Virus

Que es un Virus?

Es un programa o una serie de instrucciones que van encaminadas hacia el daño y la destrucción de la información cibernética, es

decir estos virus no hacen mas que borrar información, o modificarla, también pueden reproducirse y acaparar toda la memoria disponible de la computadora o bloquear las redes informáticas generando tráfico

inútil.

Funcionamiento del Virus

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.

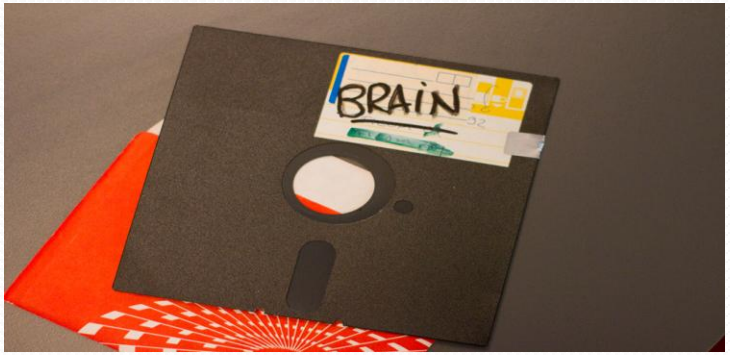
Historia de los Virus

1970: Virus Creeper

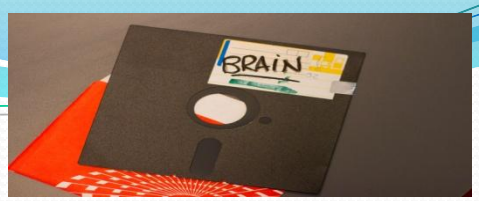
El virus mostraba el mensaje "SOY CREEPER...ATRAPAME SI PUEDES!"

1980: La red ARPANET es infectada por un "gusano" y queda 72 horas fuera de servicio

1986: Se crearon los virus Brain, Bouncing Ball, donde fueron las primeras especies representativas de difusión masiva. Estas 2 especies virales tan sólo infectaban el sector de arranque de los diskettes

