ANEXO A

1. DEFINICIÓN DE LOS DISTINTOS VIRUS INFORMÁTICOS

1.1 Clasificación de virus

Dependiendo del lugar donde se alojan, la técnica de replicación o la plataforma en la cual trabajan, podemos diferenciar en distintos tipos de virus.

- Virus de sector de arranque
- Virus de archivo
- Virus de macro
- Virus bat
- Virus del mirc
- Virus polimorficos
- Virus stealth
- Virus multipartitos

- Virus de sector de arranque (boot).

Utilizan el sector de arranque, el cual contiene la información sobre el tipo de disco, es decir, numero de pistas, sectores, caras, tamaño de la FAT, sector de comienzo, etc. A todo esto hay que sumarle un pequeño programa de arranque que verifica si el disco puede arrancar 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 el Boot original como defectuosos; de esta forma impiden que sean borrados. En el caso de discos duros pueden utilizar también la tabla de particiones como ubicación. Suelen quedar residentes en memoria al hacer cualquier operación en un disco infectado, a la espera de replicarse.

- Virus de archivos.

Infectan archivos y tradicionalmente los tipos ejecutables COM y EXE han sido los mas afectados, aunque es estos momentos son los archivos (DOC, XLS, SAM...) los que están en boga gracias a los virus de macro (descritos mas adelante). 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 se continué de modo normal. El Viernes 13 es un ejemplar representativo de este grupo.

Dentro de la categoría de virus de archivos podemos encontrar mas subdivisiones, como los siguientes:

- Virus de acción directa. Son aquellos que no quedan residentes en memoria y que se replican en el momento de ejecutarse un archivo infectado.

- Virus de sobre escritura. Corrompen el archivo donde se ubican al sobrescribirlo.

- Virus de compañía. Aprovechan una característica del DOS, gracias a la cual si llamamos un archivo para ejecutarlo sin indicar la extensión el sistema operativo buscara en primer lugar el tipo COM. Este tipo de virus no modifica el programa original, sino que cuando encuentra un archivo tipo 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 este pasara el control a la aplicación original.

- Virus de macro.

Es una familia de virus de reciente aparición y gran expansión. Estos están programas usando el lenguaje de macros WordBasic, gracias al cual pueden infectar y replicarse a través de archivos MS-WORD . En la actualidad esta técnica se ha extendido a otras aplicaciones como Excel y a otros lenguajes de macros, como es el caso de los archivos

SAM del procesador de textos de Lotus. Se ha de destacar, de este tipo de virus, que son multiplataformas en cuanto a sistemas operativos, ya que dependen únicamente de la aplicación. Hoy en día son el tipo de virus que están teniendo un mayor auge debido a que son fáciles de programar y de distribuir a través de Internet. Aun no existe una concienciación del peligro que puede representar un simple documento de texto.

Porcion de codigo de un tipico virus Macro:

```
Sub MAIN
  DIM dlg As FileSaveAs
  GetCurValues dlg
  ToolsOptionsSave.GlobalDotPrompt=0
  Ifcheckit(0)=0 Then
    MacroCopy FileName$() + ":autoopen",
    "global;autoopen"
  End If
```

- Virus bat.

Este tipo de virus empleando ordenes DOS en archivos de proceso por lotes consiguen replicarse y efectuar efectos dañinos como cualquier otro tipo virus. En ocasiones, los archivos de proceso por lotes son utilizados como lanzaderas para colocar en memoria virus comunes. Para ello se copian a si mismo como archivos COM y se ejecutan. Aprovechar ordenes como @ECHO OFF y REM traducidas a codigo maquina son <<comodines>> y no producen ningun efecto que altere el funcionamiento del virus.

- Virus del mirC.

Vienen a formar parte de la nueva generación Internet y demuestra que la Red abre nuevas forma de infección. Consiste en un script para el cliente de IRC Mirc.

Cuando alguien accede a un canal de IRC, donde se encuentre alguna persona infectada, recibe por DCC un Archivo llamado "script.ini".

- Virus polimorficos

Estos virus tienen la particularidad de cambiar de forma cada vez que se ejecutan o con cada infección que realizan, este tipo de polimorfismo es llevado a cabo utilizando métodos criptográficos cuando están dormidos en el disco duro y se desencriptan cuando se activan y pasan a la memoria RAM, esto les permite cambiar de forma simplemente cambiando de clave de encriptación adoptando millones de formas. La única forma de detectar estos virus es mediante métodos heurísticos no por comparación de cadenas como los antivirus tradicionales.

- Virus stealth

Estos virus utilizan una técnica especial que les permite esconderse cada vez que un antivirus trata de localizarlos o mediante ordenes del sistema operativo, normalmente lo que hacen es enmascararse mediante las interrupciones (son peticiones que hacen el hardware o software al procesador para poder utilizarlos recusor de la computadora) del sistema que normalmente utiliza el sistema operativo o el software antivirus para acceder a los recursos. Para poder ser encontrado suele cambiar el tamaño de los archivos o modificar la estructura de los directorios. Para detectar este tipo de virus se requiere que el software antivirus provoque al virus cuando se encuentra residente en memoria y luego de identificarlos eliminarlos lo más pronto posible.

