Universidad Católica Nuestra Señora de la Asunción.
Facultad de Ciencias y Tecnología.
Ingeniería Informática

TRABAJO PRACTICO DE TAI 2

Virus Informáticos

Alumnos:

- Christian Daniel von Lücken M.
- Miguel Angel Willigs.

30-09-2000

Introducción.

Definición.

Biológicamente, los virus son formas de vida que contienen fragmentos minúsculos de código genético (ADN o ARN) que pueden tomar el control de la organización de una célula viva y trucarla para hacer miles de réplicas impecables del virus original. De forma similar los virus informáticos están formados por una secuencia o conjunto de secuencias de código de máquina o de un lenguaje de programación que copia su código en otros programas cuando se activa provocando una infección. Cuando el programa infectado se ejecuta, el código entra en funcionamiento y el virus sigue extendiendose.

Podemos definir un virus informático como un **programa** capaz de **autorreplicarse** mediante la infección de otros programas, que intenta permanecer **oculto** en el sistema hasta darse a conocer, momento en el cual produce **o provoca daños**, problemas o molestias al sistema informático y, por ende, al usuario.

Similitud con los virus biológicos.

Existe cierta notoria similitud entre los virus informáticos y los biológicos, siempre manteniendo las distancias entre el mundo virtual y el mundo real, y en cierto modo, se puede pensar que los virus informáticos son una emulación de los virus biológicos en el mundo virtual. Hay una serie de características de los virus informáticos que también los asemejan a los virus biológicos: su escaso tamaño con respecto al sistema que infectan, su capacidad de "mutación" (en algunos virus) e incluso su extinción cuando se les somete a un agente externo hostil (como puede ser un programa antivirus).

Origen.

Los virus informáticos se originaron partiendo de una investigación científica relativa a los conceptos de inteligencia artificial y vida artificial, por lo que en sus comienzos, tuvieron un carácter de investigación científica, y hasta el momento en que alguien decidió usar la idea para causar, deliberadamente, daños en sistemas informáticos, no eran más que meros experimentos universitarios, y de hecho, la mayoría de sus creadores son estudiantes de informática deseosos de probar su destreza, acerca de estos, los creadores, [GOR94] presenta un estudio de cuatro clases de individuos envueltos en la construcción de virus, su comportamiento, conocimientos, etc, asi como cuestiones éticas y morales relativas.

¿Qué es y qué no es un virus informático?.

Con el objeto de distinguir lo que es y lo que no es un virus informático, es conveniente analizar las cuatro caracteristicas que definen un virus:

- Los virus son **programas**, y al igual que todos los programas han sido programados usando una secuencia de código y cumple una función para el cuál ha sido diseñado, ahora, la forma, los fines y su modo de operación difiere por completo de los programas que los usuarios de informática utilizamos habitualmente.

- Son **autorreplicanes**: es decir una de sus cualidades es la de poder clonarse, crear copias, ya sean identicas o evolucionadas, de sí mismos y reproducirse dentro del sistema o sistemas informáticos en los cuales operan. Un tiempo atrás, antes de que existan los virus informáticos, existían los llamados worms o gusanos, cuya única función era reproducirse y extenderse a lo largo y ancho de los sistemas informáticos de una red para, eventualmente, ralentizarla al concurrir la acción de replicación con la ejecución de otras tareas del sistema, el fin nocivo de estos era

debido a su propia capacidad de autoreplicación. Por otro lado los gusanos no son cosa del pasado, ya que su técnica se utiliza aún y con notable éxito gracias a la Internet. El famoso incidente Morris es un ejemplo de ataque con worms, una descripción sobre tal incidente se encuentra en [TA 92] , y una descripción exaustiva en [SPA89]. Las formas en que los virus llevan a cabo su reproducción son diversas y han evolucionado con los años. La difencia entre los gusanos y los virus radica en que un virus está a cuesta de programa existente y a partir de allí se disemina, mientras que un gusano es un programa completo en sí mismo cuya función es diseminarse.

- Permanece **oculto** en el sistema hasta el momento de su explosión, los virus intentan pasar desapercibidos en el sistema hasta que llevan a cabo la acción para la cual han sido programados, y aún en este caso (algunos) intentan ocultar el daño causado hasta el último momento.

- Provoca **daños**: esta es una cuestión discutible pues hay virus que no provocan daño alguno al sistema y que han sido creados con el mero fin de experimientar y no son en absoluto destructivos, lo cierto es que dañinos o no se introducen en nuestro sistema contra nuestra voluntad, alteran de una forma u otra el sistema aunque sea tan sólo modificando mínimamente el tamaño de un archivo, y por esa razón ya puede ser calificado como molesto.

Los daños que pueden provocar los virus informáticos varian enormemente. Desde el daño mínimo que comentamos que no pasa de una mera molestia, hasta el borrado de la Flash-BIOS y de los datos del disco duro.

Naturaleza de los virus.

Debemos hacer notar que para que un virus sea virus debe cumplir los cuatro requisitos expuestos anteriormente, y diversas amenazas de hoy día aunque comparten sus mismas cualidades no podemos calificar como virus informático, como los Caballos de Troya, los gusanos, la bombas lógicas, etc...; en ciertos casos es difícil determinar el tipo del agente infector, es el caso, por ejemplo, de Win32.Sk.A (Happy99), del cual sepuede encontrar una discusión técnica sobre si es un virus, un gusano o un troyano en [Geo1] los virus y amenazas afines son catalogadas como ***malware*** [STA92], o código malicioso, código escrito malintencionadamente o programas que se aprovechan de los defectos de programación de otras aplicaciones para causar daños en el sistema.

Por otro lado, se debe estar alerta ante toda una serie de mitos y leyendas generadas en torno a los virus y que siembran desinformación entre los usuarios, este es el caso de los llamados hoaxes – mensajes que vienen difundiendose por internet que amenazan con provocar daños, por lo que se insta al usuario a difundir la advertencia – hoy popularizados mediante mensajes de correo que alertan sobre virus y peligros inexistentes, pero que también siembran la preocupación entre aquellos usuarios menos informados en torno a estas cuestiones.

Tenemos que tener presente en todo momento que un virus puede hacer cualquier cosa que hagan los programas y que la única diferencia es que se engancha a otro programa, se ejecuta de forma oculta cada vez que se ejecuta el programa anfitrión, y posee algún metódo de modo que se autopropague.

Durante su vida, un virus típico pasa por las siguientes cuatro etapas:

1- Una fase **latente**, en la que el virus está inactivo. El virus será finalmente activado por algún suceso, como una fecha, la presencia de otro programa o

archivo o que la capacidad del disco exceda de cierto límite. No todos los virus pasan por esta etapa.

