
UNIVERSIDAD DON BOSCO
VITAM IMPENDERE VERO

UNIVERSIDAD DON BOSCO

FACULTAD DE INGENIERÍA

ESCUELA DE COMPUTACIÓN

TEMA:

"INVESTIGACIÓN DOCUMENTAL DE VIRUS DE COMPUTADORAS"

TRABAJO DE GRADUACIÓN PARA OPTAR AL TÍTULO DE INGENIERO EN CIENCIAS DE LA COMPUTACIÓN.

PRESENTADO POR:
EDGARD ALEXANDER PEÑA BELTRÁN

Ciudadela Don Bosco, Julio Del 2003.

San Salvador, El Salvador Centroamérica

UNIVERSIDAD DON BOSCO

FACULTAD DE INGENIERÍA

ESCUELA DE COMPUTACIÓN

AUTORIDADES

RECTOR:

ING. FEDERICO MIGUEL HUGUET RIVERA

DECANO DE LA FACULTAD DE INGENIERÍA:

ING. CARLOS BRAN

ASESOR DE TRABAJO DE GRADUACIÓN:

ING. JULIO ADALBERTO RIVERA PINEDA

JURADO EVALUADOR:

ING. ERICK FLORES
LIC. GERARDO CALDERÓN
ING. JULIAN RIVERA

UNIVERSIDAD DON BOSCO

FACULTAD DE INGENIERÍA

ESCUELA DE COMPUTACIÓN

TEMA:

"INVESTIGACIÓN DOCUMENTAL DE VIRUS DE COMPUTADORAS"

ING. JULIAN RIVERA PINEDA	**LIC. GERARDO CALDERÓN**
Jurado	**Jurado**
ING. ERICK FLORES	**ING. JULIO RIVERA PINEDA**
Jurado	**Asesor**

DEDICATORIA

A mi DIOS padre todo poderoso *que siempre estuvo conmigo en todo mi camino, por darme la fuerza, paciencia y sabiduría necesaria para poder cumplir esta misión tan importante, la cual le dedico con todo mi corazón y mi mente. También a MARIA AUXILIADORA, no mas me queda decirle Gracias y Misión Cumplida.*

A mis amados padres: Ramon Peña y Irma Gamez*: quienes me dieron todo lo que un padre le puede dar a un hijo, en especial por la herencia más valiosa que pudieron darme , el amor.*
Quienes sin escatimar esfuerzo alguno , sacrificaron gran parte de su vida para formarme y educarme. Y a quienes nunca podré pagar todos sus desvelos ni aún con la riqueza más grande del mundo.

A mis hermanos*: quienes un día me inspiraron a seguir adelante. Los quiero mucho.*

A todos mis amigos*: En especial a mi mejor amigo Mario Dubon, por su apoyo moral y académico, porque siempre que necesite un consejo ahí estuvo.*

A mi novia Jennifer Martínez *con mucho amor, por toda la comprensión y paciencia que me brindó, por dejarme aprender y enseñar a ser un ejemplo para todos.*

A mi asesor Ing. Julio Rivera*, por el apoyo y confianza que me hizo sentir de poder realizar todo lo necesario y transmitirme parte de su conocimientos para culminar mi carrera. Pero en especial por haberme dado su amistad junto a la de su hermano Julian Rivera.*

A mis maestros *que participaron en mi formación académica con mucho agradecimiento y respeto. En especial al Teacher Méndez (Q.D.D.G) a quien aprecio y admiro mucho por toda la sabiduría que nos brindó.*

A mi amiga Lic. Maria del Transito Cruells Reyna *por su colaboración y amistad incondicional.*

Edgard Alexander Peña Beltran.

PROLOGO

El presente trabajo de investigación representa para el autor , el haber culminado con mucho éxito el trabajo y dedicación realizado, durante muchos años de estudio.

La investigación que en este momento les presento es una obra de investigación, donde se ha puesto toda la capacidad y empeño, la cual comprende la historia y evolución de los virus informáticos en El Salvador y el mundo.

La razón que impulso a seleccionar este tema tiene su origen en la necesidad de conocer el comportamiento y causas de esta realidad, en la cual convivimos todos los usuarios de computadoras, llamada virus informáticos.

Va también un profundo agradecimiento a la universidad Don Bosco por haberme dado la oportunidad de culminar la carrera profesional y de tener la misión de seguir siendo un buen cristiano y honrado ciudadano.

Mi esfuerzo ha culminado pero mi labor profesional apenas ha comenzado.

I. INTRODUCCIÓN

Cada vez es más frecuente encontrar noticias referentes a que redes de importantes organizaciones han sido violadas por criminales informáticos desconocidos. A pesar de que la prensa ha publicitado que tales intrusiones son solamente obra de adolescentes con propósitos de entretenerse o de jugar, ya no se trata de un incidente aislado de una desafortunada institución. A diario se reciben reportes de ataques a redes informáticas, los que se han vuelto cada vez más siniestros: los archivos son alterados subrepticiamente, las computadoras se vuelven inoperables, se ha copiado información confidencial sin autorización, se ha reemplazado el software para agregar "puertas traseras" de entrada, y miles de contraseñas han sido capturadas a usuarios inocentes.

Estos son algunos de los tantos sucesos que ocurren en estos días, a pesar de todo, la mayoría de los usuarios informáticos carecemos de suficiente información acerca de este mal llamado virus informáticos.

A raíz de estos eventos se consideró necesario realizar una investigación científica que abarque un estudio profundo acerca de los virus informáticos, en el cual se detalle información acerca del funcionamiento, adquisición y prevención de estos programas llamados VIRUS.

El propósito es brindar una fuente amplia de información, la cual ayude a conocer las causas y efectos de estos programas computacionales.

Para la elaboración del diseño de investigación científica ha utilizar en el presente trabajo no hubiera sido posible sin el conocimiento adquirido en la esfera de las ciencias de la computación, con este conocimiento no fue difícil comprender las escuelas metodológicas vigentes en este principio del siglo XXI, que nos enfrenta entre el método positivista idealista del estructural funcionalismo y el método dialéctico e histórico. En consecuencia se ha escogido el método científico y se ha utilizado en sus tres niveles:

Método histórico, el método en sentido general para los procesos de análisis-síntesis, análisis sinópticos y presentación de tablas, con el objeto de hacer mas preciso y conciso los contenidos y finalmente el método en sentido particular para los enfoques exclusivos de las ciencias de la computación en el área de los virus de computadoras.

El presente trabajo contiene información sobre los tipos de virus existentes, así como sus funcionamientos y modos de infección. Además posee una breve reseña histórica de la evolución de éstos. También se ha introducido un manual de políticas básicas de seguridad contra la infección de virus y los pasos necesarios a seguir en caso de una infección

La utilidad práctica de este tipo de investigación permite brindar un conocimiento sobre las causas y efectos de los virus informáticos, de una forma científica, al estudiante y a toda la comunidad involucrada en el mundo de la informática.

II. OBJETIVOS

Objetivo General.

Recopilar información detallada sobre la generalidad de los virus de computadora existentes: I. Como se desarrollan, funcionan, su historia y evolución; II. Cual es su clasificación: tipos, su proceso de contaminación, daños que causan, su infección y antivirus; III. Demostrar cuales son los virus más relevantes: en el pasado, presente, los más frecuentes y los pronósticos para el futuro.

Objetivos Específicos.

- *Clasificar los distintos virus por sus características.*

- *Demostrar en forma practica los efectos de los virus de computadoras sobre los datos, considerando solamente plataformas Windows.*

- *Establecer políticas básicas para evitar la infección de virus de computadoras en diferentes sistemas. Utilizando los principales antivirus del mercado.*

- *Determinar el perfil de los creadores de virus informáticos.*

III. ALCANCES Y LIMITACIONES.

Alcances.

- *Explicar de forma esquemática las herramientas que utilizan los antivirus; así como sus métodos y estrategias contra la infección de nuevos virus.*

- *Se descargarán muestras de virus existentes en Internet, con el objetivo de verificar sus efectos sobre la información.*

- *Demostrar la necesidad de implementar políticas de seguridad contra la infección de los virus de computadora. Así como los pasos necesarios a seguir cuando una computadora ó red completa ha sido infectada.*

- *Documentar y explicar la vulnerabilidad de los sistemas operativos que son víctimas de los virus informáticos.*

- *Las demostraciones y pruebas se llevaran a cabo solamente en plataformas Windows.*

- *Investigar y documentar casos reales de ataques de virus de computadoras en las distintas empresas en El Salvador, así como los costos que esto conlleva por los daños causados.*

Limitaciones.

- *No se desarrollaran virus ni antivirus para efectos de demostración.*

- *Las políticas de seguridad básicas se plantearan en relación a una red Ethernet, de tres computadoras como máximo, utilizando una topología de bus.*

- *No se recopilará información de todos los virus existentes, solamente los diez más importantes según su tipo y época.*

IV. JUSTIFICACIÓN DEL TEMA.

Los virus de computadoras son una realidad que hemos afrontado con el transcurrir del tiempo. Algunas veces sus efectos son inofensivos y otras veces se convierten en un problema grave para los usuarios de sistemas informáticos.

Lamentablemente esta realidad existirá por mucho tiempo entre nosotros; por lo tanto tenemos que aprender a convivir y defendernos de ella. En la actualidad existen varios tipos de virus que dependiendo de sus características son capaces de hacer destrozos informáticos.

Se ha considerado necesario realizar una investigación sobre la evolución histórica de los virus de computadora, tomando en consideración los principales tipos que atacaron en el pasado y presente, y para el futuro habrá que plantear nuevas tendencias, es decir nuevas tecnologías involucradas y nuevas características que nos ayudarán a darnos cuenta de dónde venimos y hacia dónde vamos. Todo esto con el objetivo de tener un criterio más amplio sobre el origen, propósito y efectos de los virus informáticos.

Partiendo de lo anterior se hace necesario establecer estrategias para la defensa contra los virus de computadoras considerando sus tipos y características, dando a conocer las posibles causas y efectos que se podrían presentar.

V. PROYECCIÓN SOCIAL.

El beneficio social que la presente investigación tiene como objetivo se resume en el cumplimiento de los siguientes campos:

1. *A todos los estudiantes de la Universidad Don Bosco y otras instituciones que desconocen acerca de los Virus Informáticos. Se les proporciona este trabajo para generar la pauta a posteriores investigaciones sobre el comportamiento de los mismos.*

2. *Que este documento sirva para el desarrollo de la cultura y educación de todos los usuarios de sistemas informáticos.*

3. *Facilitar a los docentes un recurso didáctico para la educación del estudiante.*

4. *Que el centro de cómputo de la Universidad Don Bosco utilice este manual de políticas de seguridad y herramienta como obra de consulta en caso de necesidad.*

Índice de Contenido

INDICE DE CONTENIDO

CAPÍTULO II. MARCO TEÓRICO

CAPÍTULO III. CLASIFICACION DE LOS VIRUS

INDICE DE CONTENIDO

INDICE DE CONTENIDO

CAPÍTULO VIII. CONCLUSIONES Y GLOSARIO

TABLA DE FIGURAS

ANEXOS

CAPÍTULO I

GENERALIDADES DE LOS VIRUS

PREÁMBULO.

INTRODUCCIÓN.

Este capítulo describe las generalidades más importantes acerca de los virus informáticos. Esto nos sirve como preámbulo para comenzar a entender que son estos programas llamados Virus informáticos.

OBJETIVOS.

- Definir lo que son los Virus Informáticos.
- Conocer las características generales de los Virus.
- Conocer las causas y motivos de desarrollo.
- Conocer el perfil de los desarrolladores de virus informáticos.

1.1 ¿QUÉ SON LOS VIRUS INFORMÁTICOS?

Los virus de las computadoras no son más que programas. Simples programas de computación elaborados por programadores comúnmente llamados "hakers". Son programas similares al de un procesador de texto o de una hoja de cálculo, a un programa de bases de datos o a un programa de control de inventarios. (Es decir, programas que contienen instrucciones para que las ejecute la computadora). Los virus informáticos pueden, por tanto, realizar todas las operaciones que sean soportadas por el sistema operativo de la computadora principal.

Un virus informático es un fragmento de código nocivo que se introduce en áreas importantes de las máquinas, como los archivos ejecutables o las áreas de arranque de los disquetes y los discos duros. Los virus pueden destruir datos después de introducirse en archivos o discos. Se propagan al ejecutarse el archivo en el que se encuentren y quedar libre el código nocivo. Pueden llegar a propagarse con rapidez a la memoria si la máquina se arranca desde un disco infectado.

Una vez en ella, los virus pueden infectar otros archivos ejecutables u otros sectores de arranque. En circunstancias normales, permanecen en estado latente hasta que se produzca algún evento desencadenante, como puede ser una fecha concreta. Además de reproducirse, los virus informáticos suelen realizar otras actividades, normalmente dirigidas a provocar daños o distribuir mensajes.

Siendo igualmente programas, los virus informáticos casi siempre los acarrean las copias ilegales o piratas. Provocan desde la pérdida de datos o archivos en los medios de almacenamiento de información, hasta daños al sistema y, algunas veces, incluyen instrucciones que pueden ocasionar daños al equipo.

1.1.2 ¿POR QUÉ LLAMARLOS VIRUS?

La gran similitud entre el funcionamiento de los virus informáticos y los virus biológicos, propició que estos pequeños programas se denominaran virus.
Mientras que los virus biológicos infectan las células del organismo humano (y modifican su información genética al irse reproduciendo dentro de estas células afectadas), también pueden estar latentes en el organismo durante bastante tiempo sin que este presente ningún síntoma de infección.

Adicionalmente, cuando sufren mutaciones resulta muy difícil detectarlos, lo cual lo hace extremadamente complicado de combatirlos una vez que se han presentado los síntomas.
Sin embargo los virus biológicos no afectan a todas las células con las que entran en contacto. Afortunadamente, los avances de la ciencia médica permiten prevenir la infección aplicando vacunas (elaboradas con el mismo virus) en dosis muy pequeñas.
Los virus informáticos atacan la parte más vulnerable del software: los archivos de extensión .COM o .EXE, modifican su estructura y se reproducen dentro de éstos. También pueden estar latentes en el sistema (infectando discos y programas), y no presentar problemas durante largos períodos. Además se modifican por sí solos para evitar que sean detectados fácilmente; no afectan a todos los programas que entran en contacto con ellos y, por último, se pueden prevenir su contagio por medio de "vacunas" o programas antivirus que permiten su detección y eliminación antes que empiecen su destructiva acción.

Para satisfacer los criterios mínimos para diseño de virus, un programa "Malicioso" tiene que:

- Ser ejecutable.
- Capaz de reproducirse.
- Convertir otros objetos ejecutables en clónicos víricos.

1.2 CARACTERÍSTICAS GENERALES DE LOS VIRUS

Estos programas contienen algunas características especiales: son muy pequeños (en muy pocas líneas contienen instrucciones, parámetros, contadores de tiempo o del número de copias, mensajes, etc.), casi nunca incluyen el nombre del autor, ni el registro de Copyright, ni la fecha. Se reproducen a sí mismos y toman el control ó modifican otros programas.

Están escritos generalmente en lenguaje ensamblador, pero muchos de ellos han sido elaborados utilizando algunos de los lenguajes más populares, como C, C++, Java, Pascal, Turbo C ó Turbo Pascal. Cabe mencionar también que los diferentes tipos de computadoras, como por ejemplo Atari, Macintosh, PC compatibles con el estándar de IBM y Comodore, por mencionar algunos, funcionan también con diferentes sistemas operativos, por lo que la mayoría de los virus informáticos son específicos para cada tipo de sistema operativo; es decir un virus hecho para atacar las computadoras Macintosh generalmente no afecta a las PC´s.

Los virus se transportan a través de programas tomados de BBS (Bulletin Boards), llamado también servicio de tableros de boletines electrónicos, o copias de software no original, infectadas a propósito o accidentalmente. También cualquier archivo que contenga "ejecutables" o "macros" puede ser portador de un virus: descargas de programas de lugares inseguros; e-mail(correo electrónico) con archivos adjuntos, archivos de Word y Excel con macros. Inclusive ya existen virus que se distribuyen con Power Point.

Los archivos de datos, texto o HTML NO PUEDEN contener virus, aunque pueden ser dañados por éstos.
Los virus de sectores de arranque se instalan en esos sectores y desde allí van saltando a los sectores equivalentes de cada uno de las unidades de almacenamiento de la PC. Pueden dañar el sector o sobrescribirlo.

Lamentablemente obligan al formateo del disco de la unidad de almacenamiento infectada. Incluyendo discos de 3.5" y todos los tipos de Zip de Iomega, Sony y 3M.

En cambio los virus de programa, se manifiestan cuando la aplicación infectada es ejecutada, el virus se activa y se carga en la memoria, infectando a cualquier programa que se ejecute a continuación. Puede solaparse infecciones de diversos virus que pueden ser destructivos o permanecer inactivos por largos periodos de tiempo.

1.3 ¿LOS VIRUS INFORMÁTICOS SON REALIDAD?