- Virus multipartitas.

Este tipo de virus es el más difícil de detectar ya que combina las características anteriores y puede infectar tanto al sector de arranque como también archivos. Estos virus usan la técnica stealth, en combinación con la mutación y la encriptación.

- Virus invisibles

- Este tipo de virus intenta esconderse del Sistema Operativo mediante varias técnicas.
- Pueden modificar el tamaño del archivo infectado, para que no se note que se le ha añadido un virus.
- Pueden utilizar varias técnicas para que no se les pueda encontrar en la memoria del computador engañando a los antivirus.
- Normalmente utilizan la técnica de Stealth o Tunneling.

Tenemos entre los tipos de virus mas conocidos los siguientes:

- Caballo de Troya

Caballo de Troya es un programa maligno 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.

- Bomba Lógica

Se trata simplemente de un programa maligno que permanece oculto en memoria y que solo se activa cuando se produce una acción concreta, predeterminada por su creador: cuando se llega a una fecha en concreto (Viernes 13), cuando se ejecuta cierto programa o cierta combinación de teclas, etc.

- Gusano o Worm

Por último, un gusano en un programa cuya única finalidad es la de ir consumiendo la memoria del sistema, mediante la realización de copias sucesivas de sí mismo, hasta desbordar la RAM, siendo ésta su única acción maligna.

1.2. Proceso de Infección.

Hay que tener en cuenta que un virus es simplemente un programa. Por lo tanto, debemos de dejar a un lado las histerias y los miedos infundados y al mismos tiempo ser consientes del daño real que puede causarnos. Para ello, lo mejor es tener conocimiento de como funcionan y las medidas que debemos tomar para prevenirlos y hacerles frente. El virus puede estar en cualquier sitio. En ese disquete que nos deja un amigo, en el último archivo descargado de Internet.

Dependiendo del tipo de virus el proceso de infección varia sensiblemente. Puede que el disco contaminado tenga un virus de archivo en el archivo ARCHIVO.EXE por ejemplo. El usuario introduce el disco en la computadora (por supuesto no lo escanea con un antivirus o si lo hace es con un antivirus desfasado) y mira el contenido del disco... unos archivos de texto, unas .dll's, un .ini ... ah, ahí esta, un ejecutable. Vamos a ver que tiene. El usuario ejecuta el programa. En ese preciso momento las instrucciones del programa son leídas por el computadora y procesadas, pero también procesa otras

instrucciones que no deberían estar ahí. El virus comprueba si ya se ha instalado en la memoria. Si ve que todavía no está contaminada pasa a esta y puede que se quede residente en ella. A partir de ese momento todo programa que se ejecute será contaminado. El virus ejecutará todos los programas, pero después se copiará a sí mismo y se "pegará" al programa ejecutado "engordándolo" unos cuantos bytes. Para evitar que usuarios avanzados se den cuenta de la infección ocultan esos bytes de más para que parezca que siguen teniendo el mismo tamaño. El virus contaminará rápidamente los archivos de sistema, aquellos que están en uso en ese momento y que son los primeros en ejecutarse al arrancar la computadora. Así, cuando el usuario vuelva a arrancar la computadora el virus se volverá a cargar en la memoria cuando se ejecuten los archivos de arranque del sistema contaminados y tomará otra vez el control del mismo, contaminando todos los archivos que se encuentre a su paso.

Puede que el virus sea también de "Sector de arranque". En ese caso el código del virus se copiará en el primer sector del disco duro que la computadora lee al arrancar. Puede que sobrescriba el sector original o que se quede una copia del mismo para evitar ser detectado. Los virus de sector de arranque se aseguran de ser los primeros en entrar en el sistema, pero tienen un claro defecto. Si el usuario arranca la computadora con un disquete "limpio" el virus no podrá cargarse en memoria y no tendrá el control. Un caso menos probable es que el virus sea de "Tabla de partición". El mecanismo es muy parecido al de los de sector de arranque solo que el truco de arrancar con un disquete limpio no funciona con estos. En el peor de los casos nos encontraremos con un virus multipartita, que contaminará todo lo que pueda, archivos, sector de arranque...

- Síntomas de un equipo infectado

El Procedimiento de Detección de los virus informáticos debe garantizar que la posible existencia de un virus en un medio magnético u óptico no ingrese directamente al Sistema.

Para ello, el programa de detección de virus debe ser instalado en la memoria, a fin de que permanentemente se controle cualquier medio de almacenamiento que sea utilizado con el equipo de cómputo.

- Se consideran medios de infección por virus a los siguientes :
- De un diskette infectado proveniente de una fuente exterior al equipo de cómputo.
- A través de la adquisición o movimiento de máquinas infectadas en el centro de cómputo.
- A través de los diferentes tipos de comunicación entre equipos de cómputo.

