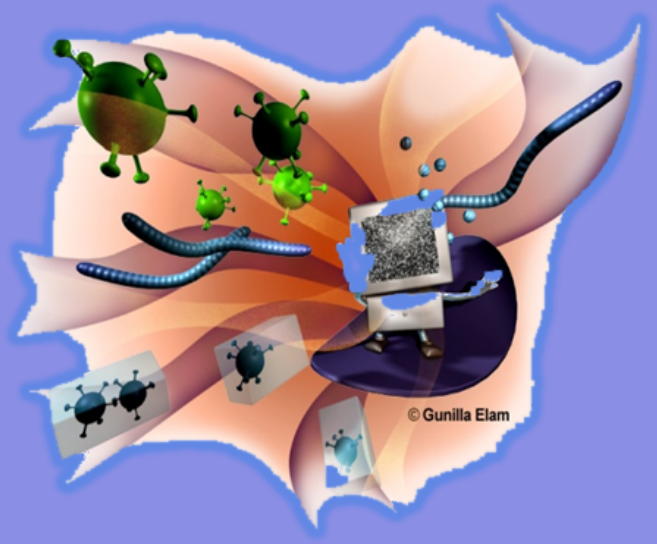


Virus de Hoy,
Antivirus de Ayer,
Usuarios de Siempre
y los Daños...

¡Como Nunca!

Presentado: PROF.JAIME CORONEL S.

Antes de que sea

demasiado TARDE...

¡PROTÉJELO!

Los 90

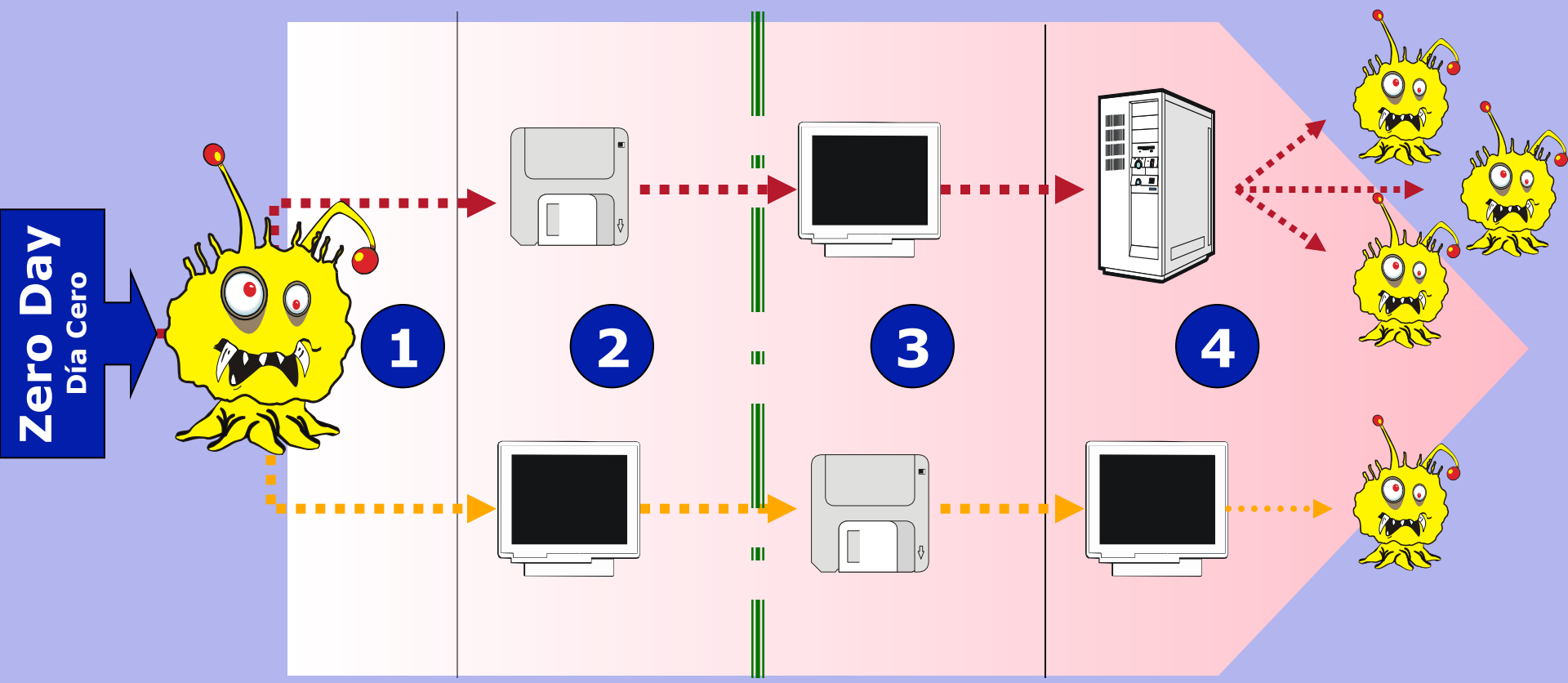
¡¡ Nacen los Primeros Virus !!