2- Una fase de **propagación**, durante la cual el virus sitúa una copia idéntica suya en otros programas o en ciertas zonas del sistema del disco. Cada programa infectado contendrá ahora un clón del virus, que entrará a su vez en la fase de propagación.

3- La fase de **activación**, en la que el virus se activa para llevar a cabo la función para la que está propuesto. Como en la fase latente, la fase de activación puede ser causada por una variedad de sucesos del sistema, incluyendo la cuenta del número de veces que esta copia del virus ha hecho copias de sí mismo.

4- La fase de ejecución, en la que se lleva a cabo la función. Como dijimos, la función puede ser no dañina, como dar un mensaje por la pantalla, o dañina, como la destrucción de los archivos de programas y datos.

La mayoría de los virus llevan a cabo su trabajo de manera específica para un sistema operativo concreto y, en algunos casos, específicamente para una plataforma de hardware en particular. Así pues, están diseñados para sacar partido de los detalles y las debilidades de los sistemas concretos.

Historia de los virus.

Los primeros virus aparecieron en 1986, el primer virus se llamó Brain, de origen paquistaní, un virus que infectaba los diskettes de 5,25 pulgadas, sobreescribia el sector de arranque y desplazaba el sector de arranque original a otra posición del disco, el virus apenas provocabaa daños, pero llamó la atención por su capacidad de ocultamiento, fue descubierto recién en 1987. En el mismo año apareció Virdem, que estaba preparado para generar copías de sí mismo en otros archivos.

En 1987 aparece Charlie (Vienna), cuyo código se publico en un libro, lo que provocó muchas variantes, en el mismo año apareciño Lehigh, virus que tenia un contador, y cada cuatro archivos sobreescribia el contenido de un diskette al azar, causando los primeros daños constatados por un virus.

También encontramos Viernes 13 o Jerusalén, primer virus residente en memoria que permanecía latente hasta la fecha de su activación para a continuación borrar los archivos infectados.

Stoned fue el primer virus de arranque. Sus efectos eran sencillos: una vez cada ocho arranques con un disco infectado, aparecía el mensaje “Your PC is now Stoned”, este dio origen al famosisimo Michelangelo, cuyos efectos fueron magnificados por la prensa hasta que se convirtió en una plaga inexistente.

En 1988 se tuvo el primer gran aviso de lo que podía llegar a provocar un virus descontrrolado y marcó el comienzo de la guerra contra los virus con el nacimiento de los primeros programas antivirus informáticos, el 2 de noviembre de 1988, se liberó un progama gusano en Internet, que produjo fallas en cientos de computadoras en universidades, corporaciones y laboratorios de gobiernos en todo el mundo antes de que fuera rastreado y eliminado, lo que hizo que internet, por quel entonces Arpanet colapsara, el creador del gusano, Robert Morris, fue capturado, juzgago siendo declarado culpable de un delito informático, lo cual lo convirtió en el primer condenado por la recientemente aprobada ley de fraudes informáticos de 1986.

El año 1988 trajo consigo la concientización, por parte de la industria informática, de la necesidad de defenderse contra los virus y amenazas afines. Era el comienzo de la industria antivirus. Uno de los primeros antivirus se llamaba Flu Shot (“Inyección opara la gripe”) y fue creado por un programador norteamericano en Nueva York; Ross Greenberg. El surgimiento de la industria antivirus provocó el nacimiento de la CVIA (Computer Virus Industry Association).

A finales de 1988 ocurrieron tres hechos importantes, que condujeron a esta concientización: la infección de una importante institución financiera por Jerusalem, la organización del primer seminario dedicado a los virus y el primer gran circo mediatico debido al Viernes 13, ya que, el 13 de enero de 1989 era viernes, y la prensa convirtió los avisos de las casas antivirus en un autentico espectaculo, algo que se volvió ahora habitual.

En 1989 apareció el primer antivirus heurístico, capaz de detectar, no sólo los virus que ya eran conocidos, sino aquellos virus que surgieran en el futuro y que reprodujesen patrones sospechosos. La heurística monitoriza la actividad del ordenador hasta el momento en que encuentra algo que puede ser dentificado con un virus, esto dio lugar, durante la década del 90 y hasta ahora, a nuevas tecnicas de ocultamiento, lo que a su vez provocó nuevas técnicas de detección. Además aparecieron losprimeros kits para la construcción de virus, lo que facilitaba la creación de virus y el aumento del número a mayor velocidad. El primero de ellos fue el VCL (Virus Creation Laboratory), creado por Nowhere Man, y más tarde apareció el Phalcom/Skism Mass-Produced Code Generator, de Dark Angel. Estos kits facilitan la

tarea de crear virus por cualquier usuario de ordenador mediante experimentación, así en pocos meses surgieron docenas de virus creados de esta forma, incluso en el primer semestre de 1994, el VCL fue utilizado en el LED, para crear varios virus que dejaron fuera al laboratorio unas semanas.

Si antes de Internet la difusión de los virus era importante, con la llegada de Internet en el transcurso de los años 90 la cantidad de virus en circulación se ha disparado, existiendo en la actualidad más de 40.000 virus circulando. El correo electrónico es probablemente la via principal para la difusión de virus. Además del correo, otras vias para la entrada de virus son, la descarga de programas infectados, el IRC, el ICQ (programa de mensajería instantánea con graves fallos de seguridad), o incluso la propia navegación por paginas web puede introducir virus en nuestras máquinas, debido a los recientes virus de HTML, java o de controles ActiveX.

Los virus producen un perjuicio enorme, que en terminos monetarios, según Computer Economics [ComE], en 1998 fue de unos 1500 millones y la misma consultora determino que el impacto total del ataque de los virus en 1999 causaron perdidas de $12.100 millones, que derivan de gastos por pérdidas en productividad y costos de reparación, por lo que no es de extrañar que se realicen notables esfuerzos en proteger a los sistemas, hoy día hay antivirus de actualización diaria, servicios técnicos enormemente eficientes para crear vacunas contra nuevas amenazas en pocas horas, lo que convierte a los virus en un gran negocio.

Estructura de los virus.

Un virus puede añadirse por delante o por detrás de un programa ejecutable o bien puede incrustarse de algún modo. La clave para su funcionamiento es que el programa infectado, cuando se le invoque, ejecute primero el código del virus y, después, el código original.

Un virus muy sencillo en lenguaje ensamblador que no haga más que infectar programas podría hacer algo como lo siguiente:

1. Encontrar la primera instrucción de programa.
2. Sustituirla por un salto a la posición de memoria siguiente a la última instrucción del programa.
3. Insertar una copia del código del virus en dicha posición.
4. Hacer que el virus simule la instrucción sustituida por el salto.
5. Saltar de vuelta a la segunda instrucción del programa anfitrión.
6. Terminar la ejecución del programa anfitrión.

