

## **INTRODUCCIÓN**

Uno de los temas más polémicos en el entorno microinformático actual es el de los virus.

Es un tema interesante y que merece la pena conocer, ya no sólo por su dimensión didáctica, sino por su vertiente práctica. La prevención y las acciones a tomar ante la detección de un virus microinformático son elementos fundamentales para preservar la integridad del equipo.

## **VIRUS**

Los virus reciben su nombre de sus homónimos biológicos dado que existen una serie de coincidencias con los mismos.

En primer lugar habría que determinar que un virus es un programa. Los virus informáticos guardan una serie de coincidencias con los virus biológicos:

### ***REPRODUCCIÓN***

Una de las características de los virus biológicos es su capacidad de reproducirse aumentando así su número. En el caso de sus homónimos virtuales, la reproducción también se hace, pero mediante un proceso autocopiativo.

### ***FINALIDAD***

El virus informático suele tener como objeto principal, la destrucción de los datos almacenados en la computadora.

### ***VÍAS DE CONTAGIO***

Un ordenador sólo puede contagiarse de un virus por los mismos medios que cualquier programa pudiera acceder. Así, los CD-ROM, pendrives, accesos externos (redes, mail, webs...) son posibles vías de contagio.

## **EL COSTE DE LOS VIRUS**

No está bien visto que una empresa reconozca que haya sufrido un contagio por virus informático, ya que esto implica asumir una vulnerabilidad en su sistema microinformático. Se estima que en el año 1999 los virus produjeron unos daños valorados en 12.100 millones de dólares. Se trata de un problema que mueve mucho dinero en todo el mundo.

En el año 1999 se vendieron 1.200 millones de dólares en antivirus. Uno de los elementos artífices en este espectacular aumento de ventas, es, sin duda alguna, Internet, que se ha convertido en una vía perfecta para la transmisión de los virus.

En el caso de España, el Ministerio de Industria, Turismo y Comercio, de forma anual y durante un periodo limitado de tiempo, organizó acuerdos con empresas del sector antivirus para ofrecer gratuitamente a los usuarios la posibilidad de examinar su PC a través de Internet.

## EL ÁMBITO DE ACTUACIÓN DE UN VIRUS

Tradicionalmente, los virus han tenido una finalidad destructiva en el entorno del software. De este modo, se corría el riesgo de perder la información.

Dentro de estos daños en el software, la categorización es sencilla: algunos virus actúan sobre los datos y otros sobre el sistema operativo. Los que afectan a datos buscan aplicaciones tipo, ficheros ejecutables y de datos y el daño lo pueden realizar mediante la eliminación o alteración de la información.

En aquellos donde el daño se produce en el sistema operativo, es el sistema entero el que se desestabiliza.

Hasta aquí, el problema de los virus estaba en cierta medida controlado: una copia de seguridad y antivirus actualizado era el mejor de los remedios. En el peor de los casos, los daños obligaban a reinstalar el sistema operativo, aplicaciones y datos sin que hubiese ningún otro daño.

El problema se incrementa con la aparición de una nueva generación de virus en cuanto a su ámbito de actuación. Esta generación se inaugura con *Melissa*. Este virus aprovecha la vulnerabilidad que ofrecen las Flash BIOS para su programación y las borra. Ante la infección de la virus actuamos:

### **SUSTITUCIÓN DE LA BIOS**

Lo ideal sería adquirir una BIOS igual a la destruida por el virus y sustituirla en el PC dañado.

### **RÉPLICA DE LA BIOS**

Otra opción es la copia de la BIOS.

### **ACTUALIZACIÓN**

Consiste en, a partir de la disponibilidad de una BIOS idéntica a la dañada, arrancar el PC. Con él en marcha, extraer la BIOS correcta e introducir la BIOS dañada en el zócalo. Esta operación es delicada y peligrosa.