Principales Amenazas en los 90

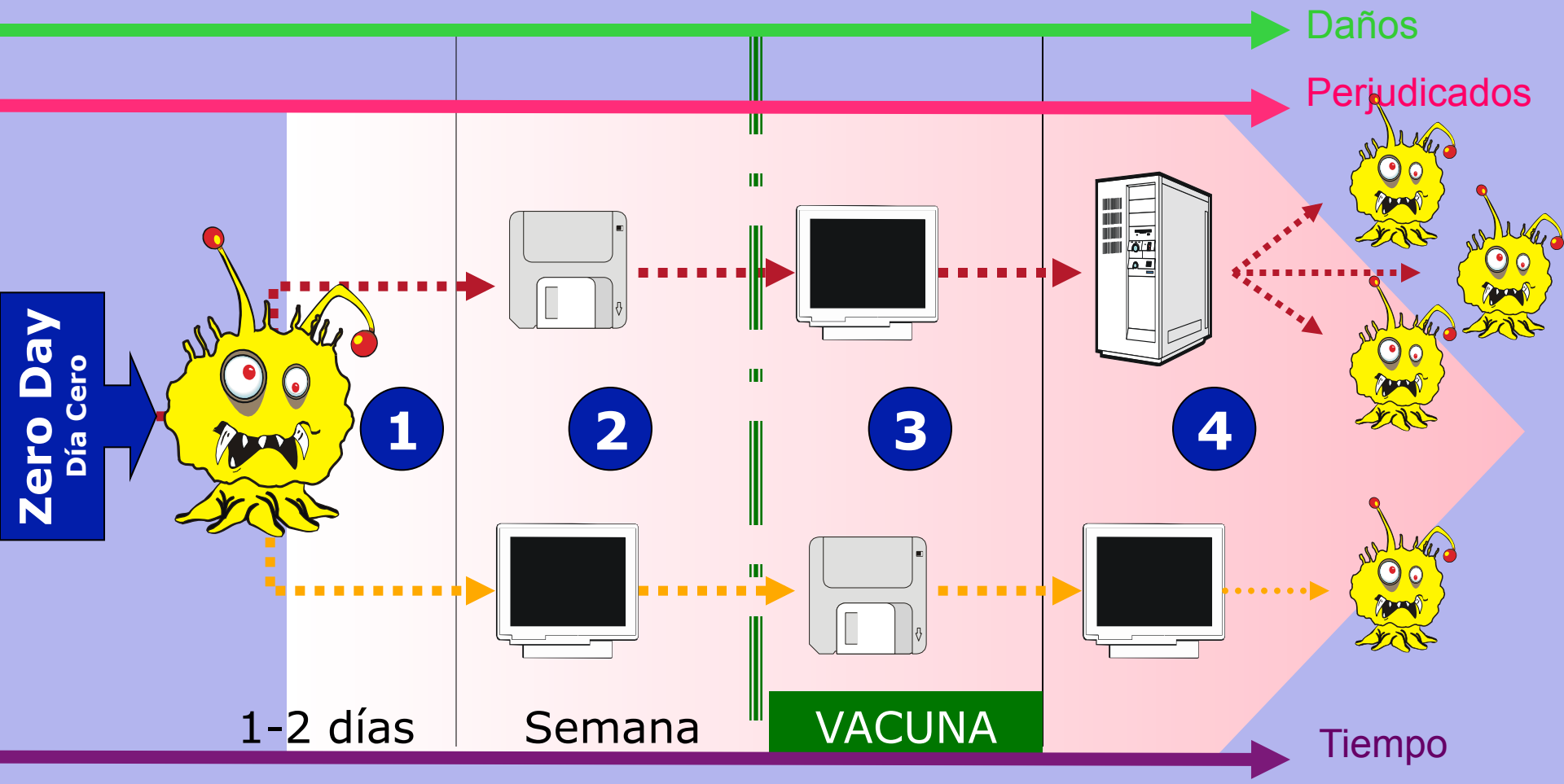
- **Virus:** Programa informático con capacidad de replicación cuya finalidad es difundirse al mayor número de usuarios a través de diferentes vías y provocar daños de distinta índole en archivos y sistemas.

