Internet

Eduardo Fainé Celis *

NADIE ESTÁ A SALVO

Aunque este tema lo he tocado anteriormente, dos experiencias de personas muy cercanas me motivaron a revisarlo y publicar una nueva versión. En las últimas semanas he visto perderse enormes cantidades de información a causa de ataques de virus, una epidemia para la que no existe la contramedida cien por ciento efectiva, dado que todos los programas antivirus existentes sólo reconocen y atacan virus ya conocidos, por lo que los creadores de estas rutinas computacionales siempre están adelantados a sus víctimas.

Ahora, ¿qué es un virus y cómo trabaja? De acuerdo a la wikipedia, es «un programa de computador que puede infectar otros programas modificándolos para incluir una copia de sí mismo».

Los virus tienen básicamente la función de propagarse, replicándose, pero algunos contienen además una carga dañina con distintos objetivos que pueden variar desde una broma hasta infligir daños importantes en los sistemas o bloquear las redes informáticas.

Esta definición, sin embargo, se hace más amplia a medida que se analiza los distintos tipos de virus existentes, ya sean gusanos, troyanos o virus a secas. A continuación se enumeran algunas variedades y su forma de trabajo, de acuerdo a la información obtenida en www.enciclopediavirus.com:

- ***Infector de Ejecutables.***

Es el virus por excelencia; una rutina o programa capaz de infectar otros archivos ejecutables, como los .EXE, .COM y .SCR bajo Windows, incluyendo dentro del código original, las funcionalidades propias del virus.

Para infectar otros archivos ejecutables, estos virus copian su contenido dentro de ellos y los modifican de manera que, cuando el archivo sea abierto por el usuario, o automáticamente si se trata de un proceso, el propio virus también se ejecute.

Los primeros virus eran de este tipo, y aún hoy en día son de los más peligrosos, dado que su presencia muchas veces no puede ser detectada si no se cuenta con un antivirus actualizado ya que se esconden dentro de programas normales ya existentes en el sistema.

- ***Infector de Archivos.***

Existen virus que aprovechan vulnerabilidades y/o funcionalidades de ciertas aplicaciones para replicarse en los archivos que éstas utilizan. Un ejemplo de esto son aquellos virus capaces de reproducirse a través de archivos PDF.

El virus copia su código dentro del archivo, de manera que cuando éste sea abierto, la aplicación que lee el archivo, también lea el código del virus y así el mismo pueda reproducirse infectando otros archivos y realizando las acciones para las que esté programado.

- ***Macrovirus.***

Clase de virus que se reproduce aprovechando la posibilidad de programación, normalmente llamada Macros, que tienen documentos de algunos programas.

* Capitán de Fragata. Oficial de Estado Mayor AV. Master en Diseño y Comunicación Multimedia. Destacado Colaborador, desde 2005.

Estos virus se alojan en documentos de Word, planillas de Excel, presentaciones de PowerPoint, archivos de CorelDraw y Visio, y pueden existir macrovirus para todos los documentos no ejecutables de aplicaciones que utilicen Macros.

- ***Gusano.***

Un gusano se parece a un virus en que su principal función es reproducirse, pero por el contrario de como lo hacen los virus, en lugar de copiarse dentro de otros archivos, un gusano crea nuevas copias de sí mismo para replicarse.

En síntesis, lo que caracteriza a un gusano es que para reproducirse genera nuevas copias de sí mismo dentro del mismo sistema infectado o en otros sistemas remotos, a través de algún medio de comunicación, como bien puede ser Internet o una red informática.

- ***Gusano de Internet.***

Un gusano de Internet es un tipo específico de gusano que aprovecha los medios que provee la red para reproducirse a través de ella. Su fin es replicarse a nuevos sistemas para infectarlos y seguir replicándose a otros equipos informáticos, aprovechando medios como el correo electrónico, IRC, FTP, y otros protocolos específicos o ampliamente utilizados en Internet.

- ***Polimórfico.***

Este tipo de virus pueden cambiar de forma. Lo que hace el virus es copiarse en memoria, volver a compilarse tras cambiar su estructura interna, tal como nombres de variables, funciones, etc., y volver a compilarse, de manera que al terminar, es distinto del original. Esto lo hace especialmente peligroso por su facilidad para eludir a los antivirus.

- ***Residente.***

Un virus residente es capaz de mantenerse en memoria desde el inicio del equipo infectado, ya sea cargándose desde el sector de arranque del mismo o como un servicio del sistema operativo, hasta que el mismo se apaga.

Un computador infectado por este tipo de virus suele ser difícil de limpiar, dado que en muchos casos requieren que se reinicie el equipo con un disco de arranque (bajo Windows 9x/Me) o con el disco de emergencia (Windows NT/2000/XP) para evitar que se carguen en memoria.

- ***Troyano.***

Es un programa que, enmascarado de alguna forma como un juego o similar, busca hacer creer al usuario que es inofensivo, para luego realizar acciones maliciosas en su equipo. Estos programas no tienen capacidad para replicarse por sí mismos, pero en muchos casos, los virus y gusanos liberan troyanos en los sistemas que infectan para que cumplan funciones específicas, como por ejemplo, capturar todo lo que el usuario ingresa por teclado.

La principal utilización de los troyanos es para obtener acceso remoto a un sistema infectado a través de una puerta trasera. Este tipo de troyano es conocido como Backdoor.

Como resumen, un virus está esperando su oportunidad para acceder al disco duro de nuestro computador. La eficacia de un antivirus está dada por lo actualizado que esté, dada la capacidad de mutar que poseen ciertos virus, y ni siquiera la última actualización nos protege del todo, como lo mencioné en el ejemplo del comienzo. Esos computadores estaban con su licencia de software al día y sus antivirus actualizados; sin embargo, sus usuarios los empleaban para bajar música de Internet y para jugar en línea. En ambos casos, los virus burlaron la detección y lograron destruir su información. Nadie está seguro, un ataque en el propio PC es cosa de tiempo y hay que estar preparados.

* * *