor, donde se encuentra alojada la página web del atacante, simulando, como en el phishing, ser la web original.
* **Pharming local:** al igual que en el caso anterior, este ataque modifica la información DNS, solo que en este caso, las modificaciones son realizadas en el equipo de la víctima a través del archivo hosts. Este, almacena la relación de nombres y direcciones IP. Es claro que modificar un DNS local es más simple que atacar los servidores DNS de Internet y el ordenador de un usuario final posee menos medidas preventivas que un servidor web.
* **Vishing:** El atacante falsifica el identificador de llamadas utilizando las comunicaciones VoIP del ordenador. En este ataque, la diferencia radica en el medio a través del cual la víctima es contactada. Otra técnica de este mismo ataque, utiliza el mismo medio que el phishing tradicional (correo electrónico) y el usuario es enlazado a un número telefónico donde se falsifica la atención al cliente de cierta organización y se solicita el ingreso de información personal a través del teléfono.
* **Smishing:** Se llama así, al phishing por SMS. El usuario es contactado a través de un mensaje de texto en su celular y es invitado a contactar telefónicamente a la organización, para verificar sus datos personales.

**Adware**

Adware (contracción de ADvertisement - anuncio - y softWARE) es un programa malicioso, que se instala en la computadora sin que el usuario lo note, cuya función es descargar y/o mostrar anuncios publicitarios en la pantalla de la víctima.

Cuando un adware infecta un sistema, el usuario comienza a ver anuncios publicitarios de forma inesperada en pantalla. Por lo general, estos se ven como ventanas emergentes del navegador del sistema operativo (pop-ups). Los anuncios pueden aparecer incluso, si el usuario no está navegando por Internet.

El adware no produce una modificación explícita que dañe el sistema operativo, sino que sus consecuencias afectan al usuario. En primer término, porque es una molestia para la víctima que el sistema abra automáticamente ventanas sin ningún tipo de orden explícita. Por otro lado, el adware disminuye el rendimiento del equipo e Internet, ya que utiliza, y por ende consume, procesador, memoria y ancho de banda.

Frecuentemente, las mismas publicidades ejecutadas por el malware, ofrecen al usuario la posibilidad de pagar una suma de dinero a cambio de no visualizar más los anuncios en su pantalla. Muchas empresas utilizan el adware como forma de comercializar sus productos, incluyendo la publicidad no deseada en sus versiones gratuitas y ofreciendo las versiones pagas sin el adware. En este caso, existen usuarios que aceptan el adware a cambio de utilizar la aplicación sin costo alguno.

Por lo general, el adware utiliza información recopilada por algún spyware para decidir qué publicidades mostrar al usuario. Estas dos amenazas frecuentemente se las observa trabajando en forma conjunta.

**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.

Los contenidos de este tipo de correos son extremadamente variables. Entre otros, podemos encontrar alertas falsas sobre virus y otras amenazas, historias solidarias sobre gente con extrañas enfermedades, leyendas urbanas o secretos para hacerse millonario.

Existen una serie de características comunes a la mayoría de los hoax que existen en la red, y cuyo conocimiento, pueden ayudar al usuario a detectar este tipo de correos:

* Están escritos de forma desprolija, sin firma y con redacción poco profesional.
* Invitan al usuario a reenviar el correo a sus contactos, conformando lo que se conoce como cadena de mails.
* El remitente, es alguien de confianza. Esto se debe simplemente a que el reenvío de esta amenaza está dado voluntariamente por víctimas que ya han creído el contenido del correo.
* Por lo general, no poseen información específica de ubicación temporal. De esta forma, al ser el contenido atemporal, la difusión del mensaje se puede dar por tiempo indeterminado.
* Algunos de ellos, indican un beneficio o donación por cada vez que se reenvíe el mensaje.

Al no ser económicos los objetivos de los hoax, existen otras motivaciones para lanzar este tipo de correos, entre las que se encuentran:

* Generar Miedo, Inseguridad y Duda (FUD en sus siglas en inglés) en los receptores.
* Armar bases de direcciones de correo electrónico. Esto se debe a que muchos clientes de correo electrónico, copian la lista de correos histórica en el cuerpo del mensaje. En un hoax se pueden llegar a encontrar cientos de direcciones de correo para enviar spam.
* Alimentar el ego del creador. Muchos hoax no persiguen otro fin que la alegría del inventor por ver "su" correo dando vueltas por la red.
* Confundir al lector.