La Computer Virus Industry Association (CVIA) reportaba ya en 1990, que solo en Estados Unidos se habían detectado más de 500 formas de infecciones vírales, las cuales afectaron a unas 2,000,000 de computadoras. No obstante, es posible que aproximadamente un 50% de casos de infección no se hayan denunciado.

Los virus no desaparecerán en ningún momento. Más de 20,000 han sido identificados hasta el año 2002 y se crean mensualmente entre 200 y 400 virus nuevos, de acuerdo con la International Computer Security Association. Con cifras tan alarmantes, la mayoría de las empresas luchan regularmente con ataques de virus. Nadie que use computadoras está inmune a los virus.

Los costos generados por los virus informáticos son muy altos de muchos millones de dólares, fundamentalmente por concepto de pérdida de información que deberá ser regenerada, así como por la limpieza y respaldo (backup) de los archivos y programas. Por su parte, los virus conocidos son constantemente modificados para causar mayores o diferentes daños y evitar su detección. Es necesario afrontar el problema con medidas adecuadas y no ser víctima del pánico, ni tomar medidas extremas, como dar formato al disco fijo que se suponga está infectado. Ya que eso debería de ser la última opción al cual recurrir en caso de haberse agotado todas las medidas pertinentes.

La mejor manera de enfrentar a los virus informáticos consiste en reconocer que existe un problema, y pensar que la mayoría de los problemas de las computadoras son causados en primer lugar por los humanos. Luego, hay que indagar si se trata de fallas en el hardware. Finalmente, cuando se hayan agotado todas las posibilidades de fallas conocidas: Hay que tener cuidado, ya que podría ser un terrible virus el causante de todas las preocupaciones.

Pero lo mejor que se puede hacer al detectar algo extraño en la computadora es apagarla. Eso hará que, si efectivamente se ha introducido un programa de virus a la memoria, el mismo queda temporalmente eliminado ya que éstos sólo actúan mientras el sistema esté encendido.

Un virus es dañino sólo cuando está activo en la memoria de la computadora, y siempre se activará cuando se inicie la carga del sistema desde un disco infectado o ejecute un programa que haya sido infectado por algún virus.
Al encender la computadora nuevamente, se podrá aplicar algunas medidas preventivas de detección y erradicación del virus que haya invadido su sistema. Esto logra que el sistema operativo arranque desde la unida A o disquetera, con un disquete protegido contra escritura, cuyo contenido sepamos que está libre de virus. Ya que este disco puede contener los antivirus y demás herramientas que le permitan "curar" la computadora enferma.

1.3.1 ¿QUIÉNES DESARROLLAN LOS VIRUS INFORMÁTICOS?

Los primeros virus informáticos que alcanzaron un gran nivel de dispersión aparecieron durante la década de los 80. Cuando todo esto empezó, quienes escribían aquellos primeros virus eran programadores expertos, que conocían en profundidad lenguajes de programación de bajo nivel como el Ensamblador y la arquitectura de los procesadores. La poca disponibilidad de memoria y la velocidad de procesamiento de la época exigía programas muy eficientes para poderse ocultar en ese contexto.
Hoy en día, se necesitan muchos menos conocimientos para escribir un virus, se pueden generar con cualquier herramienta de programación sencilla, como las incluidas en el Word o el Excel. Además, se cuenta con la ayuda de múltiples web sites(sitios web) de "cracking"(Programadores de antivirus) que existen en Internet. Generalmente, los creadores de los virus, son personas maliciosas que desean causar daño a las computadoras.

1.3.2 ¿POR QUÉ SE HACE UN VIRUS?

La gran mayoría de los creadores de virus lo ven como un pasatiempo, aunque también otros usan los virus como un medio de propaganda o difusión de sus quejas o ideas radicales, como por ejemplo el virus Telefónica, que emitía un mensaje de protesta contra las tarifas de esta compañía a la vez que reclamaba un mejor servicio, o el famosísimo Silvia que sacaba por pantalla la dirección de una chica que al parecer no tuvo una buena relación con el programador del virus.

En otras ocasiones es el orgullo, o la competitividad entre los programadores de virus lo que les lleva a desarrollar virus cada vez más destructivos y difíciles de controlar.

1.3.3 PERFIL DE LOS DESARROLLADORES DE VIRUS.

Por lo general se trata de personas entre 25 a 35 años y la mayoría de ellos, un 70%, tiene conocimientos técnicos sobre programas informáticos", comenta Andrés Espinosa, director de la BSA.

El 85% de estas personas, menciona Andrés Espinosa, trabaja en lugares clandestinos o en sus propias casas, donde realizan las copias de los programas, los cuales luego son distribuidos a través de empresas "fachada" que ofrecen software legal y versiones piratas a menores precios.

Básicamente los hackers son fanáticos de la computación que desde temprana edad (8, 10 años) se vuelcan activamente al estudio tanto de comunicaciones (Internet) como de lenguajes y sistemas operativos, especialmente linux. Para su operatoria precisan saber como funciona la web; para realizar los "asaltos", lo hacen desde terminales linux que les proveen acceder o trabajar sobre la máquina o sitio a hackear desde la barra de comandos o símbolo del sistema (como sí fuera la pantalla negra de D.O.S..

Al operar comandos y no programas, trabajan sobre el sistema operativo mismo de la Pc objetivo; y pueden ayudarse con programas hechos en C o Pascal, rutinas que detectan fallas de seguridad o puertas accesibles para el ingreso.

El hacker en si no es dañino; vimos que su perfil es de una persona precoz e intelectualmente superior a los de su generación, autodidacta, cuyo fin máximo es este: DEMOSTRAR SU SUPERIORIDAD FRENTE A LOS SISTEMAS SUPUESTAMENTE SEGUROS. Es decir, lo suyo es tomar un área o sistema supuestamente impenetrable y encontrar la forma de penetrarlo. Una vez que lo hace, se retira; no comete vandalismo (destrucción de datos) o actos de sabotaje. Por supuesto existen aquellos que toman su conocimiento en pos de algún lucro o destruyendo por el hecho de demostrar su superioridad. Por supuesto, existen los grandes maestros, aquellos que han penetrado sistemas tales como la NASA o el FBI. Pero en general, los hackers prefieren experimentar y ensayar con objetivos más modestos y abundantes, como suelen ser los sitios de adultos.

1.4 ¿CÓMO FUNCIONAN LOS VIRUS INFORMÁTICOS?

Los virus informáticos tienen muchas formas de operar, comenzaremos por conocer como funcionan la mayoría de los programas de aplicación que se usan diariamente. Los programas operan casi todos de manera semejante y se ejecuta tan pronto se teclea su nombre de archivo sin necesidad de teclear la extensión y pulsar enter.

El programa se carga de inmediato en la memoria convencional o RAM, y permanece ahí mientras se tenga encendida la computadora y no se le indique que deseamos terminar su ejecución. El procedimiento correcto para salir de un programa no sólo se encarga de borrarlo de la memoria, sino que también cerrar apropiadamente todos los archivos que éste mantenía abiertos para grabar o leer la información necesaria.

Los programas de virus no se ejecutan de la misma forma, sino que se infiltran en sistema cuando alguien introduce un disco infectado a la unidad de disquetes y trata de inicializar la computadora utilizándolo; ó cuando se ejecuta uno de los programas infectados que ese disco contiene. Inmediatamente el virus busca alojarse en la memoria RAM de la computadora, infectar el área de carga (boot) del disco, tabla de asignación de archivos, FAT (File Alocation Table), que contiene todos los datos de direccionamiento de los archivos, o programas ejecutables con extensión .COM y .EXE, aunque algunos virus de las nuevas generaciones infectan ejecutables auxiliares como .BAT, .OVR, .DLL y otros. Lo anterior no significa que el virus se vaya a ejecutar en ese preciso momento, sino que el sistema ha sido infectado.

El virus puede actuar inmediatamente, o bien esperar a que se den las condiciones o señales propicias que fueron programadas en su codificación. Hay virus que esperan una determinada fecha u hora para actuar, o la ejecución de alguna orden o comando; otros activan un contador (counter) en el momento de la infección y cierto tiempo después comienzan su acción destructiva.

Algunos virus, al infectar un disco flexible (disquete) o un disco duro, se alojan en el sector 0, en el área denominada sector de carga, y se posicionan en la memoria de la computadora cuando se hace la carga del sistema, o incluso cuando solamente se hace un intento de carga con el disco infectado. En este caso el virus informático toma el control de la computadora desde el principio y, desde ese momento, todo disco quedará infectado al realizar cualquier acceso de lectura o escritura con cualquiera de los comandos Copy, Dir, Format, etc.

Otros virus infectan los programas ejecutables con extensiones .COM o .EXE y se instalan en la memoria cuando se ejecuta el programa infectado. Una vez en la memoria, el virus controla todos los accesos de lectura y grabación en los discos y, la mayoría de veces, aunque se dé por terminada la ejecución del programa infectado, el virus seguirá en la memoria de la computadora, por lo que cualquier programa que se ejecute quedará también infectado. Al ejecutar un nuevo programa, el virus verifica si éste ha sido infectado y si contiene el byte marcador. Si no encuentra esta marca, procede a modificar el programa ejecutado y le contagia con ese byte marcador.

La infección consiste en almacenar una copia de sí mismo en el programa, la cual servirá para que al ejecutar este nuevo programa infectado, a su vez reproduzca en otros programas.
En este proceso, difícil de detectar, se pierde parte del programa infectado porque el virus ocupó ese lugar; lo más recomendable es reinstalar el programa original para que funcione correctamente. El usuario lo único que pudo haber notado al momento de la infección, es que la luz de la unidad de disco en uso se enciende para indicar un acceso al disco cuando el virus grabó ahí el byte marcador y su núcleo.

A la vez se ha creado toda una industria para programar esquemas de protección, se han desarrollado programas que permiten copiar casi todo el software de aplicación, burlando tales aplicaciones.

1.4.1 MÉTODO DE PROPAGACIÓN DE LOS VIRUS.

Los virus de programa se propagan mediante redes, módem o soportes magnéticos. La mayor parte de los virus de arranque se propagan sólo a través de disquetes. Los virus múltiples, por su parte, son especialmente esquivos debido a que pueden desplazarse como si de virus de programa se tratara, infectar los sectores de arranque y trasmitirse mediante disquetes.

El impresionante crecimiento de redes de área local (LAN), de Internet y de la conectividad global mediante correo electrónico ha acelerado extremadamente la velocidad de propagación de los virus. Una infección vírica localizada puede propagarse rápidamente a otra parte de una empresa o del mundo cuando los archivos infectados se envíen por correo electrónico. La amenaza de infección más importante procede de la apertura y utilización de archivos compartidos.

1.5 DEFINICIÓN GENERAL DE LOS VIRUS INFORMÁTICOS.

Antes de presentarse el problema de los virus informáticos en las grandes empresas, en las dependencias del gobierno y hasta en los centros de investigación había un gran escepticismo sobre el tema, y nadie se atrevía a opinar o decir algo sobre los virus informáticos, por lo que hasta hace poco todavía no se había dado una definición exacta de ello.

Según RALPH BURGER creador del libro "What you should know about Computer Viruses", (Lo que debes saber sobre Virus de Computadora), define a los virus como programa que puede insertar copias ejecutables de sí mismo en otros programas. El programa infectado puede infectar a su vez otros programas.

Un programa debe clasificarse como virus si combina los siguientes atributos:

- Modificación de códigos del software que pertenecen al propio programa virus, a través del enlace de la estructura del programa virus con la estructura de otros programas.

- Facultad de ejecutar la modificación en varios programas.

- Facultad para reconocer, marcándola, una modificación realizada en otros programas.

- Posibilidad de impedir que vuelva a ser modificado del mismo programa, al reconocer que ya está infectado o marcado.

- El software modificado asimila los atributos anteriores para, a su vez, iniciar el proceso con otros programas en otros discos.

Por su parte El Dr. Fred Cohen, un reconocido estudioso del fenómeno de los virus, nos da su definición de los virus:
"Los virus son unos pequeños programas que copian su propio código en forma parcial o total a otros programas y se auto reproducen así mismos logrando daños y alteraciones de los archivos infectados, la función de un virus es hacer más copias de si mismo".

Cohen se refiere a los virus como "Trojan Horses"(Caballos de Troya), debido a la forma oculta que emplean para ingresar a los sistemas y a las terribles sorpresas de sus efectos posteriores. También los denomina " Worms" o gusanos por ser " despreciables programas ", que esperan que se produzca un evento (una fecha determinada) para diseminarse.

Esta definición esta mas cerca de la realidad, pues en teoría todo programa que tiene la capacidad de modificar la estructura de otro programa y realizar operaciones de sobre escritura en la información que contiene los discos, podría ser virus potencial. Esto es que los virus nunca piden permiso y jamás avisan de su presencia en el sistema o programa infectado.

Por último el club de Virologos de Micro computadoras de Guadalajara los enuncian así: Son programas que en forma prevista por sus autores, causan daños a otros programas, archivos, discos y otras partes de la computadora algunas veces sé auto replican completa o parcialmente.

1.6 ¿QUÉ NO ES UN VIRUS INFORMÁTICO?

Existen algunos programas que, sin llegar a ser virus, ocasionan problemas al usuario. Estos no-virus carecen de por lo menos una de las tres características identificatorias de un virus (dañino, auto reproductor y subrepticio.) Veamos un ejemplo de estos no - virus: "Hace algunos años, la red de I. B. M., encargada de conectar más de 130 países, fue virtualmente paralizada por haberse saturado con un correo electrónico que contenía un mensaje de salutación navideña que, una vez leído por el destinatario, se enviaba a sí mismo a cada integrante de las listas de distribución de correo del usuario. Al cabo de un tiempo, fueron tantos los mensajes que esperaban ser leídos por sus destinatarios que el tráfico se volvió demasiado alto, lo que ocasionó la caída de la red".

Asimismo, es necesario aclarar que no todo lo que altere el normal funcionamiento de una computadora es necesariamente un virus.

A continuación se describen algunas de las pautas principales para diferenciar entre qué podría ser un virus y qué no:

1.6.1 BUGS (ERRORES EN PROGRAMAS).

Los bugs no son virus, y los virus no son bugs. Todos los usuarios de computadoras utilizan programas que tienen graves errores (bugs). Si se trabaja por un tiempo largo con un archivo muy extenso, eventualmente algo puede comenzar a ir mal dentro del programa, y éste a negarse a grabar el archivo en el disco. Se pierde entonces todo lo hecho desde la última grabación. Esto, en muchos casos, se debe a ERRORES del programa. Todos los programas, lo suficientemente complejos, tienen bugs.

1.6.2 FALSA ALARMA.

Algunas veces se tiene problemas con el hardware o software y, luego de una serie de verificaciones, se llega a la conclusión de que se trata de un virus, pero el usuario se encuentra con una FALSA ALARMA luego de correr los programa antivirus.

Desafortunadamente no hay una regla estricta por la cual guiarse, pero contestarse las siguientes preguntas puede ser de ayuda:

- ¿Es sólo un archivo el que reporta la falsa alarma (o quizás varios, pero copias del mismo)?.
- ¿Solamente un producto antivirus reporta la alarma? (Otros productos dicen que el sistema está limpio).
- ¿Se indica una falsa alarma después de correr múltiples productos, pero no después de bootear, sin ejecutar ningún programa?.

Si al menos una de las respuestas fue afirmativa, es muy factible que efectivamente se trate de una falsa alarma.

1.6.3 PROGRAMAS CORRUPTOS.

A veces algunos archivos son accidentalmente dañados, quizás por problemas de hardware. Esto quiere decir que no siempre que se encuentren daños en archivos se debe asegurar de que están infectados.

CAPÍTULO II

MARCO HISTÓRICO

PREÁMBULO.

INTRODUCCIÓN.

En este capítulo se describe de manera detallada el desarrollo histórico de los virus de computadoras, luego se explica el comportamiento evolutivo de este fenómeno.

Para conceptuar el tema de manera que brinde una base técnica a la investigación y se aporte un marco histórico de apoyo completo al lector, se describe la evolución de los virus informáticos en forma cronológica.

OBJETIVOS.

- Conocer el desarrollo y evolución histórica de los virus informáticos a nivel mundial.
- Describir el comportamiento histórico de los virus.
- Analizar la tendencia futura de este fenómeno.

2.1 HISTORIA DE LOS VIRUS INFORMÁTICOS

Desde la aparición de los virus informáticos en 1984 y tal como se les concibe hoy en día, han surgido muchos mitos y leyendas acerca de ellos. Esta situación se agravó con el advenimiento y auge de Internet.

A continuación, un resumen de la verdadera historia de los virus que infectan los archivos y sistemas de las computadoras.

Hasta la fecha no se sabe con exactitud la historia de los virus y los contagios virales. Las empresas, institutos de investigación, agencias gubernamentales e instituciones educativas que ya habían padecido alguna infección por virus, lo negaban, para no reconocer que los sistemas de seguridad implantados con grandes esfuerzos y considerables sumas de dinero y que se suponía que nadie ajeno al sistema podría burlar, de pronto se veían infiltrados por agentes terroristas informáticos.