Un virus como el descrito es fácil de detectar porque la versión infectada del programa es mayor que la correspondiente no infectada. Una forma de frustrar un medio tan sencillo de detectar el virus es comprimir el archivo ejecutable de forma que tanto la versión infectada como la no infectada sean de longitud idéntica. Para ver la lógica de infección consideremos el siguiente ejemplo, donde se supone que el programa P1 está infectado con el virus CV, cuando este programa sea invocado, el control pasa a su virus, que efectúa los pasos siguientes:

1. Para cada archivo no infectado P2 que se encuentre, el virus comprime primero el archivo para generar P2', reduciendo el programa original en el tamaño del virus.
2. Se añade una copia del virus por delante del programa comprimido.
3. Se descomprime la versión comprimida del programa original infectado P1'.
4. Se ejecuta el programa original descomprimido.

En este ejemplo, el virus no hace otra cosa que propagarse. Como en el ejemplo anterior, el virus puede incorporar una bomba lógica.

Infección inicial.

Una vez que un virus ha tenido acceso a un sistema por la infección de un solo programa, está en posición de infectar algunos o todos los archivos ejecutables del sistema, cundo se ejecute el programa infectado. Así pues la infección vírica puede ser prevenida por completo impidiendo que el virus entre por primera vez. Por desgracia, la prevención es extremadamente difícil porque un virus puede formar parte de cualquier programa exterior a un sistema. Así pues, a menos que uno se conforme con tomar un pedazo de acero en bruto y escribir su propio sistema y todos los programas de aplicación, es vulnerable.

Sólo una pequeña parte de las infecciones tienen comienzo a través de conexiones de red. La mayoría de ellas se obtienen a través de la descarga de archivos, un juego, un crack, o cualquier utilidad aparentemente útil.

En resumen los medios usados por un virus para llevar a cabo la infección son los siguientes:

- Unidades de disco extraíbles: las unidades de disco son aquellos medios de almacenamiento en los que se guarda información, mediante documentos o archivos. Con ellos se puede trabajar en una computadora para, posteriormente, utilizarlos en otro diferente. Algunos de estos medios de

almacenamiento pueden ser los disquetes, CD-ROMs, unidades Zip y Unidades Jazz. Estos dos últimos tipos no son más que unos discos especiales con mayor capacidad que los disquetes. Si alguno de ellos se encontrase infectado y trabajásemos con él en una computadora, ésta será infectada.

- Redes de computadoras: una red es un conjunto o sistema de computadoras conectados entre sí físicamente, para facilitar el trabajo de varios usuarios. Esto quiere decir que existen conexiones entre cualquiera de las computadoras que forman parte de la red, pudiendo transferirse información entre ellos. Si alguna de esta información transmitida de un ordenador a otro estuviese infectada, el ordenador en el que se recibe será infectado.

- Internet: cada día más se utilizan las posibilidades que brinda Internet para obtener información, realizar envíos y recepciones de archivos, recibir y publicar noticias, o descargar archivos. Todas estas operaciones se basan en la transferencia de información, así como en la conexión de diferentes computadoras en cualquier parte del mundo. Por tanto, cualquier virus puede introducirse en nuestro ordenador al mismo tiempo que la información recibida. A través de Internet la infección podría realizarse empleando diferentes caminos como los siguientes:
    - **Correo electrónico:** en un mensaje enviado o recibido se pueden incluir documentos o archivos (archivo adjunto o anexado o atacheado). Estos archivos podrían estar infectados, contagiando a la computadora destinataria.
    - **Páginas Web:** las páginas que visitamos en Internet son archivos de texto o imágenes escritos en un lenguaje denominado HTML. No obstante también pueden contener programas denominados Controles ActiveX y Applets de Java que son programas. Estos sí pueden estar infectados y podrían infectar al usuario que se encuentre visitando esa página.
    - **Descarga de archivos (FTP):** el término FTP significa File Transfer Protocol, es decir, Protocolo de Transferencia de Archivos. Mediante él se pueden colocar documentos en computadoras que se encuentran en cualquier parte del mundo o copiar archivos de estas computadoras al nuestro (bajar archivos o download). Estos archivos pueden contener virus que infectarán nuestra computadora.
    - **Grupos de noticias:** mediante las denominadas "News" es posible debatir sobre un determinado tema con cualquier otra persona del mundo y recibir correo electrónico con nuevas noticias sobre ese tema. Estos mensajes con noticias pueden tener documentación adjunta infectada que permita la introducción de virus en nuestro ordenador.

Tipos de virus.

Como hemos dicho anteriormente, desde que los virus aparecieron por primera vez, se ha producido una carrera de armamento entre los escritores de virus y los escritores de software antivirus. A medida que se han desarrollado contramedidas eficaces para los tipos de virus existentes, se han desarrollado nuevos tipos. [STEP93] propone las siguientes categorías de entre los tipos de virus más significativos:

- **Virus parásitos**: La forma más tradicional y, todavía, más común de virus. Un virus parásito se engancha a archivos ejecutables y se reproduce, al ejecutar el programa infectado, buscando otros archivos ejecutables que infectar.
- **Virus residentes en memoria**: Se alojan en la memoria principal como parte de un programa del sistema residente. Desde ese momento, el virus infecta todos los programas que se ejecutan.
- **Virus del sector de arranque**: Infecta el sector principal de arranque o el sector de arranque y se propaga cuando el sistema se arranca desde el disco que contiene el virus.
- **Virus clandestino:** Una forma de virus diseñado explícitamente para esconderse de la detección por software antivirus.
- **Virus polimorfo**: un virus que muta con cada infección, haciendo que la detección por la "firma" del virus sea imposible.

Un ejemplo de virus clandestino es el discutido antes: un virus que utiliza compresión para que el programa infectado tenga exactamente la misma longitud que una versión no infectada. Son posibles técnicas mucho más sofisticadas. Por ejemplo, un virus puede poner alguna lógica de intercepción en las rutinas de E/S con el disco, de modo que cuando haya un intento de leer partes sospechosas del disco con estas rutinas, el virus presente el programa original no infectado. Así pues, el término clandestino no se aplica a los virus como tales sino, más bien, es una técnica empleada por los virus para evitar se detección.

