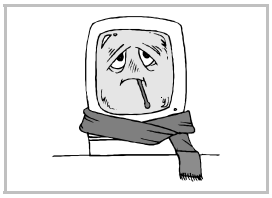

Los virus informáticos

Qué son los virus informáticos

Una fuente de problemas y preocupaciones es la existencia de virus informáticos. Son programas de ordenador, normalmente pequeños, que tienen la capacidad de **autorreproducirse**: se incrustan en disquetes, ciertas zonas de los discos duros, mensajes de correo electrónico, etc. y a partir de ahí intentan contagiar otros ordenadores. Mientras ocurre toda esta actividad, intentan pasar desapercibidos a los ojos de los usuarios, para poder reproducirse cuanto puedan.

Daños de los virus

Cuando llega un momento determinado, que depende de cada virus, se desencadena alguna acción característica, llamada el ***payload*** del virus. Pueden borrar archivos, modificarlos o dañarlos; los virus más dañinos pueden llegar a borrar las particiones de Microsoft Windows; algunos virus se limitan a molestar, sin destruir nada.

Infección

Un ordenador puede quedar contaminado por un virus al leer un disquete que lo contenga, al ejecutar un programa e incluso al abrir algunos mensajes de correo electrónico con algunos programas poco seguros. Cuando el virus se instala en el disco duro, contamina los disquetes que se van introduciendo en el ordenador, o intenta reproducirse por la red a otros ordenadores o manda mensajes de correo electrónico a los conocidos que estén en la libreta de direcciones del usuario.

Extensión

Para Windows existen miles de virus, muchos menos para Macintosh y apenas hay alguno muy controlado en GNU/Linux. Los virus producen daños económicos muy importantes en el primer mundo y pueden destruir el trabajo de mucho tiempo.

Curación

Existen muchos tipos de virus con muchas formas de actuación, lo que hace su estudio una materia muy compleja. Según el daño que produzca, será más fácil o más difícil recomponer el ordenador atacado. En los casos sencillos, un antivirus puede eliminarlo sin más problemas; en casos difíciles, será necesario instalar el sistema operativo de nuevo.

Métodos de protección

Para protegerse contra los virus se aconsejan varias acciones:

1. **Hacer copias de seguridad**. Si nuestros datos y programas están seguros, un virus no conseguirá que los perdamos.
2. **Utilizar sistemas operativos seguros**. GNU/Linux es, por su diseño, prácticamente inmune a los virus, y Windows es especialmente sensible. La gran diferencia de entre el número de virus para uno y otro sistema no se debe sólo a que Windows está instalado en muchos más ordenadores, y por tanto es más atractivo para los creadores de virus, sino principalmente a que la seguridad es un concepto inherente al diseño de GNU/Linux, y es algo secundario en Windows y poco desarrollado por Microsoft.
3. **No usar programas ilegalmente**. Corrieron rumores de que en los programas ilegales alguna vez se introdujeron virus, adrede. Probablemente esto no se pueda demostrar, o quizá sea falso, pero lo que es evidente es que si se usa software ilegal es imposible reclamar al fabricante.
4. **Instalar un antivirus**. Podemos tener cargado permanentemente un antivirus que proteja las partes esenciales del disco duro contra su modificación no autorizada. Así, aunque llegue a entrar un virus, no podrá llegar a actuar.

5. **Comprobar *todos* los disquetes y CD-ROM**. Cada vez que vayamos a utilizar un disquete o CD-ROM que obtengamos desde *cualquier* fuente, hay que pasarle un programa antivirus para comprobar que está limpio.

6. **Instalar un cortafuegos**, para proteger las comunicaciones por Internet. Los programas cortafuegos monitorizan constantemente la conexión a Internet, detectan los accesos no autorizados que producen muchos virus y avisan al usuario. Si se usa Windows, es muy recomendable instalar *ZoneAlarm*, que es gratuito para uso personal y algunas organizaciones.
   - http://zonelabs.com
7. **Comprobar los ficheros obtenidos en Internet**. Tanto si se reciben ficheros junto con el correo electrónico como si se cargan desde una sede Web, por FTP o por IRC, hay que hacer con ellos las mismas comprobaciones que con los disquetes.
8. **Desactivar la ejecución automática de adjuntos de correo**. Muchos virus se reproducen de esta manera.
9. **Usar antivirus actualizados**. Es vital que los antivirus sean lo más recientes posible, ya que aparecen nuevos virus constantemente. Los buenos programas antivirus lanzan **actualizaciones** (en inglés, *updates*) cada mes. Normalmente cuando se compra un programa antivirus se tiene acceso gratuito a un año de actualizaciones y por una pequeña cuota se puede alargar este periodo. También existen antivirus gratuitos, entre los que citamos:
   - *AntiVir*: http://www.free-av.com/