Solamente una serie de hechos y nombres aislados se habían difundido en los medios especializados, como revistas de computación o científicas, pero daban una insuficiente visión del proceso de desarrollo de la VIROLOGIA INFORMATICA; sin embargo, se trata de dar una idea de la evolución de los virus informáticos, sobre los cuales cada día se sabe más y más.

En 1949, John Von Neuman, llamado padre de la computación, en su libro (Theory and Organization of Complicated Autómata), describió algunos programas que se reproducen a sí mismo, aunque no se enfocaba a la creación de programas que se diseminan sin permiso de los usuarios de computadoras, si no con el comienzo de los virus, sí es el primer indicio de código auto reproductor.

En cambio, la primera información de programas que incluyen códigos que trabajan como virus, nos remonta a la década de los años 60, y es acerca de los estudiantes de computación en el Instituto Tecnológico de Massachussets (ITM) Para ese entonces, el término Hacker se traducía como programador genial, no como ahora se utiliza para nombra a los piratas, o en su mejor acepción, se refiere a personas talentosas que se entretienen infiltrándose en los sistemas de las grandes empresas, acontecimiento que representa un hecho para cada uno de nosotros.

Los jóvenes estudiantes se reunían por las noches y se dedicaban a elaborar Código Sofisticado, así se desarrollaron notables programas, como Guerra en el espacio (Space war), ya que uno de sus pasatiempos favorito era jugar amistosamente entre ellos con los programas que los demás no pudieran detectar.

Además, bombardeaban, al programa del contrincante, que no sabía de donde recibía el ataque y el qué lo provocaba. Estas modificaciones que se hacían a los códigos de los programas ajenos no eran propiamente virus, sino "bomba" que actuaban "explotando" inmediatamente.

En esa misma década, varios científicos estadounidenses de los laboratorios de computación de la AT&T (Bell Laboratories): H. Douglas Mcllory, Robert Morris Sr., Victor Vysottsky y Ken Thomson ingeniero en sistemas, creador de la primera versión del sistema UNÍX, para entretenerse inventaron un juego al que llamaron COREWAR (Guerra Nuclear), inspirado en un programa escrito en lenguaje ensamblador llamado Creeper. El cual tenía la capacidad de reproducirse cada vez que se jugaba.

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

También diseñaron otro programa llamado Reeper, el cual sería el antivirus, en ese momento, cuya función era destruir cada copia hecha por Creeper. Estaban conscientes de la peligrosidad que el juego representaba para los sistemas de computación y se prometieron mantenerlo en secreto, pues sabían que en manos irresponsables, el Core War, podría ser empleado nocivamente.

Sin embargo, en 1983 el Dr. Thompson durante una alocución en la Assocation for Computing Machinery, da a conocer la existencia de esos programas de virus, con detalle acerca de su estructura. La revista Scientific American, lo publica en su artículo Computer Recreations en la edición de mayo de 1984, ofreciendo por 2 dólares las guías para la creación de virus propios.

Desde el año de 1974, Xerox Corporation presentó en Estados Unidos el primer programa que ya contenía un código auto duplicador. Los equipos Apple II se vieron afectados a fines de 1981 por un virus llamado Cloner que presentaba un pequeño mensaje en forma de poema. Se introducía en los comandos de control e infectaba los discos cuando se hacía un acceso a la información utilizando el comando infectado.

En 1983, el Dr. Fred Cohen realizó un experimento en la Universidad del Sur de California, presentó el primer virus residente en una PC, por lo que hoy se le conoce como El Padre de los virus informáticos. Cohen trataba de demostrar, y lo logró, que el código de programas para computadoras podía auto duplicarse, introducirse a otros códigos y alterar el funcionamiento de las computadoras.

Era un virus muy grande, ya que incluía unas 200 líneas de código en lenguaje C, pero en comparación con los programas desarrollados en ese tipo de computadora y sistema operativo –Blank-, resulta que no fue tan grande, sino más bien muy pequeño.

Existe una referencia a un programa con un nombre muy similar al Core War, que en los datos de autor y fecha de creación, dice: Escrito por Kevin A. Bjorke, mayo de 1984, en Small-C y fue cedido al dominio público.

En 1986 es cuando ya se difunde ampliamente un Virus con la finalidad de causar destrozos en la información de los usuarios. Este ataca una gran cantidad de computadoras en todo el mundo. Fue desarrollado en Lahore, Pakistán, por dos hermanos que comerciaban en computadoras y software.

Uno de ellos escribió un programa administrativo de gran utilidad. Por este motivo los usuarios copiaban en grande cada original vendido, hasta que, cansados de sufrir efectos de la piratería decidieron vender copias ilegales de programas populares, y en éstos, así como su propio programa, introdujeron un virus "benigno" con códigos muy elegantes, el cual permitió que otros programadores lo modificaran para hacer de él, en sus nuevas versiones, uno de los virus más dañinos que se conocen, por la cantidad de bytes en que reducen la capacidad de almacenamiento de los disquetes.

En su compañía, Brain Comters, se ofrecían programas, como Lotus 123 a precios ridículos de $1.50 dólares, lo que propició que los turistas que llegaban a comprar en su tienda se llevaran a sus lugares de origen los programas infectados. Se supone que el referido virus infectó más de 30,000 computadoras solamente en Estados Unidos. Informaciones posteriores encontradas en Compuserve, red de servicios informáticos de nivel internacional, anunciaban infecciones del virus Brain ó Paquistaní, que habían borrados archivos de estudiantes de la universidad de Miami, de una editorial, y de un periódico.

También se decía que a causa de ese mismo virus, se habían destruidos discos de algunos estudiantes de Maryland. Acerca de la versión difundida en México, nunca se supo que borrara archivos, pero sí utilizaba los disquetes marcando sectores buenos como defectuosos.

Las computadoras Commodore, especialmente la Amiga, fueron atacadas en noviembre de 1987 por un virus que infectaba el sector de carga y se posicionaba en la memoria de la computadora. Al introducir otros disquetes, quedaban infectados en la misma área de arranque, por lo que al circular a través de otras computadoras, diseminaban el contagio.

En diciembre de 1987, los expertos de IBM tuvieron que diseñar un Programa antivirus para desinfectar su sistema de correo interno, pues éste, fue contagiado por un virus no dañino que hacía aparecer en las pantallas de las computadoras conectadas a su red un mensaje navideño, el cual a reproducirse a sí mismo múltiples veces hizo muy lento el sistema de mensajes de la compañía, hasta el punto de paralizarlo por espacio de setenta y dos horas.

El virus presentaba un mensaje navideño con un árbol al lado, y pedía al usuario que tecleara la palabra CHRISTMAS. Si tecleaba la palabra, el virus se introducía a la lista de correspondencia del correo electrónico del operador y se seguía diseminando por toda la red.

Cuando no se accedía a la demanda y se apagaba el equipo, el virus impedía que se pudieran grabar los trabajos inconclusos, perdiéndose así muchas horas de trabajo.

El uso de programas originales evita en un gran porcentaje la posibilidad de infección viral. Sin embargo, Aldus Corporation, una empresa de gran prestigio, lanzó al mercado, originales de su programa FRENAD para Machintosh infectados por un virus benigno llamado Macintosh Peace, Mac Mag o Brandow. Este virus se desarrolló para poner un mensaje de paz en las pantallas de las computadoras, a fin de celebrar el aniversario de la introducción de la Macintosh II, el 2 de marzo de 1988.

El virus Macintosh Peace fue difundido por muchos de los servicios de software compartido, y aunque se esperaba que en área de la frontera de Estados Unidos con Canadá se encontraran pocas copias infectadas, se cree que el mensaje apareció en unas 350,000 pantallas de computadoras de Estados Unidos y Europa.

Richard R. Brandow, editor de la revista Macmag de Montreal, Canadá, contrató a un programador para realizar el mencionado virus, que pronto se propagó por los medios de los servicios de cartelera electrónica, (BBS) que son sistemas de servicios de software o información compartida por computadora vía módem y línea telefónica. Aldus inadvertidamente distribuyó originales de su programa que contenían el virus. Su defensa se basó en el hecho de que la infección partió de un disco de demostración que proporcionó a un proveedor. Este adquirió el virus de un programas de juego tomado de un servicio de cartelera electrónica, y sin saberlo lo incluyó en el disco que contenía el programa de demostración y se comercializó sin sospechar que llevaba el virus. De su diseminación se encargaron las copias ilegales que de él se hicieron.

Actualmente siguen aconteciendo accidentes de esta naturaleza; es decir, algunas empresas inocentemente distribuyen copias infectadas de sus programas. El caso más sonado es el del representante de Borland en México, que distribuyó entre los asistentes a Softeach México 94, el disquete de demostración del programa dBASE IV para Windows, infectado con el virus Monkey.

La compañía ofreció públicamente disculpas y asesoría para eliminar el virus, así como un antivirus proporcionado por McAfee Associates de México y distribuyó a través de BBS Spin, para contrarrestar el efecto del mencionado virus, en caso de haber recibido la infección en sus computadoras.

En 1988 se identificó el virus de Jerusalén, que según algunas versiones, fue creado por la organización para la liberación de Palestina con motivo de la celebración del cuarenta aniversario del ultimo día en que Palestina existió como nación, el viernes 13 de mayo de 1988.

Por estas fechas, se comenzaron a difundir informaciones sobre virus o caballos de Troya que eran colocados en BBS´s, para que en un determinado momento desataran una serie de funciones dañinas, que incluso, en ocasiones causaron la destrucción completa del tablero electrónico (BBS). Al bajar los programas del tablero infectado, se esparcía el virus hacia las computadoras conectadas al sistema. Esto propició que durante un tiempo se considerará a los BBS´s como el principal foco de contaminación de los virus informáticos.

En Estado Unidos se forma una asociación de profesores, programadores y empresas de software, para estudiar, investigar y clasificar a los virus, con la finalidad de diseñar y elaborar medidas de protección y programas antivirus, de una manera coordinada, evitando así esfuerzos en vanos en la titánica lucha que se echaba encima; la CVIA, Computer Virus Industry Association, con sede en Santa Clara, California.

La Nuclear Regulatory Comisión, de Estados Unidos, anunció el 11 de agosto de 1988 su intención de sancionar hasta con 1,250,000 dólares a la planta de energía nuclear Peach Bottom, en Pensilvania, porque sorprendió a los operadores de la planta jugando en las computadoras con copias piratas de programas de juegos.

El 2 de noviembre del mismo año, las redes ARPANET y NSFnet en Estados Unidos son infectadas por un virus (Gusano) que se introdujo en ella, afectando a más de 6,000 equipos de instalaciones militares de la NASA, universidades y centros de investigación públicos y privados. Este gusano se infiltró aprovechando las fallas de seguridad que persistían en archivos del sistema operativo UNÍX que se estaba utilizando. También el gusano invadió la red Internet.

Investigaciones posteriores dieron como resultado el descubrimiento del causante de la invasión del Gusano a las mencionadas redes: el estudiante Robert Morris Jr., Aunque sus declaraciones y las de sus compañeros indicaban que no lo hizo con malas intenciones, sino que fue un descuido al trabajar con un programa auto reproductor, que se le fue de las manos.
En su defensa, se mencionó en el hecho de que trató de avisar a los operadores de la red para ayudar a detener la infección.

"Recordemos el programa Core War, desarrollado desde hace más de 20 años científicos de los laboratorios Bell, uno de los cuales era Robert Morris padre, luego trabajó, conoció el programa y lo divulgó entre algunos amigos, los cuales se encargaron de diseminarlo."

En octubre de 1989 ya se visualizaba a otros virus como una terrible epidemia, y empezaron a suceder hechos deplorables. Un comunicado de un desconocido comando tecnoterrorista manifestaba que había infectado una gran cantidad de computadoras, y el viernes 13 se destruirían automáticamente los archivos almacenados en disquetes o en discos fijos, desatando el pánico entre los usuarios, el cual estaba fundado básicamente en la superstición que provoca esa fecha.

Aunque no se realizó esta catastrófica profecía, sirvió replantar el grave peligro al que están expuestos los datos de cualquier sistema. Esta tesis se refuerza con la publicación del 30 de octubre en el diario The New York Times, la cual anunciaba que las computadoras de la NASA habían sido interferidas por desconocidos causando problemas en el lanzamiento del transbordador espacial Atlantis.
En Estados Unidos, unas sesenta computadoras de la NASA fueron infectadas en esa ocasión y el programa intruso se siguió reproduciendo por medio de la red comercial que tiene la NASA con empresas privadas en aquel país. Se estima que muchos grandes bancos de datos internacionales y más de medio millón de PC´s han sido atacadas por diversos tipos de virus.

En España también se han propagado varios tipos de virus, al grado de que una conocida revista de computación, que incluye programas en cada ejemplar, distribuyó copias de esos discos contagiados con el virus de Jerusalén en uno de sus números en 1990.

La revista reconoció públicamente su error y, además de retirar los ejemplares del mercado, en el siguiente numero distribuyó discos de programas que contenían un antivirus para combatir al mencionado virus.

Lógicamente la revista en cuestión ha sido victima más de los terroristas de la informática, y excepto por el cuidado que debemos tener todos para no caer en estos problemas de diseminación de los virus, no puede culpársele de la existencia del virus. Los medios de información españoles no especializados en informática, exageraron los daños que el virus podía causar, con lo que no desprestigiaron a la revista. Por esto es muy importante que no se mal informe a los usuarios de las computadoras sobre supuestas acciones o daños que los virus informáticos pueden realizar.

Se especula mucho acerca de la cantidad de virus que se conocen hasta ahora, pero se supone que son mucho más de 20,000. En algunos medios se informa que aparecen entre 200 y 400 virus por mes, pero los programas antivirus más modernos reportan poco más de 20,000 incluyendo las variantes de los más conocidos.

Bulgaria se ha identificado como uno de los países más prolíficos en cuestiones de virus informáticos, por lo que no es raro que unos de los virus también más prolíficos, por aquello de las familias de virus; es decir que ha servido para crear muchísimas variantes a partir de su código, sea el Virus Vienna, cuyo origen se localiza en Bulgaria.

Tan sencillo y bien estructurado era el código de dicho programa, que se logró incluso reducir su tamaño; es decir, la cantidad de byte, de 648 a 348. Esto, en lugar de reducir la capacidad de reproducción e infección, al contrario, aumentó su eficiencia como virus. En ese tiempo, se fabricaron los virus Old Yankee y Vaccina.

En Junio de 1991 el Dr. Vesselin Bontchev, que por entonces se desempeñaba como director del Laboratorio de Virología de la Academia de Ciencias de Bulgaria, escribió un interesante y polémico artículo en el cual, además de reconocer a su país como el líder mundial en la producción de virus da a saber que la primera especie viral búlgara, creada en 1988, fue el resultado de una mutación del virus Vienna, originario de Austria, que fuera desensamblado y modificado por estudiantes de la Universidad de Sofía. Al año siguiente los autores búlgaros de virus, se aburrieron de producir mutaciones y empezaron a desarrollar sus propias creaciones.

Su connacional, el virus Dark Avenger o el "vengador de la oscuridad", se propagó por toda Europa y los Estados Unidos haciéndose terriblemente famoso por su ingeniosa programación, peligrosa y rápida técnica de infección, a tal punto que se han escrito muchos artículos y hasta más de un libro acerca de este virus, el mismo que posteriormente inspiró en su propio país la producción masiva de sistema generadores automáticos de virus, que permiten crearlos sin necesidad de programarlos.

A partir de 1992, con el avance de Internet, las técnicas para la creación de virus se globaliza, y cualquier ínter nauta, podía adquirir los conocimientos necesarios para crear su propio programa.... así es como comienza la epidemia vírica, que llega hasta nuestros días.

Diariamente se descubren nuevos tipos de virus con códigos diferentes y muy variadas formas de funcionamiento. Esto se debe en gran parte a la facilidad de programación en el ambiente de MS-DOS, y a la vulnerabilidad que este sistema operativo ofrece, ya que no es sistema que trabaje en modo protegido.

2.1.1 EL PÁNICO QUE CAUSAN LOS VIRUS INFORMÁTICOS.

El desconocimiento de los conceptos de virus informáticos, tecnovirus o tecnosida, que son algunos de los nombres que se han dado al fenómeno de los programas que se ejecutan sin permiso del usuario provocando pérdida de información, ha creado una psicosis ó pánico informático y se ha cubierto con un velo de misterio, mistificando el uso de las computadoras.

Si el nombre aplicado a estos programas hubiera sido cualquier otro, tal vez no hubiera producido este fenómeno, pero con el nombre de virus se han creado una serie de tabúes y rumores que hacen que algunos programadores o usuarios de computadoras desarrollen su trabajo temiendo a cada momento ser atacados por algún monstruo maligno.

Otras personas con menos conocimiento en informática creen que los virus de las computadoras son algo parecido a los virus biológicos, con capacidad para salirse de los sistemas, e incluso contagiarlos físicamente. Exageradamente, los han llegado a considerar un castigo divino enviado a los programadores ó usuarios como un escarmiento por utilizar una tecnología que ellos no alcanzan a comprender. En algunos casos, y debido a los nombres con que se bautizan los virus (SATAN, Baile con el Diablo, Dark Avenger, etc.) se han considerado como una obra satánica.