Un virus polimorfo crea copias durante la reproducción que son funcionalmente equivalentes pero que tienen diferentes patrones de bits. Como con los virus clandestinos, la finalidad es vencer a los programas que buscan virus. En tal caso, la "firma" del virus varía con cada copia. Para lograr esta variación, el virus puede insertar aleatoriamente instrucciones superfluas o intercambiar el orden de las instrucciones independientes. Un método más eficaz es usar técnicas de cifrado. Una parte del virus, generalmente llamada motor de mutación, crea una clave de cifrado aleatoria para cifrar el resto del virus. Dicha clave es almacenada junto con el virus y el motor de mutación es modificado. Cuando se invoca a un programa infectado, el virus utiliza la clave aleatoria almacenada para descifrar el virus. Cuando el virus se reproduce, se escoge una clave aleatoria diferente.

Otra arma del armamento de los escritores de virus es un juego de utilidades para la creación de virus, los kits que hemos comentado antes. Dicho juego permite que un novato cree rápidamente una serie de virus diferentes. Aunque los virus creados con estas utilidades tienden a ser menos sofisticados que los virus diseñados desde cero, el número absoluto de nuevos virus que pueden generarse crea un problema par los procedimientos antivirus. Otra herramienta más del escritor de virus es el tablero de noticias para intercambio de virus. Una serie de estos se pueden encontrar en Internet. En estos se ofrecen copias de virus que pueden traerse por la red, así como consejos para la creación de virus.

Entre las múltiples clasificaciones de virus que existen una muy común es la clasificación de virus según el tipo de archivo o aplicación que infectan, así tenemos los famosísimos virus de macros MS-Word, de rtf, Excel, etc. De los que hablaremos más adelante, otra clasificación común es según familias de virus, donde a partir de un

primer virus se puede construir una familia según las nuevas versiones o evoluciones del mismo.

Métodos antivirus.

La solución ideal para la amenaza de los virus es la prevención: en primer lugar no permitir que los virus entren en el sistema. Esta meta es, en general, imposible de alcanzar, aunque la prevención puede reducir el número de ataques víricos fructuosos. El siguiente mejor método es ser capaz de hacer lo siguiente:

- Detección: Una vez que se ha producido la infección, determinar que ha tenido lugar y localizar el virus.

- Identificación: una vez que se ha logrado la detección, identificar el virus específico que ha infectado el programa. Eliminar el virus de todos los sistemas infectados, de forma que la plaga no pueda extenderse más.

- Eliminación: una vez que se ha identificado el virus específico, eliminar todo rastro del virus de los programas infectado y reponerlo a su estado original.

Si la detección tiene éxito, pero la identificación o la eliminación no son posibles, la alternativa es descartar el programa infectado y reponerlo a su estado original.

Los avances de la tecnología de virus y antivirus van de la mano. Los primeros virus eran trozos de código relativamente simple y podían identificarse y liquidarse con paquetes antivirus relativamente sencillos. A medida que la carrera de armamentos de los virus ha avanzado, tanto los virus como, necesariamente, los antivirus han crecido en complejidad y sofisticación. [STEP93] identifica cuatro generaciones de software antivirus:

- Primera generación: rastreadores simples.
- Segunda generación: rastreadores heurísticos.
- Tercera generación: trampas de actividad.
- Cuarta generación: protección completa.

Un rastreador de primera generación requiere una firma del virus para identificarlo. El virus puede contener comodines, pero tiene básicamente la misma estructura y patrón de bits en todas las copias. Dichos rastreadores de firmas específicas están limitados a la detección de virus conocidos. Otro tipo de rastreadores de primera generación mantiene un registro de la longitud de los programas y buscan cambios en la longitud.

Un rastreador de segunda generación no depende de una firma especifica. Más bien, el rastreador emplea reglas heurísticas para buscar infecciones probables por virus. Un tipo de tales rastreadores busca trozos de código que suelen estar asociados con virus. Por ejemplo, un rastreador puede buscar el comienzo de un bucle de cifrado empleado por un virus polimorfo y descubrir la clave de cifrado. Una vez que se ha descubierto la clave, el rastreador puede descifrar el virus para identificarlo, eliminar entonces la infección y volver a poner el programa en servicio.

Otro método de segunda generación es la prueba de integridad. Se puede añadir un código de prueba (checksum) a cada programa. Si un virus infecta el programa sin cambiar el código de prueba de integridad detectará el cambio. Para contrarrestar un virus suficientemente sofisticado, como para cambiar el código de prueba cuando infecta a un programa, se puede emplear una función de dispersión (hash) cifrada. La clave de cifrado se almacena por separado del programa, de forma que el virus no

pueda generar un nuevo código de dispersión y cifrarlo. Utilizando una función de dispersión en vez de un sencillo código de prueba, se impide que el virus prepare el programa para producir el mismo código de dispersión que antes.

Los programas de tercera generación son programas residentes en memoria que identifican un virus por sus acciones más que por la estructura de un programa infectado. Dichos programas tienen la ventaja de que no hace falta construir firma y heurísticas para una amplia muestra de virus. Más bien, sólo es necesario identificar el pequeño conjunto de acciones que indican que se está intentando una infección y, en tal caso, intervenir.

Los productos de cuarta generación son paquetes que constan de una variedad de técnicas antivirus utilizadas en conjunto. Estos programas antivirus incorporan varias medidas de búsqueda de virus y protección más avanzadas como las siguientes:

- ***Búsqueda de cadenas:*** cada uno de los virus contiene determinadas cadenas de caracteres que le identifican. Estas son las denominadas firmas del virus. Los programas antivirus incorporan un archivo denominado "archivo de firmas de virus" en el que guardan todas las cadenas correspondientes a cada uno de los virus que detecta. De esta forma, para encontrarlos, se analizarán todos los archivos especificados comprobando si alguno de ellos las contiene. Si un archivo no contiene ninguna de estas cadenas, se considera limpio, mientras que si el programa antivirus la detecta en el interior del archivo avisará acerca de la posibilidad de que éste se encuentre infectado.

- ***Excepciones:*** una alternativa a la búsqueda de cadenas es la búsqueda de excepciones. Cuando un virus utiliza una determinada cadena para realizar una infección pero en la siguiente emplea otra distinta, es difícil detectarlo mediante la búsqueda de cadenas. En ese caso lo que el programa antivirus consigue es realizar la búsqueda concreta de un determinado virus.

- ***Análisis heurístico:*** cuando no existe información que permita la detección de un nuevo o posible virus desconocido, se utiliza esta técnica. Se caracteriza por analizar los archivos obteniendo información sobre cada uno de ellos (tamaño, fecha y hora de creación, posibilidad de colocarse en memoria,...etc.). Esta información es contrastada por el programa antivirus, quien decide si puede tratarse de un virus, o no.

