19
24

UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO

FACULTAD DE CONTADURIA Y ADMINISTRACION

VIRUS INFORMATICOS

SEMINARIO DE INVESTIGACION INFORMATICA

QUE PARA OBTENER EL TITULO DE:

LICENCIADO EN INFORMATICA

P R E S E N T A :

LILIANA ROSAS TROCHI

ASESOR DEL SEMINARIO
ACT. EDITH ARIZA GOMEZ

MEXICO, D. F.

1997

TESIS CON
FALLA DE ORIGEN

Universidad Nacional Autónoma de México
UNAM
Biblioteca Central
Dirección General de Bibliotecas de la UNAM

UNAM – Dirección General de Bibliotecas
Tesis Digitales
Restricciones de uso

DERECHOS RESERVADOS ©
PROHIBIDA SU REPRODUCCIÓN TOTAL O PARCIAL

Todo el material contenido en esta tesis esta protegido por la Ley Federal del Derecho de Autor (LFDA) de los Estados Unidos Mexicanos (México).

El uso de imágenes, fragmentos de videos, y demás material que sea objeto de protección de los derechos de autor, será exclusivamente para fines educativos e informativos y deberá citar la fuente donde la obtuvo mencionando el autor o autores. Cualquier uso distinto como el lucro, reproducción, edición o modificación, será perseguido y sancionado por el respectivo titular de los Derechos de Autor.

Señor,

tú sabes el secrificio que realiza cada uno de tus hijos en el andar de la vida, y sabes también quienes ayudan al necesitado, por eso Señor te pido por todos aquellos que en algún momento de la vida y el transcurso de la educación me tendieron la mano y me ayudaron a salir adelante, logrando así concluir una etapa más de estudios por el saber y conocer más sobre las creaciones que nos permites disfrutar, por todo esto Señor te doy gracias.

Quiero dar las gracias en una forma muy especial a mi madre por su confianza y apoyo que me ha dado en cada una de mis decisiones, a cada uno de mis hermanos: Paty, Guillermo, Agus, y Juanito, gracias por darme su apoyo y principalmente su amor.

Gerardo,
gracias por todo lo que me haz apoyado, tu participación en mi vida ha sido muy importante y espero algún día logre recompensarte.

INDICE

PREFACIO

Con el avance de la tecnología, se ha logrado una penetración en casi todos los campos de actuación del ser humano. En el caso de las computadoras, el almacenamiento y procesamiento de información se ha efectuado a una mayor velocidad con una mayor cantidad de datos, permitiendo obtener información procesada en forma mucho más ágil que en un principio. Por otra parte la aparición de programas de cómputo accesibles para todas las personas hace que su uso se generalice y no sean ya para uso exclusivo de matemáticos, físicos o ingenieros; estas herramientas son casi indispensables en nuestras actividades cotidianas. Por lo que hoy en día podemos encontrarlas desde el uso comercial o industrial hasta el uso personal.

En el campo de la informática nos enfrentamos a cambios continuos en software y hardware que hacen más rápido el manejo de la información, pero esta acción, no sólo ofrece beneficios, como es el de estar informado de acontecimientos que suceden en otras partes del mundo en forma casi inmediata; sin embargo, la manipulación que se ejerce sobre la información se considera negativa, ya que la censura, nos indica qué podemos conocer y qué no debemos conocer.

Si bien es cierto que existen personas que se dedican a investigar y a crear mejoras en el equipo y en su aplicación con fines

beneficios, por otra parte se da el caso de personas que se dedican a inventar la forma de destruir estas creaciones.

El tema de esta tesis es el Virus Informático, el cual a pesar del poco tiempo de haberse dado a conocer, ha causado gran preocupación por los daños que pueden causar no sólo a la computadora y a la información sino que incluso pueden generar quebrantos al patrimonio de las personas y de las empresas, ya que cuando no se tienen copias de seguridad de la información se pierden muchas horas-hombre recuperando la información dañada por estos programas.

Hasta ahora, solo los especialistas del área de informática conocían sobre el tema, en esta tesis se pretende que el publico en general (que lea esta tesis) puedan conocer acerca de estos programas, es decir, que son, como se generan, como se desarrollan y lo mas importante como se combaten o en un determinado momento como poder evitarlos.

Asimismo pretende servir como apoyo para el Centro de Informática de la Facultad de Contaduría y Administración de la Universidad Nacional Autónoma de México (CIFCA de la UNAM), ya que en el mes de marzo de 1994 se detectó un virus llamado NATAS, el cual ha sido difícil de erradicar debido al desconocimiento general acerca de la auténtica naturaleza de los virus informáticos y sus efectos.

Esperando dar una idea clara y precisa sobre que son dichos Virus Informáticos, solo me queda inducirlos a la lectura del presente trabajo.

INTRODUCCIÓN

A fin de entender el comportamiento de los virus informáticos, conozcamos el significado y procedencia de sus hermanos biológicos que les proporcionan su nombre. Esta similitud se debe a que el desarrollo de los virus informáticos por el ser humano, se ha basado en el comportamiento de los virus biológicos.

Durante muchos siglos, el hombre sólo pudo conocer a fondo lo que tenía a corta distancia y podía percibir a simple vista. Por largo tiempo la humanidad ignoró, entre otras cosas, la existencia de un mundo de extraordinaria importancia: el de los diminutos organismos conocidos ahora como microbios.

En la evolución del hombre, éste ha ido descubriendo e inventado una serie de objetos que ha ido adaptando a sus necesidades, es así que para descubrir, conocer y estudiar los microbios fue necesario el perfeccionamiento del microscopio. Actualmente tenemos muchos conocimientos respecto de los microbios. El hombre los clasifica en dos tipos importantes que son: Bacterias y Virus.

La mayoría de las bacterias son útiles al hombre, como las que producen fermentaciones, las que desintegran restos orgánicos para reincorporar sus componentes al medio, etc. Los virus son siempre parásitos. Unos producen padecimientos leves, pero otros ocasionan enfermedades graves y aún mortales.

Los virus, desintegran las células. El virus que produce la poliomielitis, por ejemplo, destruye células del sistema nervioso y ocasiona parálisis en determinas partes del cuerpo del huésped, la mayoría

de los virus son muy exigentes en la elección del ser vivo que van a infectar y además saben en qué células de ese ser deben continuar su vida parasitaria.

El ser humano, los animales y los vegetales, son infectados en un momento u otro de su vida por los virus, y a menudo continúan infectados durante toda su vida, aún cuando no lleguen nunca a enfermar conviven con ellos.

El comportamiento de los virus se da a través de su infectividad y su variabilidad. La primera puede darse en tres formas:

1. Al introducirse en la bacteria parasitaria se reproduce en menos de media hora, dentro de ella, de cien a doscientas réplicas idénticas de sí mismo, ya maduras. Al formarse hacen estallar la célula y quedan libres.

2. De igual forma se introduce en la célula, sólo que se confunde químicamente con su núcleo y quedarse "dormido" durante dos o tres generaciones de bacterias, después un momento determinado, el virus se reproduce dentro de las células "nietas" y las hace estallar.

3. Una última posibilidad es que el virus permanezca en el interior de la célula, obligándola a crecer y dividirse rápidamente, mientras que él también se reproduce al mismo ritmo que las células.

Su variabilidad está dada en que, todo lo que es cierto para un determinado virus, es casi seguro que no lo es para otro.

Los virus son parásitos del reino animal, y aunque no mantengamos buenas relaciones con ellos, parece que han venido decididos a quedarse con nosotros. No existe ninguna razón para dudar que existen sobre la tierra desde que apareció el hombre y probablemente mucho antes, considerándolos algunos científicos como la primera forma de vida, mientras que otros los suponen la degeneración última de la evolución de la vida. En todo caso, estamos poblados por un número increíble de estos parásitos perfectos.

Derivado de lo anterior, podemos deducir el porque se les asignó el nombre de VIRUS INFORMÁTICOS ya que es claro que sus semejanzas son asombrosas en cuanto a infectividad y variabilidad. El huésped es la computadora, los fines son la reproducción y la destrucción.

CAPITULO I

¿ QUE ES UN VIRUS INFORMÁTICO ?

¿QUÉ ES UN VIRUS?

La palabra VIRUS, que viene del latín VENENUS es un microorganismo que al introducirse a una célula, modifica la información genética de ésta a fin de generar réplicas de sí mismo, adicionalmente cuando ocurren mutaciones se dificulta su detección así como el combate al mismo cuando se presentan los síntomas. Algunas veces, los virus en las células infectadas, permanecen ocultos, pero no quiere decir que estén inactivos, porque están latentes y solo esperan que las condiciones sean favorables para que puedan iniciar su actividad destructiva.

¿ QUÉ ES UN VIRUS INFORMÁTICO ?

La palabra virus, es tomada de las siglas "Vital Information Resources Under Siege", cuya traducción es: "Ataque a recursos vitales de información", por lo que un virus informático se puede utilizar para alterar la información que se encuentra almacenada en una determinada computadora.

Un virus informático se puede definir como:
"Un pequeño programa que se adhiere a otro en un momento dado, y que de acuerdo a las características que le proporcionó el programador que lo diseñó, es la forma en que puede excitar a la computadora para que realice instrucciones no deseadas por el usuario.

¿QUÉ ES UN VIRUS?

La palabra VIRUS, que viene del latín VENENUS es un microorganismo que al introducirse a una célula, modifica la información genética de ésta a fin de generar réplicas de sí mismo, adicionalmente cuando ocurren mutaciones se dificulta su detección así como el combate al mismo cuando se presentan los síntomas. Algunas veces, los virus en las células infectadas, permanecen ocultos, pero no quiere decir que estén inactivos, porque están latentes y solo esperan que las condiciones sean favorables para que puedan iniciar su actividad destructiva.

¿ QUÉ ES UN VIRUS INFORMÁTICO ?

La palabra virus, es tomada de las siglas "Vital Information Resources Under Siege", cuya traducción es: "Ataque a recursos vitales de información", por lo que un virus informático se puede utilizar para alterar la información que se encuentra almacenada en una determinada computadora.

Un virus informático se puede definir como:
"Un pequeño programa que se adhiere a otro en un momento dado, y que de acuerdo a las características que le proporcionó el programador que lo diseñó, es la forma en que puede excitar a la computadora para que realice instrucciones no deseadas por el usuario.

Existen otros programas que generalmente se confunden con los virus, estos programas son: "el gusano, el caballo de troya y la bomba lógica". La principal diferencia entre un virus y un programa de este tipo es que los virus destruyen información con programas y/o datos, y en ocasiones pueden causar daños al equipo.

Un "gusano" es un programa que se desplaza por la memoria interna del ordenador con identidad propia, a diferencia del virus, que generalmente se adhiere a otros programas. Está diseñado para que busque zonas de memoria desocupadas, donde realiza copias sucesivas de sí mismos, hasta que consigue un desbordamiento físico de la memoria.

"El caballo de Troya" es un código pernicioso que está en el seno de un programa legítimo. Como característica esencial indicaremos que carecen de autoréplica, por ello su código sólo se activa al ejecutarse el programa que lo porta. Se utiliza para extorsionar operaciones rutinarias, como el redondeo de cuentas en los procesos de actualizaciones bancarias.

Se denomina "bomba lógica" o "bomba de tiempo" a un programa que se ejecuta al producirse un hecho predeterminado. La condición o hecho que motiva la activación es variable y comprende desde una fecha determinada, hasta secuencias especiales de teclas. Si no se produce el suceso programado, el programa permanece oculto para el usuario, sin ejercer más acción que ocupar una porción de memoria.

CARACTERÍSTICAS DE LOS VIRUS INFORMATICOS

Un virus informático puede presentar algunas de las siguientes características:

- Son programas pequeños.
- Se reproducen rápidamente.
- Generalmente se desconoce quien los programó.
- Permanecen ocultos.
- Se activan de diferente modo, que puede ser:
  - En un determinado tiempo (fecha u hora).
  - Por una determinada condición.
  - Por sentir la presencia de un detector.
- Son destructores de archivos.
- Son difíciles de erradicar.

1.1. ORIGEN DE LOS VIRUS

El origen de los virus, se remonta a 1949, año en que John Von Neumann, el Padre de la Computación, en su libro "Theory and Organization of Complicated Automata" describe algunos programas que son capaces de reproducirse a si mismos.

En la década de los años 60 aparece información acerca de algo que parece incluir códigos que trabajan como virus, desarrollados por estudiantes de computación en el Instituto Tecnológico de Massachusetts.

Estas personas se reunían por las noches y se dedicaban a elaborar programas "sofisticados" , así se desarrollaron notables programas como Space War (Guerra en el espacio).

Uno de sus programas favoritos consistía en bombardear al programa del contrincante que no sabia de donde recibía el ataque y que lo provocaba.

En esa misma época en los laboratorios de computación de AT&T (Bell Laboratories) H. Douglas, Mellory, Robert Morris, Víctor Vysottsky y Ken Thompson (creador del sistema Operativo Unix) inventaron como entretenimiento un juego al que llamaron "Core War" inspirados en un programa llamado "Creeper" el cual estaba escrito en lenguaje ensamblador y tenía la característica de reproducirse cada vez que era ejecutado.

El juego consistía en invadir la computadora del adversario con un código que contenía una serie de información destinada a destruir la memoria del rival o impedir su correcto funcionamiento.

Conscientes de la peligrosidad que representaba para los sistemas de computación, diseñaron un programa al que llamaron "Reeper", cuya función era la de destruir cada copia hecha por "Creeper".

Al hacerlo prometieron mantenerlo en secreto, pues sabían que en manos irresponsables el "Core War" podía ser usado inadecuadamente.

Sin embargo, en 1983 el Dr. Ken Thompson en un discurso efectuado ante la Association for Computing Machinery, da a conocer la estructura de estos programas en detalle.

En Mayo de 1984, la revista "Scientific American" lo publica en su artículo "Computer Recreations" firmada por A.K. Dewdney, como el juego de "Core Wars" (ofreciendo por dos dólares las guías para la creación de sus propios programas).