Lo anterior, aunado a los rumores alarmantes que se propagan en cuanto a la existencia de los virus, de su origen y sus reacciones, hace que los nuevos usuarios sientan un temor infundado hacia las computadoras. Hay incluso quienes justifican ante sus superiores su ineficiencia, achacando a ataques virales los trabajos que tardan demasiado tiempo en entregar, o que aunque se presentan sin demora, no son bien aceptados, pues contienen muchos errores o defectos.

Como ejemplo de esta histeria citaremos las actividades terroristas que ya realizan algunos grupos en varios países: en estados Unidos un grupo de tecnoterroristas se hace llamar la plaga, y en sus mensajes incluyen Slogan ó lemas como Quisiera ver más virus por ahí y amenazan infectar sistemas de todo el mundo, incluyendo China y las Republicas Soviéticas, en donde ya existe un virus llamado Lágrimas que caen, que como virus Cascada de Estados Unidos, hace que las letras que se están viendo en la pantalla caigan como una lluvia y se amontonen en la parte inferior de ésta.

Otros virus presentan en la pantalla lluvias multicolores o dibujos espectaculares y tocan alguna pieza musical, mientras sus archivos son borrados al mismo ritmo. Asimismo existe otro de estos virus que se conoce como la Muchacha Holandesa (Holland Girl) ó Silvia, que cuando se manifiesta en la computadora da el nombre y la dirección de una muchacha en Holanda y un breve mensaje en el cual se solicita que le envié una postal.

También se cuenta con el virus Gastronómico, el cual contagió a las computadoras DECsystem 10. La característica de este pequeño personaje era que permanecía latente por tiempo indefinido en el sistema y cuando se activaba presentaba en la pantalla el mensaje: I WANT A COOKIE! (Quiero una Galleta!), la única manera de normalizar el funcionamiento era tecleando la palabra COOKIE, con lo que se lograba desactivarlo durante algún tiempo. La versión Cookie 2232, incluso al recibir la palabra COOKIE, despliega en la pantalla el mensaje BURPS...

Un virus más peligroso es el que actúa de tal manera que cuando detecta cantidades de cuatro cifras, las reacomoda, alterando el orden, lo que hace que cuando un operario trabaja con números, estados de cuentas, cobranzas, etc., utilice cantidades falseadas.

Finalmente, se conoce de fraudes a empresas y bancos utilizando un programa que, aunque no se reproduce, sí realiza operaciones por su cuenta. A este tipo de programas se les denomina Salami, y trabajan enviando a una cuenta del programador, los centavos producto de redondeos en las cantidades de las cuentas de los clientes. El cliente, o no se percata del error, ó no le importa, ya que son sólo centavos; pero al beneficiarlo de estos redondeos le significa un gran negocio. Afortunadamente ya se han tomado medidas en contra de estos programadores y se han procesado algunos en Estados Unidos. El colmo del terrorismo viral ha sido que hasta los mismos programas vacunas, que se supone deberían ser los más confiables, han sido modificados por los CIBERPUNKS como se le han llamado también a los programadores de los virus.

2.1.2 RESUMEN CRONOLÓGICO DE LOS VIRUS INFORMÁTICOS.

A continuación se presenta una breve cronología de lo que ha sido los orígenes de los virus:

- **1949:** Se da el primer indicio de definición de virus. John Von Neumann (considerado el Julio Verne de la informática), expone su "Teoría y organización de un autómata complicado". Nadie podía sospechar de la repercusión de dicho artículo.

- **1959:** En los laboratorios AT&T Bell, se inventa el juego "Guerra Nuclear" (Core Wars) o guerra de núcleos de ferrita. Consistía en una batalla entre los códigos de dos programadores, en la que cada jugador desarrollaba un programa cuya misión era la de acaparar la máxima memoria posible mediante la reproducción de sí mismo.

- **1970:** El Creeper es difundido por la red ARPANET. El virus mostraba el mensaje "SOY CREEPER...ATRAPAME SI PUEDES!". Ese mismo año es creado su antídoto: el antivirus Reeper cuya misión era buscar y destruir al Creeper.

- **1974:** El virus Rabbit hacía una copia de sí mismo y lo situaba dos veces en la cola de ejecución del ASP de IBM lo que causaba un bloqueo del sistema.

- **1980:** La red ARPANET es infectada por un "gusano" y queda 72 horas fuera de servicio. La infección fue originada por Robert Tappan Morris, un joven estudiante de informática de 23 años aunque según él fue un accidente.

- **1983:** El juego Core Wars, salió a la luz publica en un discurso de Ken Thompson. Dewdney explica los términos de este juego. Ese mismo año aparece el término virus tal como lo entendemos hoy.

- **1985:** Dewdney intenta enmendar su error publicando otro artículo "Juegos de Computadora virus, gusanos y otras plagas de la Guerra Nuclear atentan contra la memoria de los ordenadores".

- **1987:** Se da el primer caso de contagio masivo de computadoras a través del MacMag Virus también llamado Peace Virus sobre computadoras Macintosh. Este virus fue creado por Richard Brandow y Drew Davison y lo incluyeron en un disco de juegos que repartieron en una reunión de un club de usuarios. Uno de los asistentes, Marc Canter, consultor de Aldus Corporation, se llevó el disco a Chicago y contaminó la computadora en el que realizaba pruebas con el nuevo software Aldus Freehand. El virus contaminó el disco maestro que fue enviado a la empresa fabricante que comercializó su producto infectado por el virus. Se descubre la primera versión del virus "Viernes 13" en los ordenadores de la Universidad Hebrea de Jerusalén.

- **1988:** El virus Brain creado por los hermanos Basit y Alvi Amjad de Pakistán aparece en Estados Unidos.

- **1988:** Aparecen los primeros programas antivius.

- **1989:** Aparece el primer antivirus heurístico, y los primeros virus con nuevas técnicas de ocultamiento.

- **1990:** Virus de infección rapida provenientes de Bulgaria: el virus DARK AVENGER.

- **1991:** Aparecen los primeros Kits para la construcción de virus.

- **1992:** El virus Michelangelo y el pánico generado por la magnificación de la prensa.

- **1994:** El auge de Internet y el correo electrónico: el crecimiento desmesurado del número de virus.

- **1995:** El nacimiento de los virus de Macro: el virus Concept.

- **1997:** Aparece el virus Lady Di.

- **1998:** Aparecen los primeros virus de Macro para Excel y Access.

- **1998 (Agosto):** Aparece el primer virus de Java: el virus Strange Brew.

- **1999:** Aparecen los virus de "tercera generación": los virus de Internet.

- **Mayo 2000**: VBS/Loveletter, alias "I LOVE YOU", el gusano con mayor velocidad de propagación de la historia.

- **2002:** Surge el W32/Nimda@mm , es un gusano que utiliza diversos métodos para propagarse mediante el envío masivo por correo electrónico.

- **2003(Enero):** Aparece el SQL Slammer, un gusano que logro que el trafico en Internet se disminuyera súbita y dramáticamente durante horas.

2.2 Evolución De Los Virus Informáticos.

Hablar de virus a nivel escritorio y su desarrollo en el tiempo se puede hacer de diversas maneras, sin embargo, al revisar esta cronología es factible dividir en tres etapas lo que hasta hoy, ha venido sucediendo y de esta manera podemos suponer lo que vendrá en un futuro. De manera general se puede ver esta evolución en 3 etapas:

1. Antes de Windows 95.

La plataforma que durante más de 10 años fue el atractivo primordial para el desarrollo de virus se centralizó en DOS, el sistema operativo que permitió el uso de las computadoras en forma masiva:

- **Virus de Arranque:**

Este tipo de virus se aloja el área de Master Boot Record del sector de arranque en el FAT (File Allocation Trable), se aloja después de la revisión del bios y antes de la identificación de unidades lógicas y sistema operativo correspondiente, para tomar control de la computadora en todo lo referente a I/O.

- **Virus de Archivo.**

Cualquier pedazo de código que se inserta en un archivo, se activa normalmente al ejecutar el archivo host se carga en RAM e infecta toda la aplicación que se ejecute.

2. Después de Win95.

Con la llegada de esta nueva plataforma y bajo la amenaza del usuario de 32 bits, los virus anteriores han desaparecido (arranque y de archivo) sin embargo gracias a la apertura de Office 95 con macro-lenguaje de programación y encriptación se abrió una nueva gama de virus, los llamados Macrovirus de los cuales hoy existen más de 6,800.

Los Macrovirus aún siendo virus de Archivos son tantos que se han ganado un espacio especial. Se tuvieron que implementar nuevos desarrollos en la tecnología Antivirus para poder atacar esta epidemia, ya que con una simple variable en un macro de Office es posible crear una nueva variante. Lo anterior se apoya en que un macro lenguaje es fácil de identificar y de desarrollar, lo que lo hace una herramienta ideal para el desarrollo de virus. Ejemplos: concept, wazzu, cap, market, notepad, etc.

3. Internet.

Esta es la era más interesante de los virus, ya que no solo existe un crecimiento exponencial de los macro virus por la facilidad de compartir información, sino que además surgen nuevas formas de códigos maliciosos: los ya conocidos gusanos de Internet y caballos de Troya, que se diseminan a una gran velocidad, no solo en redes locales, sino a nivel mundial.

Actualmente, se espera que el desarrollo de virus y códigos maliciosos se enfoque cada vez mas en la tecnología móvil, que es la que está evolucionando y cambiando constantemente.
Según comunicado de Panda Software, desde la aparición de Melissa, en 1999, este tipo de código malicioso ha sido el que mayor impacto ha tenido en todo el mundo.

En marzo se ha cumplido el tercer aniversario de Melissa, cuya aparición marcó un antes y un después en la historia de los códigos maliciosos. Hasta entonces pocos virus ó gusanos se habían reproducido con tanta rapidez y afectado a tantas corporaciones y usuarios. A la gran repercusión obtenida por Melissa se suma el hecho de haber sido el iniciador de una tendencia continuada por códigos maliciosos -como I Love You, Sircam o Nimda-, a los que cada día se suman nuevos ejemplares que, como su antecesor, tiene como principal objetivo difundirse al mayor número de equipos.

Melissa es un virus de macro para Word con características de gusano gracias a su habilidad para auto enviarse, adjunto a un mensaje de correo electrónico, a los 50 primeros contactos de la libreta de direcciones de Outlook del ordenador al que afecta. Esta técnica, que desgraciadamente hoy es muy habitual, tiene su origen en este virus que, en apenas unos días, protagonizó uno de los casos de infección masiva más importantes de la historia de los virus informáticos. De hecho, compañías de la talla de Microsoft, Intel o Lucent Technologies tuvieron que bloquear sus conexiones a Internet debido a la acción de Melissa.

La escuela iniciada por Melissa fue continuada en 1999 por ejemplares como VBS/Freelink que, a diferencia de su predecesor, se enviaba a sí mismo a todas los contactos que el PC afectado tuviese incluidos en su libreta de direcciones. Ese mismo año también apareció VBS/Bubbleboy que, aprovechando un agujero de seguridad de Internet Explorer 5, se activaba sin necesidad de ejecutar ningún fichero adjunto, ya que con tan solo abrir el mensaje de correo o visualizarlo lleva a cabo su acción.
Con posterioridad, en mayo del 2000, apareció I Love You, cuyo impacto económico -10.000 millones de euros- aún no ha sido superado. Como se recordará, para atraer la atención del usuario, y así conseguir propagarse, se mandaba por correo electrónico en un mensaje cuyo asunto era "ILOVEYOU" e incluía adjunto un fichero denominado "LOVE-LETTER-FOR-YOU.TXT.VBS".

Tras I Love You surgieron otros gusanos -como W32/Hybris ó Sircam y AnnaKournikova" -, que tuvieron una gran propagación gracias al empleo de la Ingeniería Social.
El primero aludía a una posible versión erótica del cuento de Blancanieves y los Siete Enanitos, mientras que el segundo intentaba engañar al usuario haciéndole creer que había recibido un archivo que contenía una fotografía de la tenista Anna Kournikova.

En el año 2001 se consolidó la tendencia de los virus a "aprovecharse" de vulnerabilidades existentes en programas de uso habitual, siendo dos claros ejemplos Code Red y Nimda.

El primero explotaba una vulnerabilidad .ida de los servidores IIS y era capaz de propagarse a gran velocidad sin dejar ningún rastro en los medios de almacenamiento tradicionales. Por su parte, Nimda se transmitía por correo electrónico utilizando una vulnerabilidad en el navegador Internet Explorer 5 y en los clientes de correo Outlook y Outlook Express.

En definitiva, Melissa inauguró una nueva etapa en la historia de los códigos maliciosos, convirtiéndose en el primer gusano de propagación masiva. La posterior aparición de otros ejemplares, que mediante técnicas más sofisticadas ó recurriendo a la Ingeniería Social han alcanzado mayores índices de difusión que su predecesor, ponen de manifiesto su constante evolución y la necesidad de no bajar la guardia.

2.2.1 TENDENCIA DE LOS VIRUS INFORMÁTICOS.

Existen compañías alrededor del mundo encargadas del estudio y tendencia de ataques de virus informáticos.

La compañía Trend Micro ha realizado un estudio donde anuncia que el número de ataques procedentes de virus informáticos aumentaron en un 175% en el año 2002. Según el estudio titulado "Tendencias actuales en código malicioso: Pronósticos para el año 2003" esta tendencia alcista viene manifestándose desde el año 2001, en el que también se alcanzó un aumento en torno al 175%.

El estudio refleja las nuevas preocupaciones en cuanto a seguridad informática, y cómo ha evolucionado el "modus operandi" de los virus y de sus distribuidores. Los gusanos electrónicos son de los más utilizados debido a que se han perfeccionado propagándose cada vez de forma más rápida y a un mayor número de equipos.

Otro incremento de las incidencias de los virus se debe al producido por los envíos masivos de correos electrónicos y la mensajería instantánea en la red. Esta es la principal vía de trasmisión de virus utilizada hoy en día, por su potencial vulnerabilidad en cuanto a la seguridad del usuario.

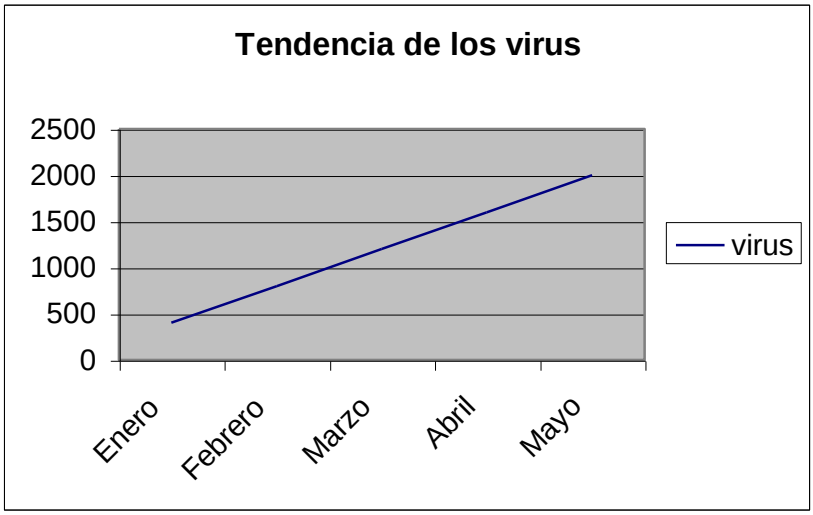


Figura 2.1

CAPÍTULO III

CLASIFICACIÓN DE LOS VIRUS

PREÁMBULO.

INTRODUCCIÓN.

Este capítulo tiene como objetivo primordial clasificar los virus informáticos en distintas categorías según su tipo y características particulares.

Todo esto con el objetivo de poder conocer y distinguir los diferentes tipos de virus que existen en el mundo de la informática.

OBJETIVOS.

- Clasificar los diferentes tipos de virus existentes según características propias.
- Conocer los diferentes tipos de virus informáticos que existen.
- Conocer el modus operandi de cada tipo de virus.

3.1 TIPOS DE SOFTWARE ROGUE.

Los software Rogue (Maliciosos), son programas que se cargan y se llevan a cabo sin que los usuarios les pidan la ejecución. Los virus informáticos son solo una variedad de este tipo de software.

Por lo menos hay nueve familias diferentes de software Maliciosos que pueden encontrarse en el mercado de la PC. Los virus informáticos, aunque tienen muy mala fama, no son, de ningún modo, los más dañinos. Todo software Malicioso supone una serie de amenaza para la integridad de los datos informáticos.

La mayoría, si no todos, de los nombres dados a los programas de software informático maliciosos han sido otorgados por la comunidad general de usuarios.
Estos nombres tienden a ser dramáticos, a veces inquietantes y siempre pegadizos. A continuación se presentan una serie de variedades más conocidas de software Maliciosos.

3.1.1 BUG-WARE

Bug-Ware es el término dado a programas informáticos legales diseñados para realizar conjuntos de funciones concretas.

