Prof. José Hernández

Malware

El malware es un tipo de software que tiene como objetivo infiltrarse o dañar una computadora o sistema de información sin el consentimiento de su propietario. El término malware es muy utilizado por profesionales de la informática para referirse a una variedad de software hostil, intrusivo o molesto. El término virus informático suele aplicarse de forma incorrecta para referirse a todos los tipos de malware, incluidos los virus verdaderos.

El software se considera malware en función de los efectos que provoque en un computador. El término malware incluye virus, gusanos, troyanos, la mayor parte de los rootkits, scareware, spyware, adware intrusivo, crimeware y otros softwares maliciosos e indeseables.

Virus informático

Un virus es un malware que tiene por objetivo alterar el funcionamiento normal 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 producen molestias.

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.

El funcionamiento de un virus informático es conceptualmente simple. Se ejecuta un programa que está infectado, en la mayoría de las ocasiones, por desconocimiento del usuario. El código del virus queda residente (alojado) en la memoria RAM de la computadora, incluso cuando el programa que lo contenía haya terminado de ejecutar. El virus toma entonces el control de los servicios básicos del sistema operativo, infectando, de manera posterior, archivos ejecutables que sean llamados para su ejecución. Finalmente se añade el código del virus al programa infectado y se graba en el disco, con lo cual el proceso de replicado se completa.

Tipos de Virus:

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

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 dé 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.

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.

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 desactualizado. 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.

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.