Cuando un Sistema Operativo está infectado, se presenta cualquiera de los siguientes síntomas:

- El cargado de los programas toma más tiempo de lo normal.
- Demora excesiva en los accesos al disco, cuando se efectúan operaciones sencillas de escritura.
- Se producen inusuales mensajes de errores.
- Se encienden las luces de acceso a los dispositivos, cuando no son requeridos en ese momento.
- Disposición de menos memoria de lo normal.
- Desaparecen programas o archivos misteriosamente.
- Se reduce repentinamente el espacio del disco.
- Los archivos ejecutables cambian de tamaño.
- Aparecen, inexplicablemente, algunos archivos escondidos.
- Aparece en la pantalla una serie de caracteres especiales sin ninguna explicación lógica.
- Algunos comandos no pueden ser ejecutados, principalmente los archivos con extensión .COM y .EXE.
- A veces infectan primero el COMMAND.COM, pero como su función es la de seguir infectando éste continuará operando.

- La razón por la que ciertos ejecutables no pueden ser activados se debe a que simplemente el virus puede haberlos borrado.
- Los archivos ejecutables de los gestores de bases de datos como dBase, Clipper, FoxPro, etc., están operativos, sin embargo la estructura de los archivos DBF están averiados o cambiados. Lo mismo puede ocurrir con las hojas de cálculo como Lotus 1-2-3, Q-Pro, Excel, etc.

- El sistema empieza a ´colgarse´. Puede ser un virus con la orden de provocar reseteos aleatorios.
- Cierto periféricos tales como: la impresora, módem, tarjeta de sonido, entre otros no funcionan.
- El sistema no carga normalmente o se interrumpe en los procesos.
- Los archivos ejecutables seguirán existiendo pero como el código del virus está presente en la mayoría de los casos aumentará el tamaño de los archivos infectados.
- La pantalla muestra símbolos ASCII muy raros comúnmente conocidos como basura, se escuchan sonidos intermitentes, se producen bloqueos de ciertas teclas.

2. Los Antivirus Informáticos

Un antivirus es cualquier metodología, programa o sistema para prevenir la activación de los virus, su propagación y contagio dentro de un sistema y su inmediata eliminación y la reconstrucción de archivos o de áreas afectadas por los virus informáticos.

Los antivirus permiten la detección y eliminación de virus. Un virus es identificado mediante una cadena del antivirus que busca, encuentra y elimina los distintos virus informáticos.

El software antivirus contrarresta de varias maneras los efectos de los virus informáticos para detectarlos. La mayoría de las soluciones se basan en tres componentes para la detección: exploración de acceso, exploración requerida, y suma de comprobación.

La exploración de acceso: Inicia automáticamente una exploración de virus, cuando se accede a un archivo, es decir al introducir un disco, copiar archivos, ejecutar un programa, etc.

La exploración requerida: El usuario inicia la exploración de virus. Las exploraciones se pueden ejecutar inmediatamente, en un directorio o volumen determinado.

La suma de comprobación o comprobación de integridad: Método por el que un producto antivirus determina si se ha modificado un archivo. Como el código vírico se une físicamente a otro archivo, se puede determinar tal modificación guardando la información del archivo antes de la infección.

La suma de comprobación es generalmente exacta y no necesita actualizaciones. Sin embargo la suma de comprobación no proporciona ni el nombre, ni el tipo de virus.

Los programas antivirus se componen fundamentalmente de dos partes: un programa que rastrea (SCAN), si en los dispositivos de almacenamiento se encuentra alojado algún virus, y otro programa que desinfecta (CLEAN) a la computadora del virus detectado.

2.1 Tipos de antivirus

- **Antivirus Detectores o Rastreadores:** Son aquellos antivirus que usan técnicas de búsqueda y detección explorando o rastreando todo el sistema en busca de un virus. Estos programas se utilizan para detectar virus que pueden estar en la memoria, en el sector de arranque del disco duro, en la zona de partición del disco y en algunos programas. Dependiendo de la forma de analizar los archivos los podemos clasificar a su vez en antivirus de patrón y heurístico.

- **Antivirus de Patrón:** Realizan el análisis de los archivos por medio de la búsqueda en el archivo de una cualidad particular de los virus. Existen antivirus específicos para un determinado virus, conociendo su forma de atacar y actuar.
- **Antivirus Heurístico:** Este antivirus busca situaciones sospechosas en los programas, simulando la ejecución y observando el comportamiento del programa.
- **Limpiadores o Eliminadores:** Una vez desactivada la estructura del virus procede a eliminar o erradicar el virus de un archivo, del sector de arranque de un disco, en la zona de partición de un disco y en algunos programas.

Estos antivirus deben tener una base de datos con información de cada virus para saber que método de desinfección deben usar para eliminar el virus.

Dependiendo de los efectos de la especie viral procederá a reconstruir las partes afectadas por el virus informático.

- **Protectores o Inmunizadores:** Es un programa para prevenir la contaminación de virus, estos programas no son muy usados porque utilizan mucha memoria y disminuyen la velocidad de la ejecución de algunos programas y hasta del computador.
- **Residentes**: Permanecen en memoria para el reconocimiento de un virus desde que es ejecutado. Cada vez que cargamos un programa, el antivirus lo analiza para verificar si el archivo esta infectado o no, con algún virus informático.