



# Virus y Antivirus

---

# Virus

## ¿Qué son?

---

Un virus informático es un programa o software que se auto ejecuta y se propaga insertando copias de sí mismo en otro programa o documento.

Troyano

Gusano

De Sobre-Escritura

De Enlace

Múltiple

- Residentes
- Mutantes
- Virus Falsos
- De Macros
- De Compañía

Antivirus

Precauciones



# Virus Troyano

## ¿Cómo funciona?

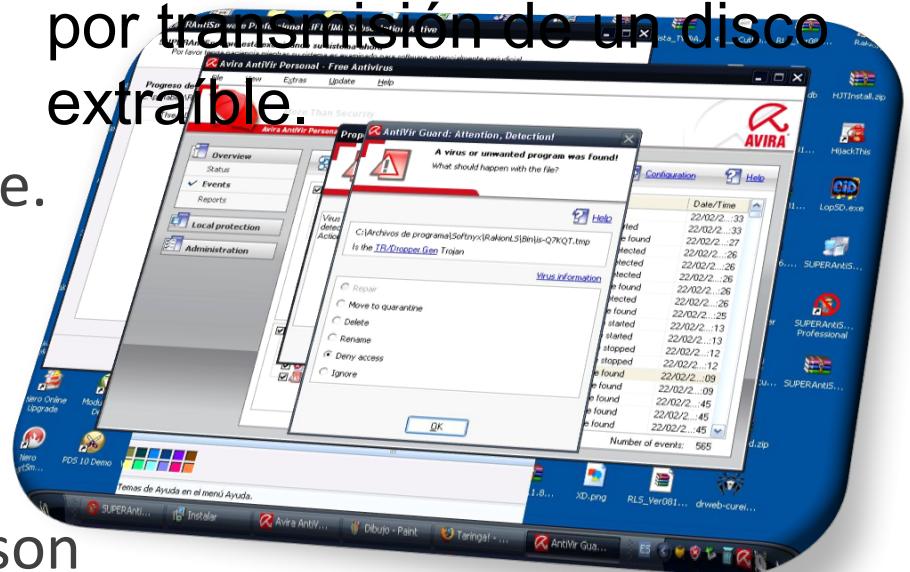
Se ejecuta cuando se abre un programa infectado por este virus. No es capaz de infectar otros archivos o soportes, y sólo se ejecuta una vez, pero es suficiente. El efecto más usual es el robo de información.

## Nombres

NetBus, Back Orifice, Sub7. Éstos son los mas importantes.

## ¿Cómo actúan?

Esperan que se introduzca una contraseña, clickear un link, o por transmisión de un disco extraible.



# Gusano

## ¿Cómo funciona?

Se propaga de computador a computador, con la capacidad de enviarse sin la ayuda de una persona. Se aprovecha de un archivo o programa para viajar. Las tareas ordinarias se vuelven excesivamente lentas o no se pueden ejecutar.

## ¿Como Actúan?

Utilizan partes que son invisibles al usuario. Se detecta la presencia cuando los recursos se consumen, parcial o totalmente.

## Nombres

Ej: Blaster, Sobig Worm, Red Code, Klezz, etc..



# Virus de Sobre-Escritura

## ¿Cómo funcionan?

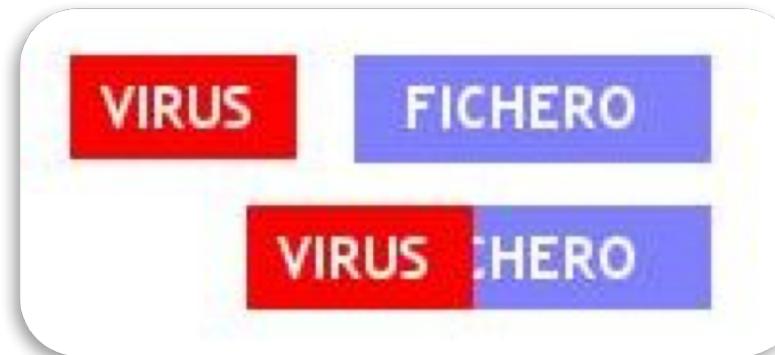
No respetan la información contenida en los archivos infectados, haciendo que estos queden inservibles. Hay otros que, además, son residentes o no. Aunque la desinfección es posible, no se pueden recuperar los archivos infectados.

