VIRUS Y OTROS MALES

Es frecuente utilizar el término genérico "virus" para referirse a cualquier programa que altere el normal comportamiento de una computadora sin el conocimiento o consentimiento del usuario. Existen, no obstante, una variedad de segmentos de código que se diferencian de un virus propiamente dicho en la forma en que ingresan al sistema, en el tipo de daño que generan y en la forma en que se reproducen. De acuerdo a estas características y diferencias, estos pequeños programas se dividen en virus, trojans, worms, hoaxes y jokes.

Qué es un virus?

El nombre de virus informático surge como analogía con los virus biológicos. De la misma forma en que los virus biológicos entran en el cuerpo humano infectando células del sistema, generando síntomas de esa infección, para luego reproducirse e infectar a otros sistemas; un virus informático entra en el ordenador infectando archivos del sistema, generando síntomas como dañar programas o eliminar información, para luego 'contagiar' a otros ordenadores. De estas características surgen 2 condiciones para que un programa sea un virus:

Debe ser autoejecutable
Debe poder replicarse a sí mismo, para poder reproducirse dentro de una misma computadora o infectando a otras computadoras.

Algunos virus están diseñados para dañar a la computadora destruyendo programas, borrando archivos o formateando el disco rígido. Otros virus -denominados "benignos"- no están programados para hacer daño sino que simplemente muestran su presencia a través de textos e imágenes, pero generando un comportamiento anormal y afectando la performance del sistema.

Qué es un Trojan?

Los programas denominados "Troyanos" o "Caballos Troyanos", a diferencia de los virus, no se "contagian", sino que el usuario los "invita" a entrar a su computadora creyendo que son programas deseables cuando en realidad no lo son. Su nombre evoca la ocupación de la ciudad de Troya por parte de los griegos, donde los troyanos dejaron entrar a su fuerte a un gran caballo de madera pensando que era un regalo cuando en realidad estaba ocupado por soldados griegos que terminaron destruyendo la ciudad. Cuando el Troyano está instalado en la computadora, permite que un usuario remoto tenga acceso total a la computadora de la víctima sin que ésta lo sepa. Con este acceso, el intruso puede apropiarse de información valiosa como claves bancarias, números de tarjetas de crédito, etc. o directamente utilizar a su antojo la computadora de la víctima de forma remota.
Las fuentes más comunes por donde ingresan los Troyanos son:
Al ejecutar archivos de origen desconocido
Al abrir un attachment de un e-mail de origen desconocido
Permitiendo a un "amigo" acceder a la computadora
Al ejecutar archivos recibidos de una actividad on-line -MSN Messenger, ICQ, etc.-
Un ejemplo de un Troyano es el **PWSteal.Trojan**.

Que es un Worm?

Un Worm -'Gusano' en español- es un programa similar a un virus, pero que difiere de éste en la forma de reproducirse. Mientras que los virus intentan infectar a otros programas copiándose dentro de ellos, los gusanos solamente realizan copias de ellos mismos. En el caso de un worm, no se considera que un archivo está infectado por él, sino que el archivo mismo es el worm. Un ejemplo bastante común de worm es el llamado PrettyPark.

Qué son los Hoax y Jokes ?

Un hoax -'engaño' en español- no es un virus sino falsos mensajes que se distribuyen por correo electrónico alertando sobre supuestos virus y sus terribles consecuencias con la intención de generar falsos rumores y aterrorizar a los usuarios.
Frecuentemente, los hoax pretenden engañar a los usuarios mediante el uso de palabras técnicas y citando empresas reconocidas como fuente. Ante la aparición de este tipo de mensajes lo aconsejable es no prestarles atención y no distribuirlo a otras personas.
En http://www.symantec.com/avcenter/hoax.html puede encontrarse una lista de los hoax en inglés más frecuentes.
Los jokes -'bromas' en español- tampoco son virus, sino bromas de mal gusto, generalmente inocuas, que tienen por objeto hacer pensar a los usuarios que han sido infectados simulando los efectos de un virus destructivo. Al igual que con los hoax, no hay que prestarles mayor atención.

TIPOS DE VIRUS

Existen distintos tipos de virus, de acuerdo al tipo de infección que producen y a la forma en que se reproducen y contagian entre archivos de una misma computadora y entre distintos ordenadores. Estas son las clasificaciones más importantes:

Virus de archivo

Este tipo de virus afecta archivos de programa; generalmente archivos ejecutables como -.com, .exe, etc.- Cuando un programa infectado se ejecuta, la infección se expande a otros archivos.
Muchos de estos virus residen en la memoria. Esto significa que una vez que el la memoria está infectada, cualquier archivo ejecutable se infecta al ejecutarse.
Algunos ejemplos de virus de archivo son el Jerusalem y el Cascade.

Virus de Sector de Arranque

Este tipo de virus infecta el sector de arranque -boot sector- de un disquete o disco rígido. Una vez que el sector de arranque está infectado, el virus intenta infectar cualquier sistema de almacenamiento de datos que se inserte en el sistema, ya sea un disquete, un CD-R, una unidad ZIP o cualquier otro formato de almacenamiento de datos.
Algunos ejemplos de virus de Sector de Arranque son el Disk Killer, Michelangelo, AntiExe y Unashamed.

Virus multi-parte

Los virus multi-parte pueden infectar tanto el sector de arranque como los archivos ejecutables. Son una combinación de distintos tipos de virus, lo que le da un poder de destrucción muy superior a los demás tipos de virus. Son virus particularmente difíciles de reparar, teniendo en cuenta que si se pudo remover del sector de arranque pero no de los archivos, el sector de arranque volverá a infectarse, y viceversa. Algunos ejemplos de virus multi-parte son el Emperor, Anthrax y Tequilla.

