UNIVERSIDAD DE VALENCIA

ESCUELA UNIVERSITARIA DE ESTUDIOS EMPRESARIALES

DEPARTAMENTO DE DIRECCIÓN DE EMPRESAS

INFORMÀTICA APLICADA A LA GESTIÓN DE EMPRESAS

Curso 1998-99

VIRUS

INFORMÁTICOS

Salvador Climent Serrano

Virus:

El primer indicio de definición de virus informático aparece en el año 1949 por *John Von Neuman* en el artículo "Teoría y organización de un autómata complicado" donde expone su teoría de programas con capacidad de multiplicarse.

Diez años después en los laboratorios AT & T Bell inventan el juego de guerra nuclear (Core Wars) o guerra de núcleos, consistía en una batalla entre los códigos de dos programadores, en la que cada jugador desarrollaba un programa cuya misión era la de acaparar la máxima memoria posible mediante la reproducción de sí mismo. En esta lucha cada uno de los programas intentaba destruir al oponente y tras un periodo de tiempo ganaba quien tuviera la mayor cantidad de memoria ocupada a su oponente con su programa.

El termino "Virus " tal como lo entendemos hoy aparece en 1983 donde *Fred Cohen* lo definió en su tesis doctoral como " Un programa que puede infectar otros programas modificándolos para incluir una versión de sí mismo".

En los años 86-87 es cuando se produce la explosión del fenómeno virus en PCs y fue en el entorno universitario donde se detectaron los primeros casos de infección masiva, los protagonistas fueron:

- BRAIN un virus paquistaní en la Universidad de Delaware
- LEHIGH en la Universidad de su mismo nombre
- VIERNES 13 en la Universidad hebrea de Jerusalén.

Los virus son sin duda alguna los programas dañinos por excelencia, pero existen otras rutinas que pueden destrozar los sistemas de los PCs así tenemos:

- **Los gusanos y conejos**: son programas que tienen la capacidad de reproducción al igual que los virus, tienen por objetivo realizar múltiples copias de sí mismo que suele terminar por desbordar y colapsar el sistema. El gusano más famoso fue el de *Robert Moris* que consiguió bloquear la red ARPANET.
- **Los caballos de Troya o troyanos**: son programas que se presentan en forma de aplicación normal, pero que en su interior poseen un código destructivo, no tienen capacidad de replicación. Uno de los más conocidos fue el AIDS.
- **Bomba lógica**: es un programa que se ejecuta al producirse un hecho determinado (una fecha, una combinación de teclas, etc.) si no se produce la condición el programa permanece oculto sin ejercer ninguna acción, esta técnica cabe su utilización por programadores

fraudulentamente, para así asegurarse una asistencia técnica que solo ellos podrán saber de donde viene y además de forma periódica.

- **Los applests Java y active X**: vienen de la mano de los lenguajes orientados a Internet, que han permitido la potenciación y flexibilidad de la red, pero también abren un nuevo mundo a explotar por los creadores de virus.

FUNCIONAMIENTO

Los virus son simplemente programas creados por personas con un alto grado de conocimientos sobre programación. El lenguaje más utilizado en su desarrollo es el ensamblador por su potencia aunque se utilizan todos: El objetivo del virus consiste en replicarse a sí mismo de forma transparente al usuario, dificultando así al máximo su detección. Para poder replicarse necesita ser ejecutado en el ordenador, por lo que recurre de manera habitual a unirse a ficheros ejecutables modificándolos o a situarse en los sectores de arranque y tabla de partición de los discos. Una vez que se ejecutan suelen quedar residentes en la memoria a la espera de infectar a otros ficheros y discos. Los virus residentes interceptan los vectores de interrupción, modificando la tabla que contiene, para que apunten su código. Los vectores son los encargados de prestar los servicios al sistema; de esta manera, cuando una aplicación llame a uno de esos servicios el control es cedido al virus. Con el control del sistema, el virus se dispone a la reclinación, ya que una llamada al servicio de ejecución o copia de un fichero puede ser interceptada gracias a las modificaciones de los vectores de interrupción y proceder a su infección, lo más usual para ello consiste en añadir el código vírico al final del fichero y modificar la cabecera de ésta para que apunte el virus. Al final del código del virus habrá un nuevo salto al comienzo del programa original para que se ejecute con normalidad y el usuario no sospeche. Por último el virus suele contener un efecto que se hará visible en determinadas circunstancias (una fecha, un número determinado de infecciones, etc.) que harán despertar el efecto, que puede variar desde un inocente mensaje que aparece en pantalla hasta la perdida total de la información de nuestro disco duro.

Los virus mas avanzados utilizan técnicas para hacer más efectivo su trabajo así mediante la técnica de:

Stealh el virus esconde los signos visibles de la infección que podrían delatar su presencia

Tunneling , intentan burlar los módulos residentes de los antivirus mediante punteros directos a los vectores de interrupción (los módulos residentes de los antivirus funciona de forma parecida a los virus pero con propósito totalmente diferente).