Una segunda tecnología es la de John F, Scoch, del Centro de Investigación de Xerox en Palo Alto, Estados Unidos, quien diseño a "Worm", el cual fue creado para obtener el máximo rendimiento de una red de miniordenadores interconectados de Xerox. Este programa se cargaba a una maquina inactiva encargada de controlar a todo el sistema, después en combinación con otros worms residentes en otras máquinas, hacían funcionar grandes programas de aplicación y obtenían como resultante un sistema multiprocesador.

En septiembre del mismo año durante la conferencia "IFIC/SEC'84", el Doctor Fred Cohen, en su ponencia "Computer Viruses: Theory and Experiments", define por primera vez, el término "virus de ordenador", expone a este tipo de programas como software maligno capaz de reproducirse a sí mismo.

En 1985 otro artículo de la revista "Scientific American", titulada "Juegos de Ordenador: virus, gusanos y otras plagas de la Guerra Nuclear atentan contra la memoria de los ordenadores", en él manifiesta las consecuencias de su juego de acuerdo a los testimonios escritos por sus lectores.

No se puede juzgar a Dewdney como el inventor de los virus, por el hecho de haber difundido un inocente y creativo juego, pero no perdamos de vista que colaboró en dar a conocer el fenómeno vírico como hoy lo conocemos, cuando transcribió parte del código de su juego el cual fue

modificado por otros programadores.

Uno de los casos mas notables es el de Jim Hauser y William R, Buckley, de la Universidad Politécnica de California, quienes crearon a Apple Worm, el cual sacaba copias de sí mismo, y las enviaba a las unidades de diskettes a través de la memoria del Apple II con un procesador 6502 sin la intervención del usuario

Durante 1986, se difunde ampliamente un virus llamado Brain, el cual se dio a conocer en 1988, el virus activo se caracterizó por
el mensaje:

"Welcome to the Dungeon ... (c) 1986 Brain & Amjads (pvt) Lyd ... VIRUS_SHOE RECORD V9.0 ... Dedicated to the dynamic memories of millions of virus who are no longer with us today Thanks GOODNESS!! ... BEWARE OF THE er... VIRUS..."

cuya traducción sería:

"Bienvenidos a la mazmorra ... [Marca del copyright de los hermanos Amjad], [Fecha de creación del virus] 1986 [versión del programa]... Dedicado a las memorias dinámicas de los millones de virus que ya no están con nosotros [se supone que por haber sido detectados y desactivados] ¡GRACIAS A DIOS! ... CUIDADO CON EL... VIRUS...!.

Fue diseñado en Lahore Pakistán por dos hermanos que comerciaban su propio software, y a través

del virus se ayudaban para seguir el rastro de las copias pirateadas por los usuarios. Lo que no se explicaron fue cómo es que llego a otros países y a otros programas que no fueran de los creados por ellos.

En 1987, se descubrió en la Universidad Hebrea de Jerusalén un virus llamado "viernes 13" ó "Jerusalén" el cual fue diseñado para borrar los archivos que se ejecutaran el 13 de mayo de 1988, en cuya fecha se cumplía el 40 aniversario de la independencia de Israel. Se pudo detectar debido al notable tamaño de los archivos .EXE y la lentitud con que trabajaba en cierto tiempo la computadora. En el mismo año se identifica en el Estado de California al virus "alameda" cuya función era reproducirse varias veces y en un determinado momento procedía a borrar toda la información almacenada en el disco duro del equipo. Un virus no dañino descubierto en el mismo año es el virus de la pelota en el cual aparece en la pantalla un carácter rebotando a través de toda la pantalla.

En 1988, se descubre el virus "Stoned" en Wellington, Nueva Zelanda el cual infectaba discos flexibles con mensajes en pro de la mariguana, las últimas versiones de este virus no sólo afectan a discos flexibles sino también a discos fijos del equipo emitiendo además del mensaje un sonido.

Es hasta 1992 cuando se tenía considerado como el último virus más dañino al "Miguel Ángel" o "Michelangelo", que fue descubierto en el mismo año, el cual se cree que procede de Suecia, lugar donde se reportó su existencia. Este virus está programado para activarse cada 6 de marzo, fecha en que se celebra el nacimiento de Miguel Ángel Buonarroti, quien fuera un reconocido Arquitecto, Pintor y Escultor Italiano.

Todavía a principios de 1994 se seguía considerando como el virus más temido por los usuarios, sin embargo, no fue así, ya que en este año se propaga otro virus mucho más dañino dado por las pérdidas tan rápidas de información que se originaron sin poder tener un control del mismo, a este virus se le identificó como "SATAN" o "NATAS".

El enlistar cada uno de los virus que fueron detectados en un determinado año y lugar, con sus diferentes versiones, nos llevaría mucho tiempo, ya que se podría tratar un tema entero (por lo que se anexa un apéndice que muestra una lista de virus), es por esto que sólo se mencionan los casos más relevantes que dan origen a la creación de muchos otros virus informáticos, cuya finalidad dependerá de cada programador y la utilidad que le quiera dar, puesto que cada programador lo utilizará de manera diferente, puede ser desde mandar un mensaje en pantalla hasta causar daños a la misma computadora.

En resumen se puede decir que los virus informáticos tuvieron origen en una forma de casualidad, ya que algunos programas servían de diversión, mientras que otros daban mantenimiento o protección a otros. Pero como la ciencia debe seguir avanzando surgen nuevas ideas sobre estos mismos programas dándole otra nueva utilidad que consiste en dañar tanto el software como el hardware, debido a la piratería principalmente.

1.2. MITOS Y TABÚES

Existen personas mal intencionadas e ignorantes que causan rumores y alarmas acerca de algunos virus, lo que ocasiona que el usuario tenga miedo en cierto momento de utilizar la computadora.

Por el hecho de llamarse VIRUS el tipo de programas que causa daños a la información o a la computadora, ha ocasionado que los usuarios o personas que tienen acercamientos con las computadoras piensen que se tratan de virus biológicos, por lo que han llegado a creer que pueden ser contagiados por los mismos en una forma directa, causándoles daños inimaginables.

Hay quienes piensan que las computadoras pueden ser contagiadas al estar cerca de una que tenga virus o si se encuentran conectadas a una misma fuente de energía.

Cabe mencionar que nada de lo anterior puede ser posible, pues los virus son programas independientes que sólo afectarán a determinados programas o sectores de la computadora, en ningún momento puede causar una enfermedad vírica al usuario o a personas que trabajen cerca de una computadora.

Por otro lado los virus no pueden ser transmitidos a través de la energía o corriente eléctrica; los virus informáticos sólo son adquiridos por medio de diskettes contaminados, por lo que se debe tener cuidado de introducir diskettes de procedencia dudosa a las computadoras.

El hecho de no utilizar la computadora o utilizar otros diskettes externos, la salvan de contraer algún virus, ya que desde que se adquiere el equipo, puede estar contaminada debido al software que le fue instalado, esto no quiere decir que todas las computadoras que tengan instalados algunos programas de software va a estar contaminado, esto suele suceder en algunos casos solamente.

El hecho de que estos programas estén contaminados puede ser por que los programas originales hayan contenido el virus o por que con los diskettes que se realizó la instalación contenía alguno que en el momento no fue detectado.

Generalmente cuando se contrae un virus, el usuario no lo detecta en el momento. Después de un tiempo de estar trabajando con la computadora se detectan "anomalías" en el funcionamiento que no son propias del programa que se esté utilizando.

En la actualidad en la mayoría de los equipos se encuentra instalado un antivirus que detecta la presencia de un virus. Sin embargo, si es un nuevo virus este antivirus no lo detectará.

Se piensa que por el hecho de que una computadora puede contaminarse, la información que se encuentre en ella no será confiable y estará en peligro de perderse en su totalidad. Este temor no siempre está justificado, ya que en la actualidad se cuentan con ciertas herramientas que ayudan a detectar y eliminar determinados virus, estas a su vez ayudan a prevenir posibles "epidemias" o contagios a otras computadoras cuando es detectado a tiempo el virus. Hay personas que no creen en dichas herramientas y propagan rumores de que no sirven para nada, ya que cada año se

descubren distintos tipos de virus, por lo que no son eficaces. Esta razón no es válida, debido a que muchos virus no llegan a activarse por errores de programación y los que logran sobrevivir son descubiertos y eliminados con rapidez, además las personas que se dedican a crear las herramientas para eliminar los virus deben estar al tanto de los nuevos productos para computadora que se lanzan al mercado e identificar posibles alteraciones en el software.

Cuando una persona crea un virus, le asigna ciertas características para poder activarse en un determinado tipo de computadoras, por lo que existen virus propios de Pc, Macintosh, para redes, etc. (se detallan éstos en el apéndice c).

1.3. TIPOS DE VIRUS Y SU CLASIFICACIÓN

En un principio se clasificaban a los virus en benignos y malignos, es decir, los virus benignos son aquellos que no causaban daño a la información o a la computadora y que sólo mandaban mensajes en pantalla, y por otro lado los malignos, que como su nombre lo dice, son aquellos que causan daños a la información o a la propia computadora.

A causa de los avances de programación que se va desarrollando cada día, los virus dejan de ser simples mensajes en pantalla para pasar a ser programas tan poderosos que llegan a tomar el control de la computadora y realizar las operaciones destructoras para lo que fueron creados.

Una clasificación de los virus informáticos, se puede determinar de acuerdo al lugar en que se ubiquen, éste puede ser en los discos flexibles o en la computadora, tal es el caso de:

- El Sector de Arranque (boot sector).
- La Tabla de Partición (File Alocation Table).
- Los Archivos Ejecutables (archivos con extensión .EXE, .COM y .OVL)

(para mayor información sobre la arquitectura de la computadora, consulte el apéndice A)

Virus de Sector de arranque (boot sector).- Estos virus son capases de modificar a este sector ya sea del disco duro o de un diskette, generalmente sustituyen el archivo original (que posteriormente es guardado en un sector libre) por una versión propia del virus, para así poder controlar las funciones de la computadora, por otro lado el virus para no ser detectado deposita su código en algunos sectores libres, que tras su grabación los marcará como sectores en mal estado.

Su característica principal es que al alterar a este sector, consiguen el control sobre el propio sistema, ya que son cargados inmediatamente al encender el equipo, antes de que cualquier otro programa del sistema operativo.

Algunos ejemplos de estos virus son:

- Korea
- EDV
- Chaos
- Ghost Boot

- Disk Killer
- Typo
- Ping Pong-B
- NATAS

Los virus de la Tabla de Partición (File Alocation Table) buscan un pequeño registro llamado Registro Maestro de Arranque (Master Boot Récord).

La tabla de partición es el primer sector físico del Disco Duro, contiene la información relativa a las divisiones y a las direcciones de los archivos y/o comandos contenidos en la unidad, al atacar a ese pequeño sector ocasionan que el equipo o sistema sea incapaz de encontrar cualquier archivo o activar cualquier comando que se le indique.

Ejemplos de este tipo de virus son:

- Stoden o Mariguana.
- EDV.
- NATAS.

El grupo de Virus de Programas son aquellos que están a la expectativa para contaminar a los programas que presentan generalmente extensiones del tipo .COM, .EXE o .OVL. Este tipo de virus se inserta al inicio o al final de cada archivo sin alterar o modificar generalmente el programa original, lo que hacen es, que una vez que se han adherido al programa ejecutable se active en

memoria al utilizar dicho programa. Cuando el usuario termina de utilizar el programa este es guardado, sin embargo el virus permanece residente en la memoria permitiéndole así contaminar un programa que no esté infectado, y así sucesivamente hasta que la computadora es apagada, volviendo a activarse el virus al utilizar un programa contaminado.

Los virus de este tipo generalmente para infectar un programa realizan una búsqueda de su propio código, es decir cuando contaminan un programa inmediatamente lo "marcan" para así saber que ya contiene su código destructor, al cerciorarse de que no esta contaminado, entonces proceden a "marcarlo" para que una vez que se utilice infecte a otros que no lo estén.

Algunos ejemplos de estos tipos de virus son:

- Kennedy.	- Eigth Tunes.
- June 16th.	- 1392.
- V2000.	- Virus-101.
- Perfume.	- Taiwan.
- 4096.	- Payday.
- Iib.	- Sunday.
- Dark Avenger.	- Fu Manchu.
- Jerusalén.	- Jerusalén-B.
- SURIV03.	- NATAS.

Existen algunos virus que al activarse en la memoria por primera vez buscan un programa que no esté contaminado y cuando lo encuentran se adhieren a él dejando libre la memoria. (Para mayor información sobre nombres de virus y su clasificación ver apéndice "C")

CAPITULO II

COMPORTAMIENTO DE LOS VIRUS INFORMATICOS

Cada virus tiene un comportamiento diferente de los demás, ya que algunos se pueden insertar, añadir o realizar un bucle en archivos ejecutables de programas normales o sanos, algunos pueden tener combinaciones de los anteriores, otros se activan en memoria quedando residentes e interceptando las órdenes del usuario y las llamadas del sistema controlando así las entradas y salidas del sistema redireccionándolas o simplemente sustituir archivos buenos por malos.

2.1. TIPOS DE INFECCIÓN

Los virus dependiendo de su programador pueden tomar el control de los programas a través de una infección de cualquiera de los siguientes tipos o bien a través de combinaciones de las mismas. Los tipos más comunes de infección son:

- Añadidura.
- Inserción.
- Reorientación.
- Sustitución.
- Cubierta Vírica.

Los virus que actúan a través de añadidura se adhieren al final del programa ejecutable ocasionando una alteración en el tamaño del archivo, el cual puede crecer a cualquier tamaño, algunos virus tienen diferentes técnicas para identificar el tipo de archivo que van a contaminar, ya que los archivos con

extensiones .EXE y .COM tienen diferentes rutinas de ejecución por lo que hay virus que sólo atacan archivos .EXE y otros a los .COM, en la actualidad existe un virus llamado NATAS que ataca a ambos tipos.