- **Gusano**: Posee las mismas características que los virus salvo que no necesitan infectar otros archivos para reproducirse. Se limitan a guardar en el sistema copias de sí mismos pudiendo llegar a colapsar por saturación los sistemas en los que se infiltran.

Mecanismo de Difusión (I)



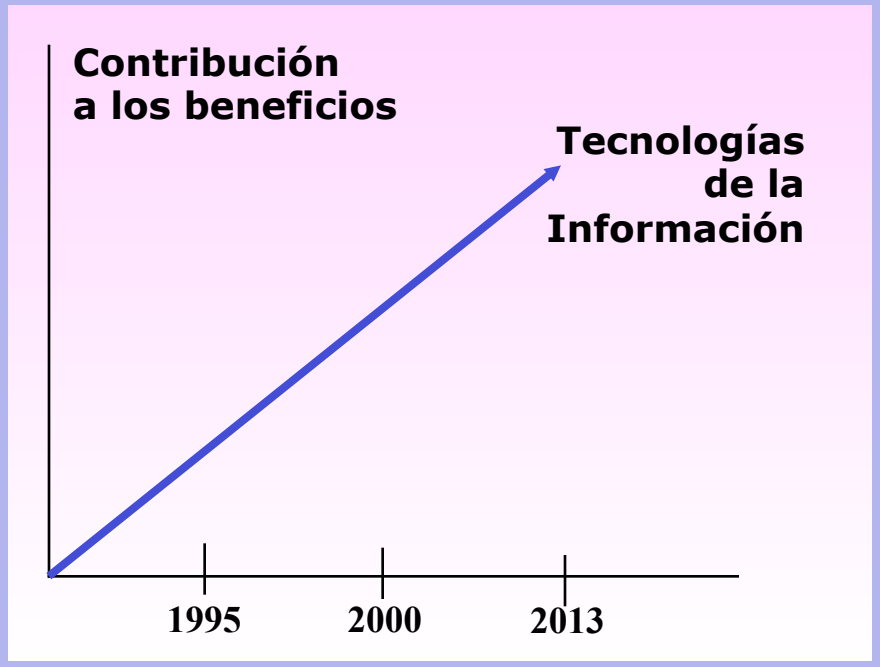
Mecanismo de Difusión (II)