- ***Protección permanente:*** durante todo el tiempo que el ordenador permanezca encendido, el programa antivirus se encargará de analizar todos los archivos implicados en determinadas operaciones. Cuando éstos se copian, se abren, se cierran, se ejecutan,...etc., el antivirus los analiza. En caso de haberse detectado un virus se muestra un aviso en el que se permiten la desinfección. Si no se encuentra nada extraño, el proceso recién analizado continúa.

- ***Vacunación:*** mediante esta técnica, el programa antivirus almacena información sobre cada uno de los archivos. En caso de haberse detectado algún cambio entre la información guardada y la información actual del archivo, el antivirus avisa de lo ocurrido. Existen dos tipos de vacunaciones: Interna (la información se guarda dentro del propio archivo, de tal forma que al ejecutarse él mismo comprueba sí ha sufrido algún cambio) y Externa (la información que guarda en un archivo especial y desde él se contrasta la información).

La carrera entre creadores de virus y antivirus continúa. Como vemos en los paquetes de cuarta generación se emplea una estrategia de defensa más completa, ampliando el alcance de la defensa a más medidas generales de seguridad en los computadoras.

Virus de macro de Word, Excel, etc.

Las macros son secuencias automatizadas de comando,que sirven para llevar a cabo en varias acciones con un mínimo de teclas que oprimir, que con el tiempo fueon creciendo en complejidad hasta que llegaron a ser pequeños archios ejecutables capaces de llevar a cabo tareas complejas,Microsoft incluyo en Office 4.2 nuevas posibilidades a las macros ya que podían ser programasdos en un lenguaje de programación llamado Word Basic, está provocó la aparición casi inmediata del primer virus de macro (Concept).

No todos los programas con posibilidades de creación de macros pueden ser objetos de ataque mediante virus de este tipo, los programas deben cumplir con las siguientes características: las macros deben poder ser incluidas en un documento concreto, debe poder ser posible copiarse macros de un archivo a otro de la misma aplicación, deben poder ejecutarse en forma automática sin intervención de los usuarios al abrir el documento. Los programas de este tipo que han sido objeto de los creadores de virus incluyen: Word, Access, Excel, PowerPoint y Corel Draw.

Los virus de macro son fáciles de generar, la mayoría de las macros son un subconjunto del BASIC, el daño que pueden causar esta dado por la capacidad de las macros de llamar a subrutinas externas por ejemplo funciones de una dll de Windows, lo que permite a los virus de macro realizar prácticamente cualquier operación, la característica más novedosa de estos es su independencia de sistema operativo, un virus de macro para un programa x funciona en cualquier plataforma donde haya una versión de x.

Las actividades comunes que llevan a cabo los virus de macro son:

- Infectar la máquina con un virus convencional.
- Borrado de archivos.
- Copia de documentos personales a lugares públicos.
- Envío de archivos desde el disco duro a una dirección de correo Internet.
- Formateo del disco duro.

Ahora vamos a explicar como funcionan los virus de macro para Microsoft Word, para ver conun ejemplo como es que funcionan estos virus.

Microsoft Word utiliza un lenguaje para macros llamado Visual basic for Aplications y además soporta una serie de macros automáticos, si un documento contiene una o más macros con un nombre específico, Word las ejecuta automáticamente cunado ocurran determinados eventos. Por ejemplo, vamos a ver los macros automáticos para Word y cuándo se ejecutan:

- AutoExec: éste tipo de macro se ejecuta automáticamente cada vez que se inicia Word.
- Auto New. Se ejecuta siempe que se creaa un documento nuevo.
- AutoOpen: siempre que se abre undocumento Word comprueba la existencia de macros del tipo AutoOpen y los ejecuta.
- AutoClose: Igual que el anteriior, aunque en éste caso lleva a cabo la ejecución de los macros al cerrar el documento.

Como se puede suponer basta suministrar un documento que contenga una macro llamada Autoopen para poder tomar el control cuando Word abre el citado documento. Una vez tomado el control, la macro puede replicarse en otros documentos, borrar archivos, etc.

Sucede que mientras en verisones anteriores de word las macros se guardaban en las famosas .dot, lo que dificultaba la extensión de los virus ya que se debían cambiar de .doc a .dot en word 97b y 2000 esto ya no es así, lo cual facilita aún más la labor de los virus de macro.

Algunos ejemplos de estos virus son:

- **Ethan**: que aparecio en enero de 1999, consta de una única macro que se copia en normal.dot, así como en los documentos que se infectan. Para realizarla infección el virus genera un archivo de nombre c:\ethan._. Este archivo se crea con el atributo oculto, el virus se activa de manera aleatoria, tres de cada diez veces el virus cambia las propiedades del documento, modifica el título por el de "ethan From", el autor por "EW/LN/CB" y la compañía por "foo Bar industries, Inc".

- **Bandung.A**: es originario de indonesia, infecta la plantilla normal.dot cuando un documento infectado es abierto, el resto de lo sdocumentos serán infectados con Filesaave o Filesaveas. Su efecto destructivo se activa al abrir Word, el viru chequea la hora y fecha, en caso de que sea mayor al 19 del mes y la hora despues de las 11, el virus borra los archivos de todos los directorios salvo c:\Windows, c:\Winword y c:\Windword6 y creaun archivo c:\pesan.txt con un mensaje.

- **Melissa y familia**: este ha tenido enorme impacto económico, de alli el interes, un analisis sobre el perjuicio economico del mismo se puede encontrar en [ComE], el 26 de marzo de 1999, aparecio melissa en algunos grupos de noticias en inernet, el virus de macro iba incluido en un archivo de Word llamado melissa y fue distribuído inicialmente en el grupo alt.sex dentro de un archivo llamado List.doc, que supuestamente contenia una lista de con claves para acceder a lugares reservados de internet. El virus actuaba de la siguiente forma:cuando el usuario llevaba a cabo la apertura del archivo se ejecutaba automáticamente el virus de macro. Lo primero que hacia el virus era abrir el programa Outlook, seleccionarlos primeros 50 nombres de la libreta de direcciones, y enviar a cada una de estas personas 50 mensajes con documentos con el siguiente asunto: "here is that document you ask for.Don't show anyone else", el subject común, más el hecho de que el mensaje era enviado por un conocido, facilito su extensión, despues de autoenviarse el virus continuaba infectando otros documebtos del usuario si las conçdiciones le son favorables. El código maligno se activa se al ejecutarse coinciden los minutos de la hora con el día del mes, por ejemplo. El día 29 a las 10:29h. En ese momento el virus inserta la siguiente frase en el documento que le usuario tenga abierto u otro que abra en ese minuto:
  "Twenty-two point, plus triple-word-score, plus fifty points for using all my letters. Game's over. I'm outta here".