Los virus que actúan a través de Inserción se insertan dentro del código del programa, sin alterar el tamaño del archivo, por lo que es un tanto difícil detectarlos.

La reorientación es una forma más sofisticada de la actuación de los virus ya que se introducen en una o más posiciones físicas del disco, como es el caso de las áreas de partición del disco, sectores o por archivos escondidos.

Estos virus utilizan las técnicas de añadidura o inserción ya que implantan pequeños segmentos entre archivos normales, dichos segmentos se activan cuando los programas que los contienen se ejecutan, reorientan el flujo del programa mediante una llamada a sus masters víricos, los cuales dirigen procesos víricos y después se descargan devolviendo el control al programa que los contiene.

Los programas infectados por sustitución son reemplazados por un programa vírico que en realidad no infecta al programa, sino al sistema, es decir el virus se encarga de borrar y ocupar el lugar de un programa ejecutable, esto ocasiona la pérdida total del archivo y también la pronta detección del mismo.

La cubierta vírica consiste en cubrir en su totalidad con operarios víricos todas las funciones básicas de una computadora, interceptando y enmascarando las acciones que de alguna forma podrían detectarlo o amenazar su supervivencia

2.2. TRANSMISIÓN DE VIRUS

Las computadoras tienen dos partes muy vulnerables por donde le son transmitidos los virus informáticos, que son:

- Por medio de discos magnéticos flexibles (diskettes)
- Los puertos de comunicaciones

La forma más común de transmisión es a través de los discos magnéticos, pues debido a su facilidad de manejo, su manuabilidad y capacidad de almacenamiento de información permiten que se adhieran programas no deseados.

El simple hecho de introducir un disco de este tipo a algún equipo y visualizar el contenido del mismo en pantalla, permite que el virus (dependiendo el tipo) se active en memoria en espera de que se ejecute algún programa y logre contaminarlo, comenzando así a contaminar todo el sistema.

Este tipo de transmisión es muy común entre los estudiantes, ya que debido a los grandes costos de adquisición de software, estos logran conseguir copias de programas originales y comienzan a prestárselos entre ellos mismos, logrando así la proliferación de los virus.

Debido al avance de la tecnología hoy en día las computadoras pueden estar conectadas mediante el teléfono a una o varias redes de información, también pueden comunicarse vía satélite a través del mismo medio. Todo esto se puede realizar a través de los "enchufes" llamados "Puertos de comunicaciones".

Este tipo de conexión permite la proliferación de virus difíciles de detectar. Las computadoras conectadas en res están ahora bajo la amenaza de un nuevo tipo de virus, una variedad de software autónomo que genera copias de sí mismo y que sigilosamente avanza en la red y ataca a la computadora que es su objetivo, a menudo con propósitos lucrativos.

A un virus de este tipo se le denomina virus de crucero, por la analogía con un crucero portador de misiles. El software de ataque es diferente a los programas virales por el hecho que es un proceso autónomo que no depende de otros procesos para su existencia. Como cualquier virus, infecta a otros programas y es portador de una carga destructiva. Los intrusos explotan el ambiente de la red apuntando hacia los dos eslabones más débiles, la computadora conectada y el usuario, para penetrar las defensas de un sistema, el intruso sólo necesita infectar la computadora del usuario.

Otro tipo de software de ataque captura contra señas de acceso de los usuarios o privilegios de alto nivel. El intruso sustituye una pantalla real de entrada en sesión con una falsa, quizá simulando el software de comunicaciones o tomando control de alguna de las conexiones de la red. Al entrar en sesión los usuarios el software de ataque registra secretamente sus nombres y contraseñas. Esta información es almacenada o enviada al intruso, quien entonces podrá tener acceso al sistema como si fuera un usuario autorizado. Esta información: archivos criptados, comunicaciones y controles de acceso es vulnerable a los caprichos del intruso. Este enfoque comprende cuatro etapas:

- Lanzamiento,
- Penetración,
- Reporte de la conquista del blanco y

- Detonación.

En la primera etapa el intruso lanza un virus de crucero a un medio de dominio público, confía en que alguno de los usuarios de la red introduzca inocentemente el virus en el sistema.

La penetración en sistemas grandes se logra casi siempre haciéndose pasar por algún usuario con privilegios u otra fuente de mensajes de confianza.

Para reportar que ha penetrado exitosamente en el sistema al que estaba dirigido, va a depender de cuanto sabe el intruso sobre el sistema en cuestión, si está trabajando dentro de esa compañía sabrá todo, sin embargo, alguien externo tendrá más dificultades, pero al final lo conseguirá.

A diferencia de los virus más comunes con fines destructivos un ataque de este tipo pasa casi desapercibido perturbando al sistema portador y al blanco lo menos posible. Un virus de este tipo una vez logrado su objetivo es probable que se autoelimine en un cierto tiempo.

Por otra parte, a través de los mismo medios se puede contagiar a toda una red con el fin de desestabilizar el mayor número de equipos en un determinado tiempo, esto se logra intentando filtrar un virus que rompa las barreras de las claves de seguridad, a este tipo de virus se le conoce normalmente con el nombre de "gusanos", quien a través de persistencia y adivinación consigue la clave de acceso.

2.3 PERIODO DE GESTACIÓN Y DESARROLLO

El periodo de gestación y desarrollo es la fase en que el virus comienza a vivir dentro de su huésped, esta actividad la realiza en cuatro etapas que son:

1. INFECCIÓN:

Los disco flexibles con datos se comparten con más frecuencia que los programas. Los usuarios de las computadoras creen por lo general que los discos con programas y juegos infectados difunden los virus. Esto no es verdad. ya que un disco flexible en blanco es un portador común. Como el sector de arranque está bien documentado se infecta con facilidad sin efectos colaterales extraños.

Para entender esto analicemos el proceso de arranque, como este ocurre tan rápido en la mayor parte de las computadoras, es muy fácil no darse cuenta de la cantidad de pasos de que consta el arranque de una computadora. El actor principal es el ROM-BIOS, los pasos que ejecuta son: Exhibe los mensajes a color, realiza un autoexamen de encendido, el cual consiste en verificar los dispositivos conectados a la máquina como son: impresoras, mouse, pantalla, unidades de disco y verifica cuanta memoria tiene, A continuación ROM-BIOS intenta cargar DOS de un disco flexible en la unidad "A" (el primer sector de cada disco flexible es el sector de arranque). Si el disco es autoiniciable, el sector de arranque contiene un pequeño programa que localiza y ejecuta al DOS, por otra parte si es un disco de datos, el sector de arranque contiene un pequeño programa que exhibe el mensaje "NON SYSTEM DISK OR DISK ERROR" y espera que el usuario pulse cualquier tecla para continuar.

Si no introdujo un disco flexible en la unidad "A", ROM-BIOS continua con el intento de arranque y busca en el primer sector (o la tabla de partición) del disco duro, que por lo general es la unidad "C".

ROM-BIOS ejecuta un pequeño programa que activa al DOS (los dos archivo ocultos del sistema MSDOS.SYS y IO.SYS), por último DOS se carga y se configura así mismo automáticamente según los comandos del archivo CONFIG.SYS

Lo anterior le permite al diseñador de un virus aprovechar la forma en que ROM-BIOS busca y ejecuta al DOS. Suponiendo que un disco flexible está en la unidad "A" (esta infectado y la computadora apagada). Es posible que en la última sesión se haya utilizado este disco y por un olvido se quede en la unidad de forma accidental. Al encender la computadora busca el disco de arranque en la unidad "A" y se prepara para ejecutar el sector de arranque de dicho disco.

Cuando ROM-BIOS realiza esta acción, el virus del sector de arranque es el que realmente se ejecuta, una vez activado el virus busca con rapidez la presencia de un disco duro e infecta la tabla de partición de dicho disco o el sector de arranque de la partición activa, de regreso al disco flexible de la unidad "A" el virus se ejecuta en el sector de arranque del disco flexible original, es decir, con el mensaje "NON SYSTEM DISK OR DISK ERROR"; la computadora ahora está infectada.

Cuando el virus llega a la computadora toma el control de la misma sin que el usuario se de cuenta del peligro que corre tanto su información como su equipo (depende del virus que entre), originando así un periodo de gestación.

2. OCULTAMIENTO:

Para evitar ser descubierto y eliminado el virus necesita ocultarse, para que el usuario detecte su código, y por otro lado sus acciones. No todos los virus tienen interés en ocultarse, algunos son de aplicaciones rápidas, y no tiene tiempo el usuario de observar nada antes de que el virus actué, el código del virus está mezclado con el código del programa que le sirve de huésped. Pero algunas veces tiene un tamaño voluminoso y ocupa demasiado espacio dentro del archivo, por lo que necesita dividirse, dejar una parte pequeña dentro del huésped y guardar en algún lugar oculto la parte más gruesa del programa.

El virus puede utilizar una de las siguientes técnicas:

- Marcar el archivo en donde está almacenado con el atributo de archivo oculto. Lo que hará que no pueda ser listado con el comando DIR.

- Almacenar el código en uno o varios sectores del disco, marcándolos como sectores defectuosos.

- Mediante técnicas de formateo no estándar, con lo que se logra introducir sectores extraños, que permanecen ocultos a la vista del DOS y este no podrá leerlos.

3. LATENCIA:

En esta etapa el virus está al tanto de las instrucciones que se le proporcionan a la computadora, y comienza a infectar a cuanto programa se ejecute en la misma, incluyendo los discos que se lleguen a introducir, ocasionando así la contaminación a otras computadoras.

4. ACTIVACIÓN:

Dependiendo del virus y de las circunstancias de programación, va a ser su acción destructora, la cual dependerá del tipo de programas que se utilizó, tal es el caso de los caballos de troya, bombas lógicas o gusanos, cada uno tiene una característica diferente de activación, por ejemplo, una fecha específica, una señal o al cumplirse una condición.

2.4. REPRODUCCIÓN.

La diferencia entre un virus y un programa, consiste en su capacidad de reproducirse, por lo que es su cualidad más temida, pues debido a que existen muchas copias del mismo, se hace más difícil erradicarlo. Esta capacidad de reproducción depende del tipo de virus, ya que existen los que realizan una sola copia, y por otro lado están los que realizan varias copias de sí mismos en otros programas no infectados.

Para que la reproducción sea efectiva, la copia realizada ha de quedar permanente en alguna parte del sistema, además debe cumplir dos objetivos comunes en cualquier virus que es: a) su propagación en otros sistemas y b) aumentar esfuerzos en alcanzar su meta o fin.

El proceso de reproducción se da mediante:

1. La búsqueda de un huésped que le permita reproducirse.

2. Verifica la existencia del mismo en algún otro programa que se encuentre en la computadora o sea introducido.

3. Recuperación de su código en su totalidad.

4. Realiza la copia del mismo en otro programa, para asegurar su ejecución en otro sistema o computadora.

CAPITULO III

PROTECCIÓN CONTRA LOS VIRUS INFORMATICOS

La protección contra los virus es realmente un problema de actualidad, ya que a menos que usted guarde su computadora en una caja fuerte y no la utilice nunca tendrá este problema.

Sin embargo, se considera que una de las mejores defensas en contra de ellos es el de no utilizar programas contaminados, es decir, tratar siempre de utilizar programas que han sido adquiridos en los establecimientos que venden software.

Pero, aún así no existe una seguridad del 100% de que se pueda evitar este problema.

Existe una serie de medidas de protección que se deben seguir como son:

3.1. TÉCNICAS DE PREVENCIÓN

a) No trabajar con los diskettes de programas originales. Antes de iniciar la instalación de dicho programa es recomendable colocar una etiqueta de protección contra escritura (en diskettes de 3 ½" bastará con "correr" el botón indicador) y al finalizar la instalación efectuar una copia de seguridad de sus diskettes, protegiéndolos de la misma forma

   Para mayor seguridad utilice la copia y no los originales.

b) Obtenga copias de seguridad de los datos. Es recomendable que cada vez que haga una

actualización de sus datos, obtenga una copia de seguridad de éstos en diskette, poniéndoles una etiqueta de protección contra escritura.

c) No guarde toda su información en disco duro. Es recomendable que si no está utilizando los paquetes o los datos en un período determinado, no los deje en el disco duro, guárdelos en diskettes para prevenir cualquier eventualidad.

d) Verificar los diskettes antes de introducirlos al equipo. Es indispensable que antes de utilizar diskettes propios y más si son ajenos el revisarlos con algún detector de virus, previa instalación de etiqueta de protección contra escritura.

e) Este paso es el más importante, ya que es el uso de vacunas. Las vacunas tiene como objetivo principal el intentar prevenir la infección de los virus, antes de que éstos empiecen a producirse.

Estas vacunas funcionan igual que las que se utilizan para el ser humano, es decir, existe una vacuna para cada tipo de virus. Cuando se presenta un tipo de virus que la vacuna reconoce, ésta avisa al usuario de la presencia del mismo.

La desventaja, es que si no se cuenta con la vacuna adecuada, este virus atacará al equipo.

3.2 TÉCNICAS DE DETECCIÓN

La forma más evidente de detección es cuando el mecanismo destructor del virus ya ha sido activado y se empieza a tener problemas con el equipo, tal como la distorsión de la pantalla, ya que el sistema despliega ciertos mensajes como son: una pelotita brincando, caracteres o símbolos (♥ ♣ ● ○ ◘ ◘ ♠ _ _ _, etc) que no son propios del programa que se este ejecutando.

Para detectar la presencia de un virus se recomienda principalmente, instalar software de seguridad.

El instalar este tipo de software los detectores (ANTIVIRUS) y los protectores (VACUNAS), ayudarán a delatar el virus en su período de incubación, antes de causar el daño para el que fue creado.