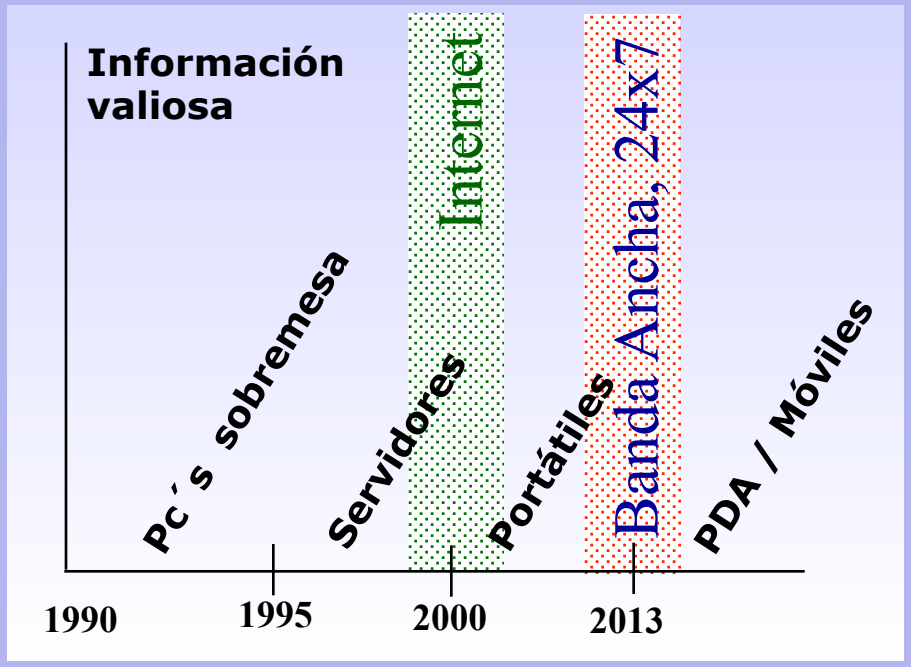


23 Años Después,

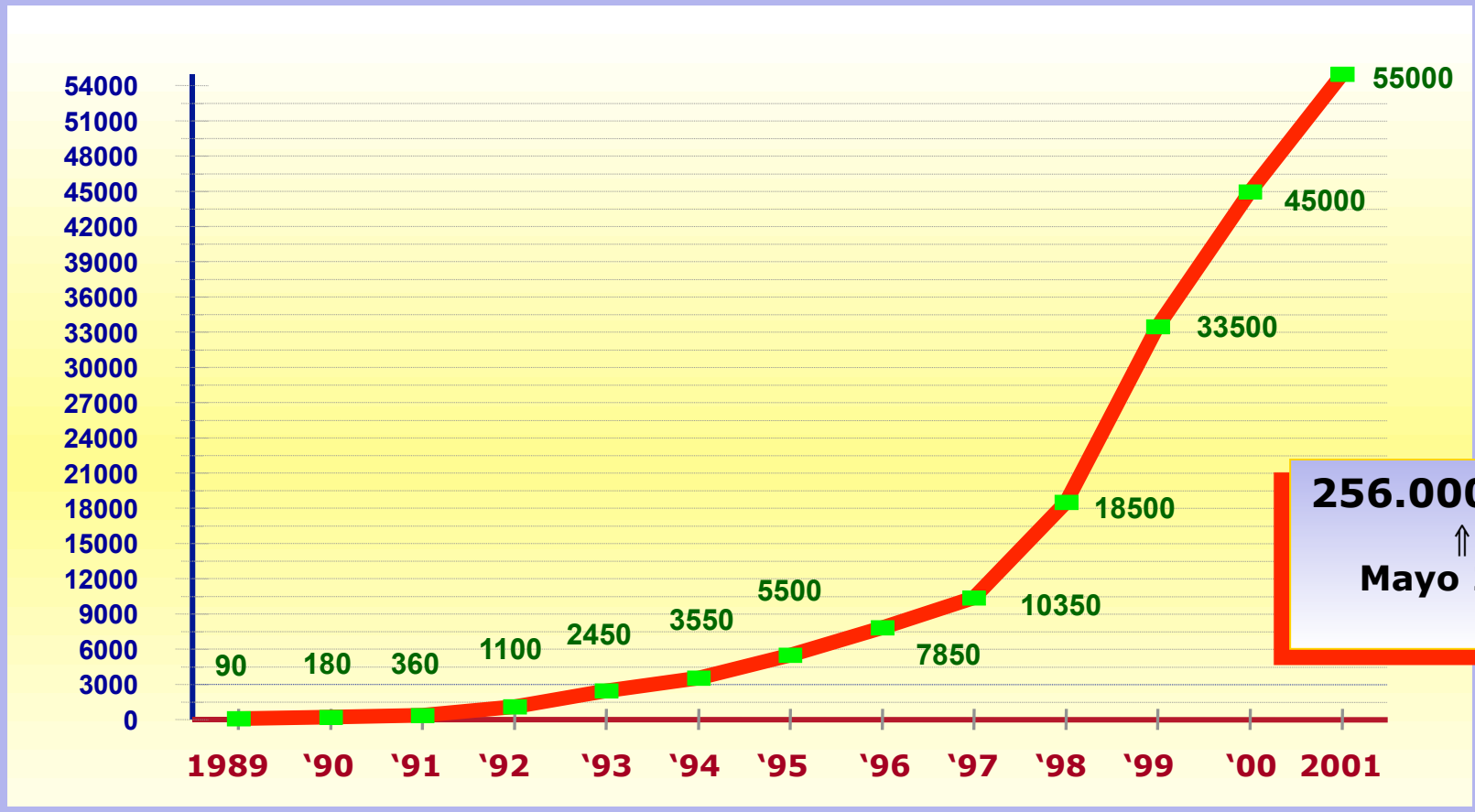
¡¡El Mundo se Mueve!!

Evolución de las Tecnologías de la Información





Crecimiento de los Virus



TIPOS DE VIRUS

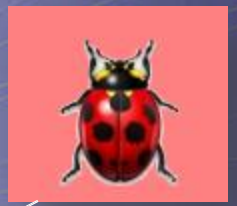
TROYANO

GUSANO

DE MACROS

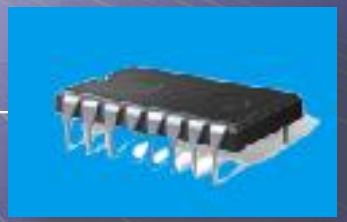
BOMBA

PARÁSITOS



DE ARRANQUE

RESIDENTES



VIRUS TROYANO

Es un programa dañino que se oculta en otro programa legítimo, y que produce sus efectos perniciosos al ejecutarse este ultimo. En este caso, no es capaz de infectar otros archivos o soportes, y sólo se ejecuta una vez, aunque es suficiente, en la mayoría de las ocasiones, para causar su efecto destructivo.