  El virus apareció un viernes y para el lunes a causa del virus los servidores de las compañias infectadas se ralentizaron, incluso Microsoft llego a cerrar su servidor de correo para minimizar la propagación del código maligno, cuando la gente empezo a enviar cientos de documentos de word vía mail, aunque su carga maligna era mínima, dio origen a otros como el Explore.Zip, Freelinks o el Papa.

- W97M/CHANTAL.A (CHANTAL.A) pertenece a al familia W97M, que realiza sus infecciones en documentos de Microsoft Word 97/2000 y la plantilla global **NORMAL.DOT** que éste utiliza. Por tratarse de un virus de macro las infecciones se realizarán mediante documentos de Word que tengan asociada alguna. No obstante, W97M/Chantal.A puede infectar también documentos que no las tengan. Es un virus escrito en Visual Basic que produce efectos destructivos, a modo de payload. Cuando uno de los documentos infectado se abre, el virus desactiva la protección antivirus que Word tiene prevista con relación a las macros

e impide cualquiera de éstas, ya sea para su modificación, como para su creación. W97M/Chantal.A tiene como objetivo la infección de todos los archivos que se encuentren en el directorio raíz del disco duro. Pero sin duda, el payload más importante es el que realiza cuando llega la fecha del año 2000, y de hecho esto fue así. Cuando detecta que el reloj del sistema tiene ese año, automáticamente elimina todos los archivos que se encuentren en el directorio actual y en el directorio raíz del disco duro (C:\), presentando un mensaje. Además, todos los días que sean 31 y se esté trabajando en Microsoft Word, ejecuta el asistente para la ayuda que éste contiene. La forma que emplea para extenderse suele ser la habitual de la mayoría de los virus: disquetes, CD-ROM, red, Internet, archivos adjuntos o incluidos en mensajes de correo electrónico, FTP,... etc. El virus realiza dos payloads conocidos. Uno de ellos cuando detecta que se ha llegado al año 2000 y el otro todos los días 31 de cada mes. Mediante el primero de ellos, el más dañino sin comparación, borra todos los archivos que se encuentren en el directorio raíz del disco duro y, además, también todos aquellos que se encuentren en el directorio actual, es decir, en el que se encuentra el usuario en ese instante. Una vez ha terminado de eliminarlos, presenta el siguiente mensaje por pantalla: "*Chantal 4ever !*". El otro payload es molesto pero no perjudicial ya que simplemente muestra el típico mensaje propio del asistente on-line que Word tiene para mostrar ayuda o facilitar alguna tarea. En este caso dicho asistente mostrará sólo un cuadro con texto indicando que se realizó la infección. Estos cuadros son de color amarillo y además de contener el texto que presenta el virus, tienen un botón (más bien un check) que permite ser pulsado para retirar en mensaje. Adicionalmente, cuando la infección ya se ha llevado a acabo, el virus impide las precauciones de seguridad antivirus que Word tiene prefijadas con relación a las macros. En este sentido W97M/Chantal.A hace imposible que Word presente el cuadro de diálogo mediante el cual se pide al usuario si desea abrir un documento que contiene macros habilitándolas, o no. Cuando se pretenda abrir un documento que contiene macros, éstas simplemente serán activadas. De la misma forma, el virus se encargará de impedir el acceso a las opciones que permiten la manipulación de macros. Por ello será imposible el acceso a cualquiera de las opciones accesibles a través de: Herramientas - Macro. Esto significa que no se podrán crear nuevas macros (Grabar nueva macro), no se podrán eliminar o modificar las ya existentes (Macros) o no se podrá trabajar con el Editor de Visual Basic. Tampoco se permite la activación de cualquiera de las opciones anteriormente comentadas, mediante las combinaciones de teclas asociadas (*Alt+F8* y *Alt+F11*) El método de infección es el siguiente en primer lugar copia o crea el archivo de proceso por lotes CB2.BAT en el directorio raíz del disco duro (C:\) y modifica la línea final del archivo AUTOEXEC.BAT para que éste ejecute el archivo que se acaba de crear en el directorio raíz. Recordemos que el archivo AUTOEXEC.BAT se ejecuta siempre que arranca el ordenador, con lo cual siempre que éste se encienda (si no conseguimos detener su ejecución o controlarla) el archivo CB2.BAT será finalmente ejecutado. Con ello consigue la infección de todos los archivos del directorio raíz del disco duro. Por otro lado W97M/Chantal.A, crea otros dos archivos a los que llama con los nombres de CB4.VXD y CB1999.VBS. El primero de ellos será colocado en el directorio C:\WINDOWS, mientras que el segundo aparecerá en el directorio C:\WINDOWS\SYSTEM. Para que estos dos archivos sean cargados siempre que se inicie una sesión de trabajo en Windows, el virus modifica el Registro Windows, introduciendo en él dos líneas de comando que se encargan de este tema. La importancia que tiene esta ejecución para el virus es la posibilidad de infectar la plantilla global NORMAL.DOT que Word utiliza. Una vez conseguido este objetivo, los archivos DOC serán más fáciles de infectar ya que la plantilla será quien lo haga.

Virus en Internet.

Como ya dijimos Internet puede servir como medio para propagar la plaga, en la actualidad es bastante generalizado el uso de mensajes de correo HTML, la tendencia de algunos programas de permitir enviar mensajes que incluyen botones, formularios, y otras formas de automatización, como podemos imaginar esta complejidad adicional facilita nuevas formas desinfección por medio de correo electrónico.

En la actualidad existen los llamados virus HTML, al agregar capacidades extra al HTML ha permitido la creación de virus cuya infección puede producirse mediante la mera visualización de una página infectada, por el momento el daño potencial no es muy grande, y es fácilmente combatible, este tipo de rutinas se programa con rutinas VB-script, al ejecutarse el archivo infecta todas las páginas con las extensiones .htm o html que hayan en el mismo directorio. Los virus de Html no son una grave amenaza hoy por hoy, basta tener nuestro antivirus al día y los niveles de seguridad de nuestro navegador activados.

En cuanto a los virus Java, podemos decir que Java tiene una serie de protecciones de seguridad que limitan enormemente las posibilidades de utilización de applets para producir daños, ya que no se puede trabajar con los archivos de la máquina a menos que el usuario de la misma lo permita, sólo se puede conectar, a través de una conexión por Internet, con la máquina que envió el applet, estas limitaciones del lenguaje hace que los applets puedan acceder sólo a un conjunto limitado de recursos, lo que hace que los daños a través de applets sean mínimos, sin embargo, a través de Java ejecutado como aplicación se puede acceder a disco con las funciones normales de Java, puede sufrir una serie de ataques como robo o destrucción de información, robo de recursos y denegación de servicio, sin embargo, en general para que esto ocurra debe haber una autorización por parte del usuario, cosa que no es así con los controles active X que tienen la funcionalidad de los applets de Java, sin embargo, a diferencia de estos que se ejecutan en un sandbox, los ActiveX pueden acceder a todos los recursos de la máquina, lo que sin duda da más poder pero los convierten en más inseguros.