## ¿Cómo actúan?

Utilizan un método muy simple, que consiste en sobrescribir el archivo con los datos del virus. (ej Imagen)

## Nombres

Way, TRJ. Reboot, Trivial.88.D. , son los más peligrosos



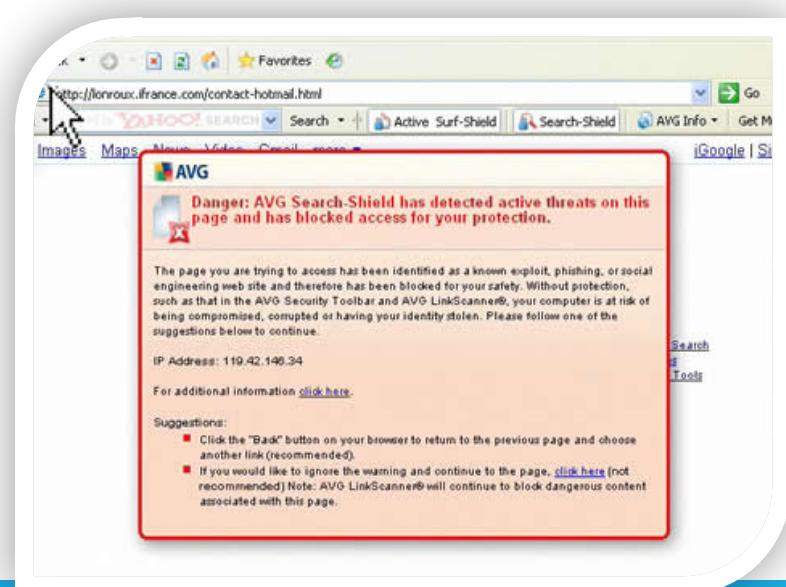
# Virus de Enlace

## ¿Cómo funcionan?

Modifica la dirección donde se almacena un fichero, hacia donde se encuentra el virus. La activación del virus se produce cuando se utiliza el fichero afectado. Es imposible volver trabajar con el fichero original.

## ¿Cómo Actúan?

Atacan las direcciones de directorios, la modifican y, al momento de utilizarlo, se ejecuta el virus.



# Virus múltiples

## ¿Cómo funcionan?

Infectan archivos ejecutables y sectores de booteo, combinando la acción de virus de programa y del sector de arranque.

## ¿Cómo Actúan?

Se auto ejecutan al ingresan a la máquina, y se multiplican. Infectan, gradualmente, nuevos sectores. Hay que eliminarlos simultáneamente en el sector de arranque y archivos de programa

## Nombres

Los más comunes son:  
One\_Half, Emperor,  
Anthrax y Tequila.



# Residentes

## ¿Cómo funcionan?

Se ocultan en memoria RAM permanentemente. Así, pueden controlar todas las operaciones llevadas a cabo por el sistema operativo, infectando los programas que se ejecuten.

## ¿Cómo Actúan?

Atacan cuando se cumplen, por ej, fecha y hora determinada por el autor. Mientras tanto, permanecen ocultos en la zona de la memoria principal.

## Nombres

Algunos ej. De éste virus son: Randex, CMJ, Meve, MrKluny.



# Mutantes

---

## ¿Cómo funcionan?

Modifican sus bytes al replicarse. Tienen incorporados rutinas de cifrado que hacen que el virus parezca diferente en variados equipos y evite ser detectado por los programas antivirus que buscan específica y concretamente.

## ¿Cómo Actúan?

---

Su estrategia es mutar continuamente. Se utilizan como competencia contra otros crackers, y dañan archivos, temporalmente.