La forma más fácil de hacerlo es que en todos los discos de arranque se introduce un detector que sea llamado por el programa AUTOEXEC.BAT, éste comprobará los programas del sistema, cada vez que se prenda el equipo.

Este tipo de programa, pertenece a los denominados COMPROBADORES.

a) **COMPROBADORES:** Este tipo de programas explora los archivos para identificar si es que éstos han sido alterados, dicha alteración puede ser en el tamaño del archivo (cuando es un programa), es decir "guarda" la información inicial del tamaño del programa y después verifica si éste se ha incrementado. Cuando esto sucede avisa al usuario. A este procedimiento también se le conoce como "Técnica de Fotografía". Es importante destacar

que éste tipo de programas únicamente detecta los problemas, -independientemente del causante del problema- por lo tanto, no puede combatirlo.

b) **OPERACIÓN ANORMAL DEL EQUIPO:** Las operaciones que realiza el equipo parecen lentas al usuario. Es decir, que el usuario va a sospechar algo anormal en el comportamiento del equipo cuando al cargar un programa para utilizarlo, éste se tarda demasiado en activarse. Adicionalmente, el tiempo de respuesta se va incrementando, o bien de la pantalla empieza a desplegar mensajes que no están relacionados con ningún programa.

Diferencias entre el ataque de un virus y una falla del equipo.

En caso del ataque de un virus como es el caso del Stoned, al encender el equipo, no se desplegará en la pantalla ningún mensaje del sistema, simplemente aparece en la pantalla el mensaje "YOGUR COMPUTER IS NOW STONED!". Así mismo, otros virus envían mensajes similares anunciando el daño que han ocasionado, es importante destacar que los mensajes se visualizan cuando el equipo está totalmente dañado y no puede seguir infectando a otros discos flexibles.

No todos los virus envían mensajes, otra forma de darse cuenta de su existencia, es comparar el tamaño de un programa, por ejemplo, darle el comando DIR y tomar nota al azar de cualquier programa, ejecutarlo, y después regresar a visualizar nuevamente con el comando DIR, se apreciará que el programa ha incrementado su tamaño.

Es importante destacar que el tamaño de un programa adquirido no puede incrementar por sí mismo su tamaño, lo que no ocurre con los archivos de datos capturados, ya que estos podrán incrementarse o decrementarse de acuerdo a las actualizaciones que le haga el usuario.

Las fallas de equipo pueden ser: Error de lectura en discos flexibles, error de grabación, encendido del monitor, error al imprimir, error en el teclado, error en el mouse. Lo que se acostumbra en estos casos es verificar todas las conexiones de los cables correspondientes, revisar el estado físico de los discos flexibles, existencia de corriente eléctrica, y por último apagar todo el equipo y volver a encenderlo.

3.3 TÉCNICAS PARA EVITAR LA PROPAGACIÓN

Existen varias técnicas para evitar la propagación de los virus siendo las más conocidas:

a) **Utilerías Antivirus.** Son programas dirigidos contra tipos particulares de virus informáticos. Estos antivirus funcionan analizando los ficheros en busca de secuencias de bytes características de un determinado virus, una vez que lo detecta lo desactiva.

   Sin embargo, la misma acción específica, de que los antivirus puedan limpiar los ficheros contaminados, hace que éstas utilerías tengan ciertas limitaciones: un antivirus protegerá contra un tipo particular de infección, pero basta con que alguien realice una pequeña modificación en el código del virus para que esta protección desaparezca.

Además, aun cuando se disponga de un programa que detecte diferentes virus, es claro que un nuevo virus brincará la protección de este antivirus.

b) **Método Quirúrgico**. Este método es en realidad una forma de probar todo el equipo así como los accesorios o periféricos que estén conectados a él. Es decir, que la desactivación y activación progresiva de cada una de las partes permitirá identificar paso a paso posibles problemas con estos. El método consta de:

-Apagar el equipo por un tiempo aproximado de dos minutos.
-Retire todos los medios de almacenamiento
-Desconecte todos los periféricos conectados a los puertos como son: impresoras, modems, y demás.
-Proteja contra escritura todos los medios de almacenamiento.
-Inserte en la unidad A una copia maestra industrial del DOS, protegida contra escritura y encienda el equipo.
-Borre todos los archivos con extensión .EXE, .COM ó .SYS
-Apague nuevamente el equipo por dos minutos.
-Vuelva a insertar en la unidad A la copia maestra del DOS.
-Reinstale los archivos del DOS a través de los comandos:

SYS C:
COPY COMMAND.COM C:

-Reinstale todos sus programas de aplicación (Extensiones .COM y .EXE)
-Apague el sistema, retire el diskette, conecte todos los periféricos y vuelva a encender el equipo, ya sin el diskette del DOS en la unidad A.

Si este método no funcionó, sólo le quedará el de formatear el disco duro, con lo que esto implica: La pérdida total de archivos y puede ocasionar daños al equipo.

CAPITULO IV

LOS VIRUS INFORMATICOS Y LA LEY

El derecho informático nace a partir de los 70's principalmente en Europa y Estados Unidos de Norteamérica con la aplicación de la informática al campo jurídico y legislativo en donde da como resultado la disciplina llamada informática jurídica o jurismática.

Sin embargo esta se extiende a la protección jurídica de los programas de computación (Derechos de Autor), régimen de contratos de bienes y servicios informáticos, delitos informáticos y el flujo de datos entre diferentes países.

De lo que se desprende, es que la ley busca darle protección primeramente al equipo a través del registro de marcas y patentes, para evitar la reproducción o copia no autorizada de estos, esto se hace a través de convenios internacionales y en la aplicación de medidas administrativas en el país en que se producen.

A través de los derechos de autor y contando con convenios internacionales, el derecho intenta frenar las copias no autorizadas de programas que utilicen las empresas sin pagar un sólo centavo por concepto de licencias de uso. Adicionalmente esta ley protege a los desarrolladores de nuevas aplicaciones que se hacen con las computadoras.

Existe una controversia respecto a castigar legalmente al creador de un virus, esto se debe a que los usuarios opinan que la creación de programas de virus es una acción terrorista y de manifiesta falta de ética, los fabricantes de software opinan que en algunos casos se justifica su utilización como esquemas de protección.

Justifican su proceder alegando que se han hecho demasiadas copias de algún programa fabricado por ellos y que al detectar demasiadas copias no pueden ser tratadas como copias legalmente autorizadas para uso personal. Los fabricantes los utilizan como esquemas de protección ya que destruyen los archivos en el disco que supuestamente tiene una copia ilegal o "pirata".

Puede ser que mientras no exista una ley que sancione el hecho anterior esta práctica se considere "legal".

Richard B. Levine en su libro Virus Informáticos (versión en español) nos dice: " En Estados Unidos de Norte América y sus estados existe un gran cuerpo de ley Penal disponible para procesar a personas que entreguen programas malignos a usuarios confiados. Pero ha habido sólo dos personas así procesadas hasta la fecha: Donald Burleson, que fue condenado bajo el antiguo estatuto de Texas, y Robert T. Morris, que ha sido acusado bajo la Ley Federal del Fraude y Abuso Informático. Muchos legisladores, tanto en el nivel estatal como federal, han llegado a la conclusión de que lo que se necesita son más leyes y más duras.

En el nivel estatal, Nueva York, siguiendo la iniciativa de California, está considerando una legislación (S.B. 5999-A) que castigará a las personas que inserten virus a sabiendas, aunque su efecto sea benigno o no se pretenda causar daño. Incluido con sanciones delictivas usuales está el obstáculo para empleo relacionado con la informática y una prohibición de instituciones académicas que concedan algún título o certificado relacionado con la informática durante la duración de los cargos calificados bajo la ley. La ley no ha sido eficaz y es dudoso si lo será alguna vez a la hora de controlar el problema de software destructivo. El problema con esto programas no es la suavidad de las leyes; es la vulnerabilidad de las computadoras y la dificultad de hacer cumplir la ley. "

CAPITULO V

EL VIRUS NATAS O SATAN

Este virus fue detectado en México a principios de 1994. Es necesario aclarar que se trata de un virus muy contagioso de tipo sigiloso y multipartita, es decir que es difícil de detectar y puede infectar la tabla de partición del disco duro, el sector de arranque los discos flexibles, el intérprete de comandos del sistema operativo y los archivos de tipo ejecutables, adicionalmente en últimas fechas se ha detectado que este virus tiene otra forma de presentación denominado " SEMILLA " o " EMBRIÓN ", con muy pocos bytes (al rededor de 170), esta forma de presentación es la responsable de la mayoría de las reinfecciones, por lo que si un archivo contiene esta "SEMILLA" y es ejecutado, el virus se regenera totalmente, reinfectando todo lo anterior.

La característica multipartita de este virus quiere decir que tiene varias facetas distintas y emplea alguna de ellas para atacar:

a) La tabla de particiones del disco duro.
b) El sector de arranque de los disco flexibles.
c) Todos los tipos de archivos ejecutables (.EXE, .COM, .SYS, .OVL, etc.)

Otra forma de actuar de este virus, es la alteración de la fecha del archivo en el momento de infectarlo, la mayoría de las fechas son incrementadas en 100 años (la de los programas o archivos ejecutables), es decir, que si el archivo tenía originalmente fecha de 1993, el NATAS lo cambiará a 2093. El usuario no podrá notar el cambio, ya que el comando DIR del DOS (Sistema Operativo) sólo leerá los dos últimos dígitos del año.

Adicionalmente el NATAS infecta de manera muy distinta a los diferentes tipos de archivos

ejecutables y en cada una de sus otras facetas, por estas razones estamos en el umbral de una nueva generación de virus.

El algoritmo para detectar y limpiar al virus NATAS es actualmente demasiado grande para simplemente adicionarlo a los programas actuales, esto dificulta la detección y eliminación de este virus.

Por otra parte, al generarse nuevas versiones o mutaciones del mismo virus las versiones normales no detectarán la presencia del NATAS en la memoria, en los archivos, ni en la tabla de particiones. Esto ocasiona que este virus sea de alta peligrosidad.

Es conveniente resaltar que para desactivar la presencia de este virus existen en la actualidad 21 versiones diferentes de vacunas.

En la facultad de Contaduría y Administración se utiliza el Scan de McAfee en su Versión 21.1; los pasos a seguir para detectar y combatir a este virus son:

- SCANPT C: Se emplea para detectar al virus en la tabla de particiones del disco duro y/o en la memoria de la Pc.

- CLEANPT C:(GenP) Se emplea para borrar el virus de la tabla de particiones del disco duro.

- SCANFIL C:*.* /REMOVE Se emplea para detectar los archivos ejecutables que contienen al virus en su forma natural (4744 bytes) y restaurar la gran mayoría de los archivos infectados.

- SCAN A:/MENÚ Para detectar en todos los discos flexibles.

CAPITULO VI

DISEÑO DE UN VIRUS

El desarrollo de un virus sólo se justifica si la persona que lo diseña va a utilizarlo para proteger el software que elaboró para un proyecto específico. Es conveniente resaltar que debido a las controversias que ha suscitado este tipo de problema, la ley no contempla medidas restrictivas al respecto.

La realización de un virus pasa como todos los programas por una etapa de planeación, diseño y desarrollo de las rutinas que servirán para los propósitos que son fijados con anterioridad.

La primera consideración es la de fijar el objetivo, el cual puede ser muy simple como hacer una broma, causar daño, superar dificultades, etc.

En la etapa de diseño es necesario que se preparen discos flexibles sin tener que utilizar el comando externo FORMAT del sistema operativo, esto se logra aprovechando un servicio del BIOS que permite formatear una pista entera del disco.

Con esta acción se crea una división en sectores, accesibles individualmente y que contendrán un número determinado de caracteres que se escribirán y leerán en bloque. Los sectores se van grabando uno a continuación del otro y se le van asociando los bytes identificadores según se van encontrando en el buffer, independientemente de que los valores encontrados en los mismos correspondan a la realidad o no.

En este punto podemos suponer dos situaciones diferentes: que todavía no se haya cargado el DOS y por otra que ya se haya cargado el DOS y por consiguiente ejecutado el IBMBIO.COM y el IBMDOS.COM, con lo que se podrán utilizar las rutinas de manejo y ejecución de archivos.

Si no se ha cargado el DOS habrá que utilizar las rutinas y las interrupciones del BIOS. Los nombres utilizados se asociarán a un número lógico (File_handle), esto permitirá utilizar posteriores accesos al mismo, este archivo que se crea no tendrá ningún atributo especial, por lo cual el valor que se coloca es cero. El programa del virus se coloca en la pista que fue formateada y la función de acarreo será uno por uno de los caracteres del programa particionado en ocho unidades (bit de acarreo), es necesario utilizar las funciones que permiten abrir, crear, cerrar, leer y escribir archivos que sean necesarios utilizando siempre una cadena de caracteres ASCII (Caracteres propios de la máquina).

Para crear un segmento de código residente desde la BIOS (única posibilidad para los contaminadores del BOOT) habrá que buscar una zona adecuada de memoria, llevar ahí el programa y proteger a la misma de posibles intentos de escritura.

Dentro del diseño se tendrá que considerar los siguientes pasos:

- Ejecución simultánea y repetida junto con el programa del usuario, es decir, que en esta parte se hará que el programa del virus se active cuando el usuario ejecute cualquier programa ejecutable (extensiones .EXE, .COM y .OVL).

Retardo de la acción, aquí se debe considerar los métodos de retardo, por ejemplo, en tiempo real que se alcanza con una fecha determinada tal es el caso del virus Viernes 13. Otro método consiste en predeterminar un número de veces que se ejecuta una rutina, y cuando se alcance un número determinado se activa la acción fatal, por último puede ser un retardo en una misma sesión con objeto de realizar la acción una o varias veces dentro de la misma.

- Otra parte a considerar será el desarrollo del método de ocultamiento y el desarrollo de la rutina de manifestación, es decir, si al activarse el virus este mandará un mensaje o no.