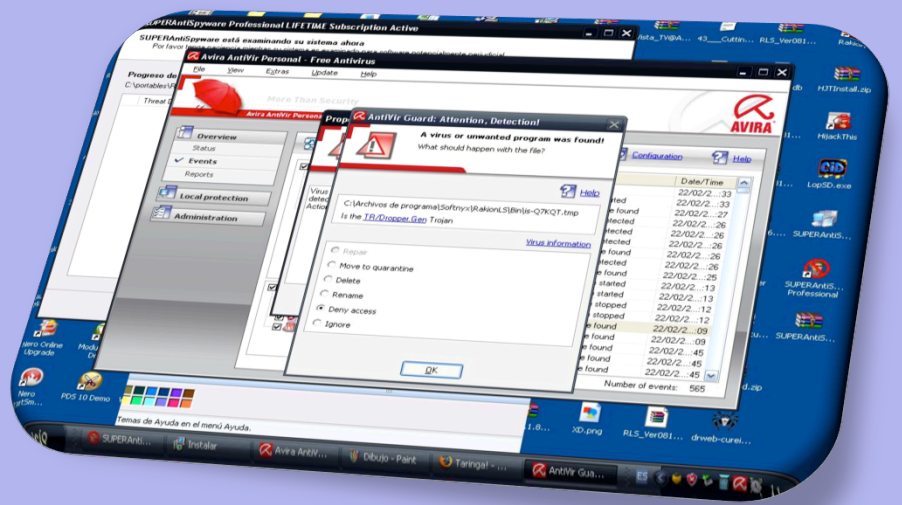
Virus Troyano

¿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.



Códigos Maliciosos

- Troyanos Downloader: Al comprometer una computadora se encargan de descargar otros códigos maliciosos.
- Troyanos Bancarios: Utilizados para realizar fraudes a través de datos confidenciales de los usuarios.
- Troyanos Clicker: Aquellos que realizan fraudes a través de clic en sitios con publicidad.
- Troyanos Backdoors: Permite el acceso a un sistema de una manera no convencional.
- Troyanos Bot: Convierte las computadoras en equipos zombies que luego forman parte de los botnets.

VIRUS Gusano o Worm

Es un programa cuya única finalidad es la de ir consumiendo la memoria del sistema, se copia así mismo sucesivamente, hasta que desborda la RAM, siendo ésta su única acción maligna.

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 parcial o totalmente.

Nombres

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

Virus de macros

Son aquellos virus que infectan a aquellos ficheros creados mediante aplicaciones macro. Suelen afectar a programas como Word y Excel, por ejemplo.

La mayoría de los programas que utilizan macros poseen una protección específica, pero en algunos casos los virus sobrepasan esa barrera con facilidad.

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

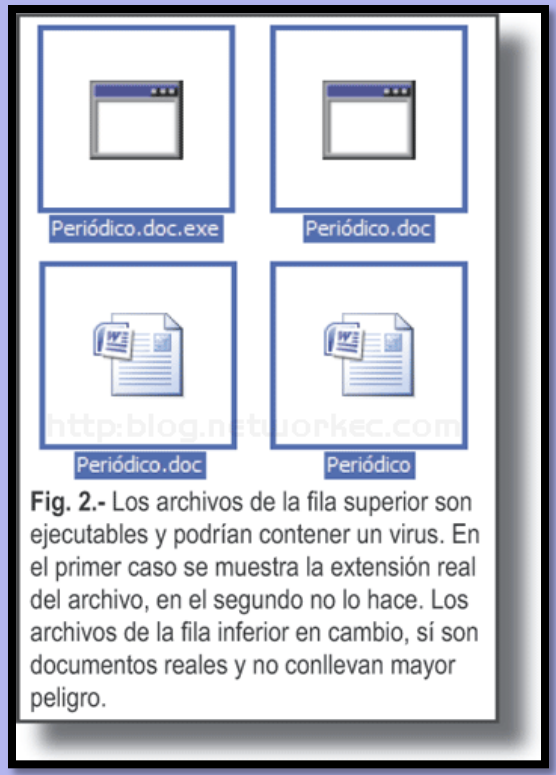


Fig. 2.- Los archivos de la fila superior son ejecutables y podrían contener un virus. En el primer caso se muestra la extensión real del archivo, en el segundo no lo hace. Los archivos de la fila inferior en cambio, sí son documentos reales y no conllevan mayor peligro.

VIRUS PARÁSITOS

Se les denomina parásitos, porque viven del trabajo de otros. Pero la otra razón, es porque llegan a nuestra computadora como "parásitos" a su vez de otro software.