Se conoce como el primer hoax por e-mail al "Good Times", correo enviado desde el año 1994, cuyo contenido indicaba la presencia de una amenaza que aparecía adjunta a un correo electrónico cuyo asunto era justamente "Good Times". Las advertencias indicaban no descargar el archivo adjunto al mensaje ya que este podía reescribir todo el disco rígido y el usuario perdería toda su información. Como cierre, al pie del correo se leía la inscripción "Sea cuidadoso y reenvíe este mail a todos sus conocidos". Desde la fecha del lanzamiento del hoax no se ha encontrado virus alguno que responda al nombre y características del mencionado en el bulo.

Ciertos hoaxes pasan años distribuyéndose por la red, con picos de alto tráfico luego de etapas de poca difusión. Esto se debe a que la misma depende exclusivamente del usuario y de cuánto este cree o no en el contenido de los correos con estas características. Entre los hoax más famosos se pueden encontrar aquel que alerta sobre el cierre de hotmail, otro que menciona que el MSN se volverá pago o uno que indica que Bill Gates está repartiendo su fortuna con cualquier usuario que reenvíe el correo electrónico.

Aunque no persigan fines económicos o extremadamente dañinos, no es prudente subestimar esta amenaza. Han existido casos en donde el contenido del correo ha hecho que el receptor borrara los archivos de su sistema. Ante la duda, existen bases de datos confiables en Internet para identificar si un correo ya fue detectado como hoax.

**Rootkit**

Rootkit es una o más herramientas diseñadas para mantener en forma encubierta el control de una computadora. Estas pueden ser programas, archivos, procesos, puertos y cualquier componente lógico que permita al atacante mantener el acceso y el control del sistema.

El rootkit no es un software maligno en sí mismo, sino que permite ocultar las acciones malignas que se desarrollen en el ordenador, tanto a través de un atacante como así también ocultando otros códigos maliciosos que estén trabajando en el sistema, como gusanos o troyanos. Otras amenazas incorporan y se fusionan con técnicas de rootkit para disminuir la probabilidad de ser detectados.

Los rootkits por lo general, se encargan de ocultar los procesos del sistema que sean malignos. También intentan deshabilitar cualquier tipo de software de seguridad. Las actividades ocultadas no son siempre explícitamente maliciosas. Muchos rootkits ocultan inicios de sesión, información de procesos o registros.

Inicialmente los rootkit aparecieron en el sistema operativo UNIX y eran una colección de una o más herramientas que le permitían al atacante conseguir y mantener el acceso al usuario de la computadora más privilegiado (en los sistemas UNIX, este usuario se llama \*root\* y de ahí su nombre). En los sistemas basados en Windows, los rootkits se han asociado en general con herramientas usadas para ocultar programas o procesos al usuario. Una vez que se instala, el rootkit utiliza funciones del sistema operativo para ocultarse, de manera tal de no ser detectado y es usado en general para ocultar otros programas dañinos.

Un rootkit ataca directamente el funcionamiento de base de un sistema operativo. En linux, modificando y trabajando directamente en el kernel del sistema. En Windows, interceptando los APIs (Interfaz de Aplicaciones de Programación) del sistema operativo. Estas, interactúan entre el usuario y el kernel; de esta forma, el rootkit manipula el kernel sin trabajar directamente en él como en el caso del software libre.

Existen otros tipos de rootkit, que persiguen el mismo fin: ocultar actividades en el sistema. Los BootRootkits atacan el sector de arranque y modifican la secuencia de arranque para cargarse en memoria antes de cargar el sistema operativo original. Otros rootkits atacan, en lugar del sistema operativo, directamente las aplicaciones utilizando parches o inyecciones de código y modificando su comportamiento respecto al habitual.

**Spam**

Se denomina spam al correo electrónico no solicitado enviado masivamente por parte de un tercero. En español, también es identificado como correo no deseado o correo basura.