CAPITULO VII

DISEÑO DE UN ANTIVIRUS

La primera parte para diseñar un programa de antivirus será la consideración de que este programa detecte el virus en memoria, y mucho mejor si además lo elimina o desactiva. Hay que tener en cuenta que si se elimina el virus del disco, pero sigue en memoria es posible que se transmita de nuevo a aquel.

Será necesario diseñar rutinas de comprobación que indique que vectores de interrupción redirecciona, para poder restaurar sus valores originales, valores que estarán almacenados en alguna posición de memoria.

En segundo lugar para la detección de un determinado virus en disco será necesario conocer alguna cadena de caracteres característica de ese virus en concreto. Una vez conocida habrá que recorrer el sector de arranque o los ficheros ejecutables en busca de dicha cadena.

En el diseño al conocerse que los virus atacan el sector de arranque, los archivos .EXE, .COM u .OVL, primero se ejecutara a través del programa que busque todas las áreas marcadas como dañadas en ese sector, con el fin de detectar caracteres y eliminarlos. Por otra parte si se trata de un virus que ataque a los archivos .EXE, .COM. u .OVL se tomarán los datos iniciales del número de caracteres que ocupa cualquiera de estos programas, se compararán contra la información proporcionada por los fabricantes y por diferencia se encontrará si el virus del programa se encuentra al final o al principio de este. Otra parte a considerar es el desciframiento de la cadena de caracteres sobrante. Una ve conocida esta información (la diferencia entre caracteres será el tamaño del programa del virus).

CONCLUSIÓN

A través del presente trabajo, se ha visto cómo los virus ya forman parte de nuestra vida cotidiana, esto es debido a que los usuarios finales de los equipos de cómputo, no han desarrollado una cultura informática que les permita cumplir con normas básicas de seguridad e higiene, tal como: no utilizar discos flexibles de otros usuarios en sus propios equipos (de trabajo o personales), o compartir programas y/o datos.

Es posible que la ventaja que existe en la actualidad con los diferentes programas para combatir los virus se vean menos favorecidos con la aparición de nuevos y sofisticados virus (como es el caso del NATAS), que hará casi imposible que se frene la proliferación de estos. Ya que sólo es cuestión de tiempo para que se generen virus más potentes y hagan la lucha aún más difícil, sin embargo, es tiempo de que los usuarios adquieren consciencia plena de los peligros que le acechan si siguen utilizando copias piratas o ilegales de software desarrollado por personas capases y dedicadas a esta labor, por lo que considero que es mejor pagar al creador de un programa que utilizar una copia ilegal de su trabajo.

Los fines para los que fueron creados los virus informáticos se han cumplido en gran parte, pero, no ha sido un obstáculo para que las personas continúen con prácticas desleales en el uso de copias ilegales de software.

APÉNDICES

APÉNDICE A

ARQUITECTURA DE LA COMPUTADORA

Una computadora es una máquina capaz de aceptar, almacenar y procesar datos de manera que se obtenga información, y se presente esta de una forma que permita a las personas utilizarla en forma ágil y oportuna.

Tiene un comportamiento bastante parecido al ser humano. Los órganos sensoriales son el teclado, los puertos de comunicaciones, las memorias secundarias, los scaners, lápices ópticos, etc, el cerebro propiamente dicho será el procesador central, con su unidad de control, unidad aritmético lógica y la memoria principal y finalmente las extremidades serían la pantalla la impresora, etc.

De la misma manera que se puede diferenciar entre conocimientos, que es algo no material, y el soporte físico que la sustenta y que la hace real son las células nerviosas que forman la estructura física del cerebro, podemos diferenciar en una computadora una estructura física que se denomina HARDWARE y una estructura lógica llamada SOFTWARE. El HARDWARE es el conjunto de elementos materiales, circuitos electrónicos, mientras que el SOFTWARE son los programas o instrucciones para procesar la información.

De la misma manera que el cerebro recibe estímulos y emite órdenes al resto de los órganos del cuerpo, la computadora se comunica con el exterior recibiendo y enviando datos. Los recibe codificados en forma de impulsos eléctricos, los decodifica y procesa (siguiendo las instrucciones

de un programa) y obtiene nuevos datos o nuevas representaciones de los mismos enviando los resultados a los dispositivos de presentación al usuario.

Los dispositivos de procesamiento es la parte que se encarga de interpretar los datos que recibe y de enviar las órdenes a los demás elementos.

Dispositivos de almacenamiento, son las partes que se encargan, como su nombre lo indica de almacenar datos, programas y resultados, estos dispositivos pueden ser de almacenamiento primario como es el caso de la memoria principal de la computadora, o almacenamiento secundario como son los discos flexibles o un disco rígido instalado en el equipo (disco duro).

Dispositivos de comunicación se denominan dispositivos de entrada y salida ya que reciben datos del exterior y los transforman en impulsos eléctricos que serán enviados al dispositivo de procesamiento y por otro lado reciben las órdenes en forma de señales eléctricas del procesador y las transforman en imágenes en la pantalla, textos en la impresora, etc.

ANATOMÍA DE UN DISCO FLEXIBLE

Existen dos tipos de discos flexibles, uno de 5 1/4" y otro de 3 1/2". La estructura física de un disco flexible se compone de una cubierta protectora de vinilo, o de plástico, que sirve para proteger al disco contra el polvo, las huellas de los dedos, los líquidos, etc. en su interior se encuentra el disco, que es una lámina circular de un plástico llamado Mylar, recubierto en ambas caras por una fina película de óxido férrico.

ELEMENTOS DEL DISCO

Los campos magnéticos se registran en circunferencias concéntricas llamadas pistas a su vez estas se dividen en trozos pequeños del mismo tamaño llamados sectores. En los disco flexibles de doble cara un cilindro estará compuesto por las dos pistas de la cara anterior y posterior del disco. Para el acceso de la información contenida del disco se numeran los elementos que la componen (cilindros, pistas y sectores) al cilindro externo se le conoce como el cilindro cero, la primera pista de este cilindro estará situada en la cara cero y será la pista cero, la numeración continuará con la segunda pista del cilindro cero, cara uno y así sucesivamente.

Un sector es la mínima cantidad de información que se puede leer o escribir en el disco.

ANATOMÍA DE UN DISCO DURO

La estructura física de un disco rígido se compone de un conjunto de discos metálicos magnetizables, instalado dentro de la computadora para protegerlo contra el polvo, los líquidos, etc.

ELEMENTOS DEL DISCO DURO

Los campos magnéticos se registran en circunferencias concéntricas llamadas pistas a su vez estas se dividen en trozos pequeños del mismo tamaño llamados sectores. En los disco Duros un cilindro estará compuesto por todas las pistas del disco. Para el acceso de la información contenida del disco

se numeran los elementos que la componen (cilindros, pistas y sectores) al cilindro externo se le conoce como el cilindro cero, la primera pista de este cilindro estará situada en la cara cero y será la pista cero, la numeración continuará con la segunda pista del cilindro cero, cara uno y así sucesivamente.

Un sector es la mínima cantidad de información que se puede leer o escribir en el disco.

SECTOR DE ARRANQUE

Es siempre el primer sector (sector uno, cara cero, pista cero) de un disco flexible. En un disco duro este sector está reservado para la tabla de particiones del mismo, en él se encuentra toda la información necesaria para informar al DOS sobre las características del disco (o de la partición). Es por esto que todos los discos del DOS tienen este sector sean autoarrancables o no.

TABLA DE PARTICIÓN O ASIGNACIÓN DE ARCHIVOS

El tamaño de sectores de la FAT dependerá del tipo y la capacidad del disco, esta tabla contiene una entrada por cada cluster (parte física del disco). La secuencia de entrada corresponde con la numeración de los clusters esto quiere decir que el cluster número 250 del disco está asociado con la entrada 250 de la tabla.

ATRIBUTOS DE LOS ARCHIVOS

Los atributos de los archivos informan acerca de las características del mismo, las cuales pueden ser archivos de sólo lectura, archivos ocultos, archivos del sistema, etiqueta del volumen o subdirectorios.

APÉNDICE B

GLOSARIO

- ACCESO: Localización de datos almacenados en un sistema de cómputo o en un equipo relacionado con la computadora para fines de lectura, escritura o traslado de datos o instrucciones.

-ALMACENAMIENTO AUXILIAR: Almacenamiento que complementa la sección de memoria principal de la unidad central de proceso. Este puede estar en línea o fuera de línea

-APLICACIÓN: Uso de rutinas basadas en computadoras para fines específicos. Software o programas de cómputo que procesan datos que proporcionan datos para un fin determinado.

-ARCHIVO: Una colección de registros coleccionados que se almacenan juntos (también se llaman conjuntos de datos).

-BLOQUE: Conjunto de datos que se tratan como una sola unidad.

-BUFFER: Área de almacenamiento o dispositivo que se utiliza para reunir o ensamblar la entrada y salida para su procesamiento.

-CILINDRO: Grupo de pistas a las que se puede acceder al mismo tiempo sin mover las cabezas lectoras de los dispositivos de disco magnético.

-CLUSTER: Sectores contiguos. No se pueden representar o visualizar fisicamente en el disco.

-DATOS: Hechos ideas o conceptos que pueden ser reunidos y presentados electrónicamente y presentados en forma digital.

-DISCO MAGNÉTICO: Dispositivo de almacenamiento secundario, semejante a un disco fonográfico.

-DIRECCIÓN: Ubicación de una área en la cual se pueden almacenar datos o instrucciones en un equipo.

-DOS: Disk Operating System (ver sistema operativo).

-ENTRADA: Suministro o ingreso de datos o instrucciones al sistema de cómputo.

-HARDWARE: Es el equipo de computación o sean los dispositivos electrónicos, eléctricos y mecánicos que componen o constituyen un sistema de cómputo.

-INFORMACIÓN: Datos que han sido procesados en forma inteligible.

-PERIFÉRICO: Equipo que se conecta aun sistema de cómputo para ampliarlo.

-PISTA: Parte de un dispositivo de almacenamiento secundario que es accesada por una cabeza de lectura y escritura.

-RED: Interconexión de múltiples ubicaciones a través de algunos o varios canales para transmitir o recibir datos.

-RESPALDOS: Componente disponible sustituto o alterno en un sistema de procesamiento que puede ser utilizado en caso de una falla o daño.

-SECTORES: Trozos del mismo tamaño de una pista.

-SISTEMA OPERATIVO: Elemento de procesamiento que controla la operación de un sistema proporcionando medios para la entrada y la salida, ubicación de espacios de memoria, traducción de programas, etc.

-SOFTWARE: Nombre de uso extenso para los programas de computación.

-USUARIO: Persona que en realidad utiliza un sistema o salida de información.

APÉNDICE C

LISTA DE VIRUS

VIRUS QUE INFECTAN EL BOOT DE DISCOS FLEXIBLES Y ALGUNOS PROGRAMAS

- Angelina [Genb]
- Israeli Boot [Iboot]
- Den Zuk (5) [GenB]
- Predator Dropper [PDrop]
- Pakistani Brain (8)[Brain]
- Sundevil [Sun]
- Scythe2D [Scy]
- Windmill [Wm]
- Yale/Alameda (3) [Alameda]
- AirCop (3) [AirCop]
- DiskWasher [Genb]
- Ohio [Ohio]
- Swap Boot [Swb]
- Jack the Ripper [Genb]
- Stealth Boot B [Genb]
- World Peace [WP]
- Virus-101 [V101]
- _2kb [Genb]

VIRUS QYE INFECTAN PROGRAMAS Y EL BOOT DE DISCOS DUROS Y FLEXIBLES

- BFD [100]
- Curse Boot [Curse]
- Disk Killer (4) [Killer]
- Cannabis (2) [CB]
- Chaos [GenB]
- Empire (3) [Emp]

- Form (5) [Form]
- Horse Boot [DRP]
- Lockz [Genb]
- Microbes [Micro]
- Pirate [Pir]
- Stamford [Stam]
- WXYC [Genb]
- Ghost Dos-62 [Gho]
- Invader (8) [Invader]
- Mardi Bros. (3) [Mardi]
- Ping Pong-B (7) [Ping]
- Print Screen (2) [PrtScr]
- Typo Boot (2) [TBoot]

VIRUS QUE INFECTAN EL BOOT DE DISCOS DUROS Y FLEXIBLES , LA TABLA DE PARTICION Y ALGUNOS PROGRAMAS

- Aragon [Arag]
- Farcus [Farc]
- Malage [Mlg]
- Joshi (4) [Joshi]
- Loa Duong [Loa]
- Anti-Tel [A-Vir]
- EDV (2) [EDV]
- Night Grawler [Grwl]
- V82 [V82]
- Michaelangelo [Mich]

VIRUS QUE INFECTAN PROGRAMAS, LA TABLA DE PARTICION Y EL BOOT DE DISCOS FLEXIBLES

- Boot 437 [Genb]
- Boot Killer [BKil]
- Cansu [Can]
- Francois [Fra]
- Filler [Filler]
- Crepate [Cpte]
- Bloody! [Bloody]
- Germ [Grm]
- Catman [Ctm]
- Exebug1 [ExeBug1]
- Danny [Dan]
- Coruña3 [Cor]

- Fish Boot [GenB]
- Fish Boot [GenB/P]
- Kilroy [Klr]
- Michelangelo - E [Mich]
- Mugshot [Msht]
- No-Int [Stoned]
- Stoned [Stoned]
- Snafu [Sn]
- Swiss [Swiss]
- Zharinov [Zha]
- Exebug2 [ExeBug2]
- NOP [NOP]
- Michelangelo - D [Mich]
- Monkey [Mon]
- Music Bug (11) [MBug]
- Kurvy [Genp]
- Prism [Flip]
- Queen's [GenB]
- Swiss Variant [Swiss]
- Anthrax - Boot (2) [Atx]È

VIRUS QUE INFECTAN PROGRAMAS Y EL BOOT SECTOR DE DISCOS DUROS

- Gingerbread Man [GinB]
- Jackal [Jackal]
- BSI [Genb]
- NewBug [Genb]