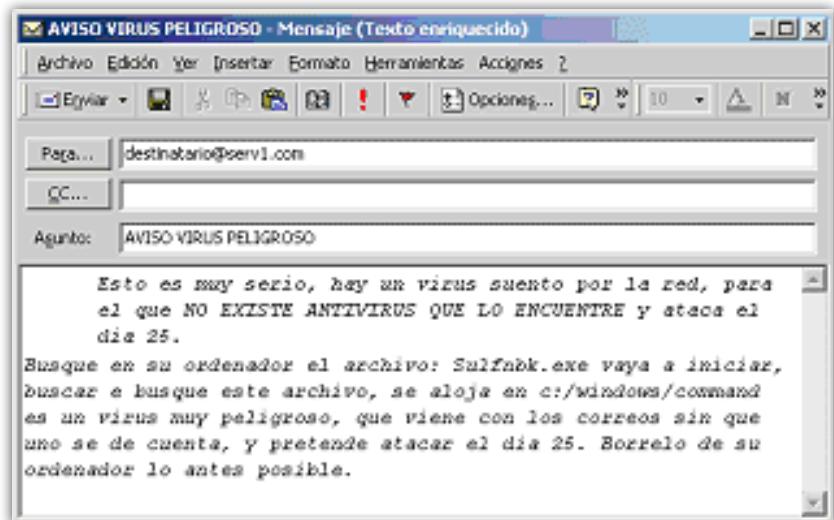


# Virus Falsos

---

Estos tipos de programas, están mal denominados “virus”, ya que no funcionan ni actúan como tales. Tan solo son programas o mensajes de correo electricos, que debido a que estan compuestos por hoaxes o bulos.

En caso de recibirlas, no hay que prestarles atencion ni reenviarlos.



# Virus de Macros

## ¿Cómo funcionan?

Infectan ficheros usando determinadas aplicaciones que contengan macros: documentos de Word, Excel, datos de Access, presentaciones de PowerPoint, etc.

## ¿Cómo Actúan?

Cuando se abre un fichero que contenga este virus, las macros se cargarán automáticamente, produciéndose la infección. Se pierden los datos en la plantilla.

## Nombres

Los más comunes son: Relax, Melissa.A, Bablas, O97M/Y2K.



# Virus de Compañía

## ¿Cómo funcionan?

Son virus de fichero que pueden ser residentes o de acción directa.

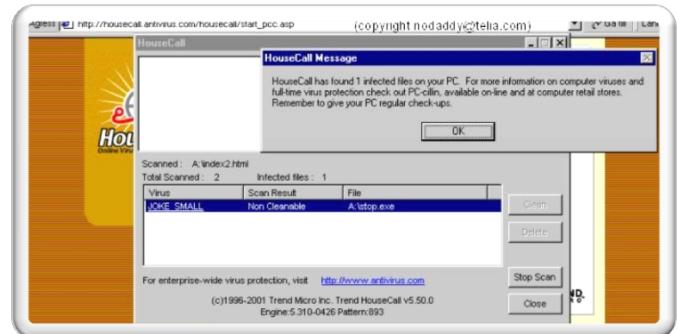
"Acompañan" ficheros existentes en el sistema, antes de su llegada.

## ¿Cómo actúan?

Pueden esperar ocultos en la memoria hasta que se lleve a cabo la ejecución de algún programa (sin modificarlos como virus de sobre escritura o residentes), o actuar directamente haciendo copias de sí mismos.

## Nombre

Stator, Asimov.1539, Terrax.1069., son los mas usuales



# Antivirus

## ¿Qué es?

---

Los Antivirus son softwares utilizados para prevenir, detectar y eliminar virus y otras clases de malwares, utilizando todo tipo de estrategias para lograr este principal objetivo. Hay en total mas de 40 antivirus en el mundo, pero los mas importantes son:

AVG

Norton

Microsoft Security

Avira

- Kaspersky
- Panda
- Avast!



# AVG

## ¿Qué es?

Es un grupo de productos antivirus. Su producto mas destacado es una versión gratuita de su antivirus para usuarios hogareños. Tiene mas de 45 millones de usuarios.

## Caracteriza por

Ser uno de los softwares gratuitos mas utilizados y ser uno de los mas “libres”.

**Apto para  
Windows y Linux**



# Norton

## ¿Qué es?

**Norton** es uno de los programas antivirus más utilizados. Presenta varias características que no se encuentran en sus otros sistemas antivirus.

## Caracteriza por

Negativamente, tiene un alto consumo de recursos y bajo nivel de detección. Positivamente, tiene intercambio de tecnología con la CIA y el FBI.

