¿Qué es un virus?

En informática, un virus de computadora es un programa malicioso desarrollado por programadores que infecta un sistema para realizar alguna acción determinada. Puede dañar el sistema de archivos, robar o secuestrar información o hacer copias de si mismo e intentar esparcirse a otras computadoras utilizando diversos medios.

El término usado para englobar todos estos códigos es malware, formado por la unión de las palabras malicious y software, es decir, software maléfico. Actualmente, existen muchos tipos de virus (malware), con comportamientos característicos que permiten clasificarlos en diferentes categorías.

Estos pequeños programas de computadora tienen la capacidad de incorporar (“infectar”) su código en otros programas, archivos o sistemas y usarlos para hacer copias de sí mismos. El término “virus de computadora” fue instalado en 1983 por el ingeniero eléctrico americano Fred Cohen, que concluyó su doctorado en 1986 con un trabajo sobre este tema. El nombre fue inspirado en los virus biológicos, la mas pequeña forma de vida conocida, que se reproducen infectando una célula y usando el material genético de esta para crear nuevos especímenes. Hoy existen muchos tipos de virus, clasificados de acuerdo con sus acciones o características, como virus infectores de archivos, virus de boot, virus de macro, de redes, de script, furtivos, polimórficos, etc.

Tipos de virus de computadora

A continuación se detallan los distintos tipos de virus de computadoras hasta ahora conocidos:

Virus de Boot

Uno de los primeros tipos de virus conocido, el virus de boot infecta la partición de inicialización del sistema operativo. El virus se activa cuando la computadora es encendida y el sistema operativo se carga.

Time Bomb o Bomba de Tiempo

Los virus del tipo “bomba de tiempo” son programados para que se activen en determinados momentos, definido por su creador. Una vez infectado un determinado sistema, el virus solamente se activará y causará algún tipo de daño el día o el instante previamente definido. Algunos virus se hicieron famosos, como el “Viernes 13” y el “Michelangelo”.

Lombrices, worm o gusanos

Con el interés de hacer un virus pueda esparcirse de la forma más amplia posible, sus creadores a veces, dejaron de lado el hecho de dañar el sistema de los usuarios infectados y pasaron a programar sus virus de forma que sólo se repliquen, sin el objetivo de causar graves daños al sistema. De esta forma, sus autores tratan de hacer sus creaciones más conocidas en internet. Este tipo de virus pasó a ser llamado gusano o worm. Son cada vez más perfectos, hay una versión que al atacar la computadora, no sólo se replica, sino que también se propaga

por internet enviandose a los e-mail que están registrados en el cliente de e-mail, infectando las computadoras que abran aquel e-mail, reiniciando el ciclo.

Tienen la capacidad de hacer copias de sí mismos, al contrario de los virus no necesitan infectar otros programas para esta tarea. Basta que sean ejecutados en un sistema. Hay varios gusanos o worms, con muchas funcionalidades diferentes. Algunos son destructivos (borran o dañan archivos), otros sólo se diseminan en gran cantidad provocando atascos en las redes de computadoras.

Troyanos o caballos de Troya

Ciertos virus traen en su interior un código aparte, que le permite a una persona acceder a la computadora infectada o recolectar datos y enviarlos por Internet a un desconocido, sin que el usuario se de cuenta de esto. Estos códigos son denominados Troyanos o caballos de Troya.

Inicialmente, los caballos de Troya permitían que la computadora infectada pudiera recibir comandos externos, sin el conocimiento del usuario. De esta forma el invasor podría leer, copiar, borrar y alterar datos del sistema. Actualmente los caballos de Troya buscan robar datos confidenciales del usuario, como contraseñas bancarias.

Los virus eran en el pasado, los mayores responsables por la instalación de los caballos de Troya, como parte de su acción, pues ellos no tienen la capacidad de replicarse. Actualmente, los caballos de Troya ya no llegan exclusivamente transportados por virus, ahora son instalados cuando el usuario baja un archivo de Internet y lo ejecuta. Práctica eficaz debido a la enorme cantidad de e-mails fraudulentos que llegan a los buzones de los usuarios. Tales e-mails contienen una dirección en la web para que la víctima baje, sin saber, el caballo de Troya, en vez del archivo que el mensaje dice que es. Esta práctica se denomina phishing, expresión derivada del verbo to fish, “pescar” en inglés. Actualmente, la mayoría de los caballos de Troya simulan webs bancarias, “pescando” la contraseña tecleada por los usuarios

de las computadoras infectadas. Existen distintas formas para saber si estás infectado con un troyano y cómo eliminarlo de tu PC.