VIRUS QUE INFECTAN PROGRAMAS, EL BOOT DE DISCOS DUROS Y LA TABLADE PARTICION

- Ekoterror [100]
- Telecom Boot [Telc]

VIRUS QUE INFECTAN PROGRAMAS Y LA TABLA DE PARTICION

- Crusher [Crsh]
- Datos [GenP]
- Invisible Man [IMP]
- Generic MBR [GenP]
- DiskWasher [Genp]
- Stealth Boot B [Genp]
- PL [PL]
- USSR 3103 [SVC]
- Parity Boot [Genp]
- Nice Day [GenP]
- Marzia [Marz]
- Jack the Ripper [Genp]
- X-2 [100]
- Azusa (2) [Azusa]
- Galicia [Genp]
- BSI [Genp]
- Flip (6) [Flip]
- Hasita [Genp]
- Crazy Eddie [Crazy]
- Tequila [Teq]
- Stealth Boot [Genp]
- Sticky [ML2]
- SVC 5.0/6.0 (2) [SVC50]
- NewBug [Genp]
- QMU [QML]
- _2kb [Genp]
- 2622 [2622]
- Angelina [Genp]

VIRUS QUE INFECTAN EL BOOT DE DISCOS FLEXIBLES

- Essex [Ess]
- Pentagon [Pentagon]

VIRUS QUE INFECTAN EL BOOT Y LA TABLA DE PARTICION

- Korea (4) [Korea]
- X-3A [X3B]
- Replicator [Rep]

VIRUS QUE INFECTAN LA TABLA DE PARTICION

- Coruña [Cor]
- Compiler2 [Cpl2]

VIRUS QUE INFECTAN PROGRAMAS

007 [007]
1008 [1008]
1024 (2) [Alf]
1024PSRC [PS10]
1049 [1049]
1076 [1076]
1210 [1210]
1241 [1241]
1253 - Boot [1253]
1260 (4) [V2P2]
1330 [1330]
1376 [1376]
1385 [1385]
1436 [1436]
1452 [1452]
1496 [1496]
1559/1554 (2) [1559]
1575/1591 (5) [15xx]
1677 [1677]
1 [N1]
1014 [1014]
1024E [1024E]
1030 [1030]
1067 [1067]
109 [109]
1236 [1236]
1244 [1244]
1253 - COM [1253]
1280 [1280]
1339 [1339]
1381 [1381]
1392 [1392]
145 [145]
1491 [1491]
1530 [1530]
1575 [1475x]
1605 (2) [Jeru]
1689 [1689]

1701 variant [17XX]
1701E [1701E]
1701F [1701F]
1720 (4) [1720]
1757 [1757]
1784 [1784]
1803 [1803]
1804 [1804]
1835 [1835]
1840 [Alf]
191 [Tiny]
1963 [1963]
1971/8 Tunes (2) [1971]
1984 [1984]
1984 [Genp]
1992 [1992]
1992B [1992B]
2000 [2000]
2014 [2014]
203 [203]
205 [205]
2062 [2062]
2153 [2153]
2300 [2300]
2330 [2330]
2470 [2073]
2559 [2559]
2560 [2560]
262 [262]
2803 [2083]
2930 [Spain]
?936 [2936]
2Kb [2Kb]
302 [302]
304 [304]
304-2 [304-2]
3040 [3040]
310 [GS]
337 [337]
344 [344]
3445 [4096]
355 [355]
365 [365]
370-B [370]
382 (2) [Pir]
384 [OW]
405 [Burger]
408 [408]
4096 (9) [4096]
422 [OW]
439 [439]
487 [487]

4915 [OW]
4Mat2 [4M2]
4Res [4Res]
500 [500]
510 [VHP]
512 (5) [512]
5120 (3) [5120]
547 [547]
555 [BWish]
557 [557]
560 [560]
578 [578]
592 [592]
5LO [5LO]
621 [621]
644 [644]
651 [Alf]
654 [640]
658 [657]
7% Solution [7%]
7% Solution 3 [7%3]
7% Solution v2.0 [7%v2]
702 [702]
709 [CSL]
727 [727]
733 [733]
737 [GN]
748 [748]
765 [765]
777 [777]
7808 [7808]
789 [Zar]
7th Son (4) [7S]
7thson 284a [100]
7thson 332b [100]
7thson 284 [100]
800 [800]
8000 [OW]
812 (2) [812]
834/Arab Virus [Ar]
855 [GN]
889 [889]
90210 [90210]
903 [903]
905 [905]
923 [923]
99%-B [99B]
99% [100]
A & A [AA]
A-403 [A-403]
ABC [ABC]
Abraxas [Abrx]

Acid [Acd]
Ada [Ada]
AGI-Plan [AGI]
AI [AI]
AIDS Trojan (13) [Aids]
Ajax [OW]
Alabama (3) [Alabama]
Alfa (2) [Alf]
Alien3 [Alien]
Ambulence 795 [Ambu]
Ancient [Anc]
Andre2 [And]
Andromeda [Andr]
Anninja [ANJ]
ANT [Ant]
Anti-D [GR]
Anti-Pascal II (4) [G3]
Arab 1600 [A1600]
Arcv-3 [ARC]
Arcv-2 [ARC]
Arcv-7 [100]
Arcv-5 [100]
Arcv-1 [ARC]
Arcv 773 [ARC]
ARCV 670 [ARC]
ARCV 718 [ARC]
Acme [100]
Agena [Agn]
Ah [Alf]
AIDS [N1]
AIDS II [A2]
Akuku (2) [Akuku]
Albanian [Alb]
Alien1 [Alien]
Alpha 743 [Alph]
Amstrad (7) [Amst]
Andre [And]
Andromeda [634]
Anna [Anna]
Ant-Cow [ACow]
Anthrax - File (4) [Atx]
Anti-Daf [ADaf]
Anti-Pascal (3) [AP]
Aragorn [Arag]
Arcv-3A [100]
Arcv-1A [100]
Arcv-6 [100]
Arcv-9 [100]
Arcv-8 [100]
ARCV 570 [ARC]
ARCV 693 [A693]
Arcv10 [ARC]

AREG [AREG]
Arka [Ark]
Armagedon (3) [Arma]
ASC [AC]
ASP-472 [472]
AT144 [144]
Atas-400 [400]
Athens [Ath]
Atomic1b [A1B]
Atomic2b [A2B]
August 16 [A16]
Aurea [Aurea]
Australian [GD]
B3 [B3]
BackTime [BT]
Bad-389 [bad]
Badcmdx [Badcmdx]
Badrom [Badrom]
Bak [Bak]
Bamestra 3 [Bam3]
Bamestra 6 [Bam6]
Bamestra 1 [Bam1]
Bamestra 8 [Bam8]
Bamestra [Bam]
Bandit [Ban]
Baobab 731 [Bao]
Argentina [GR]
Arma [Arma]
Arriba [100]
Ash [Ash]
Astra [AST]
Atas [Ata]
Atas3321 [Atas]
Atomic1A [OW]
Atomic2A [A2A]
Atte-629 [Atte]
Aurea 2 [Aurea2]
AusPar [APa]
B_Ugly [BUG]
BA101 [BA1]
Bad Sectors 1.2 [BSR]
Bad Boy (4) [BB]
BadGuy (3) [IB]
BadSectors 1.1 [BadS]
Bamestra 4 [Bam4]
Bamestra 2 [Bam2]
Bamestra 5 [Bam5]
Bamestra 7 [Bam7]
Bamestra 10 [Bam10]
Banana [OW]
Baobab 2 [Baobab2]
Barcelona [Barc]

Barrotes 2 [17SO]
Barrotes [Bar]
Basil [Basil]
Bat [Bat]
Beaches [Beaches]
Beast [Bea]
BeBe [BeBe]
Beeper (2) [Beep]
Beer [Beer]
bell [Bel]
Benoit [Ben]
Berlin [Bn]
Best Wishes [BWish]
Beta [Bet]
Beva-33 [Bv]
Beva-96 [Bv]
Beva-32 [Bv]
Beware [Bwr]
Big 2000 [2000]
Bit Addict [100]
Bit Addict [BitAdd]
Black Knight [BK]
Black Monday (3) [BMon]
Black Ice [B-Ice]
Blaze [OW]
Blinky [Blinky]
Bljec (8) [Blj]
Blood Rage [Bra]
Blood Lust [Blus]
Blood-2 [Blood]
Blood (2) [Blood]
Bob [Bob]
Bob5738 [Bob5738]
Bobo [Bobo]
Bow [5856]
Boys (3) [Boys]
Brainy [Bry]
Brotherhood [100]
Brothers [Bro]
Bryansk [100]
Bubbles 2 [Bbl]
Bubonic [Bubo]
Budo[OW]
Bugfix 1.1 [Bfix1.1]
Bumpy [Bumpy]
Burger (28) [Burger]
Burghofer [Bgh]
Burma [Burma]
Busted [Bst]
Butterfly [Bfly]
C [CV]
Cacophony [Caco]

Cacophony 2 [Caco2]
Cancer [Pix]
Carioca (6) [Carioca]
Cartuja [crt]
Cascade/170x (14) [170x]
Casino [Casino]
Casper (2) [Casper]
Caz [Zar]
CD [CD]
Cerburus [Cerb]
Cinderella [GS]
Civil War II [100]
Civil War [100]
CkSum [Cks]
Clint [Clt]
Clone Ware 2 [Clone2]
Clust [Clust]
Cobra [Cobra]
Coffee Shop [Cf]
Collor de Mello [Cdm]
Com2S [c2s]
Comspec [CSPEC]
Copyr-ug [1193]
Cossiga [1241]
Costeau [Cost]
CPXK [CX]
CADKill [GN]
Cara [Cara]
CaroEvil [CE]
Casc1621 [Cas]
Cascade [170xD]
Casino [Casino]
Casteggio [100]
CB-1530 [1530]
CD-10 [D2]
CFSK [CFSK]
Cindy [Cin]
Civil War III [CW3]
Civil War II v 1.0 [CWII]
Clint [Clint]
Clinton [Clt]
Clonewar [Clw]
Coahuila [Coa]
Code Zero
Color [GM]
Com16850 [C16]
Compiler2 [Cpl2]
Cop-Mpl [COP]
Copyright [1193]
Cossiga No Grazie [CNG]
Cpxk [Cpxk]
Cracker Jack [CRJ]

Cracky [Crk]
Crasher [Crs]
Crazy Imp [Imp]
CrazyI B [100]
Creeping Death [cd]
CreepingDeathDropper [cd]
Crew-2480 [GM]
CRF [CRF]
Criminal [Crm]
Crucified [Crucified]
Crumble [Crm]
Crunch1 [Cnch]
CSL (2) [CSL]
CV4 [CV4]
Cyber [Cybr]
Cyber-946 [100]
Cybercide [C-cide]
Cybertech 222 [C222]
Cysta 2711 [C-2711]
Cysta 8045 [C-8045]
Cysta 2954 [C2954]
Chad [Chad]
Chang [Cha]
Chaser [Chs]
Chcc [100]
Cheeba [Che]
Cheeba (2) [CHB]
Chemist [G1]
Chemnitz [Chm]
Chile Mediera [ChMe]
Chinese Blood [CHB]
Chr-869 [c869]
Chris [Chris]
Chrisj13 [Cj13]
Christmas Tree [XA1]
Christmas Violator[Vienna]
Chromosome [CG]
Chromosome Glitch [Chrome]
ChromosomeGlitch2[Chrome2]
D-Tiny (4) [DT]
Dada [Dd]
Damage [Alf]
Dark Avenger (11) [Dav]
Darkray [Darkray]
Darkray Dropper [Darkray]
Darth Vader (6) [512]
Data Rape 2.0 [DR20]
Data Lock B [Data Lock]
Datacrime/1168 (3) [Crime]
Datacrime-2 [Crime-2]
Datacrime II-B [Crime-2B]
DataLock [Data]

Datos [Datos]
Day10 [D10]
Dead [Dead]
Deceide2 [100]
Define [Def]
Demolition [Dmo]
Dennis [Den]
Deranged [De]
Dest3 [Dst3]
Devil's Dance (2) [Dance]
Digger [Dig]
Diogenes [Dio]
Dir Virus [Dir]
Dir II var [D2]
Dismember [Dsbr]
DLSU [DLSU]
DM-B [Dmb]
DNR [DNR]
Dodo 2456 [Dodo2456]
Doodle (14) [Doodle]
Dorn [Dorn]
DOS-1 [DOS-1]
Dos7-B [7-b]
Dose-A [OW]
Dot Killer [Dot]
Dr. Qumak2 [Qum]

Davis [Davis]
DBASE [Dbase]
Dec 3 [Dec3]
Dedicated [DAME]
Deicide [Dei]
Demon (6) [Dem]
Dennis [Dns]
Dest1-2 [Dst1]
Destructor [Destr]
Diamond-RS [DRS]
Dima [Dima]
Dir-2 910 [910]
Dir-2/CD 1x (3) [D2]
Dirty [Dirty]
Dk2 [DK2]
DM-330 [DM300]
DM (3) [GS]
Do Nothing [Nothing]
Dodo [Dod]
Doom II [Dm2]
Dos 7 [D7]
DOS3 [DOS]
Dos7-C [7-c]
Dot-789 [789]
Dot-801 [I-F]
Drop [Drop]

Druid [OW]
Dudley [Odud]
Dutch [Dt]
Dy [Dy]
Earthquake [EarthQ]
ECV [ECV]
Edcl [Edc]
Ein Volk [EV]
Eliza [El]
EMF 625 [100]
EMO [EMO]
Enemy [Enm]
Enola [Eno]
Error_412 virus [Err_412]
Estepa [Est]
ETC [ETC]
Evil Genius [Egn]
Explode [OW]
Exterminator [M45]
F-Word [FW]
FamC [FC]
FamE [FE]
FamJ [FJ]
FamN [FN]
FamR [FR]
FamV1 [F1]