Debido a una inadecuada comprobación o a una programación enrevesada, causan daño al hardware o al software del sistema. Muy a menudo, los usuarios finales o la prensa informática denuncian esos daños como resultado de la actividad de virus informáticos. Los programas de Bug-Ware no son, en absoluto, programas maliciosos. simplemente son fragmentos de código implementados que, debidos a fallos lógicos internos, dañan el hardware o inutilizan los datos del usuario de forma accidental.

3.1.2 CABALLOS DE TROYA

Es llamado el abuelo del software rogue, el Caballo de Troya, es llamado como el Caballo de Troya de la mitología griega.

Los programas de Caballo de Troya parecen ser aplicaciones útiles, corrientes y molientes, mientras que en realidad contienen una o más órdenes informáticas destructivas. Los usuarios que inocentemente ejecutan programas de Caballo de Troya son engañados a menudo por "enlaces", o disfraces, bien diseñados que les inducen a creer que están usando aplicaciones normales.

Estas charadas continúan hasta que se disparan los programas escondidos en los Caballos de Troya, incluidos los Virus informáticos.

3.1.3 CAMALEONES

Un pariente cercano del Caballo de Troya, los camaleones actúan como otros programas parecidos, de confianza, mientras que en realidad están haciendo alguna clase de daño. Cuando están adecuadamente programados, los camaleones pueden simular todas las acciones de programas de demostración, los cuales son simulaciones de programas reales de software.

En una ocasión, un camaleón fue programado inteligentemente para emular un gran mensaje de apremio de toma de contacto con un sistema de multiusuarios para nombres y contraseñas de los usuarios. El camaleón grabó los nombres y contraseñas de los usuarios en un archivo secreto y luego presentó un mensaje que indicaba que el sistema estaba inactivo temporalmente por motivos de mantenimiento. Algún tiempo después, el autor del camaleón introdujo su propia contraseña confidencial,

capturó la lista acumulada y así tuvo acceso a una multitud de logins de usuarios para sus propios usos ilegítimos.

Otro programa clásico de camaleón fue uno que simuló un programa bancario normal que el programador utilizó para desviar discretamente unas cuantas décimas de centavos en errores de redondeo a una cuenta secreta por cada transacción. El botín resultante ascendió a cientos de miles quizá millones de dólares.

3.1.4 BOMBAS DE SOFTWARE

La Bomba de software, es el código rogue más fácil de producir y perfeccionar, y durante cierto tiempo el más popular entre programadores de rogue.

Las Bombas de Software sencillamente detonan a pocos instantes de ser lanzadas. Con mínima fanfarria y prácticamente ningún pretexto, y ciertamente sin reproducción vírica, las bombas de software se corresponden con su nombre, explotan por impacto y vuelan los datos.

3.1.5 BOMBAS LÓGICAS

Las bombas lógicas son programas que ejecutan órdenes informáticas destructivas condicionalmente, dependiendo del estado de variables ambientales. Por ejemplo, una bomba lógica podría controlar los registros de nóminas en un esfuerzo por esperar que ocurra el despido del programador de la bomba lógica.

La bomba lógica podría ser programada para estallar (borrar y volver a calcular incorrectamente los registros de las nóminas, reformatear discos ó realizar otras acciones análogamente destructivas) cuando los registros de la nómina del programador dejen de aparecer durante tres semanas consecutivas.

3.1.6 BOMBAS DE TIEMPO

Las bombas de tiempo son programas que ejecutan órdenes informáticas destructivas condicionalmente dependiendo del estado de variables ambientales, relacionadas con números o con el tiempo. Las bombas de tiempo son iguales técnicamente a las bombas lógicas; sin embargo, la particularidad de sus horarios ambientales les ha dado su clasificación propia.

Por ejemplo, las bombas de tiempo se programan para estallar tras una cantidad fija de ejecuciones (al menos dos ejecuciones) para estallar en una fecha determinada (tal como el 1 de abril ó viernes 13) ó para estallar en un momento determinado del día.

3.1.7 REPRODUCTORES

Un "primo" del virus, los reproductores (conocidos popularmente como conejos) se reproducen continuamente hasta que haya insuficiente espacio en el disco ó memoria para almacenar su abundante descendencia. Después de que sea creado un clónico hijo entonces empieza a crear y lanzar otros clónicos, los cuales, a su vez, continúan el ciclo hasta el infinito. El propósito es agotar los recursos del sistema, especialmente en un entorno multiusuario interconectado, hasta el punto en que el sistema principal no puede continuar el procesamiento.

La diferencia entre reproductores y virus informáticos es que los reproductores no atacan los archivos de datos de los usuarios ni implican normalmente una relación parásita con tales archivos. Los reproductores son autosuficientes y autónomos.

3.1.8 GUSANOS

Confundidos regularmente con los virus informáticos, los gusanos son programas que viajan a través de un sistema informático interconectado, de ordenador en ordenador, sin dañar necesariamente el hardware o al software. Los gusanos pueden reproducirse como un medio para continuar el trabajo por la red, pero lo hacen así solo cuando es necesario y cuando están programados convenientemente, a un costo reducido para el gasto del sistema.

Los gusanos viajan a través de ordenadores anfitriones de la red en secreto, reuniendo información (posiblemente contraseñas o documentos) o dejando mensajes burlones ó misteriosos antes de trasladarse.
A menudo los gusanos borran todos los vestigios de sus visitas con objeto de permanecer invisibles ante los Sistemas Operativos de la red.

3.1.9 VIRUS

Los virus informáticos son los favoritos del archivo de delincuentes. Los virus informáticos son programas que modifican otros programas para incluir una copia ejecutable y posiblemente alterada de ellos mismos. Fáciles de crear y difíciles de detectar, los virus contaminan los sistemas mediante la inserción de copias de ellos mismos, añadiendo clónicos creando cubiertas alrededor de archivos ejecutables. Los virus logrados expertamente no cambiarán la fecha del archivo o marcas de tiempo ni alteran atributos, tamaños o totales de control.

Para gestionar sus actividades y para evitar volver a infectar a los archivos, los virus colocan mensajes codificados (llamados v-markers o marcadores de virus) dentro de los archivos durante las infecciones iniciales.

Cuando no se pueden encontrar archivos no marcados, los virus suponen que sus anfitriones han sido sobrecargados totalmente con códigos víricos. En ese momento empieza normalmente la intromisión en las operaciones del sistema y en los datos del usuario final.

Los virus pueden empezar acciones destructivas abiertas, sencillamente divirtiéndose con los usuarios, imprimiendo en sus pantallas mensajes misteriosos o de burla, o también causando una conducta anormal del sistema.
Algunos virus se hacen pasar por errores del sistema, incitando a los usuarios a que busquen inexistentes fallos del hardware o software. Otros virus toman un enfoque más directo presentando pelotas que rebotan o caras sonrientes en las pantallas de los usuarios.

Los virus especialmente creativos realizan cualquier caso que el trabajo necesite hacer y luego borran toda prueba de su existencia, haciendo casi imposible la diagnosis vírica. A la larga, la mayoría de los virus estallan y dañan los datos del disco duro. (Un virus selecciona, en el momento de la explosión una lista de posibles técnicas de destrucción de datos, dando a cada explosión su propia identidad única; una vez más, el objetivo es hacer cada vez más difícil la investigación para los que combaten contra los virus.)

3.2 TIPOS DE VIRUS INFORMÁTICOS

Al igual que la gran variedad de software utilitario, los virus informáticos vienen en un inimaginable conjunto de gustos. Hay virus que infectan el sector de arranque, el procesador de órdenes, los archivos .COM y .EXE; demonios controladores de dispositivos, copiadores de propósito múltiple y monitores residentes en memoria, parásitos del hardware y soplones del CMOS, etc.

Cada técnica de infección proporciona notables ventajas y desventajas a los programadores. Algunos métodos de contaminación son preferidos porque es más difícil que el software antivirus los detecte; sin embargo pueden ser complejos de diseñar y por lo tanto requieren un esfuerzo adicional al escribirlos.
Otros procedimientos pueden ser más fáciles de codificar y desarrollar, pero limitados en su capacidad de saturar sistemas completos. Sin embargo, otros poseen capacidades superiores al saltar más allá de sus máquinas anfitrionas originales.
Dependiendo del lugar donde se alojan, la técnica de replicación o la plataforma en la cual trabajan, podemos diferenciar en distintos tipos de virus.

3.2.1 VIRUS CONTAMINADORES DE SECTOR DE ARRANQUE.

Utilizan el sector de arranque, el cual contiene la información sobre el tipo de disco, es decir, número de pistas, sectores, caras, tamaño de la FAT, sector de comienzo, etc. A todo esto hay que sumarle un pequeño programa de arranque que verifica si el disco puede arrancar el sistema operativo. Los virus de Arranque utilizan este sector de arranque para ubicarse, guardando el sector original en otra parte del disco. En muchas ocasiones el virus marca los sectores donde guarda el Arranque original como defectuosos; de esta forma impiden que sean borrados. En el caso de discos duros pueden utilizar también la tabla de particiones como ubicación. Suelen quedar residentes en memoria al hacer cualquier operación en un disco infectado, a la espera de replicarse. Como ejemplo representativos esta el Brain.

3.2.2 VIRUS DE ARCHIVO

Infectan archivos y tradicionalmente los tipos ejecutables COM y EXE han sido los mas afectados, aunque es estos momentos son los archivos (DOC, XLS, SAM...) los que están en boga gracias a los virus de macro (descritos mas adelante). Normalmente insertan el código del virus al principio o al final del archivo, manteniendo intacto el programa infectado.

Cuando se ejecuta, el virus puede hacerse residente en memoria y luego devuelve el control al programa original para que se continué de modo normal. El Viernes 13 es un ejemplar representativo de este grupo.

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

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

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

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

3.2.3 VIRUS CONTAMINADORES DE ARCHIVOS ESPECÍFICOS

Al igual que los contaminadores del sector de arranque y de los procesadores de órdenes, que restringen las infecciones a un conjunto conocido de archivos, los contaminadores de archivos específico atacan un número fijo y a un tipo fijo de archivos. Al contrario de la mayoría de las otras especies víricas, los contaminadores de archivo especifico son, como norma, escritos por alguien que tiene cuentas pendientes.

Los archivos de destino son normalmente los creados, vendidos o confiados al programador rogue, quizá un ex empleado, o alguna persona o compañía con la que dicho programador ha tenido una disputa. Los contaminadores de archivos especifico se introducen en los sistemas no infectados utilizando los canales estándar de infección, fijándose en discos y archivos aparentemente no infectados y esperando oportunidades para saltar.

3.2.4 VIRUS DE MACRO

Es una familia de virus de reciente aparición y gran expansión. Estos están programas usando el lenguaje de macros WordBasic, gracias al cual pueden infectar y replicarse a través de archivos MS-Word (DOC). En la actualidad esta técnica se ha extendido a otras aplicaciones como Excel y a otros lenguajes de macros, como es el caso de los archivos SAM del procesador de textos de Lotus. Se ha de destacar, de este tipo de virus, que son multiplataformas en cuanto a sistemas operativos, ya que dependen únicamente de la aplicación.

Hoy en día son el tipo de virus que están teniendo un mayor auge debido a que son fáciles de programar y de distribuir a través de Internet. Aun no existe una concienciación del peligro que puede representar un simple documento de texto.

3.2.5 VIRUS BAT

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

3.2.6 VIRUS DEL MIRC

Vienen a formar parte de la nueva generación Internet y demuestra que la Red abre nuevas forma de infección. Consiste en un código fuente para el cliente de IRC Mirc. Cuando alguien accede a un canal de IRC, donde se encuentre alguna persona infectada, recibe por DCC un archivo llamado "script.ini".

3.2.7 VIRUS CONTAMINADORES DE PROCESADOR DE ORDENES

Estos virus informáticos están diseñados para infectar los shells de órdenes centrales, como por ejemplo COMMAND.COM de MS-DOS. Ofrecen una ventaja distinta a los programadores rogue: como muchas órdenes introducidas en el teclado de computadores compatibles con IBM, son pasados a través del programa COMMAND.COM o cualesquiera programas de enlace que puedan ser cargados a la vez, los contaminadores del procesador de órdenes tienen la gran ventaja de examinar la gran mayoría de interacción entre usuarios y sus computadoras.
Pueden explotar las oportunidades para esconderse tras accesos normales de disco mientras que se ejecutan órdenes internas COMMAND.COM (como DIR o COPY).

Por ejemplo, una forma de que los usuarios vean el contenido de los directorios de los discos es emitir órdenes DIR. Introduciendo la palabra DIR, las unidades de disco se activan para realizar funciones "leer" del directorio.

Los usuarios esperan que los accesos a los discos sean dirigidos en ese momento; los virus corresponden a esas expectativas. Antes de que las órdenes DIR del disco sean en realidad procesadas, los contaminadores del procesador de órdenes se introducen; buscan y (cuando los encuentran) infectan otros procesadores de órdenes y luego acaban con las funciones normales de la orden DIR. Aunque los tiempos de ejecución de las órdenes interceptadas por virus son mayores que los de las no infectadas la mayoría de los usuarios no notan nunca la diferencia, y eso es con lo que cuentan los programadores rogue.
Los contaminadores de procesadores de órdenes gozan, en esencia, de mucho de los beneficios de diseño que tienen los contaminadores de sector de arranque. La diferencia básica entre los dos tipos víricos es que los contaminadores de sector de arranque se instalan primero, a un nivel mucho más bajo que lo que están los contaminadores de procesos de órdenes.

3.2.8 VIRUS CONTAMINADORES DE PROPÓSITO GENERAL

Los contaminadores de propósito general son los elementos de todos los oficios del reino del virus informático. Los contaminadores de propósito general se diseñan para la gama más amplia de compatibilidades infecciosas y, como tales, no pueden infectar archivos de bajo nivel de sistemas operativos. Sin embargo, como procesadores de órdenes centrales son en muchos aspectos archivos regulares ejecutables, la mayoría de los contaminadores de propósito general pueden infectarlos y los infectarán.

Los contaminadores de propósito general llegan a los sistemas informáticos utilizando las mismas avenidas secretas que los contaminadores de sector y de procesadores de órdenes. Sin embargo, en vez de buscar archivos de bajo nivel o de atacar a los procesadores de órdenes, los contaminadores de propósito general se contentan con infectar cualquier archivo ejecutable.

Los contaminadores de propósito general sobresalen en conseguir la saturación total del sistema y, en consecuencia, son uno de los tipos de virus informáticos de propagación más rápida.

Los contaminadores de propósito general bien diseñados se adaptan bien a la mayoría de formatos de archivos ejecutables, moviéndose rápidamente entre los archivos, obteniendo velozmente un estado de todos los archivos infectados. Esta técnica de asalto infeccioso masivo es el principal mecanismo por el que los contaminadores de propósito general consiguen mantener su control mortal sobre los sistemas.

Mientras que los contaminadores de sector de arranque y de procesadores de órdenes son fáciles de eliminar una vez descubiertos (sencillamente volver a instalar el sistema y los archivos procesadores de órdenes), los sistemas informáticos saturados con backups infectados presentan unos problemas de erradicación casi insuperables para los usuarios.

3.2.9 VIRUS CONTAMINADORES MULTIPROPÓSITO

Son virus informáticos creados para combinar algunos o todos los atributos infecciosos de los contaminadores de sector de arranque, procesador de órdenes y de propósito general. Los contaminadores multipropósito son una realidad práctica, diseñados para integrar las características más activas de los virus de sector de arranque, procesador de órdenes y propósito general.

Los contaminadores multipropósito pueden infectar inicialmente a los sectores de arranque, procesadores de órdenes o ambos. Desde allí ellos producen parásitos víricos, que de hecho, son contaminadores de propósito general.

Adoptando dos ó más técnicas infecciosas, los contaminadores multipropósito logran un nivel de supervivencia más alto y tienen menos problemas reproduciéndose que los que tienen los virus que poseen una única dimensión infecciosa.

Cuando los contaminadores multipropósito obtienen el control durante los tiempos de ejecución, normalmente inspeccionan los sectores de arranque y los procesadores de órdenes en busca de marcas víricas (v-markers), los bytes codificados reveladores que identifican los archivos infectados. Cuando no se encuentran marcas víricas, los contaminadores multipropósito continúan con la infección de archivos no marcados.

Cuando se localizan marcas víricas, los contaminadores multipropósito avanzan para encontrar archivos ejecutables a infectar. (Sin embargo, a veces los virus infectarán de todas formas a los archivos con marcas víricas, siendo la suposición que las marcas víricas pueden ser señuelos víricos).

3.2.10 VIRUS CONTAMINADORES RESIDENTES EN MEMORIA

Los contaminadores de sector de arranque y de procesador de órdenes pueden clasificarse también como contaminadores residentes en memoria puesto que ambos tipos víricos permanecen cargados y activos en memoria de la computadora cuando se ejecutan. Como esas prácticas utilidades de ejecución rápida en que muchos usuarios confían, algunos virus informáticos son capaces de operaciones de memoria.