Autoencriptación, permite que el virus sé encripte de manera diferente cada vez que infecta un fichero. De esta forma dificulta la detección de los antivirus. Normalmente son detectados por la presencia de la rutina de desencriptación ya que esta no varia. La contramedida de los virus para impedir ser detectados de esta forma es variar el método de encriptación de generación en generación es decir, que entre distintos ejemplares del mismo virus no existen coincidencias ni siquiera en la parte del virus que se encarga de la desencriptación; son los llamados **polimórficos**

TIPOS DE VIRUS

DEPENDIENDO DEL LUGAR EN DONDE SE ALOJAN:

- VIRUS DE BOOT: utilizan el sector de arranque, el cual contiene información sobre el tipo de disco, numero de pistas, sectores, caras, tamaño de la FAT, sector de comienzo, etc. A todo ello hay que sumarle un pequeño programa de arranque que verifica si el disco puede cargar el sistema operativo. Los virus de BOOT utilizan este sector de arranque para ubicarse, guardando el sector original en otra parte del disco: En muchas ocasiones el virus marca los sectores donde guarda BOOT original como defectuosos; de esta forma impiden que sean borrados. En el caso de los discos duros pueden utilizar también la tabla de particiones como ubicación suelen quedar residentes en memoria al hacer cualquier operación en un disco infectado, ala espera de replicarse en otros , como ejemplo tenemos el BRAIN.

- VIRUS DE FICHERO: infectan archivos y tradicionalmente los tipos ejecutables COM y EXE han sido los más afectados, aunque en estos momentos son los ficheros de documentos (DOC, XLS, SAM....) los que están en boga gracias a los virus de macro. Normalmente insertan el código del virus al principio o al final del archivo, manteniendo intacto el programa infectado. Cuando se ejecuta, el virus puede hacerse residente en memoria y luego devuelve el control al programa original para que

continúe de modo normal: El viernes trece es un ejemplo de virus de este tipo.

DENTRO DE LOS VIRUS DE FICHEROS:

- VIRUS DE ACCIÓN DIRECTA: son aquellos que no quedan residentes en memoria y que se replican en el momento de ejecutarse un fichero infectado

- VIRUS DE SOBREESCRITURA: corrompen el fichero donde se ubican al sobreescribirlo.

- VIRUS DE COMPAÑÍA: aprovecha una característica del DOS, gracias a la cual si llamamos a un archivo para ejecutarlo sin indicar la extensión del sistema operativo buscara en primer lugar el tipo COM. Este tipo de virus no modifica el programa original, sino que cuando encuentra un fichero EXE crea otro de igual nombre conteniendo el virus con extensión COM. De manera que cuando tecleamos el nombre ejecutaremos en primer lugar el virus y posteriormente éste pasara el control a la aplicación original.

- VIRUS DE MACRO: están programados usando el lenguaje de macros Word Basic, gracias al cual pueden infectar y replicarse a través de los ficheros MS-Word (DOC). En la actualidad se han extendido a otras aplicaciones como Excel y a otros lenguajes de macros como es el caso de los ficheros SAM del procesador de textos de Lotus. Se ha de destacar que son multiplataforma en cuanto a sistemas operativos ya que dependen únicamente de la aplicación. Un ejemplo de este virus es el Concep que lo incorporo accidentalmente en un CD la compañía Microsoft.
- VIRUS BAT: empleando ordenes DOS en archivos de proceso por lotes consiguen replicarse y efectuar efectos dañinos como cualquier otro virus.
- VIRUS DE MIRC: vienen a formar parte de la nueva generación Internet y demuestran que la red abre nuevas formas de infección. Consiste en un **scrip** para el cliente de IRC mirc. Cuando alguien accede a un canal de IRC donde se encuentra alguna persona infectada, recibe por DCC un archivo llamado "scrip ini". Por defecto, el subdirectorio donde se descargan los ficheros es el mismo donde esta instalado el programa, C:\MIRC. Esto causa que el "script". Ini" original sea sobrescrito por el nuevo fichero maligno.

- NUEVO SCRIPT: permite a los autores y a cualquier persona que conozca su funcionamiento, desde desconectar el usuario infectado del IRC hasta acceder a la información sensible de su ordenador. Así, por ejemplo pueden abrir un FTP en la maquina de la víctima, acceder al archivo de claves de Windows 95 o bajarse el "etc/pasword" en el caso de que sea Linux

- VIRUS BENIGNOS: una buena utilización de las técnicas que emplean los virus puede reportarnos beneficios y ser sumamente útiles. Por ejemplo para parchear sistemas a través de extensas redes LAN. El programa se infecta de ordenador a ordenador modificando parte de un programa que causa fallos en el sistema, y una vez solucionado el error se autodestrulle.