DTR [DTR]
Dust [OW]
Dutch Tiny
E-riluttanza [E-rilutt]
Eclypse [100]
Ed [Ed]
Egg [Egg]
Einstein [Ein]
Elvirus [Elv]
EMF [EMF]
End-of [Eof]
Enigma [Eng]
Error [Er]
Espacio [Espacio]
Estepexe [Est]
Europe-92 [E92]
Exper416 [Exp]
Extasy [Ext]
Eziarch [Ezh]
Faerie [Faerie]
FamD [FD]
FamH [FH]
FamM [FM]
FamQ [FQ]
FamS [FS]
FamV2 [F2]

ESTA TESIS NO DEBE
SALIR DE LA BIBLIOTECA

FamV3 [F3]
FamV4 [F4]
Father Christmas [VHP]
Fattable [FAT]
Fear [100]
Fear [DAME]
Feist [Fst]
Fgt [GN]
Fich [Fch]
Fich897 [Fic]
Fil [Fil]
Filedate [FDt]
FileHider [FileH]
Filename [File]
Fingers [Sub]
Finn-357 [100]
Fish (2) [Fish]
Fish 2420 [Fsh]
Fish 2 [Fsh]
Fish1100 [Fsh11]
Flagyll [Flg]
Flash [Flash]
Flash [Flash]
Flex [Flex]
Flu-2 [Fl2]
Flue [Flue]
Fly11 [Fly]
Foetus 1.1 [Foetus]
Fone Sex [OW]
Forger2 [For]
Frajer [Frajer]
Fratricide [OW]
Free [Free]
Frere Jacques [Mule]
Fri13-nz [Fnz]
Friday 13th COM [Fri13]
Frodo Soft [FSof]
Frodo-458 [F458]
Frogs [Frg]
Fu Manchu (4) [Fu]
Fune [Fune]
Futhark [Futh]
Fvhs-a [OW]
Fvhs-B [OW]
Fword 383 [Fword]
G [G]
G2 [A429]
G2 [D598]
G2 [A438]
G2 [Celeste]
Galicia [Genb]
Ganeu [Ganeu]

Geek [GK]
Generic Boot [GenB]
Generic File [GenF]
Gergana (9) [Gerg]
Get Password 1 [Jeru]
Ghost COM [Ghost]
Gijon [gj]
Gliss [Gls]
Goblin [CRJ]
Gold [Gld]

Golgi-1 [Gol1]
Golgi-3 [Gol3]

Golgi-2 [Gol2]
Gomb [Gomb]

Gorlovka [Glvk]
Gosia [Gs]
Got-you [GY]
Gotch 4 [Got4]
Gotcha 2 [Got2]
Gotcha 1 [Got1]
Gotcha (4) [G4]
Gotcha 3 [Got3]
Gotcha [Gto]
Grapje [Gr]
Graveyard [Grave]
Grease [GS]
Greemlin [Alf]
Green Catapillar [Gcat]
Green [Gre]
GreenCaterpillar [GreenCat]
Grog 3.0 [Grog3]
Grog31 [G31]
Groovy [Groovy]
Growing Block [GD]
Grue [Gru]
Grunt [Grnt]
Grunt 427 [G427]
Grunt-3 [Grt]
Gsav [Gsav]
Guppy [Guppy]
H-457 [Coa]
H-2 [H-2]
HA [HA]
HACKER [HCK]
Hacktic [Hck2]
Hafen [Hafn]

Haifa [Hf]
Hallo 751 [H-751]
Hallo 759 [H-759]
Halloween [HW]
Handi [Handi]
Happy [Hpp]
Harm [Harm]
Hasita [Genb]
HBT [HBT]
Hellween 1182 [1182]
Here [Hre]
Hero-394 [HrB]
Hiccup [Hic]
Hiperion [Hip]
Hitchcock-B [Hitc-B]
Holiday [Holiday]
Holland Girl (6) [Sylvia]
Horror [Hrr]
House [House]
Huge [Huge]
Hybrid [Hyb]
Hymn (3) [Hymn]
IB Demonic [OW]
ICE9-199 [I199]
ICE9-224 [I224]
Icelandic (3) [Ice-3]

Halley [Hal]
Hallo [Hallo]
Halloechen [Hal]
Hammer [Ham]
Happy N. Y. [HNY]
Hara [kiri]
Hary [Hary]
Hate [HT]
Hello [Hlo]
Hellween [1376]
Hero (2) [G3]
Hi [Hi]
Highland[High]
Hitchcock [Hitc]
Hitler [Hit]
Holo/Holocaust (3) [Hl]
Homecoming [Home]
Horse (7) [Hrs]
HS [G4]
Hungarian [Hng]
Hydra (12) [G3]
I-B (5) [IB]
Ice 9 [I9]
Ice9-250 [I250]
ICE9-159 [I159]
Icelandic II [Ice-3]

Icelandic-3 [Ice-3]

Idle [Idle]

Ieronim [Ier]

IKV528 [G2]

Ill [Ill]

Incom [Inc]

Infinity [Inf]

Inofensivo [Ino]

Inrud-B [Intr]

Internal [Intl]

Intruder C [Intr-C]

Invisible Man [IMF]

Invol Virus [Inl]

IOU [IOU]

Iranian [Irn]

Iraqi Warrior [Lisbon]

IT [IT]

Italian Pest (3) [Murphy]

ItaVir (3) [Ita]

IVP [Yeah]

IVP EX1 [IVP]

IVP [Tuesday]

IVP [Cristal]

IVP [IVP]

IVP [Sleeper]

IVP EX2 [IVP]

James Bond [JB]

Japan [C-J]

Jason [Jason]

Jaxx [Jaxx]

JD [JD]

Jeff (3) [Jeff]

Jericho [Jericho]

Jerk (2) [Jrk]

Jeru-Dyslex [Jd]

Jeru-1663 [J1663]

Jerusalem (48) [Jeru]

Joanna [Joa]

John [OW]

JoJo (3) [JoJo]

Joke [JK]

Joker (3) [Joke]

Joker-1602 [J1602]
Jos [100]
July 13th [J13]
July13 [Jul13]
Jump4Joy [J4J]
June12 [June12]
Justice [Jus]
K-4C [K-4C]
K-4B [K-4B]
Kamikaze [Kami]
Kasimir [1994]
Kela [Kela]
Kemerov (5) [Keme]
Kersplat [Ker]
Kiev [Kiev]
Kill814 [K814]
Klaeren [GH]
KODE4v1 [100]
Kohntark dropper [Kdrop]
Kremikovtzi [Krem]
KU-448 [KU]
Kukaturbo [Kakt]
L-993 [993]
Label [Label]
Lanc [Lan]
Lanc5882 [Lan]

Joker3 [J3]
Joshua [Jsh]
July 26 [J26]
July13 [J13]
June 16th [June16]
June1530 [J1530]
JW2 (2) [Jab]
K [K]
Kalah [GR]
Karin [GN]
KBug [Kbu]
Kemerov (3) [Kem]
Kennedy (4) [Tiny]
Khobar [Khobar]
Kiev-1 [K1]
Kiwi-550 [Kiwi]
KODE4 [K4]
Kohntark [Khon]
Konrad Zuse [Zuse]
Krivmous [Krv]
Kuang [Kug]
Kuzmitch [Kzm]
L1 [L1]
Lamer [Lam]
Lanc5476 [Lan]
Larry [Lar]

Last Year [Last]
LCV [LCV]
Leech [Leech]
Lehigh (2) [Lehigh]
Lepro-B1 [OW]
Leprosy-3 (4) [Lep3]
Leprosy-B [Vip]
Lib1172 (2) [1186]
Liquid Code [LQC]
Lisbon (2) [VHP]
Little Red [Lilred]
Little Brother 299 [100]
Little Girl [LG]
Little Brother 349 [LB]
LockJaw [LJ]
Locks [Locks]
Lor [Lor]
Love Child (3) [LC]
Lozinsky (4) [Loz]
Luca-309 [Luc]
Lycee [Lyc]
LZ [LZ]
M-128 [M128]
MacGyver [MacG]
Magnitogorski 3 [Magn]
Malagda2 [Mal2]

Lazy [Lazy]
Leapfrog Virus (3) [Leap]
Leech [Leech]
Leper AOD [OW]
Leprosy (7) [Vip]
Leprosy [NC3.0]
Les [Les]
Liberty (13) [Liberty]
Liquid Code - 2 [LC2]
Little Brother [LB]
Little [Ltt]
Little Pieces [LPC]
Little Brother 361 [LB]
LixoNuke [Lix]
LockjawZ [Lckjz]
Loki [1234]
Loren [Lor]
Love Child 2710 [Lov]
LPT-OFF [LPT]
Lucifer [Alf]
Lycee-1888 [Lycee]
LZ 2 [LZ2]
Macedonia [1385]
Madismo [Mds]
Magnum [Mgm]
Malaise [Mls]

Malign [Maln]
Malmsey2 [Malm]
Maltese Amoeba [Irs]
Mandela [Mnd]
Mannequin [Mn]
Manta [Mant]
March 25th [March25]
Math Test [Math]
Mayak [Mayk]
MCWH1022 [MCW]
McWhale [MCAF]
Meditation [100]
Mem Lapse 375 [ML375]
Mercury [Merc]
Metallica 2.0 [Metal2]
Mface [Mfc]
MGTU Virus (4) [MGTU]
Miky [Miky]
Milano [Ml]
Mindless [OW]
Mini-195 [M195]
Mini-207 [M207]
Minimax [Minmx]
Minsk-GH [Mgh]
Mirror (2) [Mirror]
Mithrandir 1 [Mith1]
Malmsey Habitat v3.b [MH3]
Malsmsey[OW]
Mandela 2 [Mnd-2]
Mannequin [MN]
Manola [Mno]
Marauder [Mar]
Mark II [M-II]
Matura [Mat]
Maze [Maze]
McWhale [McW]
Medical [Med]
Mem Lapse 323 [ML323]
Memory Lapse [ML]
Merry Xmas [mXs]
Mexican [Mex]
MG (4) [MG]
Michelangelo II [MichII]
Mila [Ow]
Miles [Miles]
Mini-125 [M125]
Mini-132 [M132]
Mini Virus (4) [M45]
Minimite [Mite]
Mir (2) [DAV]
Mithrandir 3A [Mith3A]
MIX1 (4) [Ice]

Mix2 [MX2]
Moctezuma [MC]
Mono [G1]
Monxla-B [MX-B]
Morganism [Morg]
Mosquito [Mosq]
MPC [MPC]
MPS 3.1 (3) [MPS]
Mr. Vir [MV]
Mshark-S [Mshark]
MSTU [GN]
Mule [Mule]
Multi [M-123]
Mummy [Mum]
Murphy (6) [Murphy]
Mutation Engine [DAME]
Mystic 2 [Mys2]
N-Beta [N-Beta]
NAPC [NAPC]
Naught [Nau]
Nazi [Ram]
Necro (NFear) [100]
Necrophilia [Nec]
NED [100]
New-1701 [1701]
Next Generation [NG]

MLP [MLP]
Monika [Mk]
Monxla (3) [VHP]
More [More]
Mormorio [Ow]
Mozkin [Hf]
MPS 1.1 [M11]
Mr. G [MrG]
MR. D [MrD]
Msk [100]
Mule (2) [Mule]
Multi-11 [Multi1]
Multi-2 [M12]
Munich [Mnc]
Mutant (8) [Mut]
MX [MX]
Mystic [Mys]
Nanite [Nan]
Naught 2 [Naught2]
Navigator [Nav]
NCU Li [Li]
Necro [Necro]
Necrosoft [Nsft]
New Sunday [NSun]
Newcom [Alf]
Neznamy [NZ]

Nice Day [GenB]
Nines Compliment [Nns]
No Frills 3 [NF3]
No Frills [1358]
No Party [OW]
No Frills 1 [NF1]
Nocciola [Nocc]
Nomenclature (4) [Nom]
Nov17 [17th]
NPox 2.1 [NPX]
Nuke GV [NGV]
Number6 [N6]
Nympho 1 [Nymph]
Offspring [V0.05]
OffSpring 82 [V0.82]
Omud-512 [Omud]
Oropax (5) [Oro]
Over 4032 [OW]
Oxana [oxa]
P1 (7) [P1r]
PA-5792 [PA]
Padded [Pad]
Page [100]
Parasite [Par]
Paris [Paris]
Parity [G2]

Nina [Nina]
Ninja [Nja]
No Frills 1.1 [NF11]
No Wednesday [NWed]
No Frills 2 [NF2]
Nobock [Nbk]
NoCopy [NC]
Not-586 [Not]
NPox 2.0 [NPX]
Nuke 93 [Nuke93]
Null [NL]
Nygus-KL [Nkl]
Off Stealth [SVC50]
Offspring [Offs]
Omt [417]
Ontario [Ont]
Otto-415 [100]
Over4032 [O-4032]
P-45 [P45]
P529 [529]
Packet [Pack]
Page B [PB]
Paradise [Pas]
Parasite-2B [Ps2]
Parity Boot B [ParB]
Parity Boot [Genb]

Particle Man [PMN]
Pas-4260 [OW]
Pas-5220 [P5220]
Patch [OW]
PathHunt [Ph]
Patient [Pt]
Patsy [Pts]
Payday [Jeru]
PC Flu [802]
PCBB11 [PCB]
PCBB3072 [PCB]
PCBB5B [PCB]
PCV [PCV]
PE2 [PE2]
Peace Man [Peace]
Peach [Pch]
Peek [Pek]
Pegg [Pg]
Peligro [Pel]
Penis Size [Pen]
Penza [Pnz]
Perfume (2) [Fume]
Pest (8) [Murphy]
Phalcon [Phalcon]
Phantom [Pht]
PI [PI]
Piazzola [Pia]
Pig [Pig]
Pinky Ghost [Pinky]
Pirate [Pirate]
Pirate [Pir]
Pit 1228 [Pit]
Pixel (5) [Pix]
PL [PL]
Plague (3) [Plg]
Plastique (9) [Plq]
Platinum [GE]
Plov [Plov]
Plumbum [100]
Plutto [Plu]
Poem [Pm]
Pogue [Pog]
Poison [Poi]
Pojer [Poj]
Polimer [Polimer]
Polish-2 [Pol-2]
Polish-583 [P583]
Polish Tiny [Plt]
Polish 217 [P-217]
Poor Man [Poor]
Popoolar [OW]
Porridge [Prdg]