Sin embargo, al contrario que las legitimas utilidades TSR (Terminate-and stay resident), los virus residentes en memoria no tienen ninguna ejecución rápida para que los usuarios los llamen para entrar en combate; ellos atacan inmediatamente al cargar y permanecen activo a lo largo de las secciones de cálculo. Las órdenes de teclado pueden ser interceptadas, la salida en pantalla puede ser falseada y los datos de disco pueden ser controlados e, incluso peor, modificados. Además los contaminadores residentes en memoria pueden inspeccionar continuamente sus sistemas anfitriones en busca de archivos no infectados e infectados durante intervalos de calma en operaciones informáticas normales.

3.3 CLASIFICACIÓN DE DAÑOS CAUSADOS POR LOS VIRUS

Los virus son, desde hace dos años, la mayor amenaza para los sistemas informáticos y la principal causa de pérdidas económicas en las empresas. Los virus informáticos representan el máximo exponente (por ahora) de una cadena evolutiva de programas de computadora de tipo dañino.

Debe quedar absolutamente claro que son programas y, por lo tanto, que han sido creados por una persona. De allí que este problema computacional no es generado por deficiencias o anomalías de hardware ó software, sino que es creado por personas. Las consecuencias del accionar de estas personas son la producción de distintos tipos de daño a la información procesada por computadoras.

Se definirá daño como una acción indeseada, y se clasificará según la cantidad de tiempo necesaria para reparar dichos daños. Existen seis categorías de daños hechos por los virus, de acuerdo a la gravedad.

1. **DAÑOS TRIVIALES:** Sirva como ejemplo la forma de trabajo del virus FORM (el más común): En el día 18 de cada mes cualquier tecla que presionemos hace sonar el beep. Deshacerse del virus implica, generalmente, segundos o minutos.

2. **DAÑOS MENORES:** Un buen ejemplo de este tipo de daño es el JERUSALEM. Este virus borra, los viernes 13, todos los programas que uno trate de usar después de que el virus haya infectado la memoria residente. En el peor de los casos, tendremos que reinstalar los programas perdidos. Esto nos llevará alrededor de 30 minutos.

3. **DAÑOS MODERADOS:** Cuando un virus formatea el disco rígido, mezcla los componentes de la FAT (File Allocation Table, Tabla de Ubicación de Archivos), o sobrescribe el disco rígido. En este caso, sabremos inmediatamente qué es lo que está sucediendo, y podremos reinstalar el sistema operativo y utilizar el último backup. Esto quizás nos lleve una hora.

4. **DAÑOS MAYORES:** Algunos virus, dada su lenta velocidad de infección y su alta capacidad de pasar desapercibidos, pueden lograr que ni aún restaurando un backup volvamos al último estado de los datos. Un ejemplo de esto es el virus DARK AVENGER, que infecta archivos y acumula la cantidad de infecciones que realizó. Cuando este contador llega a 16, elige un sector del disco al azar y en él escribe la frase: "Eddie lives … somewhere in time" (Eddie vive … en algún lugar del tiempo). Esto puede haber estado pasando por un largo tiempo sin que lo notemos, pero el día en que detectemos la presencia del virus y queramos restaurar el último backup notaremos que también él contiene sectores con la frase, y también los backups anteriores a ese. Puede que lleguemos a encontrar un backup limpio, pero será tan viejo que muy probablemente hayamos perdido una gran cantidad de archivos que fueron creados con posterioridad a ese respaldo.

5. **DAÑOS SEVEROS:** Los daños severos son hechos cuando un virus realiza cambios mínimos, graduales y progresivos. No sabemos cuándo los datos son correctos o han cambiado, pues no hay pistas obvias como en el caso del DARK AVENGER (es decir, no podemos buscar la frase Eddie lives ...).

6. **DAÑOS ILIMITADOS:** Algunos programas como CHEEBA, VACSINA.44.LOGIN y GP1 entre otros, obtienen la clave del administrador del sistema y la pasan a un tercero. Cabe aclarar que estos no son virus sino troyanos. En el caso de CHEEBA, crea un nuevo usuario con los privilegios máximos, fijando el nombre del usuario y la clave. El daño es entonces realizado por la tercera persona, quien ingresará al sistema y haría lo que quisiera.

3.3.1 LOS VIRUS INFORMÁTICOS Y SU CONTRIBUCIÓN A LA MUERTE DE PERSONAS.

Este problema tecnológico creado intencionalmente por personas ha alcanzado una dimensión tan grande que ya se han registrado muerte de seres humanos debido a su accionar y constituyen. la mayor fuente de pérdidas en cuanto a problemas de seguridad informática en las empresas.

Desde que aparecieron los virus informáticos se especuló mucho sobre sus capacidades de acción y, probablemente debido a las fantasías que despiertan las analogías con los virus biológicos, se tejieron muchos mitos sobre el tema. Una de estas especulaciones fue la utilización de los virus informáticos en contra de las personas y no solamente de los sistemas de computadoras; si bien esto es algo imposible de lograr en forma directa, se pueden realizar acciones dañinas indirectas hacia las personas a través de una computadora.

La primera muerte oficialmente documentada debida a un virus informático se registró en la ciudad de Londres en 1994.

La situación en que se produjo consistió en que la persona que falleció estaba internada en un hospital y ante una crisis fue mal medicada por un doctor que basó sus decisiones en la información provista por una computadora infectada por un virus informático.

Ya en el año 1992 circuló la información sobre un virus informático que había atacado el sistema de computadoras que manejaba el servicio de ambulancias para emergencias de la misma ciudad de Londres. El saldo final fue la muerte de once personas debido a las demoras que se producían por el incorrecto procesamiento de la información en el sistema. Aunque esto último, nunca fue oficialmente comprobado, llamó la atención que a los pocos meses se incorporara a las leyes británicas la figura, de "virus informáticos" dentro, de la legislación que se ocupa de los delitos realizados con la ayuda de computadoras.

3.3.2 DEL VANDALISMO AL SABOTAJE.

Se puede decir que hasta el año 1994 las personas que escribían virus informáticos seguían un modelo vandálico en sus acciones. Es decir, generaban un ente (en este caso perteneciente al mundo de las computadoras) el cual se dispersaba de computadora en computadora sin ningún tipo de control de destino, por lo tanto, causaba daño de manera indiscriminada. Por supuesto (y aun en la época anterior a la Internet comercial) esta dispersión y causa de daño indiscriminado podía tener un alcance mundial debido al intercambio de programas vía módem y a la posibilidad de transportarlos en disquetes.

A partir del año 1994 comenzaron a registrarse casos donde los virus estaban hechos (al menos en un principio) para producir daño en un sistema de computadoras especifico (aunque luego se siguieran dispersando a través de otras computadoras de manera indiscriminada). Esto se lograba por medio de alguna característica especifica del sistema a atacar que pudiera ser detectada por el programa virus. Esto modificó el modelo vandálico para convertirlo en un modelo que respondió a las características de herramienta utilizada para sabotaje.

Se puede decir también que este cambio de modelo de acción "profesionalizó" el accionar de algunos autores de virus que se encontraron en la situación de que podían cobrar dinero por crear herramientas que se podían utilizar en acciones de sabotaje a nivel corporativo y más allá. De hecho, el experto en guerra infraestructural William Church sostiene que hoy en día ya debe considerarse a los virus como una de las armas de la guerra informática.

3.4 Síntomas Típicos de una Infección.

- El sistema operativo o un programa toma mucho tiempo en cargar sin razón aparente.

- El tamaño del programa cambia sin razón aparente.

- El disco duro se queda sin espacio o reporta falta de espacio sin que esto sea necesariamente así.

- Si se corre el CHKDSK no muestra "655360 bytes available".

- En Windows aparece "32 bit error".

- La luz del disco duro en la CPU continua parpadeando aunque no se este trabajando ni haya protectores de pantalla activados. (Se debe tomar este síntoma con mucho cuidado, porque no siempre es así).

- No se puede "Arrancar" desde la Unidad A, ni siquiera con los discos de rescate.

- Aparecen archivos de la nada o con nombres y extensiones extrañas.

- Suena "clicks" en el teclado (este sonido es particularmente aterrador para quien no esta advertido).

- Los caracteres de texto se caen literalmente a la parte inferior de la pantalla (especialmente en DOS).

- En la pantalla del monitor pueden aparecen mensajes absurdos tales como "Tengo hambre. Introduce un Big Mac en la Unidad A".

- En el monitor aparece una pantalla con un fondo de cielo celeste, unas nubes blancas difuminadas, una ventana de vidrios repartidos de colores y una leyenda en negro que dice Windows '98 (No puedo evitarlo, es mas fuerte que yo...!!).

- El número de sectores malos en el disco aumenta constantemente.

- La cantidad de RAM disponible disminuye de forma repentina o constantemente.

- Programas que normalmente se comportan bien funcionan de modo anormal o caen sin motivo.

- Los programas encuentran errores donde antes no los encontraban.

- Los programas generan mensajes no documentados.

- Programas aparentemente benignos, de "travesuras" divertidas se materializan misteriosamente y nadie reconoce haberlos instalado. Por ejemplo agujeros negros en pantalla, pelotas que rebotan, caras sonrientes.

- Desaparecen archivos misteriosamente.

- Los archivos son sustituidos por objetos de origen desconocido o por datos falseados.

Una infección se soluciona con las llamadas "vacunas" (que impiden la infección) o con los remedios que desactivan y eliminan, (o tratan de hacerlo) a los virus de los archivos infectados. Hay cierto tipo de virus que no se pueden desactivar ni remover, por lo que se debe destruir el archivo infectado.

3.5 ¿ QUE ES UN ANTIVIRUS ?

No para toda enfermedad existe cura, como tampoco existe una forma de erradicar todos y cada uno de los virus existentes.

Es importante aclarar que todo antivirus es un programa y que, como todo programa, sólo funcionará correctamente si es adecuado y está bien configurado.
Además, un antivirus es una herramienta para el usuario y no sólo no será eficaz para el 100% de los casos, sino que nunca será una protección total ni definitiva.

La función de un programa antivirus es detectar, de alguna manera, la presencia o el accionar de un virus informático en una computadora. Este es el aspecto más importante de un antivirus, independientemente de las prestaciones adicionales que pueda ofrecer, puesto que el hecho de detectar la posible presencia de un virus informático, detener el trabajo y tomar las medidas necesarias, es suficiente para acotar un buen porcentaje de los daños posibles. Adicionalmente, un antivirus puede dar la opción de erradicar un virus informático de una entidad infectada.

El modelo más primario de las funciones de un programa antivirus es la detección de su presencia y, en lo posible, su identificación. La primera técnica que se popularizó para la detección de virus informáticos, y que todavía se sigue utilizando (aunque cada vez con menos eficiencia), es la técnica de scanning (Escrutar). Esta técnica consiste en revisar el código de todos los archivos contenidos en la unidad de almacenamiento -fundamentalmente los archivos ejecutables- en busca de pequeñas porciones de código que puedan pertenecer a un virus informático. Este procedimiento, denominado escaneo, se realiza a partir de una base de datos que contiene trozos de código representativos de cada virus conocido, agregando el empleo de determinados algoritmos que agilizan los procesos de búsqueda.

La técnica de scanning fue bastante eficaz en los primeros tiempos de los virus informáticos, cuando había pocos y su producción era pequeña. Este relativamente pequeño volumen de virus informáticos permitía que los desarrolladores de antivirus, "escaneadores", tuvieran tiempo de analizar el virus, extraer el pequeño trozo de código que lo iba a identificar y agregarlo a la base de datos del programa para lanzar una nueva versión. Sin embargo, la obsolescencia de este mecanismo de identificación como una solución antivirus completa se encontró en su mismo modelo.
El primer punto grave de este sistema radica en que siempre brinda una solución a posteriori: es necesario que un virus informático alcance un grado de dispersión considerable para que sea enviado (por usuarios capacitados, especialistas o distribuidores del producto) a los desarrolladores de antivirus. Estos lo analizarán, extraerán el trozo de código que lo identificará, y lo incluirán en la próxima versión de su programa antivirus. Este proceso puede demorar meses a partir del momento en que el virus comienza a tener una dispersión considerable, lapso en el cual puede causar graves daños sin que pueda ser identificado.

Además, este modelo consiste en una sucesión infinita de soluciones parciales y momentáneas (cuya sumatoria jamás constituirá una solución definitiva), que deben actualizarse periódicamente debido a la aparición de nuevos virus.

En síntesis, la técnica de scanning es altamente ineficiente, pero se sigue utilizando debido a que permite identificar rápidamente la presencia de los virus más conocidos y, como son estos los de mayor dispersión, permite una importante gama de posibilidades.
En virtud del pronto agotamiento sistemático de la técnica de scanning, los desarrolladores de programas antivirus han dotado a sus creaciones de métodos para búsquedas de virus informáticos (y de sus actividades), que no identifican específicamente al virus, sino algunas de sus características generales y comportamientos universalizados.

Este tipo de método rastrea rutinas de alteración de información que no puedan ser controladas por el usuario, modificación de sectores críticos de las unidades de almacenamiento (master boot record, boot sector, FAT, entre otras), etc. Un ejemplo de este tipo de métodos es el que utiliza algoritmos heurísticos.

De hecho, esta naturaleza de procedimientos busca, de manera bastante eficiente, códigos de instrucciones potencialmente pertenecientes a un virus informático. Resulta eficaz para la detección de virus conocidos y es una de las soluciones utilizadas por los antivirus para la detección de nuevos virus. El inconveniente que presenta este tipo de algoritmo radica en que puede llegar a sospecharse de muchísimas cosas que no son virus.

Esto hace necesario que el usuario que lo utiliza conozca un poco acerca de la estructura del sistema operativo, a fin de poseer herramientas que le faciliten una discriminación de cualquier falsa alarma generada por un método heurístico. Algunos de los antivirus de esta clase son F-Prot, Norton Anti Virus y Dr. Solomon's Toolkit.

Ahora bien, otra forma de detectar la presencia de un virus informático en un sistema consiste en monitorear las actividades de la PC señalando si algún proceso intenta modificar los sectores críticos de los dispositivos de almacenamiento o los archivos ejecutables. Los programas que realizan esta tarea se denominan chequeadores de integridad.

Sobre la base de estas consideraciones, podemos consignar que un buen sistema antivirus debe estar compuesto por un programa detector de virus -que siempre esté residente en memoria- y un programa que verifique la integridad de los sectores críticos del disco rígido y sus archivos ejecutables. Existen productos antivirus que cubren los dos aspectos, o bien pueden combinarse productos diferentes configurados de forma que no se produzcan conflictos entre ellos.

3.5.1 MODELO ANTIVIRUS

La estructura de un programa antivirus, está compuesta por dos módulos principales: el primero denominado de control y el segundo denominado de respuesta. A su vez, cada uno de ellos se divide en varias partes:

1. Módulo de Control:

Posee la técnica verificación de integridad que posibilita el registro de cambios en los archivos ejecutables y las zonas críticas de un disco rígido. Se trata, en definitiva, de una herramienta preventiva para mantener y controlar los componentes de información de un disco rígido que no son modificados a menos que el usuario lo requiera.

Otra opción dentro de este módulo es la identificación de virus, que incluye diversas técnicas para la detección de virus informáticos. Las formas más comunes de detección son el scanning y los algoritmos, como por ejemplo, los heurísticos.

Asimismo, la identificación de código dañino es otra de las herramientas de detección que, en este caso, busca instrucciones peligrosas incluidas en programas, para la integridad de la información del disco rígido.
Esto implica descompilar (o desensamblar) en forma automática los archivos almacenados y ubicar sentencias o grupos de instrucciones peligrosas.

Finalmente, el módulo de control también posee una administración de recursos para efectuar un monitoreo de las rutinas a través de las cuales se accede al hardware de la computadora (acceso a disco, etc.). De esta manera puede limitarse la acción de un programa restringiéndole el uso de estos recursos, como por ejemplo impedir el acceso a la escritura de zonas críticas del disco o evitar que se ejecuten funciones de formato del mismo.

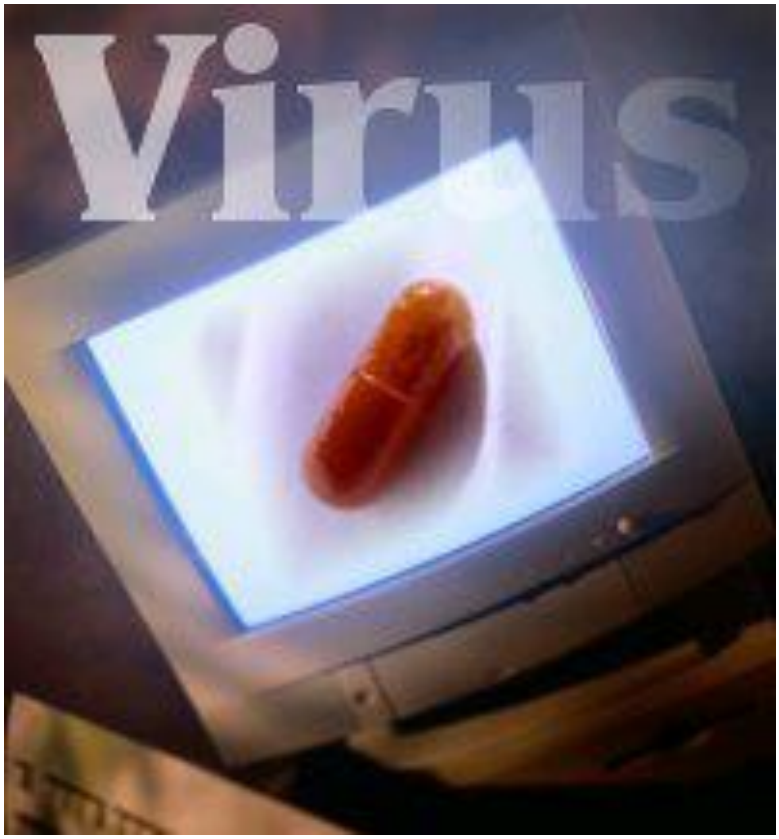
2. Módulo de Respuesta:

La función alarma se encuentra incluida en todos los programas antivirus y consiste en detener la acción del sistema ante la sospecha de la presencia de un virus informático, e informar la situación a través de un aviso en pantalla.