Es utilizado, por lo general, para envío de publicidad, aunque también se lo emplea para la propagación de códigos maliciosos. Además de los riesgos que representa el spam para el envío de contenidos dañinos, y de la molestia que causa al usuario recibir publicidad no deseada; también existen efectos colaterales de su existencia, como la pérdida de productividad que genera en el personal la lectura de correo, y el consumo de recursos (ancho de banda, procesamiento, etc.) que generan este tipo de correos.

La cantidad de spam ha ido en aumento con el pasar de los años, y es de esperar que esta tendencia continúe. También se han modificado las características de dichos correos. Inicialmente, el spam fue utilizado para enviar mensajes en formato de texto. Sin embargo, con la creación de filtros anti-spam se comenzaron a identificar este tipo de mensajes, y posteriormente, el spam evolucionó a correos con imágenes o contenido HTML. Respecto al porcentaje, algunos estudios afirman que entre un 80-85% del correo electrónico es correo basura. Algunas fuentes han aventurado valores superiores, llegando al 95%.

Aunque en ciertos países existe legislación que prohíbe el envío de este tipo de correos, las posibilidades tecnológicas para establecer infraestructuras en diversos lugares del mundo, dificultan que el problema sea erradicado solo con legislaciones locales.

La principal barrera de protección son las herramientas antispam. De todas formas, también es importante que los usuarios no reenvíen correos en cadena, utilicen la opción de copia oculta (para no difundir sus direcciones de correo) y no publicar la dirección de correo en foros o sitios web.

Aunque el spam visto con mayor frecuencia es el realizado vía correo electrónico, también se pueden observar mensajes de spam en foros, comentarios en blogs o mensajes de texto, entre otros.

**Scam**

Scam es el nombre utilizado para las estafas a través de medios tecnológicos. A partir de la definición de estafa, se define scam como el "delito consistente en provocar un perjuicio patrimonial a alguien mediante engaño y con ánimo de lucro; utilizando como medio la tecnología".

Los medios utilizados por los scam, son similares a los que utiliza el phishing; aunque el objetivo no es obtener datos sino lucrar de forma directa a través del engaño.

Las técnicas utilizadas principalmente, para engañar al usuario, son el anuncio de una ganancia extraordinaria o las peticiones de ayuda caritativa.

En el primer caso aparecen, por ejemplo, los anuncios de empleo con rentabilidades inesperadas o el premio de una lotería o juegos de azar. En estos casos, para convertir el ataque en una estafa, se le solicita al usuario que haga una entrega de una pequeña suma de dinero (en comparación con la supuesta ganancia ofrecida) para poder verificar algunos datos o cubrir los costos de envío y administración del dinero obtenido.

El segundo caso, y el más común, es el correo solicitando una donación al usuario, para una obra caritativa. Los contenidos más generales hacen referencia a países de extrema pobreza (generalmente de África), a personas enfermas o a catástrofes internacionales. El correo invita a la víctima a hacer un depósito o envío de dinero a fin de colaborar con la causa caritativa. Esta técnica de ingeniería social ataca la bondad de las personas y su interés por ayudar.

Los scam son una amenaza constante para el usuario y cientos de ellos rondan la red cada día. Sin embargo, luego de algún desastre (terremoto, inundación, guerra, hambruna) con algún impacto mediático considerable, aumenta notablemente la cantidad de correos scam que circulan por la red.

Estas estafas han tenido finales menos felices que la pérdida de dinero, con casos de individuos desaparecidos o secuestrados, que han viajado al extranjero para encontrarse con el "benefactor". En casos menos extremos, muchas personas han perdido miles y miles de dólares en estos fraudes.

Algunos consejos para evitar estas estafas:

* Los e-mails que solicitan donativos y que no han sido solicitados casi siempre son fraudulentos particularmente aquellos que aparecen rápidamente después de un desastre. Las instituciones benéficas legítimas en general envían e-mails solicitando donativos a personas que han optado de forma explícita recibir e-mails de dicha organización.
* No deje que le confunda el aspecto. Los e-mails pueden parecer legítimos copiando los gráficos y el lenguaje legítimo de una organización.
* Si tiene dudas respecto a la legitimidad del correo, vaya directamente al sitio web de la organización y encuentre las formas de donar desde allí. Considere también, las posibilidades de averiguar la veracidad de la institución benéfica.
* No haga click en links: aquellos que vienen en los e-mails pueden conducirlo a sitios web "simulados" que fingen la apariencia de una organización genuina.