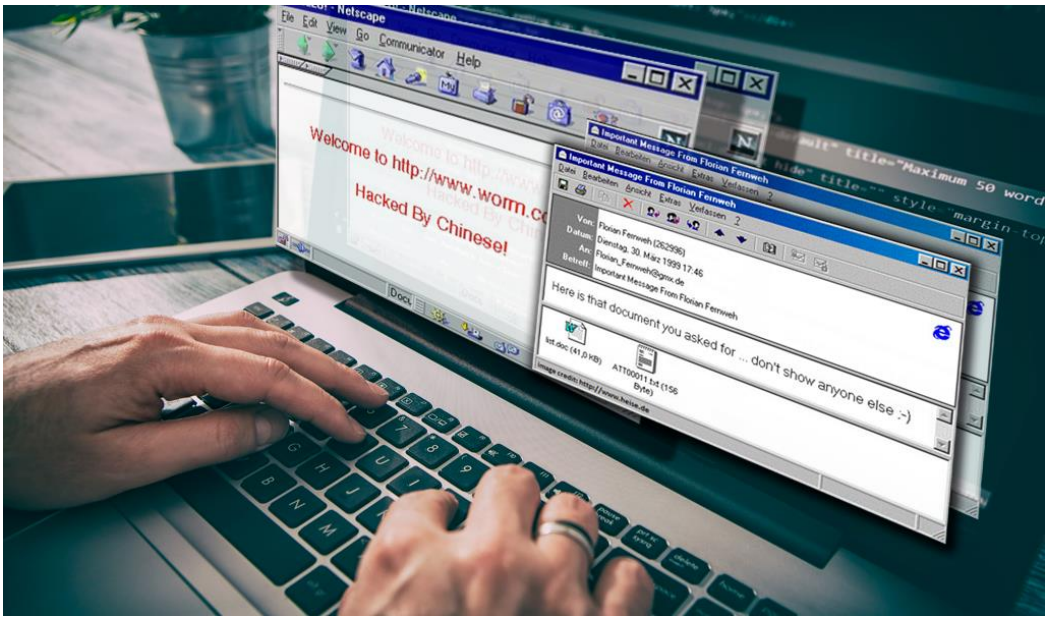
Los trojans puros no tienen capacidad de infectar otros archivos o diseminarse de un ordenador a otro, como es el caso de los virus y worms. Para que se introduzcan en un sistema, deben ser deliberadamente enviados a los usuarios, normalmente disfrazados como fotos, juegos y utilitarios en general. Muchas veces, los caballos de Troya estan compuestos de dos partes: un programa llamado cliente, que queda en la máquina del atacante, y otro llamado servidor, que queda en la máquina de la víctima. El componente cliente se comunica con el servidor, posibilitando que un intruso robe contraseñas y otra informacion privada, o incluso tome control total del sistema invadido, pudiendo abrir, cerrar, ejecutar o borrar archivos, modificar las configuracion del mouse y del teclado, abrir y cerrar el CD-ROM, etc. Todo eso a distancia.

Hijackers

Los hijackers son programas o scripts que "secuestran" navegadores de Internet,principalmente el Internet Explorer. Cuando eso pasa, el hijacker altera la página inicial del navegador e impide al usuario cambiarla, muestra publicidad en pop-ups o ventanas nuevas, instala barras de herramientas en el navegador y pueden impedir el acceso a determinadas webs (como webs de software antivírus, por ejemplo).

Keylogger

El KeyLogger es una de las especies de virus existentes, el significado de los términos en inglés que más se adapta al contexto sería: Capturador de teclas. Luego que son ejecutados, normalmente los keyloggers quedan escondidos en el sistema operativo, de manera que la víctima no tiene como saber que está siendo monitorizada.Actualmente los keyloggers son desarrollados para medios ilícitos, como por ejemplo robo de contraseñas bancarias. Son utilizados también por usuarios con un poco más de conocimiento para poder obtener contraseñas personales, como de cuentas de email, MSN, entre otros. Existen tipos de keyloggers que capturan la pantalla de la víctima, de manera de saber, quien implantó el keylogger, lo que la persona está haciendo en la computadora.