Algunos programas antivirus ofrecen, una vez detectado un virus informático, la posibilidad de erradicarlo. Por consiguiente, la función reparar se utiliza como una solución momentánea para mantener la operatividad del sistema hasta que pueda instrumentarse una solución adecuada.

Por otra parte, existen dos técnicas para evitar el contagio de entidades ejecutables: evitar que se contagie todo el programa o prevenir que la infección se expanda más allá de un ámbito fijo.
Aunque la primera opción es la más adecuada, plantea grandes problemas de implementación.

CAPÍTULO IV



ESTUDIO DE LOS VIRUS MÁS RELEVANTES

PREÁMBULO.

INTRODUCCIÓN.

En este capítulo se describe el funcionamiento y características de los virus más relevantes en el pasado y los que más protagonismo han dado en el presente.

Esto con el fin de conocer los virus más importantes y su método de infección. También servirá como un marco de referencia para evaluar la evolución que ha sufrido las técnicas de infección y detección de Virus.

OBJETIVOS:

- Conocer los virus mas importantes en la historia
- Analizar la evolución de los virus del pasado con los del presente.

4.1 Los Virus más Conocidos

Dentro de las características que encierran a los virus y los daños que ocasionan a los ordenadores, tenemos cuatro casos de virus informáticos:

- Infectores de área de carga (Sector de Arranque).
- Infector de programas ejecutables (.COM y .EXE).
- Poliformo multipartita "afecta el área de particiones"(Master Boot Record, MBR).
- Sector de arranque.

4.1.1 Los Virus más Relevantes en el Pasado.

A continuación se hará referencia a las características y relevancias de los virus más destacados en el pasado.

Estos virus marcaron una pauta muy importante en la historia de la informática, gracias a estos programas se desarrollaron las medidas de seguridad; así como la industria de los antivirus que ahora conocemos.

4.1.1.1 Virus Miguel Ángel (Michelangelo)

Este virus descubierto en abril de 1991, es del tipo Infectores del sector de carga, por tanto, infecta el sector de carga de los disquetes y la tabla de particiones de los discos duros. Se cree que su origen es holandés o sueco, ya que es en esos países europeos donde se obtienen los primeros reportes de él.

Como la mayoría de los virus, Michelangelo se posiciona en la memoria de las computadoras cuando se "cargaba" el sistema operativo desde un disquete o un disco duro infectado. A partir de ese momento, infectaba cualquier disquete de 5 ½ pulgadas en la unidad, sino estaba protegido contra escritura.

El virus se instala en la parte alta de la memoria de la computadora pero siempre debajo de los 640 KB convencionales, ocupando 2,048 bytes. Genera una protección mediante la interrupción 12h del BIOS, regresando un valor para la cantidad de memoria disponible, que es igual a la memoria real instalada menos la cantidad reservada para él mismo.

De esta manera evita que pueda ser eliminado por otros programas que se pudieran cargar en la misma localidad de la memoria. Cuando infecta un disquete de 360 KB de 5 ¼", posicionaba el sector de carga original (Boot Sector) en el sector 11; si el disquete es de 1.2 MB de 5 ¼", lo hace en el sector 28 que es último del área del directorio raíz (Root directory). Ubicando el programa de carga en este sector se protege, ya que ninguna información de datos se sobrescribirá en el área de directorios. En cambio, cuando la infección es en un disco duro la tabla de particiones o Master Boot Record se desplaza a la dirección física: Cilindro 0, lado 0, sector 7, y el virus se aloja en el lugar del MBR.

Michelangelo cabe en un sector, ya que su longitud es de sólo 429 Bytes (los sectores contienen un total de 512).

El virus Michelangelo se activa cualquier 6 de marzo, pues se cree que fue hecho para "celebrar" ese día del nacimiento de Miguel Ángel Buonarroti, escultor, arquitecto y pintor italiano deL Renacimiento.

En esa fecha si su computadora esta infectada con el virus, al "arrancar" el sistema con el disquete o disco duro "enfermo" lo primero que hace éste es verificar la fecha del reloj del sistema. Sí ésta coincide, en lugar de infectar disquetes o el disco duro, sobrescribe el disco desde el cual se realizó la carga, destruyendo la información contenida en él.

La computadora tipo XT se salvan de la terrible acción del virus de Miguel ángel al encenderse, porque cuando se carga el virus todavía no está asignada la fecha en la memoria. En las At con procesador 286 en adelante inmediatamente después de la "carga" un 6 de marzo, sobrescribe en el área de carga, en la tabla de asignación de archivos y en el directorio raíz, una serie de ceros si el sistema operativo es PC-DOS o F6, si el sistema es MS-DOS, con lo que el disco queda imposibilitado para hacer la recuperación de los datos borrados.

Investigaciones del club de "virologos" de microcomputadoras de Guadalajara en México, determinaron que el virus infecta redes que utilizan sistema operativo MS-DOS, por supuesto, pero también infectó una red que corría con NOVELL Y UNÍX. Lo anterior se debe a que el virus ocupa un solo sector en el disco, por lo tanto aL hacer la infección no necesita de DOS para poder ubicarse en el sector físico de la tabla de particiones.

El requisito es que el sistema cuente con un programador intel o compatible de la familia de 8086. Miguel Ángel se puede detectar y eliminar con varios antivirus: Scan y Clean de McAffe, en sus versiones 80 o posteriores; CPAV (Central Point Antivirus); PC-GUARDIAN, PC-Cillin, MSAV (Microsoft Antivirus), que se incluye con el MS-DOS desde la versión 6.0 y otros.

La detección y eliminación de este virus debe hacerse cuando el reloj del sistema no tenga fecha 6 de marzo, de lo contrario, al encender la computadora se borra la información del disco duro.

En febrero de 1992, en México se dio gran difusión en los medios informativos acerca de las atrocidades que podría llevar a cabo ese virus en millones de computadoras en todo el mundo. Efectivamente, si todas esas computadoras se hubieran "cargado" desde disco infectados ese día la pérdida de información hubiera sido desastrosa e irreparable, pero es casi imposible que tengan el mismo tipo de virus porque a la fecha se conocían más de 3,000 y cada uno de ellos tienen diferentes formas y fechas programadas de activación, lo anterior no quiere decir que debamos de apagar la computadora si es la fecha de activación del virus, ya que como se mencionó, existen infinidad de virus que "explotan", en diferentes fechas, horas y ante determinadas condiciones de la computadora; lo que se debe hacer es tomar medidas de precaución y prevención, y contar con uno o varios programas antivirus.

En particular para este virus se recomienda que un día antes de cualquier 6 de marzo cambie la fecha de su computadora DATE del DOS. Si su computadora no tiene batería y reloj permanente, es una buena idea no introducir la fecha de ese día. Si el virus se encuentra instalado en la memoria de la computadora y si no es 6 de marzo se debe apagar ésta para eliminar al virus. Después se puede cargar el sistema operativo desde un disquete que no este infectado y proceder a la revisión del disco duro o disquetes infectados.

La mejor manera de protegerse de éste y de otros virus que formatean el disco o sobrescriben la FAT o el Directorio, es crear un disco de rescate con Norton Utilities, o un Emergency Disk utilizando PC-TOOLS versión 8.0 en adelante; así, si se sufre un desastre en el disco duro, siempre se podrá restaurar como estaba antes de la infección, ya que la información está ahí, pero sin la FAT y el directorio no se puede acceder.

4.1.1.2 Virus De Turín

El virus de Turín o virus de la pelotita es un segmento de código que, a diferencia de la mayoría de los virus, no modifica los archivos ejecutables ni produce ningún daño a los discos, excepto infectarlos. Este virus graba el mencionado código en área de carga inicial (Área de Arranque) y, para no afectarla, traslada el programa de carga inicial al primer sector libre que encuentre y lo marca como defectuoso en la tabla de asignación de archivos (FAT), para que este sector no pueda ser accesado por el sistema operativo y no puedan hacer modificaciones en él. También es conocido como Veracruz, Booncing, Ball ó ping-Pong.

Fue reportado por vez primera en marzo de 1988, y en su versión original solo infectaba disquetes. Funciona en forma aleatoria, es decir, que no siempre se activa cuando está trabajando la computadora, pero en algunas ocasiones, cuando se producen las condiciones apropiadas, produce una molesta pelotita que rebota a lo largo de la pantalla.

Algunos usuarios que padecieron este desagradable virus en sus sistemas se acostumbraron a vivir con él, y cuando aparecía la pelotita, la única solución que aplicaban era, apagar la computadora y esperar que en la próxima sesión de trabajo no se presentara.

Como la sesión del área de carga inicial (Boot Área), conocidas como bloques de parámetros del BIOS (Bios Parameter Block, BPB) aloja los datos relativos al tipo de formato que tiene el disco, la versión del sistema operativo y las copias de la tabla de asignación de archivos (FAT), parte del virus se coloca después de los primeros 32 desplazamientos, mientras que el resto del código se anexa al grupo de sectores continuos donde se copió el programa de carga inicial.

Esto es precisamente lo que nos ayuda a detectar este tipo de virus, pues nos permite indagar si el cluster 2 aparece marcado como dañado, aunque físicamente no lo esté. De ser así ya lo tenemos localizado. También podemos buscar el programa de carga inicial en el sector 13, con lo cual se confirma las sospechas. Ocupa en el disco, 1,024 bytes, ósea dos sectores completos. La búsqueda del programa de carga inicial se facilita por la cadena de carácter de los mensajes de error que contiene por ejemplo en versión 3.3 del sistema operativo MS-DOS el mensaje de error dice: Non-System Disk or Disk Error (Relace and Strike).

Con cualquier programa de utilidades que tenga la característica de búsqueda de cadenas de caracteres en código ASCII, se puede indagar en que sector se encuentra tal programa de carga inicial, y si no esta alojado en el área INICIAL (Boot sector), puede suponerse que un virus lo ha desplazado de su sector original y ha tomado su lugar, marcándolo como dañado o no.

Contrariamente con lo que se piensa con el virus de Turín no resulta fácil infectar una computadora con él cuando no se encuentra activo en la memoria RAM. Los virus infectores del área de carga inicial solamente se alojan en la memoria RAM cuando se carga o se intenta cargar el sistema operativo con disco infectado.

No olvide que los virus informáticos son sólo programas, y el de Turín se carga en la memoria cuando la computadora lee el código del virus que se encuentra en el sector o (cero). De ninguna otra manera puede tomar control de la memoria, si desea eliminar al virus, solamente hay que apagarla.

Formas de contagio.

Si se inicializa la computadora desde unos disquetes o desde disco duro infectado, el virus será dueño de todas las operaciones de lectura, grabación o copiado que usted intente hacer, y todos los virus que introduzca en la computadora serán contagiados inmediatamente con cualquier acceso que se haga incluso cuando pida usted visualizar el directorio de un disco duro o un disquete.

Al encenderse la computadora e introducir un disco de sistema operativo que esté contaminado, lo primero que se "carga" en la memoria de la computadora son las instrucciones del segmento del código del virus. Una vez introducido en la memoria el virus le indica al sistema realizar un salto (JUMP) para redireccionar la orden de lectura del programa de carga que se encuentra alojado en algún otro sector.

Aunque el virus pareciera estar trabajando paralelamente a los procesos que se están llevando acabo, la realidad es que funciona bajo la modalidad de ROBO DE CICLO al microprocesador, si se introduce un disquete infectado a la computadora quedará infectada inmediatamente a menos que haya sido protegido contra grabación, el espacio que ocupa el virus de Turín es de apenas 1 KB en el disco, y 2 KB cuando se carga en la memoria.

La segunda parte del código del virus es la que activa la pelotita que rebota en la pantalla del monitor, de acuerdo con una señal de tiempo especifica. En el mapa del disco infectado por el virus de Turín puede verse en el cluster –grupo sectores continuos- que ha sido marcado como dañado, pero no indica ningún cambio en el área de carga inicial (Área de Arranque). Sin embargo, si se observa el sector 0 del área de carga inicial se notará que los mensajes que generalmente se encuentran en la segunda parte de ésta, han desaparecido.

Si se continua con el rastreo hasta el sector 12, se localizará la parte complementaria del virus y, finalmente, al llegar al sector 13 aparecen los mensajes perdidos. Con esto queda demostrado que el virus está ocupando el sector de carga inicial y ha enviado su parte complementaria y el programa de carga inicial (Boot Program) a los sectores 12 y 13 del cluster 2.

Algunos antivirus creados en la parte oriental de Europa, reportan versiones como Hacked ping- pong, que en lugar de presentar la pelotita en el monitor, mediante una subrutina borra los ocho primeros sectores de los disquetes, y Yankee Ping-Pong, que es una modificación hecha al de Turín, por una infección anterior del virus Yankee Doodle.

4.1.1.3 El Virus Pakistán

El virus de Pakistán o Brain, otro infector del sector de arranque, al igual que todos los demás virus conocidos ha sufrido una serie de mutaciones, adiciones, modificaciones, etc., que propician que cada investigador que lo llega a percibir se refiera a él de manera diferente.
Este virus ocupa 9 KB en la memoria y 3,072 bytes (seis sectores) en el disco infectado. Cuando está presente en la computadora, hace muy lentos los procesos de acceso de lectura y grabación, sobre todo cuando busca algún disco al cual contagiar y éste se haya protegido contra escritura, ya que antes de mostrar lo que se le pide, realiza varios intentos de infección.

Contrario a lo que cree la mayoría de las personas, ningún disco así protegido puede ser infectado. Se hace esta aclaración porque hay quienes piensan que los virus informáticos pueden transmitirse de un disco a otro, incluso cuando se guardan juntos en una misma caja, discos sanos y discos infectados.

Está considerado como muy dañino y muy difícil de erradicar en sus modalidades actuales, que difieren mucho de la suave versión original creada en Lahore, Pakistán, la cual presentaba un mensaje, los datos del registro de autor y fecha: Welcome to the dungeon...Beware of this VIRUS. Contact us for vaccination, con coryright 1986; los nombres Basit y Amjad; el nombre de la compañía, Brain Computer Services, y la dirección, 730 Nizam Block Allama Iqbal, Lahore, Pakistán, así como sus números telefónicos.

Los autores aseguraron que habían creado el virus solo para el control de su propio software. En su versión original infecta únicamente los discos flexibles de 5 ¼" y, al desatarse, reemplazan al sector de carga y lo colocan en algún sector libre; señala como sectores no utilizables todos los que ha ocupado para su protección.

Hace muy lenta la operación de carga y borra muchos archivos, la versión que se conoce en México no produce esos daños.

A diferencia del virus de Turín, este sí graba su código en el área de carga inicial sobre los primeros 32 desplazamientos, área conocida como bloque de parámetros del BIOS (BIOS Parameter Block, BPB). Después de la copia a partir del sector 118 o del primer sector vació que encuentra, y realiza una copia de sí mismo en los sectores siguientes, marcando todos éstos como dañados.

Al trabajar con disco infectado con el virus de Pakistán, se nota que la infección no es sencilla. Deben cumplirse ciertos requisitos para que esta se lleve a cabo, de modo que no se debe crear pánico por causa de los virus, ya que por lo menos las versiones conocidas resultan manejables y se les toman las precauciones necesarias, no representan mayor problema, además, con la gran cantidad de programas antivirus que se encuentran ya al alcance de cualquier usuario, este tipo de virus es muy fácil de erradicar.

Las variantes mas conocidas de este virus son Brain-B, denominado también Virus Houston y es la variante del virus de Pakistán que adicionó la opción para infectar los discos fijos o duros. Brain-C infecta los discos duros, como el anterior, pero se ha eliminado la etiqueta de copyright (Brain) del sector 5, haciéndolo más difícil su detección.

La versión V9.1 del Shoe Virus-B, se ha modificado para que no infecte a los discos fijos. La variante Clone-B corromperá la tabla de asignación de archivos (FAT) si se carga después del 5 de mayo de 1992.

4.1.1.5 Virus de Jerusalén.

A diferencia de los cuatro virus anteriores, este es un virus infector de archivos ejecutables con extensión .EXE ó .COM, es uno de los más peligrosos que se conocieron, y se difundió ampliamente en los Estados Unidos, México, países de centro y Sudamérica, España y Europa general.

