

# Virus informático

De Wikipedia, la enciclopedia libre

Un **virus informático** es un malware que tiene por objetivo alterar el normal funcionamiento del ordenador, sin el permiso o el conocimiento del usuario. Los virus, habitualmente, reemplazan archivos ejecutables por otros infectados con el código de este. Los virus pueden destruir, de manera intencionada, los datos almacenados en una computadora, aunque también existen otros más inofensivos, que solo se caracterizan por ser molestos.

Los virus informáticos tienen, básicamente, la función de propagarse a través de un software, son muy nocivos y algunos contienen además una carga dañina (payload) con distintos objetivos, desde una simple broma hasta realizar daños importantes en los sistemas, o bloquear las redes informáticas generando tráfico inútil.

El funcionamiento de un virus informático es conceptualmente simple. Se ejecuta un programa que está infectado, en la mayoría de las ocasiones, por desconocimiento del usuario. El código del virus queda residente (alojado) en la memoria RAM de la computadora, incluso cuando el programa que lo contenía haya terminado de ejecutarse. El virus toma entonces el control de los servicios básicos del sistema operativo, infectando, de manera posterior, archivos ejecutables que sean llamados para su ejecución. Finalmente se añade el código del virus al programa infectado y se graba en el disco, con lo cual el proceso de replicado se completa.

El primer virus atacó a una máquina IBM Serie 360 (y reconocido como tal). Fue llamado Creeper, creado en 1972. Este programa emitía periódicamente en la pantalla el mensaje: «I'm a creeper... catch me if you can!» («¡Soy una enredadera... agárrame si puedes!»). Para eliminar este problema se creó el primer programa antivirus denominado *Reaper* (cortadora).

Sin embargo, el término virus no se adoptaría hasta 1984, pero éstos ya existían desde antes. Sus inicios fueron en los laboratorios de Bell Computers. Cuatro programadores (H. Douglas Mellory, Robert Morris, Victor Vysotsky y Ken Thompson) desarrollaron un juego llamado *Core War*, el cual consistía en ocupar toda la memoria RAM del equipo contrario en el menor tiempo posible.

Después de 1984, los virus han tenido una gran expansión, desde los que atacan los sectores de arranque de disquetes hasta los que se adjuntan en un correo electrónico.

## Índice

- 1 Virus informáticos y sistemas operativos
  - 1.1 MS-Windows
  - 1.2 Unix y derivados
- 2 Características
- 3 Métodos de propagación
- 4 Métodos de protección
  - 4.1 Activos
  - 4.2 Pasivos
- 5 Tipos de virus

- 6 Acciones de los virus
- 7 Véase también
- 8 Enlaces externos

## Virus informáticos y sistemas operativos

Los virus informáticos afectan en mayor o menor medida a casi todos los sistemas más conocidos y usados en la actualidad.

Cabe aclarar que un virus informático mayoritariamente atacará sólo el sistema operativo para el que fue desarrollado, aunque ha habido algunos casos de virus multiplataforma.

### MS-Windows

Las mayores incidencias se dan en el sistema operativo Windows debido, entre otras causas, a:

- Su gran popularidad, como sistema operativo, entre los computadores personales, PC. Se estima que, en 2007, un 90 % de ellos usaba Windows.<sup>[*cita requerida*]</sup> Esta popularidad basada en la facilidad de uso sin conocimiento previo alguno, motiva a los creadores de software malicioso a desarrollar nuevos virus; y así, al atacar sus puntos débiles, aumentar el impacto que generan.
- Falta de seguridad en esta plataforma (situación a la que Microsoft está dando en los últimos años mayor prioridad e importancia que en el pasado). Al ser un sistema tradicionalmente muy permisivo con la instalación de programas ajenos a éste, sin requerir ninguna autenticación por parte del usuario o pedirle algún permiso especial para ello en los sistemas más antiguos. A partir de la inclusión del Control de Cuentas de Usuario en Windows Vista y en adelante (y siempre y cuando no se desactive) se ha solucionado este problema, ya que se puede usar la configuración clásica de Linux de tener un usuario administrador protegido, pero a diario usar un Usuario estándar sin permisos.
- Software como Internet Explorer y Outlook Express, desarrollados por Microsoft e incluidos de forma predeterminada en las últimas versiones de Windows, son conocidos por ser vulnerables a los virus ya que éstos aprovechan la ventaja de que dichos programas están fuertemente integrados en el sistema operativo dando acceso completo, y prácticamente sin restricciones, a los archivos del sistema. Un ejemplo famoso de este tipo es el virus ILOVEYOU, creado en el año 2000 y propagado a través de Outlook.
- La escasa formación de un número importante de usuarios de este sistema, lo que provoca que no se tomen medidas preventivas por parte de estos, ya que este sistema está dirigido de manera mayoritaria a los usuarios no expertos en informática. Esta situación es aprovechada constantemente por los programadores de virus.