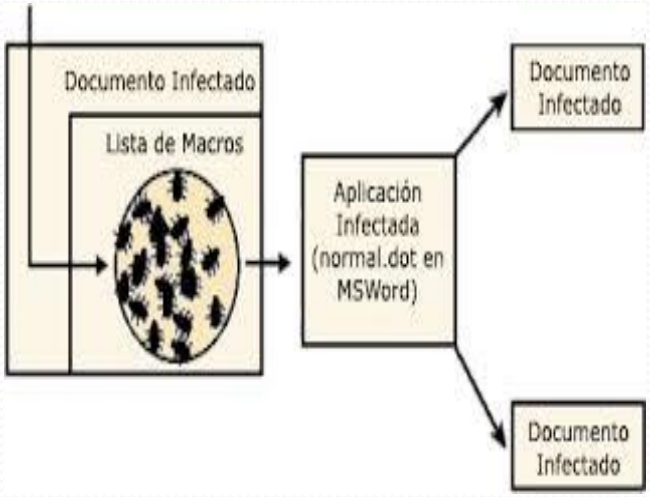


1988: El virus Brain aparece en los Estados Unidos



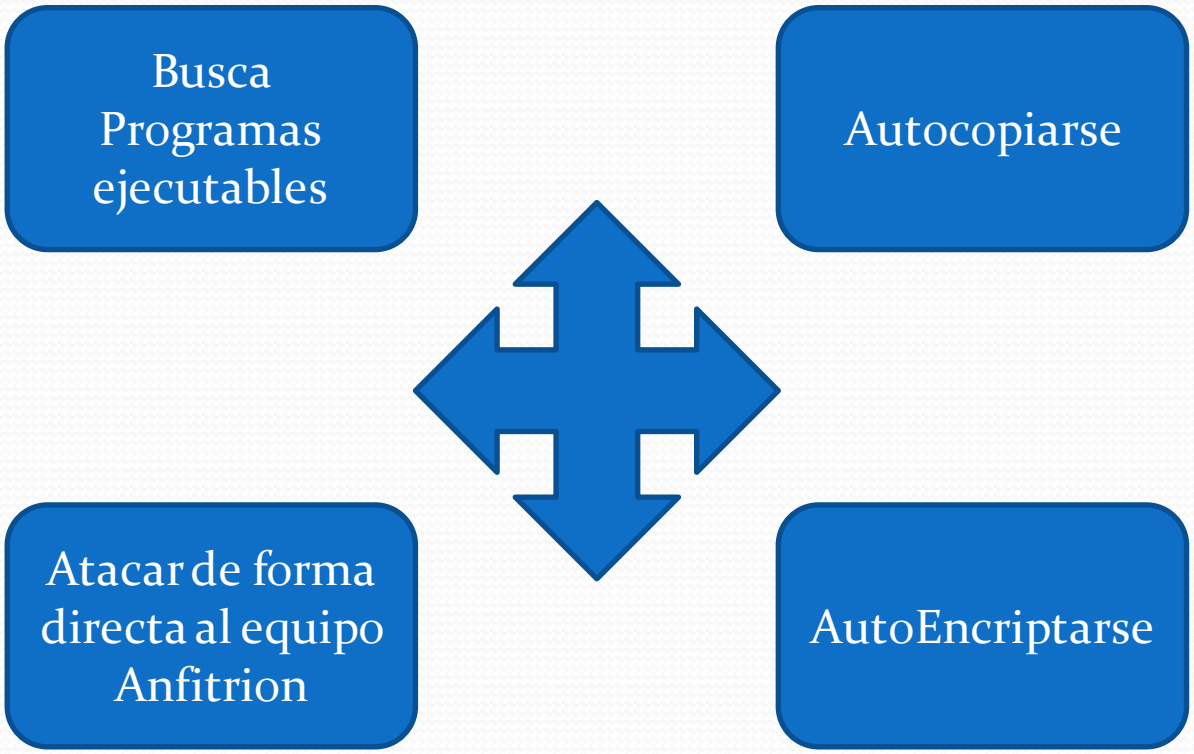
1995: No solamente infectaban documentos sino que a su vez, sin ser archivos ejecutables podían autocopiarse infectando a otros documentos.

Macro Virus: Infectaba los archivos de MS-Word



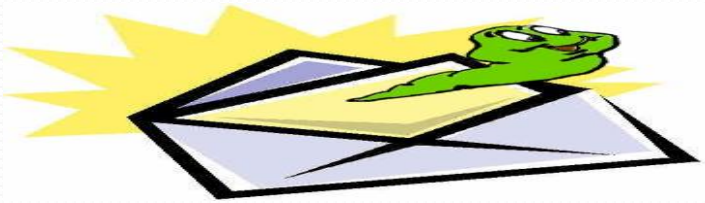
1999: Se propagaron muchos mas virus, tal como el Mellissa, ademas del CIH y ExploreZip

Caracteristicas Virus



Metodos de Propagacion

Mensajes que ejecutan automáticamente programas desde correo electrónico.



Ingeniería Social, mensajes como *ejecute este programa y gane un premio*

Entrada de información en discos de otros usuarios infectados.

Internet:
Transferencia entre ordenadores infectados.

Metodos de Proteccion

- **Activos**
  - Antivius
  - Filtro de Ficheros

- **Pasivos**
  - Evitar introducir medios de Almacenamiento.
  - No instalar Software gratis
  - No aceptar Email desconocidos

Tipos de Virus

- **Troyano**:

Roba informacion, o altera el sistema del hardware.

- **Gusano**:

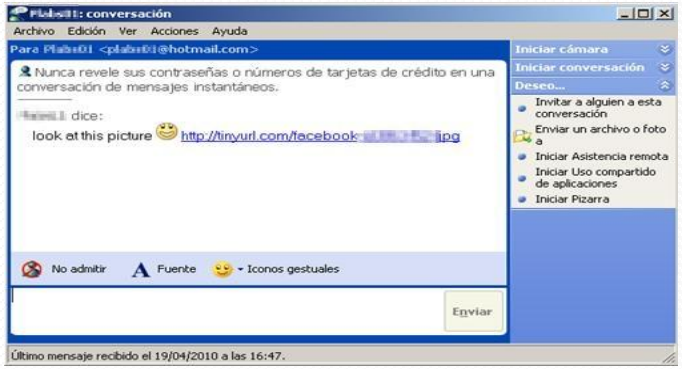
Tiene la propiedad de duplicarse a si mismo, son invisibles para el ser humano.