Los "parásitos", son aplicaciones comerciales que se instalan en nuestra computadora. Este tipo de código, es muchas veces catalogado dentro de lo que se conoce como Spyware (software que recoge información de nuestros hábitos de navegación, por ejemplo).

VIRUS DE BOOT: (DE ARRANQUE)

Son virus que infectan sectores de inicio y booteo (Boot Record) de los diskettes y el sector de arranque maestro (Master Boot Record) de los discos duros; también pueden infectar las tablas de particiones de los discos.

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 eje, fecha y hora determinada por el autor. Mientras tanto, permanecen ocultos en la zona de la memoria principal.

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.

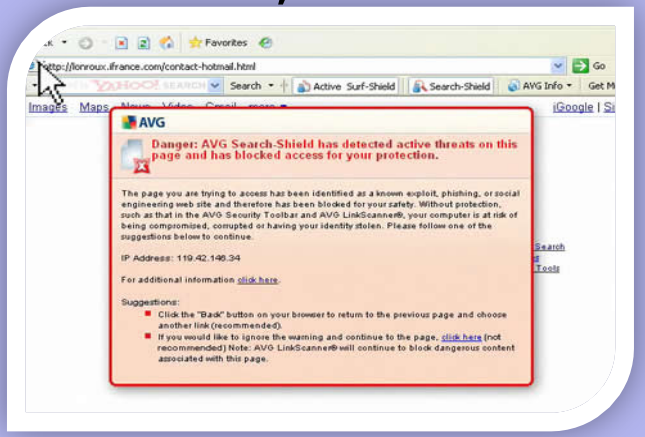
Virus de Enlace

¿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.



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 especifica y concretamente.

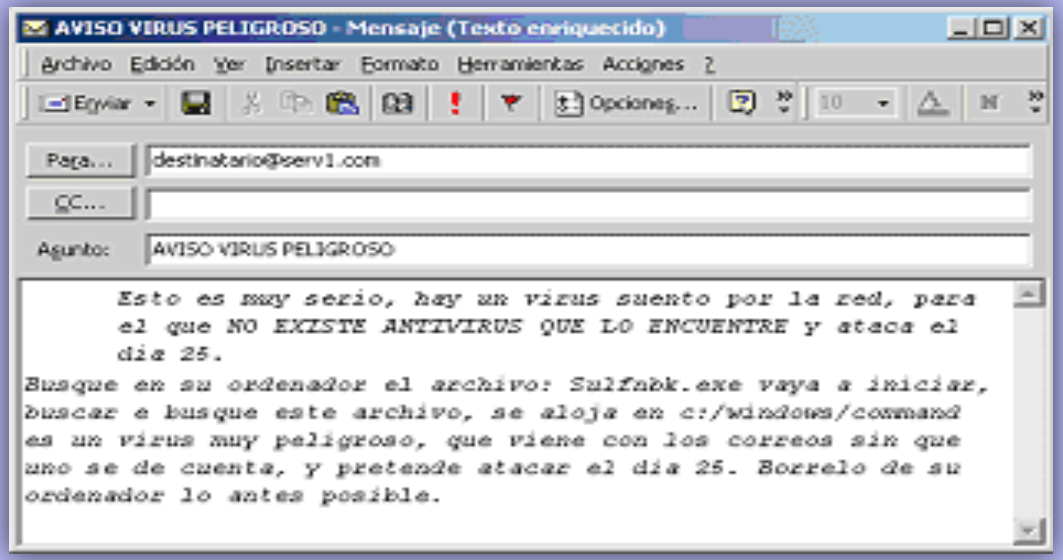
¿Cómo Actúan?

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 eléctricos, que debido a que están compuestos por hoaxes o bulos.

En caso de recibirlos, no hay que prestarles atención ni reenviarlos.



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

Antivirus

¿Qué es?

Los Antivirus son software utilizados para prevenir, detectar y eliminar virus y otras clases de malware, 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

¿Qué es?