### Unix y derivados

En otros sistemas operativos como las distribuciones GNU/Linux, BSD, OpenSolaris, Solaris, Mac OS X y otros basados en Unix las incidencias y ataques son prácticamente inexistentes. Esto se debe principalmente a:

- Los usuarios de este tipo de Sistemas Operativos suelen poseer conocimientos mucho mayores a los de los usuarios comunes de sistemas Windows por lo que están más alerta y saben mejor qué evitar y qué es seguro.
- Estos Sistemas Operativos cuentan con una cuota de uso mucho menor, por lo que son menos

interesantes a la hora de llevar a cabo ataques de phishing o similares cuyo principal objetivo es el de robar información, por ejemplo para Data mining.

- Tradicionalmente los programadores y usuarios de sistemas basados en Unix han considerado la seguridad como una prioridad por lo que hay mayores medidas frente a virus, tales como la necesidad de autenticación por parte del usuario como administrador o *root* para poder instalar cualquier programa adicional al sistema.
- Los directorios o carpetas que contienen los archivos vitales del sistema operativo cuentan con permisos especiales de acceso, por lo que no cualquier usuario o programa puede acceder fácilmente a ellos para modificarlos o borrarlos. Existe una jerarquía de permisos y accesos para los usuarios.
- Relacionado al punto anterior, a diferencia de los usuarios de Windows, la mayoría de los usuarios de sistemas basados en Unix no pueden normalmente iniciar sesiones como usuarios "administradores" o por el superusuario *root*, excepto para instalar o configurar software, dando como resultado que, incluso si un usuario no administrador ejecuta un virus o algún software malicioso, éste no dañaría completamente el sistema operativo ya que Unix limita el entorno de ejecución a un espacio o directorio reservado llamado comúnmente *home*. Aunque a partir de Windows Vista, se pueden configurar las cuentas de usuario de forma similar.
- Estos sistemas, a diferencia de Windows, son usados para tareas más complejas como servidores que por lo general están fuertemente protegidos, razón que los hace menos atractivos para un desarrollo de virus o software malicioso.
- En el caso particular de las distribuciones basadas en GNU/Linux y gracias al modelo colaborativo, las licencias libres y debido a que son más populares que otros sistemas Unix, la comunidad aporta constantemente y en un lapso de tiempo muy corto actualizaciones que resuelven bugs y/o agujeros de seguridad que pudieran ser aprovechados por algún malware.

## Características

Dado que una característica de los virus es el consumo de recursos, los virus ocasionan problemas tales como: pérdida de productividad, cortes en los sistemas de información o daños a nivel de datos.

Una de las características es la posibilidad que tienen de diseminarse por medio de *replicas* y *copias*. Las redes en la actualidad ayudan a dicha propagación cuando éstas no tienen la seguridad adecuada.

Otros daños que los virus producen a los sistemas informáticos son la pérdida de información, horas de parada productiva, tiempo de reinstalación, etc.

Hay que tener en cuenta que cada virus plantea una situación diferente.

## Métodos de propagación

Existen dos grandes clases de contagio. En la primera, el usuario, en un momento dado, ejecuta o acepta de forma inadvertida la instalación del virus. En la segunda, el programa malicioso actúa replicándose a través de las redes. En este caso se habla de gusanos.