**PayLoad**

PayLoad es una función adicional que posee cierta amenaza en particular. La traducción exacta del inglés, es más precisa respecto a su definición: "carga útil". Refiere a acciones adicionales, incluidas en virus, gusanos o troyanos; como por ejemplo robo de datos, eliminación de archivos, sobre-escritura del disco, reemplazo del BIOS, etc.

Un payload no es necesariamente maligno, sino que refiere también a efectos secundarios nocivos para el ordenador.

**Ransomware**

El ransomware es una de las amenazas informáticas más similares a un ataque sin medios tecnológicos: el secuestro. En su aplicación informatizada, el ransomware es un código malicioso que cifra la información del ordenador e ingresa en él una serie de instrucciones para que el usuario pueda recuperar sus archivos. La víctima, para obtener la contraseña que libera la información, debe pagar al atacante una suma de dinero, según las instrucciones que este disponga.

El pago generalmente es indicado a través de un depósito bancario, luego del cuál el atacante envía las contraseñas para descifrar la información del disco duro. En las primeras versiones, los métodos de cifrado utilizados fueron de lo más precarios y recuperar la información era una tarea viable sin entregar el dinero al atacante. Sin embargo, el ransomware es una amenaza cuyo desarrollo es paralelo a los nuevos métodos de cifrado y su gravedad, por lo tanto, aumenta proporcional al desarrollo de la criptografía.

El ataque, en el común de los casos, ataca solo a ciertos archivos; siendo los principales afectados los de ofimática, como procesadores de texto, hojas de cálculo o diapositivas. También las imágenes y correos electrónicos son considerados prioritarios para el común de los ataques.

El nombre proviene del término sajón "Ransom" que define la exigencia de pago por la restitución de la libertad de alguien o de un objeto, es decir, un secuestro. De todas formas, también se suele denominar a estos ataques como criptovirus.

El nacimiento de este ataque data del año 1989, cuando vía correo postal fueron distribuidos a empresas farmacéuticas, diskettes que supuestamente contenían información respecto al HIV. Al ejecutar los archivos que este contenía, se producían los efectos del ataque: la información del ordenador era cifrada y la víctima podía observar una serie de instrucciones y requerimientos para recuperar sus datos, que incluían la entrega de dinero al atacante.

A pesar que la defensa proactiva de malware, es la principal barrera de defensa con la que cuenta el usuario para prevenir esta amenaza; otro método de minimizar los daños por parte del usuario, es la creación de backups periódicos de los datos del ordenador.

**Rogue**

Rogue es un software que, simulando ser una aplicación anti-malware (o de seguridad), realiza justamente los efectos contrarios a estas: instalar malware. Por lo general, son ataques que muestran en la pantalla del usuario advertencias llamativas respecto a la existencia de infecciones en el equipo del usuario. La persona, es invitada a descargar una solución o, en algunos casos, a pagar por ella. Los objetivos, según el caso, varían desde instalar malware adicional en el equipo para obtener información confidencial o, directamente, la obtención de dinero a través del ataque.

En cualquiera de los casos, es un ataque complementado por una alta utilización de Ingeniería Social, utilizando mensajes fuertes y exagerando las consecuencias de la supuesta amenaza. Vocabulario informal, palabras escritas en mayúscula, descripción detallada de las consecuencias, e invitaciones a adquirir un producto, son algunas de las principales características de esta amenaza.

Muchas variantes de rogue, además, simulan hacer un escaneo del sistema, con barra de progreso incluida y minuciosos detalles respecto a la extensa cantidad de amenazas que se encuentran en el ordenador. Los resultados nunca son alentadores y obviamente siempre se encuentra un número de amenazas importantes para el ordenador y, además, se detallan las peligrosas consecuencias de no solucionar el problema con rapidez.

Para detectar este ataque, como usuario, es importante tener en cuenta que los mensajes de amenazas en nuestro ordenador deben prevenir únicamente de la solución anti-malware que esté instalada y que, por lo general, las empresas de seguridad no utilizan carteles extremadamente llamativos y poco formales para indicar la presencia de amenazas.

**Fuente:** <http://www.eset-la.com/centro-amenazas/amenazas>