**Apto para**  
Windows y Mac Os



# Microsoft security

---

## ¿Qué es?

Microsoft Security Essentials un software antivirus gratuito creado por Microsoft, que protege de todo tipo de malware como virus, gusanos troyanos etc..

## Caracteriza por

Es un programa muy liviano, que utiliza pocos recursos, ideal para equipos como netbooks.

**Apto Para  
Sólo Windows**



# Ayira

## ¿Qué es?

---

Avira Antivir, es un producto de la agencia de seguridad informatica “Avira”. Es gratuita para uso personal y organizaciones sin fines de lucro.

### ¿Cómo funciona?

Explora discos duros y extraíbles en busca de virus y también corre como un proceso de fondo, comprobando cada archivo abierto y cerrado.

**Apto para**  
Windows, Linux y Unix



# Kaspersky

## ¿Qué es?

Kaspersky Antivirus, pertenece a la compañía rusa homónima. Es un software privado y pago, con grandes velocidades en las actualizaciones.

### Caracteriza por

Tiene un gran sistema de asistencia técnica, y es un buen sistema para PC's portátiles. Es uno de los mejores scanners de malwares existentes.

**Apto Para**  
Todos los sistemas operativos



# Panda

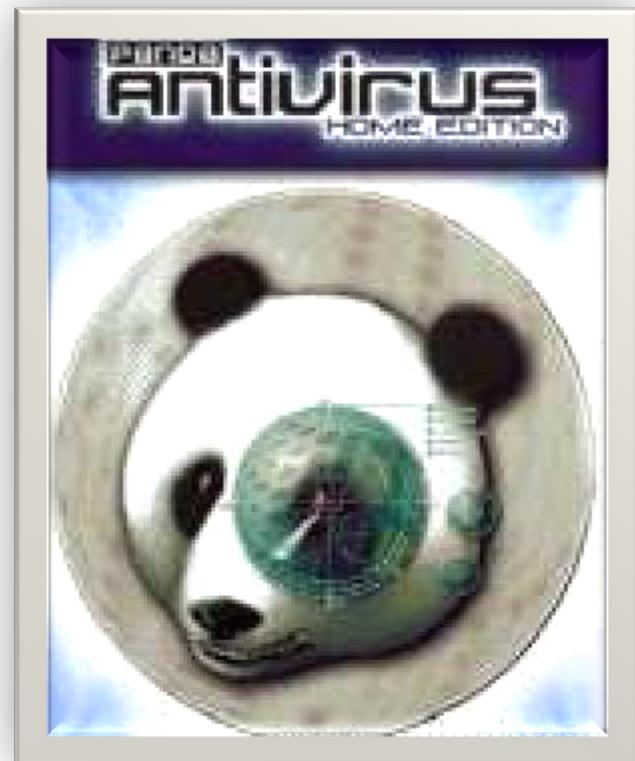
## ¿Qué es?

Panda, de Panda Security, es un antivirus que ofrece gran seguridad gracias a un sistema de análisis, clasificación y desinfección automática de nuevas amenazas informáticas.

### Caracteriza por

Negativamente, problemas administrativos envían mails no deseados a clientes. Positivamente, incluye detalles como detección de archivos con virus o intrusiones Wi-Fi.

**Apto para**  
**Sólo Windows**



# Avast!

## ¿Qué es?

---

**Avast!** es un programa antivirus de *Alwil Software*. Sus versiones cubren desde un usuario doméstico al corporativo. Es un software libre y gratuito.

## Caracteriza por

Actualizar versión automáticamente y ser uno de los software mas abiertos.

**Apto para**  
Windows, Mac Os  
y Linux



# Precauciones contra virus

No abrir correos de desconocidos.

---

No abrir archivos adjuntos si no se tiene la certeza de su contenido.

Especial cuidado con los archivos y programas bajados de Internet.

Tener activado el antivirus de forma permanente.

realizar copias de seguridad de nuestros datos en CD u otros medios, para prevenir que se borren datos.

En síntesis, utilizar un buen programa antivirus actualizado, no grabar archivos sin garantía y no abrir correos de remitente desconocido.