Amenazas afines: otros tipos de malware.

Trampillas

Una trampilla es un punto de entrada secreto a un programa que permite a alguien que la conoce conseguir el acceso sin pasar por loe procedimientos usuales de seguridad de acceso. Las trampillas las han usado los programadores de una forma legitima durante muchos años para depurar y probar los programas. La depuración y las pruebas se suelen hacer cuando el programador esta desarrollando una aplicación que dispone de un procedimiento de autenticación o una preparación muy larga, que requiere del usuario introducir muchos valores diferentes para ejecutar la aplicación. Para depurar el programa, el desarrollador puede querer disponer de privilegios especiales o evitar toda la preparación y autenticación necesarias. El programador también puede querer asegurarse que hay un método para activar el programa en el caso de que algo vaya mal en el procedimiento de autenticación que se está construyendo en la aplicación. La trampilla es un código que reconoce alguna secuencia de entrada especial o que es lanzado al ser ejecutado por un cierto ID de usuario o mediante una secuencia improbable de sucesos.

Las trampillas se convierten en amenazas cuando son empleadas por programadores desaprensivos para conseguir el acceso no autorizado. La trampilla era la idea básica de la vulnerabilidad representada en la película "Juegos de guerra" (COOP89). En caso real, los auditores descubrieron una trampilla en un producto de software comercial (GOLD85) en el nombre de su autor servía como contraseña de paso. Otro ejemplo: durante el desarrollo de la Multics, las pruebas de penetración estaban dirigidas por un "equipo tigre" de las Fuerzas Aéreas (adversarios simulados). Una táctica empleada fue enviar una versión falsa del sistema operativo a un nodo que ejecutaba Multics. La versión contenía un caballo de Troya (descrito mas tarde) que podía activarse por una trampilla y permitía que el equipo tigre lograra el acceso. La amenaza estaba tan bien implementada que los desarrolladores de Multics no pudieron encontrarla, incluso tras haber sido informados de su presencia (ENGE80).

Es difícil implementar controles para trampillas en el sistema operativo. Las medidas de seguridad deben centrarse en el desarrollo de los programas y en las actualizaciones del software.

Bomba lógica

Uno de los tipos de amenaza más antigua, anterior a los virus y gusanos, es la bomba lógica. La bomba lógica es un código incrustado en algún programa legítimo que "explota" cuando cumplen ciertas condiciones. Ejemplos: de condiciones que pueden emplearse como disparadores de una bomba lógica son presencia o ausencia de ciertos archivos, un día concreto de la semana, o una fecha, o un usuario particular que ejecute la aplicación. En un caso famoso (SPAF89), una bomba lógica inspeccionada el número de ID de un cierto empleado (autor de la bomba) y entonces se disparaba si el ID no aparecía en dos cálculos consecutivos en la nomina. Una vez disparada, la bomba podía modificar o borrar datos o archivos enteros, hacer que la máquina se detuviese o causar algún otro daño. Un ejemplo sorprendente de como se pueden utilizar las bombas lógicas fue el caso del sistema de la biblioteca del Condado de Montgomery, en Maryland (TIME90). El contratista que había desarrollado el sistema de préstamos computarizado insertó una bomba lógica que inhabilitaba el sistema en una cierta fecha, a menos que se le hubiera pagado. Cuando la biblioteca negó el pago final porque el sistema tenia un tiempo de respuesta malo, el contratista reveló la existencia de la bomba y amenazó con permitir que estallase a menos que el pago estuviese disponible.

Caballos de Troya

Un caballo de Troya es un programa o procedimiento útil o aparentemente útil que contiene un código oculto que, cuando se invoca, lleva a cabo alguna función dañina o no deseada.

Los programas con caballo de Troya se pueden usar para efectuar funciones indirectamente que un usuario no autorizado no podría efectuar directamente. Por ejemplo, para obtener acceso a los archivos de otro usuario en un sistema compartido, un usuario podría crear un programa con un caballo de Troya que, cuando se ejecutase, cambiara los permisos de los archivos de usuario que lo llamase de forma que pudieran ser leídos por cualquier usuario. El autor del programa podía entonces invitar a los usuarios a ejecutar el programa situándolo en un directorio común y dándole un nombre de forma que pareciese una utilidad provechosa. Un ejemplo es un programa que produce ostensiblemente un listado de los archivos del usuario en un formado deseado. Después de que otro usuario halla ejecutado el programa con caballo de Troya que sería difícil de detectar es un compilador que haya sido modificado para que inserte un código adicional en ciertos programas cuando son compilados, como los programas de conexión de los sistemas (THOM84). El código crea una trampilla en el programa de conexión que le permite al autor conectarse al sistema mediante una contraseña especial. Este caballo de Troya nunca se descubrirá leyendo el código fuente del programa de conexión.

Otra intención habitual de los caballos de Troya es la destrucción de los datos. El programa parece estar realizado alguna función de utilidad (por ejemplo, un programa de calculadora), pero también puede estar eliminado silenciosamente los archivos del usuario. Por ejemplo, un ejecutivo de la CBA fue víctima de un caballo de Troya que destruyó toda la información contenida en su computadora (TIME90). El caballo de Troya fue implantado en una rutina gráfica ofertado en un sistema de tablón de anuncios electrónico.

APENDICE.
Direcciones de Internet de algunas empresas antivirus.

Aladdin

Web Site: http://www.aks.com/

Productos Anti-Virus

- eSafe Protect for Windows 95/98/NT
- eSafe Protect Enterprise
- eSafe Protect Gateway

Alwil Software

Web Site: http://www.alwil.com/en/default.asp

Productos Anti-Virus

- AVAST! for MS-DOS
- AVAST! for Windows 3.1x
- AVAST! for Windows 95/98
- AVAST! for Windows NT
- AVAST! for Microsoft Exchange Server

Command Software, Inc.

Web Site: http://www.commandcom.com/
FTP Site: ftp://ftp.commandcom.com

Productos Anti-Virus

- Command AntiVirus for DOS
- Command AntiVirus for Windows
- Command AntiVirus for Windows 95
- Command AntiVirus for Windows NT
- Command AntiVirus for Microsoft Exchange
- m@ilCOMMAND

Computer Associates International, Inc.