- **Bombas Logicas**

Se activan al producirse un acontecimiento determinado. Puede activarse con cierta combinacion de teclas, o ciertas condiciones tecnicas

- **Hoax**

Son mensajes de contenido falso, trata de aprovecharse de novatos.

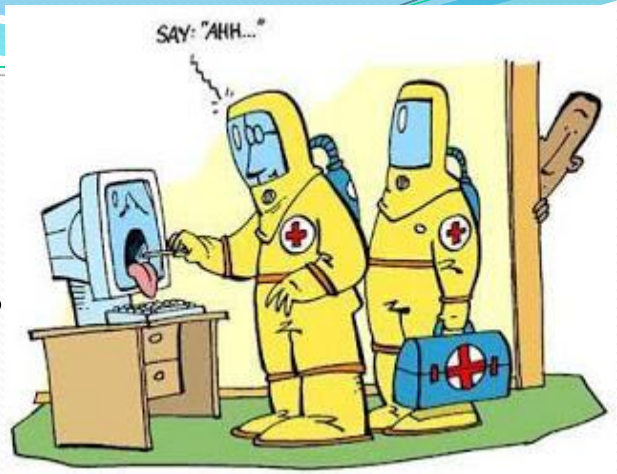


- **Joke**

Son mensajes molestosos, pero no son maliciosos.

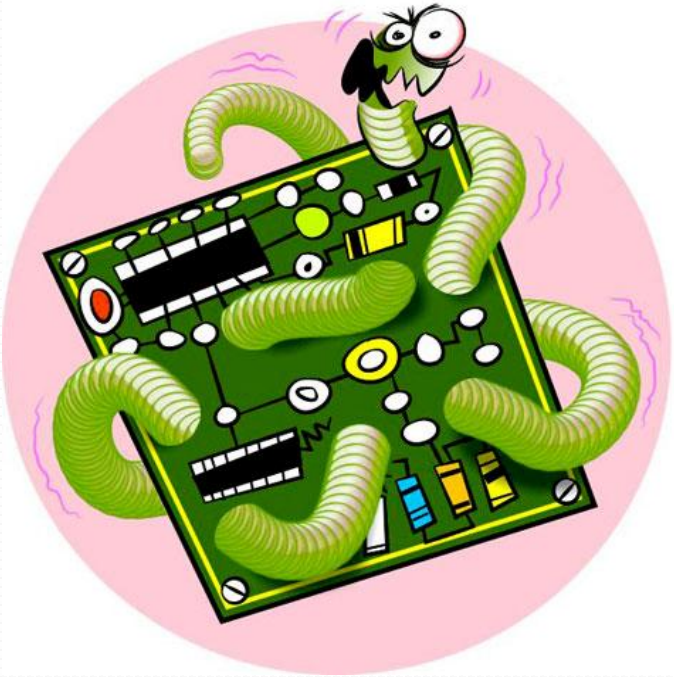
- **Virus Residentes**

Se ocultan en la memoria RAM de forma permanente o residente, pueden controlar e interceptar todas las operaciones llevadas a cabo por el sistema operativo, como por ejemplo: Randex, CMJ, Meve, MrKlunky



- **Virus de Accion Directa**

Estos virus no permanecen en memoria. Su objetivo es reproducirse y actuar en el mismo momento de ser ejecutados, se activan y buscan ficheros para contagiarlos.



- **Virus de Sobreescritura**

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 Arranque**

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.

- **Virus de Enlace o Directorio**

Alteran las direcciones que indican donde se almacenan los ficheros. De este modo, al intentar ejecutar un programa 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.

- **Virus Cifrados**

Es técnica utilizada por algunos de los virus, 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 Polimorficos**

Son virus que en cada infección que realizan se cifran de una forma distinta. 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 Fichero**

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

- **Virus FAT**

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

- 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.