

Tipos de Virus

Los virus se pueden clasificar de la siguiente forma:

Virus residentes

La característica principal de estos virus es que se ocultan en la memoria RAM de forma permanente o residente. De este modo, pueden controlar e interceptar todas las operaciones llevadas a cabo por el sistema operativo, infectando todos aquellos ficheros y/o programas que sean ejecutados, abiertos, cerrados, renombrados, copiados. Algunos ejemplos de este tipo de virus son: Randex, CMJ, Meve, MrKlunky.

Virus de acción directa

Al contrario que los residentes, estos virus no permanecen en memoria. Por tanto, su objetivo prioritario es reproducirse y actuar en el mismo momento de ser ejecutados. Al cumplirse una determinada condición, se activan y buscan los ficheros ubicados dentro de su mismo directorio para contagiarlos.

Virus de sobreescritura

Estos virus se caracterizan por destruir la información contenida en los ficheros que infectan. Cuando infectan un fichero, escriben dentro de su contenido, haciendo que queden total o parcialmente inservibles.

Virus de boot(bot_kill) o de arranque

Los términos boot o sector de arranque hacen referencia a una sección muy importante de un disco o unidad de almacenamiento CD,DVD, memorias USB etc. En ella se guarda la información esencial sobre las características del disco y se encuentra un programa que permite arrancar el ordenador. Este tipo de virus no infecta ficheros, sino los discos que los contienen. Actúan infectando en primer lugar el sector de arranque de los dispositivos de almacenamiento. Cuando un ordenador se pone en marcha con un dispositivo de almacenamiento, el virus de boot infectará a su vez el disco duro.

Los virus de boot no pueden afectar al ordenador mientras no se intente poner en marcha a éste último con un disco infectado. Por tanto, el mejor modo de defenderse contra ellos es proteger los dispositivos de almacenamiento contra escritura y no arrancar nunca el ordenador con uno de estos dispositivos desconocido en el ordenador.

Algunos ejemplos de este tipo de virus son: Polyboot.B, AntiEXE.

Virus de enlace o directorio

Los ficheros se ubican en determinadas direcciones (compuestas básicamente por unidad de disco y directorio), que el sistema operativo conoce para poder localizarlos y trabajar con ellos.

Virus cifrados

Más que un tipo de virus, se trata de una técnica utilizada por algunos de ellos, que a su vez pueden pertenecer a otras clasificaciones. Estos virus se cifran a sí mismos para no ser detectados por los programas antivirus. Para realizar sus actividades, el virus se descifra a sí mismo y, cuando ha finalizado, se vuelve a cifrar.

Virus polimórficos

Son virus que en cada infección que realizan se cifran de una forma distinta (utilizando diferentes algoritmos y claves de cifrado). De esta forma, generan una elevada cantidad de copias de sí mismos e impiden que los antivirus los localicen a través de la búsqueda de cadenas o firmas, por lo que suelen ser los virus más costosos de detectar.

Virus multipartites

Virus muy avanzados, que pueden realizar múltiples infecciones, combinando diferentes técnicas para ello. Su objetivo es cualquier elemento que pueda ser infectado: archivos, programas, macros, discos, etc.

Virus del Fichero

Infectan programas o ficheros ejecutables (ficheros con extensiones EXE y COM). Al ejecutarse el programa infectado, el virus se activa, produciendo diferentes efectos.

Virus de FAT

La Tabla de Asignación de Ficheros o FAT es la sección de un disco utilizada para enlazar la información contenida en éste. Se trata de un elemento fundamental en el sistema. Los virus que atacan a este elemento son especialmente peligrosos, ya que impedirán el acceso a ciertas partes del disco, donde se almacenan los ficheros críticos para el normal funcionamiento del ordenador

El *spyware* o **programa espía** es un software que recopila información de un ordenador y después transmite esta información a una entidad externa sin el conocimiento o el consentimiento del propietario del ordenador. El término *spyware* también se utiliza más ampliamente para referirse a otros productos que no son estrictamente spyware. Estos productos, realizan diferentes funciones, como mostrar anuncios no solicitados (*pop-up*), recopilar información privada, redirigir solicitudes de páginas e instalar marcadores de teléfono.

Un *spyware* típico se autoinstala en el sistema afectado de forma que se ejecuta cada vez que se pone en marcha el ordenador (utilizando CPU y memoria RAM, reduciendo la estabilidad del ordenador), y funciona todo el tiempo, controlando el uso que se hace de Internet y mostrando anuncios relacionados.

Sin embargo, a diferencia de los virus, no se intenta replicar en otros ordenadores, por lo que funciona como un parásito.

Las consecuencias de una infección de spyware moderada o severa (aparte de las cuestiones de privacidad) generalmente incluyen una pérdida considerable del rendimiento del sistema (hasta un 50 % en casos extremos), y problemas de estabilidad graves (el ordenador se queda "colgado"). También causan dificultad a la hora de conectar a Internet. Algunos ejemplos de programas espía conocidos son [Gator](#) o [Bonzi Buddy](#).