Web Site: http://www.cai.com/
Support Web Site: http://support.cai.com

Productos Anti-Virus

- Inoculan Client for Windows 95 (Cheyenne AntiVirus for Windows 95)
- Inoculan/InoculanIT for Windows NT

- Inoculan/InoculanIT Clients for Windows 95
- Inoculan/InoculanIT for Windows 3.x/DOS
- Inoculan AntiVirus for Windows 95 (Desktop)
- Inoculan Client for Macintosh

F-Secure, Inc.

Web Site: http://www.F-secure.com/
Support Web Site: http://www.datafellows.com/support/
Contact information for other locations: http://www.F-secure.com/corporate/
Productos: http://www.F-secure.com/products/

Productos Anti-Virus

- F-Secure Anti-Virus for DOS
- F-Secure Anti-Virus for Windows 3.1x
- F-Secure Anti-Virus for Windows 95 and 98
- F-Secure Anti-Virus for Windows NT Workstation versions 3.50, 3.51 and 4.0
- F-Secure Anti-Virus for Windows NT Server versions 3.50, 3.51 and 4.0
- F-Secure Anti-Virus for Microsoft Exchange

Grisoft Inc.

Web Site: http://www.grisoft.com

Productos Anti-Virus

- AVG Anti-Virus for Windows 95
- AVG Anti-Virus for Windows 98
- AVG Anti-Virus for Windows NT

IKARUS Software

Web Site: http://www.ikarus.at/start_e.htm

Productos Anti-Virus

- virus utilities DOS
- virus utilities Windows 3.x
- virus utilities Windows 95, Windows NT
- virus utilities Windows NT-Admin

iRiS Software

Web Site: http://www.irisav.com/

Productos Anti-Virus

- iRiS AntiVirus
- iRiS CAT for Windows CE
- iRiS Macro Defender
- iRiS AntiVirus LITE

Kaspersky Lab

Web Site: http://www.kasperskylab.ru/

Productos Anti-Virus

- AVP for DOS
- AVP for Windows 3.x
- AVP for Windows 95/98/NT
- AVP for Windows NT Server
- AVP Inspector

Network Associates, Inc.

Network Associates Web Site: http://www.networkassociates.com/
MacAfee Web Site: http://www.mcafee.com/
Dr. Solomon Web Site: http://www.drsolomon.com

Productos Anti-Virus

- McAfee VirusScan
- Dr. Solomon's Virex for the Macintosh
- Dr. Solomon's Anti-Virus for Workstations
- NetShield for Windows NT
- GroupShield Exchange
- Dr. Solomon's Anti-Virus for Server

Norman Data Defense Systems

Web Site: http://www.norman.com/local/

Productos Anti-Virus

- Norman Virus Control for Windows 95/98
- Norman Virus Control for Windows NT
- Norman Virus Control for Windows NT Server
- Norman Virus Control for MS-DOS
- Norman Virus Control for Microsoft Exchange

NovaStor Corporation

Web Site: http://www.thunderbyte.com/

Technical Support Web Site: http://www.novastor.com/techsupt.html

Productos Anti-Virus

- ThunderBYTE Anti-Virus

Panda Software

Web Site: http://www.pandasoftware.com

Productos Anti-Virus

- Panda Antivirus Platinum for Windows 95/98
- Panda Antivirus Platinum for Windows 3.1x
- Panda Antivirus Platinum for Windows NT
- Panda Antivirus Platinum for MS-DOS
- Global Virus Insurance 24H-365D Small Business Edition
- Global Virus Insurance 24H-365D Intelligent Network Security

RG Software

Web Site: http://www.rg-av.com/

Productos Anti-Virus

- Vi-Spy for Windows 3.x and Windows 95

Sophos

Corporate Headquarters

Web Site: http://www.sophos.com/

Productos Anti-Virus

- Sophos Anti-Virus for Windows 95/98
- Sophos Anti-Virus for Windows NT
- Sophos Anti-Virus for Macintosh
- Sophos Anti-Virus for MS-DOS

Symantec

Web Site: http://www.symantec.com/

Central Point AntiVirus Files and Updates:

http://www.symantec.com/techsupp/cpav/files_cpav.html

IBM AntiVirus Support

Symantec - IBM AntiVirus Updates:

http://www.symantec.com/avcenter/ibm/index.html

Norton AntiVirus Support

Norton AntiVirus Macintosh Support

Norton AntiVirus Files and Updates:

http://www.symantec.com/techsupp/nav/files_nav.html

Symantec AntiVirus for Macintosh Support

Symantec AntiVirus for Macintosh:

http://www.symantec.com/techsupp/files/sam/symantec_antivirus_for_macintosh.html

Productos Anti-Virus

Norton AntiVirus 5.0 for Windows 95/98 and NT Workstations
Norton AntiVirus 5.0 for Windows NT Servers
Norton AntiVirus 1.5 for Microsoft Exchange
Norton AntiVirus 5.0 for Macintosh
Norton AntiVirus 4.0 for Windows 3.x/DOS
Norton AntiVirus for Firewalls
Norton AntiVirus for Internet Email Gateways

TREND Micro Incorporated

Web Site: http://www.antivirus.com/products/pcc/index.htm

Productos Anti-Virus

- InterScan VirusWall
- InterScan VirusWall Windows NT Server
- InterScan WebProtect
- OfficeScan
- ScanMail for Microsoft Exchange
- ScanMail for Microsoft Mail
- ScanMail for Microsoft Outlook
- ServerProtect for Windows NT Server
- PC-cillin for Windows 95 and Windows 98

BIBLIOGRAFÍA.

- [STA98]**Stalling, William**. "Sistemas operativos", Prentice-Hall. Madrid. 1997, pp. 571-630.
- [TA92] **Tannembaum, Andrew S.:** "Modern Operating Systems", Englewood Cliffs, NJ: Prentice Hall, pp. 210-212, 1992.
- [TA96] **Tannembaum, Andrew S.**: Computer Networks, 3rd Edition, Englewood Cliffs, NJ: Prentice Hall. 1996.
- [SPA89] **SPAFFORD, E.H.:** "The internet worm: Crisis and Aftermath", Communications of the ACM, vol. 32. pp. 678-687, junio 1989.
- [MIC1] http://support.microsoft.com/support/kb/articles/Q49/5/00.asp
- http://antivirus.about.com/compute/antivirus/
- [ComE] http://www.computereconomics.com
- [Geo1] *http://www.geocities.com/SiliconValley/Heights/3652/def.html*
- [GOR94] 1994 **Gordon, Sarah**. 4th International Virus Bulletin Conference, Jersey, UK, September 1994. http://www.commandcom.com/virus/generic.html