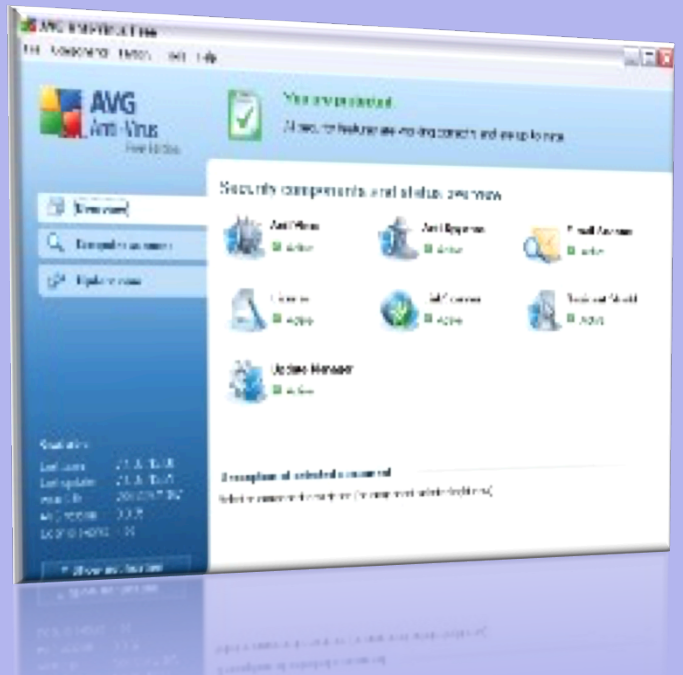
Es un grupo de productos antivirus. Su producto mas destacado es una versión gratuita de su antivirus para usuarios hogareños. Tiene mas de 45 millones de usuarios.

Caracteriza por

Ser uno de los software 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.

Apto para

Windows y Mac Os

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.

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

Avira

¿Qué es?

Avira Antivir, es un producto de la agencia de seguridad informática "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 scanner de malware existentes.

Apto Para

Todos los sistemas operativos

Panda

¿Qué es?

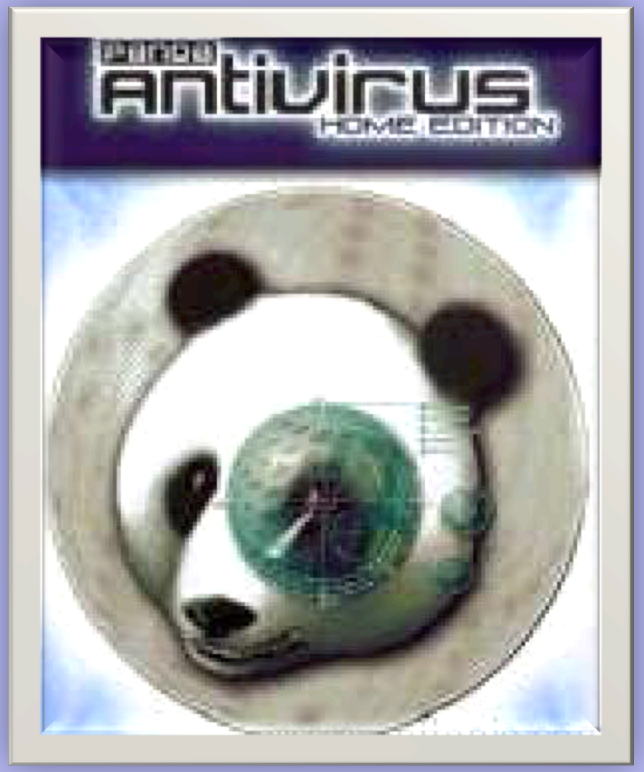
Panda, de Panda Security, es un antivirus que ofrece gran seguridad gracias a un sistema de análisis, clasificación y desinfección automática de nuevas amenazas informáticas.

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

QUIEN CREA LOS VIRUS?

Los virus son creados por expertos programadores. Su estrategia de propagación y daño demanda un excelente conocimiento de los lenguajes de programación y los sistemas operativos. Muchas personas se dedican a crear virus para pasar el tiempo, motivos publicitarios denigrantes, robo de identidades, para molestar, y hasta como forma de venganza o simplemente de diversión personal.

El 2 de noviembre de 1988, lo que antes era Internet (conocida como ARPAnet) cayó ante el ataque de un gusano que usaba toda la memoria de los ordenadores haciéndolos lentos. Se tardó varios días en recuperar la actividad de la red y los daños ascendieron a un millón de dólares.

Cuando se apresó a Robert Morris Jr.,el juez lo sentenció con tres años de libertad condicional, 400 horas de servicios comunitarios y 10.000 dólares de multa.

TIPOS DE HACKERS

- **Black hats o hackers negros:** muestra sus habilidades en informática rompiendo computadoras, colapsando servidores, entrando a zonas restringidas, infectando redes o apoderándose de ellas, entre otras muchas cosas utilizando sus destrezas en métodos Hacking. Disfruta del reto intelectual de superar o rodear las limitaciones de forma creativa.

- **White hats o hackers blancos:** es una persona que busca los bugs de los sistemas informáticos, por decir así de una manera genérica, dando a conocer a las compañías desarrolladoras de software o empresas sus vulnerabilidades, claro sin ánimo de perjudicar. Sin embargo hay algunos de ellos que si buscan el interés personal, queriendo entrar a sitios restringidos, estafando... etc.