Pose [Pose]
Predator [Pred]
Pregnant [Prg]
Prime [Prm]
Prob-734 [100]
Protipus [Protipus]
Prova [Prova]
PS-MPC [339]
PS-MPC [331]
PS-MPC [Spirit]
PS-MPC [Trex]
PS-MPC [353]
PS-MPC [DataDeath]
PS-MPC [478]
PS-MPC [351]
PS-MPC [573]
Puke [100]
Quadeque 2 [Quad2]
Quadeque 2 Dropper [Qdrop]
Quiet [Qt]
R-10 [R10]
R&S [R&S]
Radyum-C [RdC]
Rage [Rag]
Random [Rdm]
Raubkopi [Raub]
Possessed (6) [Poss]
Preditor II [PredII]
Prime Evil B [PEB]
Print Monster [PM]
Problem [Prb]
Proto-T [100]
PS-MPC [338]
PS-MPC [PS-MPC]
PS-MPC [Pussy]
PS-MPC [War]
PS-MPC [344]
PS-MPC [Helmet]
PS-MPC [564]
PS-MPC [352]
PS-MPC [337]
Psycho [Psc]
Quadequa [QQ]
Quadeque 1 [Quad1]
Quake-o [Qo]
Quito [Quito]
R-11 [R-11]
Radyum [Rad]
RadyumB [RdB]
Ram [Ram]
Rattle [Rttl]
Reaper

Rebo-715 [R175]
Red Spider [RedSpi]
Red Team [VCL]
RedX (2) [Redx]
Reklama [Rkm]
Relzfu [233]
Reset [RST]
Revelation [Pvl]
Riihi [Rii]
RMIT [RMIT]
RNA [RNA]
Robert Walls [RW]
Robert Walls 1.0X [RW0X]
Rocko [Roc]
Romanian [Rmn]
RPVS [453]
Russian Tiny [Rt]
S-847 [Pix]
Sabath [Sab]
Saddam [Saddam]
Sadist [Sadt]
Sair [Sair]
Sandra [OW]
Sandwich [Sand]
Saratoga [Doodle]
Satan Bug [SatanBug]
Saturday 14th (3) [Arma]
Saturday [Sat14]
Sayha Waptpu [SW]
SBC [SBC]
Scker [Sck]
Scott's Valley [2133]
Scr-2 [Scrm2]
Scream1 [Scr1]
Screaming Fist IIV [SFIIV]
Screaming Fist 650 [Scr]
Screaming Fist724 [SCR724]
Scribble [OW]
Scroll [Scl]
SCT [SCT]
Schrunch [Sch]
Sdir [Sdir]
Secrets [OW]
Semtex [Set]
Sentinel-X [BCV]
Sentinel (3) [Sent]
Sepage [Sepage]
Serena [100]
Sergeant [Ser]
Sh [Sh]
Shadow (3) [Sha]
Shadow [100]

Shake (2) [Shake]
Shanghai [Shg]
Shiny Happy [Shiny]
Silence [Sil]
Silver Dollar [OW]
Silly Willy [SilW]
Simulati [Sim]
Sk [Sk]
Skeleton [SkN]
Skism [Jeru]
Slant [OW]
Sleep Walker [SW]
Slow (5) [Slow]
Sma-108a [Sma]
Small 146 [S146]
Small 185 [S185]
Small 129 [S129]
Small Experiment [SE]
Small 187 [S187]
Smallexe [100]
Smell [BS]
So [So]
Solano (4) [Sub]
Sonik Youth [Sonik]
Sorlec 5 [Sorl]
Soupy [Sou]

SHAMAN [SHMN]
Shield [Shd]
Shock Therapy [ShT]
Silent Killer [Silent]
Silver3b [OW]
Simple 1992 [Sim]
Sis (2) [Sis]
Sk1 [Sk1]
Skew 469 [s469]
Skism808 [100]
Slayer [Slay]
Slovak [Slv]
Sluknov [Slu]
Small 157 [S157]
Small 178 [Smal]
Small 115 [Small]
Small 132B [S132B]
Small [100]
Smallarc [100]
Smaug [Smaug]
Smily [G2]
Socha [SCH]
Something [658]
Sorlec 3/4 [Sorl]
Sorry (3) [Sorry]
Sov (3) [Sov]

Soyun [Soy]
Spanish [Spain]
Spanz [Spz]
Split [Split]
Sprint [768]
SQR [SQR]
Squeaker [Sqe]
SRE [SRE]
Stahl Platte [Sta]
Star Dot [Sdot]
Starship [Stsh]
Stealth Boot [Genb]
Stimp [Stimp]
Stink2 [Sti2]
Storm [Storm-1163]
Stupid [100]
Subliminal (3) [Sub]
Suicide [Sui]
Sunrise [Sun]
Suriv 402 [GR]
Surrender [707]
Sverdlov (2) [Sv]
Swiss 143 [Gtc]
SX [SX]
Sylvia [Sylvia]
Syslock/3551 [Syslock]
Spanish April Fool [D28]
Spanish Holidays [Span]
Spar [Spar]
Sprint [640]
Spyer (4) [Spyer]
Squawk [Sqk]
Squisher [Squ]
Staf [Staf]
Star Dot (4) [Sdot]
Stardot-801 (3) [I-F]
Stasi [Stasi]
Scerculius II [SterII]
Stink [Sti]
Stone-90 [VHP]
Striker [STR]
Sub-Zero [SZ]
Suicidal [Scdl]
Sunday-2 [Su2]
Suriv B [Surivb]
Suriv A (2) [SurivA]
Susan [OW]
SVir (4) [Svir]
Swiss Phoenix [SPh]
Sylvia [Sylvia]
Sys Virus [Sys]
T-1 [T-1]

T-series [Tser]
Tabulero [Tab]
Tack [411]
Taiwan (11) [Taiwan]
Taiwan4 [JeruA]
Taocheng [Tao]
Tecla [Tec]
Telecom File [Tele]
Teletype-2 [Tel-2]
Terror (3) [Ter]
Teufel [Teu]
Thriller [Thrill]
Tim [Tim]
Timid 371 [T371]
Timid 290 [T-290]
Timid 557 [T-557]
Timid [Tmd]
Tiny 133 [T133]
Tiny 212 [T212]
TMTM [TMTM]
Todor [Tdr]
Tomato [100]
Tony [Tn]
Tonya2 [Ton]
Torino virus [Tor]
TP [TP]
T297 [T297]
Tabulero 2 [100]
Tack [477]
Taiwan3 [T3]
Tamper [Tamp]
Taselhoff [Tasel]
Techno [Tch]
Telekom [GTk]
Teletype [Ttp]
Tester [TV]
Texas Joker [Texas]
Thursday 12th [T12]
TimeMark [Tim]
Timid-LM [TLM]
Timid 382 [T382]
Timid 431/402 [T431]
Timid305 [Timid]
Tiny (31) [Tiny]
Tjack [TJK]
Today [OW]
Tokyo [Tokyo]
Tongue [100]
Tonya [Ton]
Topo [Topo]
Toys [100]
TPWorm [TP]

Traceback (3) [3066]
Traveller [Travel]
Traveller [GN]
Trekvir [Trek]
Tremor2 [Tremor2]
TridenT [TridenT]
Triple Shot [3Sht]
Trivial 45 [OW]
Trivial 4B [Triv4B]
Trivial 97 [T97]
Troi Two [Tr2]
Troi [GS]
Tron [Tron]
Tschantches [Tsch]
TU-482 [TU]
Tuesday (2) [Alf]
Tula [Tula]
Tumen V0.5 [Tum5]
Tumen V2.0 [Tum2]
Tumen [Tum]
Turbo (2) [Pol-2]
Turkey [Trk]
Tver [Tver308]
Twin Peaks[OW]
Twin-351 [Twin]
Typo/Fumble/712 (2) [712]
Ucender [Jeru]
Ugur [Ugur]
Ultimate [Ult]
Unbx [Unbx]
Unk [Unk]
Uriel [Uri]
Uruk 300 [U-300]
Uruk 361 [U-361]
Uruk-Hai [Uruk]
USSR 707 [U707]
USSR 696 [GR]
USSR 600 [U600]
USSR 948 [U948]
USSR 830 [U830]
USSR 711 [U711]
USSR 394 [U394]
USSR 2144 (8) [U2144]
USSR 516 (4) [Leap]
USSR (11) [USSR]
USSR 256 (5) [U256]
USSR 1049 [Alf]
USSR 257 [U257]
USSR 492 [U492]
USSR 311 [U311]
V-Label [Label]
V-388 [388]

V-3000 [V3000]
V-351 [351]
V1-Not [OW]
V1_0 [OW]
V1028 [QP2]
V125 [M128]

V1463 [1452]
V163 [163]
V2_0 [OW]
V2000 (3) [RKO]
V2100 (5) [RKO]
V270X [268P]
V299 [V299]
V2P2 [v2p2]
V2P6 [V2P6]
V400 (5) [MCE]
V483 [G3]
V5 [v-5]
V600 [V600]
V800 (3) [V800]
V801 [V801]
V914 [914]
V961 [V961]
VA [VA]
Vacsina (19) [Vacs]
Varicell [Varicell]
VCL [VCL]
VCL 596 [VCL]
VCL-HEEVE
VCL [Con]
Vcomm (5) [Vcomm]
VCS [100]
VDV-853 [VDV]
Venge-E [OW]
VHP (7) [VHP]
VHP-2 [VHP2]
Victor (2) [Victor]
Vienna 827 [Vien827]
Vienna/648 (49) [Lisbon]
Violator (5) [Vienna]
Viper [Vip]
Virdem [100]
Virflop [Flop]
Virus-90 [90]
Virus9 [V9]
VM [VM]
Voco [OW]
Volkov [Vol]
Vootie [OW]
Voronezh (2) [Vor]

Vote/Vote1000 [Vot]
Vriest [1241]
VVF-34 [vvf]
Walkabout [Walk]
Warez [Wrz]
Warrior [War]
Weak [Wek]
Wharps [Wha]
Why_win [Why]
Wild Thing A [WTA]
Willow 2 [Will2]
WinVir [WinVir]
Witcode [Wit]
Wolfman (3) [Wolf]
Woodstock [Wood]
Worm [Worm]
X-1 [100]
X-3B [X3B]
Xabaras [Xab]
Xpeh [XP]
Xute [Xute]
Yank [2189]
Yankee [Doodle]
YB-X [YB-X]
Year 1993 [Y93]
Youth [Yth]
VP [VP]
VTS [VTS]
W13 (4) [G2]
Walker [Wlk]
Warrior 2 [war2]
WAVE [WV]
Whale (34) [Whale]
WhoCares [Who]
Wilbur 3 [100]
Willistrover III [WIII]
Willow [Wi]
Wisconsin (3) [Wisc]
Wizard 3.0 [Wzd]
Wonder [Wnd]
Wordswap (4) [Ws]
WWT (3) [WWT]
X-3A [X3]
X77 [X77]
Xpeh - 2 [Xpeh]
XTAC [XTa]
Xuxa [GR]
Yankee - 2 [Doodle2]
Yap [Yap]
Yeah Right [IVP]
Youth [Hannibal]
Yukon [OW]

Z10 [Z10]
Zaragosa [Zar]
Zero Bug/1536 [Zero]
ZeroHunt [Hunt]
Zombie [Zmb]
ZU1 [ZU1]
Zak2 [Zak2]
Zeppelin [Zpp]
Zero Time [Zrt]
ZK900 [Z900]
ZRK (3) [ZRK]
ZY [ZY]

BIBLIOGRAFÍA

Acco, Alain
La peste informatique
París, Plume @1989

Haynes, Colín
The computer virus protección handbook
San Francisco, Cal. Sybex @1990

Hruska Jan
Computer viruses & anti-virus warfare
New York, E. Horwood, @1990.

Scan Antivirus: Sistema Integral de Seguridad
Viruscan, Clean-up, V-shield
México, Mcafee, @1993.

Ferbrache, David
A Pathology of computer viruses
Springer-Verlag
London, LTD @1992

Ferreyra, Gonzalo
Virus en las computadoras
México, Macrobit @1991

Kane Pamela
El libro de los virus.
Madrid, Anaya Multimedia @1991.

Levin, Richard
Virus informáticos
México, McGraw Hill @1992

Norton, Peter
Norton antivirus
México, Prentice-Hall @1993

Nombela, Juan José
Virus Informáticos
Madrid, Paraninfo @1990

PC/TIPS Byte (Edición en Español)
Año 6 No. 64
1° de Mayo de 1993

PC/TIPS Byte (Edición en Español)
Año 6 No. 61 y 62
1° de Febrero de 1993
1° de Marzo de 1993

PC Magazine (Edición en Español)
Vol. 3 No. 2
Febrero de 1992

PC Magazine (Edición en Español)
Vol. 5 No. 3 y 9
Marzo de 1994 y Septiembre de 1994.

Altmark Daniel Ricardo
Informática y Derecho
Vol. 1
Buenos Aires, 1987

Téllez Valdés Julio
El Derecho Informático
Ediciones UNAM 1987

Greer Williams
Cazadores de Virus
Ediciones Toray
Barcelona, 1966

Pennington T.H.
Virología Molecular
Ediciones Omega
Barcelona, 1979

Mur Alfonso
Guía práctica para usuarios
Ediciones Anaya Multimedia, México D.F., 1990