Se instalan en el sistema de forma oculta y su acción no es percibida por el dueño de la computadora atacada. Los keyloggers están siendo muy usados últimamente en ataques por e-mail, disfrazados como si fueran mensajes enviados por empresas legítimas. Los más sofisticados ya son capaces de grabar también las páginas que el usuario visita y el área del click del mouse, por eso están siendo llamados de screenloggers (la palabra screen, en inglés, se refiere a la pantalla del ordenador).

Zombie

El estado zombie en una computadora ocurre cuando es infectada y está siendo controlada por terceros. Pueden usarlo para diseminar virus , keyloggers, y procedimientos invasivos en general. Usualmente esta situación ocurre porque la computadora tiene su Firewall y/o sistema operativo desatualizado. Según estudios, una computadora que está en internet en esas condiciones tiene casi un 50% de chances de convertirse en una máquina zombie, pasando a depender de quien la está controlando, casi siempre con fines criminales.

Backdoors

La palabra significa, literalmente, “puerta trasera” y se refiere a programas similares al caballo de Troya. Como el nombre sugiere, abren una puerta de comunicación escondida en el sistema. Esta puerta sirve como un canal entre la máquina afectada y el intruso, que puede, así, introducir archivos maléficos en el sistema o robar informacion privada de los usuarios.

ales clasificaciones no engloban todos los tipos de virus (malware) y se refieren sólo a los ejemplares “puros”. En la práctica, lo que se observa cada vez más es una mezcla de características, de tal forma que ya se habla de worm/trojans y otras especies de códigos maléficos híbridos. Así, es perfectamente posible que un malware se disemine por e-mail, después de ser ejecutado – como lo hace un worm –, pero ademas también robe contraseñas de la máquina infectada y las envíe a través de Internet hacia el creador del programa — exactamente como lo hace un caballo de Troya.

Virus de Macro

Los virus de macro (o macro virus) vinculan sus acciones a modelos de documentos y a otros archivos de modo que, cuando una aplicación carga el archivo y ejecuta las instrucciones contenidas en el archivo, las primeras instrucciones ejecutadas serán las del virus.

Los virus de macro son parecidos a otros virus en varios aspectos: son códigos escritos para que, bajo ciertas condiciones, este código se “reproduzca”, haciendo una copia de él mismo. Como otros virus, pueden ser desarrollados para causar daños, presentar un mensaje o hacer cualquier cosa que un programa pueda hacer.

Los virus en otros medios

Mucho se habla de prevención contra virus informáticos en computadoras personales, la famosa PC, aunque hoy existen muchos dispositivos que tienen acceso a internet, como teléfonos celulares, tablets, teléfonos VOIP, etc. Hay virus que pueden estar atacando y perjudicando la performance de estos dispositivos en cuestión. Por el momento son casos aislados, pero el temor entre los especialistas en seguridad digital es que con la propagación de una inmensa cantidad de dispositivos con acceso a internet, los hackers se interesan cada vez más por atacar a estos nuevos medios de acceso a internet.

Clasificación de los virus de computadoras

En principio, los virus informáticos suelen ser divididos en dos grandes grupos principales, que describimos a continuación:

Virus que infectan archivos

Este grupo se puede dividir en dos tipos claramente definidos. El primer tipo corresponde a los llamados Virus de Acción Directa. Estos poseen la particularidad de infectar a otros programas en el momento en que son ejecutados. El segundo tipo es el de los Virus Residentes, los cuales cuando son ejecutados toman una porción de la memoria RAM del equipo esperando a que el usuario acceda a sus programas para poder infectarlos.

Virus que infectan el sector de arranque de la computadora

Este grupo contiene a los virus informáticos que pueden alojarse en el sector de arranque de nuestro disco duro, y desde allí lanzar sus rutinas de ejecución. Recordemos que este sector de arranque es vital para el funcionamiento del equipamiento. Esta clase de virus posee la habilidad de residir en la memoria de la computadora.

Fuera de estos dos grandes grupos de virus, existe además un tercero, en el que se incluyen los llamados virus de tipo Multipartite. Esta definición agrupa a los virus que infectan archivos y al sector de arranque indistintamente.

Comportamiento de los virus informáticos

Además de poder agruparlos en las anteriores categorías, los virus informáticos también pueden ser organizados según el tipo de comportamiento que exhiban.

A continuación te ofrecemos algunas de las categorías más significativas en este ámbito. Si bien también existen otras, este es un listado de las más reconocidas a nivel mundial por los fabricantes de software antivirus:

Los virus de tipo Uniforme

son aquellos virus que pueden replicarse a sí mismos en forma idéntica.

