VIRUS, ANTIVIRUS Y *MALWARE*

Malware es el acrónimo de *malicious software*, traducido como programas maliciosos y se utiliza para describir los programas tipo virus, gusano, *spyware* y casi todo el *software* que está específicamente diseñado para dañar las computadoras, *tablets* y celulares o para robar la información que los usuarios tienen almacenada en este tipo de dispositivos.

El *malware* es, entonces, un concepto mucho más abarcativo que el de virus. En un sentido estricto, un virus es un programa que se copia a sí mismo e infecta una computadora, diseminándose de un archivo a otro y luego de una computadora a otra, cuando los archivos se copian o comparten. Ingresa al equipo sin conocimiento y sin consentimiento del usuario. En cambio algunos programas *malware* son instalados con el expreso consentimiento del usuario, que ignora sus dañinas consecuencias.

La mayoría de los virus se adjuntan a sí mismo a archivos ejecutables, pero también pueden apuntar al registro de arranque de una computadora o a macros de MS Office o aún a archivos elegidos arbitrariamente. La consecuencia del ataque es, en algunos casos, hacer que los dispositivos queden completamente inoperables y en otros, corromper archivos necesarios, ya sean del sistema operativo, de algunas aplicaciones o simplemente archivos de datos del usuario.

El modo de protegerse de los virus es estar seguro de que el programa antivirus instalado en su computadora o dispositivo móvil está totalmente actualizado y habilitado específicamente para revisar los mensajes que ingresan al equipo vía *e-mail* o a través de la navegación de internet. Hay que prestar especial atención a los nombres de los archivos. Por ejemplo, si un archivo parece ser un archivo de sonido con extensión mp3, pero su nombre termina en mp3.exe, sin duda es un virus.

Los programas ***spywares*** roban la información del usuario. Podemos definirlos como todo *software* instalado en un equipo que recolecta información sin el conocimiento del usuario y la envía al creador del programa de modo de utilizarla con algún propósito perjudicial. Puede tratarse del robo de contraseñas, saber más sobre los hábitos de búsqueda de información en internet del usuario, realizar cambios en el navegador y en ciertas páginas de búsqueda, agregando barras de navegación indeseadas o hurtando información clave como los números de las tarjetas de crédito.

Como los programas *spyware* están hechos para hacer dinero a expensas del usuario, usualmente no dejan el equipo inoperable, porque no es su objetivo y, por lo tanto, el usuario puede tener muchos programas de este tipo ejecutándose en paralelo, en cuyo caso usualmente el equipo se torna más lento en su funcionamiento.

Lo que los usuarios a menudo desconocen es que no todos los antivirus remueven los programas *spyware* de la computadora. Para lograr su escaneo y eliminación, hay que asegurarse consultando específicamente al proveedor del programa que protege el equipo, para que quede liberado también de ese tipo de virus.

Hablemos de otro tipo de ataque: el ***scareware.*** En este caso, el usuario es engañado, aprovechando su desconocimiento específico sobre temas de seguridad informática, para que descargue una aplicación que simula ser un antivirus que remueve un virus ficticio instalado previamente en la computadora y que realiza tal acción solo si se paga el costo de una licencia. Si la licencia no se paga, el programa "antivirus" instalado no se puede desinstalar y en algunos casos tampoco se puede utilizar la computadora. En síntesis, el *scareware* toma a la computadora como rehén.

Si un usuario está en esta situación, conviene que de inmediato busque en Google el nombre de la aplicación en cuestión, ya que existen diversos foros que le informan cómo quitar el programa indeseado de su equipo, para volver a la normalidad. De no ser así, conviene recurrir a un técnico

de confianza para realizar los pasos necesarios para volver a la computadora al estado de operatividad plena.

Los **troyanos** son aplicaciones que aparentan ser inocuas pero secretamente tienen código malicioso que hace algo dañino. En muchos casos, estos tipos de virus crean una puerta trasera *(backdoor),* que permite que la computadora del usuario sea controlada en modo remoto, directamente o como parte de una red donde sus nodos están infectados con un troyano u otros programas maliciosos.

La mayor diferencia entre un virus y un troyano es que los troyanos no se replican, deben ser instalados por un usuario en forma involuntaria. Una vez que una computadora está atacada por un troyano, puede ser utilizada con distintos propósitos funestos.

La protección, una vez más, está dada por un antivirus completo y actualizado y por la precaución del usuario de no bajar programas cuya fuente no es absolutamente fiable o no atender a recomendaciones o solicitudes de descarga de programas bajo el pretexto de resolver problemas súbitamente creados a partir de alguna situación anómala como las ya descriptas.

¿Qué son los programas gusanos?

Los **gusanos** *(worms)* utilizan la red para enviar copias de sí mismos a otros equipos, utilizando generalmente lo que se llama un "agujero de seguridad" para viajar de un servidor a otro, automáticamente, sin intervención del usuario. Como se pueden propagar tan rápido a través de una red, infectando cada computadora a su paso, son considerados el tipo más conocido de *malware* existente. Algunos de los gusanos más famosos, como el Iloveyou, se transmiten como un adjunto de un mensaje por *mail;* otros como el SQL Slammer lograron hacer lenta a toda la internet del mundo por un breve lapso, mientras que el gusano llamado "Blaster", si ataca, reinicia la computadora una y otra vez.

Estos programas se filtran por una vulnerabilidad de la red que el usuario está utilizando. En este caso, a modo de prevención, es bueno entonces tener activo un programa ***firewall*** eficiente, que en conjunto con un antivirus actualizado, brindará la protección necesaria para un funcionamiento correcto del equipo.

Los piratas informáticos *(hackers),* en algunos casos, comenzaron realizando este tipo de *software* en universidades y luego, a modo de transgresión, migraron a su instalación en otros equipos o en redes.

Sin embargo, el concepto de *hacker* es mucho más amplio, dado que fue primero aplicada a vulnerar equipos telefónicos y a efectuar llamadas sin pagarlas. Discovery Channel realizó un documental llamado "Historia de los hackers informáticos", que muestra cuán contradictorio es el mundo de estos seres, por una parte transgresores de la propiedad ajena y por otra, creativos y pioneros, por ejemplo, en la invención de la computadora personal Apple, que transformó el mundo de la informática.