En cualquiera de los dos casos, el sistema operativo infectado comienza a sufrir una serie de comportamientos anómalos o imprevistos. Dichos comportamientos pueden dar una pista del problema y permitir la recuperación del mismo.

Dentro de las contaminaciones más frecuentes por interacción del usuario están las siguientes:

- Mensajes que ejecutan automáticamente programas (como el programa de correo que abre directamente un archivo adjunto).
- Ingeniería social, mensajes como *ejecute este programa y gane un premio*, o, más comúnmente: *Haz 2 clics y gana 2 tonos para móvil gratis..*
- Entrada de información en discos de otros usuarios infectados.
- Instalación de software modificado o de dudosa procedencia.

En el sistema Windows puede darse el caso de que la computadora pueda infectarse sin ningún tipo de intervención del usuario (versiones Windows 2000, XP y Server 2003) por virus como Blaster, Sasser y sus variantes por el simple hecho de estar la máquina conectada a una red o a Internet. Este tipo de virus aprovechan una vulnerabilidad de desbordamiento de buffer y puertos de red para infiltrarse y contagiar el equipo, causar inestabilidad en el sistema, mostrar mensajes de error, reenviarse a otras máquinas mediante la red local o Internet y hasta reiniciar el sistema, entre otros daños. En las últimas versiones de Windows 2000, XP y Server 2003 se ha corregido este problema en su mayoría.

## Métodos de protección

Los métodos para disminuir o reducir los riesgos asociados a los virus pueden ser los denominados activos o pasivos.

### Activos

- Antivirus: son programas que tratan de descubrir las trazas que ha dejado un software malicioso, para detectarlo y eliminarlo, y en algunos casos contener o parar la contaminación. Tratan de tener controlado el sistema mientras funciona parando las vías conocidas de infección y notificando al usuario de posibles incidencias de seguridad. Por ejemplo, al verse que se crea un archivo llamado *Win32.EXE.vbs* en la carpeta *C:\Windows\%System32%* en segundo plano, ve que es comportamiento sospechoso, salta y avisa al usuario.
- Filtros de ficheros: consiste en generar filtros de ficheros dañinos si el computador está conectado a una red. Estos filtros pueden usarse, por ejemplo, en el sistema de correos o usando técnicas de firewall. En general, este sistema proporciona una seguridad donde no se requiere la intervención del usuario, puede ser muy eficaz, y permitir emplear únicamente recursos de forma más selectiva.

### Pasivos

- Evitar introducir a tu equipo medios de almacenamiento extraíbles que consideres que pudieran estar infectados con algún virus.
- No instalar software "pirata", pues puede tener dudosa procedencia.
- No abrir mensajes provenientes de una dirección electrónica desconocida.
- No aceptar e-mails de desconocidos.
- Informarse y utilizar sistemas operativos más seguros.
- No abrir documentos sin asegurarnos del tipo de archivo. Puede ser un ejecutable o incorporar macros en su interior.

## Tipos de virus

Existen diversos tipos de virus, varían según su función o la manera en que este se ejecuta en nuestra computadora alterando la actividad de la misma, entre los más comunes están:

- **Troyano:** Consiste en robar información o alterar el sistema del hardware o en un caso extremo permite que un usuario externo pueda controlar el equipo.
- **Gusano:** Tiene la propiedad de duplicarse a sí mismo. Los gusanos utilizan las partes automáticas de un sistema operativo que generalmente son invisibles al usuario.
- **Bombas lógicas o de tiempo:** Son programas que se activan al producirse un acontecimiento determinado. La condición suele ser una fecha (Bombas de Tiempo), una combinación de teclas, o ciertas condiciones técnicas (Bombas Lógicas). Si no se produce la condición permanece oculto al usuario.
- **Hoax:** Los *hoax* no son virus ni tienen capacidad de reproducirse por si solos. Son mensajes de contenido falso que incitan al usuario a hacer copias y enviarla a sus contactos. Suelen apelar a los sentimientos morales ("Ayuda a un niño enfermo de cáncer") o al espíritu de solidaridad ("Aviso de un nuevo virus peligrosísimo") y, en cualquier caso, tratan de aprovecharse de la falta de experiencia de los internautas novatos.
- **Joke:** Al igual que los *hoax*, no son virus, pero son molestos, un ejemplo: una página pornográfica que se mueve de un lado a otro, y si se le llega a dar a cerrar es posible que salga una ventana que diga: OMFG!! No se puede cerrar!.