Los virus de tipo de Sobreescritura

Este tipo de virus actúa infectando y sobreescribiendo los archivos y programas mediante el uso de su propio código.

Los virus del tipo Stealth o furtivo

Tienen la particularidad de poder ocultar al usuario los síntomas de la infección.

Los Virus de encriptación

Son aquellos virus que pueden cifrar todo o parte de su código, entorpeciendo de esta manera la labor de análisis. Estos pueden utilizar a su vez dos tipos de encriptación, por un lado la denominada encriptación fija, en la cual el virus emplea la misma clave para todos las copias realizadas de sí mismo, por otro lado, la denominada encriptación variable, en el cual el virus encripta cada copia con una clave diferente, entorpeciendo la tarea de localización debido a la reducción de la porción de código empleada para su detección.

Virus oligomórficos

Estos poseen sólo una reducida cantidad de funciones de encriptación y pueden elegir en forma aleatoria cual de ellas puede utilizar.

Los virus polimórficos

Son aquellos que para poder replicase utilizan una rutina de replicación de tipo completamente variable, es decir, cada vez que se replican y encriptan van cambiando en forma secuencial. Cabe destacar que estos virus son los más difíciles de detectar y eliminar, ya que puede producir muchas y diferentes copias de sí mismo.

Los virus metamórficos

Son aquellos que poseen la singularidad de reconstruir todo su código cada vez que se replican. Es importante señalar que esta clase de virus no suele encontrarse más allá de los límites de los laboratorios de investigación.

Como actuan los virus informaticos

Los primeros virus fueron creados a través de lenguajes como Assembler y C. Hoy, los virus pueden ser creados de manera mucho más simple, pudiendo ser desarrollados a través de scripts y de funciones de macro de determinados programas.

Para que contaminen los ordenadores, los virus antiguamente usaban disquetes o archivos infectados. Hoy, los virus pueden alcanzar en pocos minutos miles de computadoras en todo el mundo. Eso todo gracias a la Internet. El método de propagación más común es el uso de e-mails, donde el virus usa un texto que intenta convencer al usuario a clickear en el archivo adjunto. Es en ese adjunto se encuentra el virus. Los medios de convencimiento son muchos y suelen ser bastante creativos. El e-mail (y hasta el campo asunto del mensaje) suele tener textos que despiertan la curiosidad del internauta. Muchos exploran asuntos eróticos o abordan cuestiones actuales. Algunos virus pueden usar un remitente falso, haciendo que el destinatario del e-mail crea que se trata de un mensaje verdadero. Muchos internautas suelen identificar e-mails de virus, pero los creadores de estas “plagas digitales” pueden usar artificios inéditos que sorprenden hasta el usuario más experto.

Estan los virus que exploran fallos de programación de determinados programas. Algunos fallos son tan graves que pueden permitir la contaminación automática del ordenador, sin que el usuario se de cuenta.

Otros virus suelen propagarse a través de la compartición de archivos, como aquellos que insertan archivos en carpetas de programas P2P (softwares de ese tipo permiten la comparticion de archivos entre usuarios de una misma red de computadoras .

Después de haber contaminado el ordenador, el virus pasa entonces a ejecutar sus tareas, que pueden ser de los más diversos tipos, desde la simple ejecución de un programa hasta la destrucción total del sistema operativo. La mayoría de los virus tiene como primera actividad la propagación hacia otras computadoras.

Mitos sobre los virus informáticos

Es importante desmentir algunos mitos: los eventos que no ejecutan el programa que contiene el virus “pegado” no lo van a accionar. Así, si un programa contaminado que este grabado en un disco rigido o disquete , no va a ejecutar el ataque del virus. Por eso, si el evento que activa el virus no es accionado nunca por el usuario, el virus quedará “dormido” hasta el día en que el programa fuera ejecutado.

Otra cosa que debe ser desmentida es la creencia de que los virus pueden dañar el hardware del ordenador. Los virus son programas y por lo tanto no hay forma que ellos quemen o rompan dispositivos de la computadora. Lo que si, existen virus que borran la BIOS de la placa-madre, dejándola sin capacidad para ser usada, dando la impresión de que fue rota. Sin embargo, con equipamiento especial utilizado en laboratorios o con un software especial, es posible recuperar la BIOS y ahí se constatará que la placa-madre funciona con sus componentes de hardware como estaban antes del ataque. Las BIOS actuales están mejor protegidos de este peligro y son más fácilmente recuperables en casos de problemas.