## EL ORIGEN DE LOS VIRUS

Una de las teorías sobre la aparición de los virus apunta por el desarrollo de un juego llamado CoreWar en la década de los sesenta. El objeto de este juego era que otras aplicaciones ejecutases ciertos comandos con la finalidad de saturar la memoria. Otro de los posibles orígenes se sitúa en Israel, donde en 1986, se distribuye a partir de una tienda especializada en la venta de software ilegal, el virus *Brian*.

Por último se asegura que el origen se debe a un estudiante de Informática llamado Fred Cohen, quien desarrolló su primer virus en 1983.

En España los virus hicieron su aparición en 1988 con el legendario virus de la pelota. Después apareció el famoso *Brian* y el popular *Viernes 13*.

### **ESTUDIANTES**

Durante la etapa de aprendizaje en la Universidad, son muchas las personas que destacan en programación debido a una experiencia previa. Una demostración de conocimiento y dominio de un entorno de programación se puede manifestar con la realización de un virus.

## **EMPRESAS DE SOFTWARE**

Algunos atribuyen una posibilidad razonada a las empresas de diseño de software genérico y otros a los desarrolladores de virus.

## **TRABAJADORES DESPEDIDOS**

Ésta es una de las teorías de las que se hablaba en etapas de declive económico. Tan popular se hizo que incluso dio pie a la definición de un tipo de virus exclusivo que recibe el nombre de *bomba lógica*.

Como dato curioso, sería interesante reseñar que existen aplicaciones encaminadas a generar virus bajo un entorno casi ofimático.

## **SOLUCIONES**

Conscientes del problema que los virus representan, han sido muchas las compañías que se han dedicado a investigar en este sector dando soluciones de todo tipo.

Dentro de las utilidades hardware mencionadas, las más comunes son las protecciones que se efectúan desde la BIOS del PC. Así, el usuario puede activar o no la opción de antivirus desde el SETUP de su PC.

Dentro de las protecciones hardware existen tarjetas que activan un antivirus que tienen implementado. Esto lo consiguen ocupando direcciones que la BIOS explora en el momento de arranque.

En cuanto a los antivirus software, los más convencionales son herramientas que suelen instalarse en el sistema de forma residente de manera que siempre están inspeccionando la actividad de la máquina.

## **TIPOS DE VIRUS**

Algunos de los tipos de virus son:

### **GUSANOS**

Se trata de uno de los virus más primitivos y fáciles de localizar. Su labor consiste en mermar las prestaciones del sistema, saturándolo, de modo que sea imposible continuar trabajando. Algunos ejemplos son: *Navidad*, *I love you* o *Pretty Park*.

### **CABALLO DE TROYA**

Los caballos de Troya o troyanos, reciben su nombre por el método de introducción. Aparentando ser una unidad, juego o aplicación, el programa consigue engañar al usuario de modo que es éste quien, de forma voluntaria, introduce el troyano en su PC. Este tipo de virus es de los más antiguos y muchos fueron programados en el arcaico y querido BASIC.

Algunos de los troyanos más conocidos son: *KillCMOS*, *MTX* y *DonaldDick*.

### **BOMBA LÓGICAS**

Este tipo de virus recibe el nombre por su modo de activación. Se trata de un virus cuya ejecución es diferida en el tiempo de modo que no sea posible

identificar el origen o autor del virus. Soy muy típicos en coincidencias de fecha que tradicionalmente han sido relacionadas con la mala suerte, como el *Viernes 13* o *Martes 13*.

## **SPYWARES**

Se trata de una tipología de virus similar a los Troyanos. Este tipo de aplicaciones tiene como misión la de enviar información a un lugar concreto sobre temas tan diversos como el sistema operativo usado, páginas visitadas... Estos datos son usados por empresas con fines de marketing.

## **MODO DE ACTUACIÓN**

A la hora de actuar ante un virus, hay dos herramientas básicas: disponer de un buen antivirus actualizado y un sistema de arranque. Si además se dispone de una copia de seguridad limpia, el éxito está asegurado.

El antivirus debe ser capaz de detectar y eliminar el virus del sistema, pero la memoria del sistema debe de estar limpia