- **Lammer o Script-Kiddes:** Son aprendices que presumen de lo que no son, aprovechando los conocimientos del hacker y lo ponen en práctica, sin saber. En resumen, no saben nada de hacker.

- **Luser (looser + user):** Es un término utilizado por hackers para referirse a los usuarios comunes, de manera despectiva y como burla.

- **Phreaker:** "monstruo telefónico“. Son personas con conocimientos tanto en teléfonos modulares (TM) como en teléfonos móviles, se encuentran sumergidos en entendimientos de telecomunicaciones bastante amplios.

- **Newbie:** son los hacker novatos, se introducen en sistemas de fácil acceso y fracasan en muchos intentos, sólo con el objetivo de aprender las técnicas que puedan hacer de él, un hacker reconocido, se dedica a leer, escuchar, ver y probar las distintas técnicas que va aprendiendo. Son más precavidos y cautelosos que los lamers.

- **Pirata Informático:** dedicado a la copia y distribución de software ilegal, tanto software comercial crackeado, como shareware registrado, etc, de una manera consciente o inconsciente uno se convierte en un pirata informático descargando programas, juegos, música…

- **Samurai:** Son lo más parecido a una amenaza pura. Sabe lo que busca, donde encontrarlo y cómo lograrlo. Hace su trabajo por encargo y a cambio de dinero, no tienen conciencia de comunidad y no forman parte de los clanes reconocidos por los hackers.

- **Trashing ("Basurero"):** Obtienen información en cubos de basura, tal como números de tarjetas de crédito, contraseñas, directorios o recibos.

- **Wannaber:** Desea ser hacker pero estos consideran que su coeficiente no da para tal fin.

¿Qué son los CRACKERS?

- **Es una persona que mediante ingeniería inversa realiza cracks, los cuales sirven para modificar el comportamiento o ampliar la funcionalidad del software o hardware original al que se aplican, sin que en absoluto pretenda ser dañino para el usuario del mismo.**
- **→ No puede considerarse que la actividad de esta clase de cracker sea ilegal si ha obtenido el software o hardware legítimamente, aunque la distribución de los *cracks* pudiera serlo.**

VIRUS EN LOS DISPOSITIVOS

La gran popularidad que en los últimos tiempos han alcanzado los dispositivos de almacenamiento USB ha provocado que los creadores de virus informáticos hayan puesto su atención sobre ellos con el fin de utilizarlos para propagar malware.

Para ello aprovechan una funcionalidad de los sistemas Windows que permite la reproducción automática de contenidos alojados en unidades de almacenamiento extraíble, pendrives, cámaras digitales, reproductores MP3 y MP4, celulares, Ipod, etc

A día de hoy no existe una solución universal y sencilla para combatir este problema, aunque se dispone de algunas medidas parciales que pueden ayudar a mitigarlo.

SÍNTOMAS DE UNA PC CON VIRUS

- Rendimiento del sistema reducido.
- La cantidad de memoria disponible cambia o disminuye continuamente.
- Arranque incompleto del sistema o fallo en el arranque.
- Escrituras inesperadas en una unidad.
- Mensajes de error extraños o no estándar.

- Actividad de pantalla no estándar (animaciones, etc.), fluctuaciones de pantalla.

- Sectores erróneos en disquetes y en discos duros.

- Cualquier operación extraña que su ordenador no realizaba antes y que de un momento a otro comienza a ejecutar.

- Errores no justificados en la FAT.

Consejos para proteger tu PC

- Utiliza un buen antivirus y actualízalo frecuentemente.
- Comprueba que tu antivirus incluye soporte técnico, resolución urgente de nuevos virus y servicios de alerta.
- Asegúrate de que tu antivirus esté siempre activo.
- Verifica, antes de abrir, cada nuevo mensaje de correo electrónico recibido.
- Evita la descarga de programas de lugares no seguros en Internet.

Consejos para proteger tu PC

- Rechaza archivos que no hayas solicitado cuando estés en chats o grupos de noticias (news).

- Actualiza el software que tienes instalado con los parches aconsejados por el fabricante de este programa.

- Retira los disquetes de las disqueteras al apagar o reiniciar tu ordenador.

- Analiza el contenido de los archivos comprimidos.

Consejos para proteger tu PC

- Mantente alerta ante acciones sospechosas de posibles virus.
- Añade las opciones de seguridad de las aplicaciones que usas normalmente a tu política de protección antivirus.
- Realice periódicamente copias de seguridad.
- Mantente informado de lo que acontece en el sector de la Seguridad Informática.


DEADLY
EBOLA
VIRUS
OUTBREAK