Virus Macro

Desde la incorporación de utilidades de programación de Visual Basic en los programas de Microsoft Office, pueden crearse muy fácilmente virus que infectan archivos de datos de Microsoft Word, Excel, PowerPoint y Access desde donde se propagan e infectan a otros archivos.
Los virus macro representan al rededor del 80% de todos los virus que existen en la actualidad y son los que más rápidamente han crecido en la historia de las computadoras en los últimos 5 años. Este tipo de virus no es exclusivo de ningún sistema operativo y se disemina fácilmente a través de archivos adjuntos de e-mail, disquetes, bajadas de Internet, transferencia de archivos y aplicaciones compartidas.
Al tener un fácil y poderoso acceso a programas de Microsoft Office, estos virus pueden ordenar al Microsof Outlook reenviar el mensaje con el archivo infectado anexado a todos los nombres de la libreta de direcciones. Algunos ejemplos de virus macro son el WM.NiceDay y el W97M.Melissa.

Breve historia de los virus informáticos

1939

En 1939 el famoso matemático húngaro Louis Von Neumann expuso su trabajo "Teoría y Organización de Autómatas Complejos", en el que presentaba la posibilidad de que un programa tomase el control de otros de naturaleza semejante.

1949

Basándose en el trabajo de Von Neumann, tres jóvenes programadores de la Bell Computer: Thomas Morris, Douglas McIlroy y Victor Vysottsky, crearon en 1949 un 'juego' al que llamaron CoreWar que consistía en activar programas dentro de un ordenador de forma que iban agotando poco a poco la memoria del mismo, y el ganador era el que conseguía eliminarla totalmente. Este juego terminó convirtiéndose en el precursor de los virus modernos.

1972

En 1972 aparece lo que podríamos considerar como el primer virus verdadero denomoinado Creeper, diseñado por su creador Robert Thomas Morris para atacar computadoras IBM y cuya única acción era mostrar en pantalla un mensaje desafiante. En respuesta a esto, los técnicos crearon el primer programa antivirus al que denominaron Reaper y cuya función era desinfectar las computadoras infectadas con el Creeper.

1983

En 1983, retomando las ideas de Von Neumann, Keneth Thompson demuestra la forma de desarrollar virus informáticos.

1986

Hacia 1986 aparecen los primeros virus que afectaban archivos .exe y .com.

De ahí en adelante...

Con la creciente popularidad de Arpanet -precursora de la Internet- los virus comienzan a difundirse internacionalmente. A partir de allí, con el advenimiento de la Internet, la creación de nuevos virus se multiplicó al ritmo del crecimiento de los usuarios de la Red, mientras se impulsaba paralelamente el desarrollo de la industria de los programas antivirus.

Cómo protegerse de los virus, trojans y worms?

Mientras muchos usuarios desprevenidos utilizan sus computadoras despreocupadamente sin considerar los riesgos que implican los virus; un número creciente de usuarios por temor limitan sus actividades informáticas por miedo a infectar sus ordenadores. Como en otras áreas, la actitud más recomendable parece no estar en los extremos. Estando informados de los riesgos así como de las medidas de seguridad disponibles, podemos crear un entorno seguro en el cual aprovechar las ventajas de las últimas tecnologías sin correr riesgos innecesarios.

Algunos consejos generales

Como precauciones generales, hay que tener en cuenta que la mayor fuente de infecciones de virus son los archivos adjuntos en mensajes de e-mail. Es necesario tener mucho cuidado con los archivos adjuntos; no sólo los que provengan de fuentes desconocidas, ya que muchos de estos programas dañinos pueden haber sido reenviados automáticamente por la computadora infectada de algún conocido.
Otra fuente bastante común de estos programas son las descargas en Internet desde sitios que no son confiables o conocidos. Es recomendable limitar la descarga de archivos a través de Internet a sitios reconocidos y que garanticen ciertas normas de seguridad informática.
Como regla general, es conveniente realizar copias de seguridad de la información de forma periódica y almacenarla en lugares seguros; preferentemente fuera de la computadora.

Antivirus

Existe en la industria del software poderosos programas que permiten la detección y eliminación de virus, troyanos y worms. Los virus tienen patrones de códigos que son como sus "huellas digitales". Los software antivirus buscan estos patrones, de acuerdo a los que tienen almacenados en una lista, para detectar y eliminar programas dañinos, así como reparar los daños ocasionados. De ahí la importancia de mantener los programas antivirus permanentemente actualizados con las últimas definiciones de programas nocivos disponibles.
Adicionalmente, algunos programas antivirus utilizan técnicas de "heurística" para analizar los archivos y detectar instrucciones, acciones sospechosas o indicios que delaten la presencia de códigos maliciosos o comportamientos similares a los de los virus, aún cuando se trate de un virus completamente nuevo.
En la actualidad disponer en nuestra computadora de un buen programa antivirus, completo y constantemente actualizado es una necesidad básica si queremos estar tranquilos navegando por Internet, descargando archivos, usando correo electrónico e intercambiando programas y archivos.

Estos son **algunos** de los programas más importantes para proteger la computadora de virus, troyanos y worms:

AVG Antivirus	http://www.grisoft.com/
Dr Solomon's	http://www.drsolomon.com/
eSafe	http://www.esafe.com/
Command Antivirus	http://www.commandcom.com/
Symantec	http://www.symantec.com/
McAfee	http://www.mcafee.com/
Panda Software	http://www.pandasoftware.es/
Trend Micro	http://www.antivirus.com/