Otros tipos por distintas características son los que se relacionan a continuación:

### **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.

Los virus de enlace o directorio alteran las direcciones que indican donde se almacenan los ficheros. De este modo, al intentar ejecutar un programa (fichero con extensión EXE o COM) infectado por un virus de enlace, lo que se hace en realidad es ejecutar el virus, ya que éste habrá modificado la dirección donde se encontraba originalmente el programa, colocándose en su lugar.

Una vez producida la infección, resulta imposible localizar y trabajar con los ficheros originales.

### **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 (del inglés *File Allocation Table*) 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.

# Acciones de los virus


Algunas de las acciones de algunos virus son:

- Unirse a un programa instalado en el computador permitiendo su propagación.
- Mostrar en la pantalla mensajes o imágenes humorísticas, generalmente molestas.
- Ralentizar o bloquear el computador.
- Destruir la información almacenada en el disco, en algunos casos vital para el sistema, que impedirá el funcionamiento del equipo.
- Reducir el espacio en el disco.
- Molestar al usuario cerrando ventanas, moviendo el ratón...

## Véase también

- |                                     |                           |
|-------------------------------------|---------------------------|
| ▪ Antivirus                         | ▪ Ingeniería social       |
| ▪ Ataques de denegación de servicio | ▪ (seguridad informática) |
| ▪ Ciencias de la computación        | ▪ Keylogger               |
| ▪ Cortafuegos (informática)         | ▪ Malware                 |
| ▪ Cracking (software)               | ▪ Melissa (informática)   |
| ▪ Criptografía                      | ▪ Packet sniffer          |
| ▪ Desbordamiento de búfer           | ▪ Phishing                |
| ▪ Escáner de puertos                | ▪ Puerta trasera          |
| ▪ Exploit                           | ▪ Rootkit                 |
| ▪ Hacker (informática)              | ▪ Seguridad informática   |
|                                     | ▪ Spam                    |
|                                     | ▪ Troyano (informática)   |
|                                     | ▪ War dialing             |
|                                     | ▪ A and A                 |

## Enlaces externos

-  Wikimedia Commons alberga contenido multimedia sobre **Virus informático**.
- Centro de Respuesta a Incidentes de Seguridad (INTECO-CERT) del Gobierno de España - Virus y el software malicioso ([http://cert.inteco.es/homeVirusAct/Actualidad/Actualidad\\_Virus/?postAction=getHomeValuesVirusAct](http://cert.inteco.es/homeVirusAct/Actualidad/Actualidad_Virus/?postAction=getHomeValuesVirusAct))
- Antivirus (<http://www.dmoz.org/World/Espa%C3%B1ol/Computadoras/Seguridad/Antivirus/>) en Open Directory Project
- Linux y virus, no sólo cuestión de popularidad (<http://www.kriptopolis.org/linux-virus-popularidad>) en Kriptópolis.
- Enciclopedia de virus informáticos (<http://www.encyclopediavirus.com/home/index.php>)

Obtenido de «[http://es.wikipedia.org/w/index.php?title=Virus\\_informático&oldid=82735879](http://es.wikipedia.org/w/index.php?title=Virus_informático&oldid=82735879)»

Categorías: Seguridad informática | Virus informáticos

- Esta página fue modificada por última vez el 26 may 2015 a las 13:08.
- El texto está disponible bajo la Licencia Creative Commons Atribución Compartir Igual 3.0; podrían ser aplicables cláusulas adicionales. Léanse los términos de uso para más información. Wikipedia® es una marca registrada de la Fundación Wikimedia, Inc., una organización sin ánimo de lucro.