Se le conoce como virus israelí o del viernes 13, esté virus, hasta hace algún tiempo, era uno de los más contagiosos y no se necesitaba más que ejecutar el programa infectado para que se instale en la memoria de la computadora. Una vez en la memoria, infectaba todos los programas que se ejecutaban en la misma sección de trabajo.

Jerusalén es un famoso virus que se descubrió a fines de 1987 en la universidad hebrea de Jerusalén en los discos de las PC de IBM y sus compatibles. Se dice que fue desarrollado por activistas de la organización para la liberación de Palestina (OLP), para que iniciara su acción el 13 de mayo de 1988 con motivo de la celebración del 40° aniversario del ultimo día de Palestina como nación.

Infecta al sistema mediante el archivo COMMAND.COM, pero también ataca los programas ejecutables, incluyéndose al final de estos e incrementando la longitud del archivo. El virus se instala como residente en memoria, haciendo que la ejecución de los programas sea considerablemente más lenta.

La versión original se producía tantas veces en los programas infectados, que crecían de tal modo que luego no se podían cargar en la memoria; su tamaño no le permitía seguir reproduciéndose en el disco por falta de espacio suficiente, pero posteriormente algún programador resolvió el problema controlando su crecimiento desmedido, facilitando así su propagación controlada.

Su detección no se dificulta si se revisa constantemente la cantidad de bytes de archivos ejecutables, y si se nota alguna modificación, probablemente se trata de alguna infección por este virus. Si se ejecuta un programa infectado en un viernes 13, se borra del disco, junto con los archivos de control o ejecución con extensiones. OVR,.OVL, etc.

Existen muchos programas antivirus para detectar y erradicar este virus, pues se han dado casos de empresas de software que distribuyen disquetes con programas originales, y por un descuido diseminaron el virus entre sus usuarios. Después desarrollaron un antivirus y lo entregaron gratuitamente para tratar de remediar el daño.

Jerusalén infecta los archivos con extensión .COM, introduciéndose en su código, al principio del programa, siempre y cuando la suma de longitud del archivo sea menor o igual a 64 KB, y lo hace una sola vez.

A los archivos con extensión .EXE los pude infectar tantas veces como sean las veces que se ejecute, hasta que el disco se llene, en este caso se posesiona al final del código del programa por medio de un APEND y modifica el punto de entrada (Start Point) del programa.

Cuando está en la memoria de la computadora, se activa una bomba de tiempo que realiza un corrimiento de una parte del texto hacia abajo, lo que produce un efecto visual en la pantalla, como si se abriera una pequeña ventanita. Causa errores en la computadora y hace lentos los procesos, y en el momento de estar trabajando en algún programa infectado puede borrar información de la memoria o congelar el sistema.

Infecta los archivos ejecutables, aunque estén protegidos contra escritura; les quita el atributo de sólo lectura, los infecta y los regresa con el atributo original para que el usuario no sé de cuenta de la infección. Cuando se cumpla con la fecha del sistema que coincida con algún viernes 13, se activa una parte del virus que va borrando cualquier programa o archivo que se ejecute, incluso los de extensión. OVL.OVR, etc.

Se ha podido comprobar que este virus puede infectar archivos protegidos con el atributo de solo lectura, y lo vuelve a proteger para que usted no se dé cuenta que ha sido modificado.

Las modificaciones que se conocen con este virus son: Jerusalén-B, que es la versión modificada con control de infecciones, y Jerusalén-C o New Jerusalén, que es la misma, pero omite el código de retraso del cronómetro, por lo que es muy difícil de detectar hasta que se activa. Black Hole, que es la misma versión que Jerusalén-C, pero con unas 21 llamadas de interrupciones que parecen no tener sentido, así como un mensaje que dice antivirus.

Jerusalén-D y Jerusalén-E son modificaciones de los anteriores para destruir la tabla de asignación de archivos en vez de borrar los programas.

4.1.1.5 Virus Natas o Satán

Este virus, posiblemente originario de México, no se puede clasificar entre los infectores de carga, pero tampoco podría estar con los infectores de archivos ejecutables. Se puede decir que es un virus multipartita, porque infecta varias partes del disco, como archivos ejecutables, controladores de dispositivos, sector de arranque y tabla de particiones.

El virus NATAS, realmente marca el principio de una época, por lo menos en México, porque se consideró que el año de 1994 había infectado el 95% de las computadoras en las empresas públicas y privadas. Todos los días se sabía de infecciones a causa de este virus como en bancos, oficinas de gobierno, institutos de investigaciones, escuela de todos los niveles y usuarios personales.

Incluso hay empresas dedicadas al soporte y asesoría contra los virus que reconocen haber atendido las computadoras del IFE (Instituto Federal Electoral), unas semanas antes de realizarse las tan sonadas elecciones del cambio en México, porque este virus se había colado a sus sistemas. Esto no es tan raro ya que las computadoras de oficinas de gobierno o las propias empresas de computación, portaban el virus en sus disquetes sin que nadie lo notara, porque hacia principios del año no existía un antivirus que lo reconociera; los síntomas que produce el virus pueden haberse atribuido a errores de los equipos o problemas de los programas.

Actualmente se sabe de infecciones en Europa, Sudamérica y Estados Unidos, por los boletines insertados en la red Internet y en los BBS de McAfee Associates.
Cuando una computadora es infectada con el virus NATAS, los primeros síntomas se manifiestan en la memoria superior ya que al infectar los archivos ejecutables y de sistema que se excluyen en el CONFIG.SYS y en el AUTOEXEC.BAT, comienza por bloquear las áreas de trabajo de Windows. También se nota la infección cuando existen problemas para grabar o leer información de los discos.

Sus efectos son aleatorios, y en ocasiones se han detectado inscripciones en bloques de 64 bytes en archivos de datos, los cuales arma como rompecabezas cada vez que se ejecuta el código de 1 KB que contiene el archivo anfitrión.

Los daños que ocasiona el virus también son aleatorios, ya que pueden mantenerse instalado en la memoria por largo tiempo y no presentar síntomas que lo delaten; sin embargo, cuando se dan las condiciones preprogramadas en su código, infecta archivos ejecutables y de sistema, buscándolas en los directorios especificados con el comando PATH en el archivo AUTOEXEC.BAT los archivos del sistema los infecta cuando tienen estructura de ejecutables.

Además, aleatoriamente algunos investigadores han calculado que una vez de quinientas, sobrescribe la tabla de particiones o formatea sectores del disco, con la cual destruye la información ahí contenida. Cuando se ejecuta un programa con el virus NATAS, o cuando se hace la carga o intento de carga con un disquete con el código del virus en el sector inicial de carga, el virus se instala en la memoria de la computadora, e infecta cuando el disquete se introduce a la unidad para leer o grabar datos.

También va infectando los programas con extensión .COM, .EXE, .SYS, .OVR, .OVL y otros con la estructura de ejecutables.

La infección consiste en grabar una parte de su código en el sector de arranque de los disquetes o en la tabla de particiones (Master Boot Record, MBR), enseguida graba el resto del código en nueve sectores; al final de los disquetes, o en los últimos nueve sectores de la localidad física Cilindro 0, Lado 0, que no es una dirección lógica en los discos duros, con lo cual se tiene asegurada su existencia, porque ninguna información se escribirá sobre el código del virus. Los sectores lógicos de los discos duros empiezan en el Cilindro 0, Lado 1, Sector 1, que corresponde al sector lógico 0, y es donde esta ubicado el programa de carga inicial.

El virus Natas se compone de varias partes que han sido estudiadas e identificadas plenamente:

- **Cabeza del virus,** que se aloja en el sector de la tabla de particiones o en el sector de carga de los discos duros y disquetes respectivamente.

- **Cuerpo de virus,** que se localiza ocupando nueve sectores; al final de los disquetes, o al final del Cilindro 0, Lado 0, en los discos duros.

- **Virus completo,** incluye cabeza y cuerpo, se aloja al final de los archivos ejecutables o de los sistemas, que muestran una estructura similar a los ejecutables.

Estos son los que se cargan inicialmente a la memoria de la computadora mediante el archivo CONFIG.SYS

Cuando se realiza la carga de sistema operativo en la computadora, lo primero que se lee en el disco es el sector de carga (Boot Sector) o la tabla de particiones (master Boot Record, MBR), para identificar el medio, desde el cual realiza la carga del DOS. Sí Natas esta ahí, lo primero que se instala en la memoria de la computadora es el virus, su cuerpo o su código, y enseguida el COMMAND.COM y los programas o manejadores de dispositivos (Device Drivers) que se encuentran en los archivos CONFIG.SYS y AUTOEXEC.BAT, en ese orden.

El código inicial o cabeza del Natas lo incluyen los archivos ejecutables en el Header, desde donde hace un salto hasta el final del código del programa, que es donde comienza el programa para que el usuario no se de cuenta. Los archivos infectados crecen en 4,744 bytes su longitud y Natas les cambia la fecha a 100 años más que la original para detectar cuando un archivo ha sido ya contaminado.

Reserva 6 KB en su memoria para su uso, interceptando la interrupción 12h para enviar de regreso, cuando se le solicite, un valor de memoria disponible igual al valor real menos a los 6KB. Esto lo protege de cualquier sobre escritura en su código porque el DOS no tomará en cuenta la dirección de memoria para cargar otros programas.

Si se carga el virus desde el sector de arranque, envía un mensaje de que no hay sistema. Utiliza encriptamiento para ocultar su código en la parte final de los archivos infectados y técnicas Stealth, evitando así su fácil detección. El encriptamiento lo realiza apoyándose en el timer (contador de tiempo) de la computadora, pero a nivel de interrupción, un codificado diferente en cada caso, ya que los valores de cada tipo de Timer varían con la computadora.

4.1.2 LOS VIRUS MÁS RELEVANTES EN EL PRESENTE.

En la actualidad, cada momento, circula en la Internet un virus que lleva como objetivo la infección de un ordenador ó archivo especifico.

Cada mes surge un virus relevante que afecta a miles de usuarios en el mundo y que causan millones de dólares en pérdidas y daños en la información. Hasta ahora es casi imposible decir que se puede vivir a salvo o sin una amenaza de infección, solamente queda por tomar todas las medidas de seguridad existentes y necesarias para reducir el riesgo de una infección.

A continuación se presenta una lista con las características de los virus más desastrosos en la actualidad, virus que ocasionaron serios daños tanto económicos como físicos en la información, gracias a las facilidades que brinda el Internet.

Los siguientes virus representan las amenazas más peligrosas y comunes en América Latina:

4.1.2.1 W32.Magistr.24876@mm.

Es un virus que posee la capacidad de un gusano que se propaga por correo electrónico. Asimismo, también puede hacerlo por red. Este virus infecta los archivos ejecutables PE (Portable Executable) de Windows, a excepción de los archivos de sistema .dll, y envía mensajes de correo electrónico a las direcciones que recopila de las carpetas de correo de Outlook y Outlook Express (.dbx y .mbx), el archivo de elementos enviados de Netscape y las libretas de direcciones de Windows (.wab), que utilizan los clientes de correo como Microsoft Outlook y Microsoft Outlook Express. El mensaje de correo electrónico puede contener un máximo de dos archivos adjuntos y tanto el asunto como el cuerpo del mensaje se crearán al azar.

Detalles técnicos

Cuando un archivo infectado con el virus W32.Magistr.24876@mm se ejecuta, busca en la memoria un área iniciada con permiso de lectura y escritura que esté comprendida en el espacio de memoria de Explorer.exe. Si se halla una, se insertará una rutina de 110 bytes en el área y la función TranslateMessage se conectará para señalar esa rutina. Este código apareció por primera vez en W32.Dengue.

Cuando el código insertado consigue el control, se crea un proceso y se llama a la función TranslateMessage original. El proceso esperará tres minutos antes de activarse. A continuación, el virus obtendrá el nombre del equipo, lo convertirá en una cadena base64 y, dependiendo del primer carácter del nombre, creará un archivo en la carpeta \Windows, en la carpeta \Archivos de programa o en el directorio raíz.

Este archivo contiene determinados datos, como la ubicación de las libretas de direcciones de correo electrónico y la fecha de la infección inicial. A continuación, extraerá del registro el nombre y la dirección de correo electrónico del usuario actual (Outlook, Exchange, Internet Mail and News) o extraerá esta información del archivo Prefs.js (Netscape).

El virus incluye en el cuerpo del mensaje un historial con los últimos 10 usuarios infectados, cuyos nombres pueden verse en los archivos infectados una vez que el virus se descifra. Acto seguido, el virus buscará el archivo Sent en la carpeta de Netscape, así como los archivos con extensiones .wab, .mbx y .dbx que se encuentren en las carpetas \Windows y \Archivos de programa.

En caso de que la conexión a Internet esté activa, el virus buscará también hasta un máximo de cinco archivos con extensiones .doc y .txt y elegirá un número aleatorio de palabras de uno de esos archivos. Con estas palabras construirá el asunto y el cuerpo del mensaje de correo electrónico.

Asimismo, el virus buscará un total de 20 archivos .exe y .scr menores de 128 KB, infectará uno de estos archivos, lo adjuntará al mensaje nuevo y lo enviará a un máximo de 100 personas de las que figuran en las libretas de direcciones.

Además de todo esto, existe un 20% de posibilidades de que el archivo que adjunte sea el mismo del que tomó el asunto y el cuerpo del mensaje y un 80% de que agregue el número 1 al segundo carácter de la dirección del remitente. Con este último cambio evitará que las respuestas le sean devueltas y que, posiblemente, se le avise de la infección.

Una vez que se ha enviado el mensaje, el virus buscará un total de 20 archivos con extensiones .exe y .scr e infectará uno de estos archivos. Es posible que el directorio de Windows se llame de una de las siguientes formas:

- Winnt.
- Win95.
- Win98.
- Windows.

En ese caso, existe una probabilidad del 25% de que el virus desplace el archivo infectado a la carpeta \Windows y altere el nombre del archivo ligeramente. Cuando se cambie el archivo de ubicación, se agregará una línea run= al archivo Win.ini para que el virus se ejecute cada vez que se inicie el sistema.

En 75% de los casos restantes, el virus creará una subclave de registro en la siguiente ubicación:

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run

El nombre de esta subclave estará compuesto por el nombre del archivo sin un sufijo y el valor será el nombre completo del archivo infectado. Entonces, el virus buscará todas las unidades de los discos duros locales y todas las carpetas compartidas en red hasta infectar a un máximo de 20 archivos .exe y .scr y agregará la línea run= si la carpeta \Windows se encuentra en esa ubicación.

4.1.2.2 W32.Magistr.39921@mm.

También conocido como: I-Worm.Magistr.b, W32.Magistr.B@mm, W32/Magistr.b@MM, Magistr.32768@mm, PE_Magistr.B, W95/Magistr.28672@mm.
Tipo: Virus, Worm.
Longitud de la infección: 39,921 bytes.

Detalles técnicos

A continuación, figura una lista de las funciones adicionales y diferencias de comportamiento entre W32.Magistr.39921@mm y W32.Magistr.24876@mm:

- Reconoce las libretas de direcciones de Eudora (enumeradas en Eudora.ini.).
- Elimina los archivos *.ntz mientras realiza una búsqueda de archivos.
- Intenta desactivar la interfaz de usuario de ZoneAlarm (aunque no desactiva el firewall de ZoneAlarm).
- Agrega una entrada en la línea Shell=explorer.exe en la sección de arranque del archivo System.ini que realiza una llamada al caballo de Troya W32.Magistr.Trojan. En algunos casos, puede agregar una o varias entradas de registro.
- Busca las carpetas de Windows (Winnt, Windows, Win95, Win98, Winme, Win2000, Win2k y Winxp).
- Envía un archivo adjunto por correo electrónico con una extensión aleatoria (.exe, .bat, .pif, o .com).

- Ocasionalmente, adjunta archivos GIF a los mensajes de correo electrónico.

- La carga útil sobrescribe los archivos Ntldr (Windows NT/2000/XP) y Win.com (todos los sistemas operativos Windows de 32 bits) en todas las unidades con código que ocasiona que se almacenen datos basura en el primer sector del primer disco duro IDE.

4.1.2.3 W32.Opaserv.Worm.

También conocido como: W95/Scrup.worm [McAfee]
Tipo: Worm
Longitud de la infección: 28,672 bytes
Sistemas afectados: Windows 95, Windows 98, Windows NT, Windows 2000, Windows XP, Windows Me
Sistemas no afectados: Windows 3.x, Microsoft IIS, Macintosh, Unix, Linux

El W32.Opaserv.Worm es un worm del grupo network-aware (que detecta la red) que intenta replicarse sobre archivos abiertos compartidos por varios usuarios en red. Se copia a sí mismo en el archivo "scrsvr.exe" en la máquina remota.

Este worm también intenta hacer downloads de actualizaciones a partir de la dirección www.opasoft.com, aunque el site ya haya sido cerrado. Entre los indicadores de infección podemos citar:

- La existencia de scrsin.dat y de scrsout.dat en el directorio raíz C: que indica infección local (el worm ha sido ejecutado en la máquina local)
- La existencia de tmp.ini en el directorio raíz C: que indica infección remota (infectado por un servidor remoto)
- La llave de registro: HKEY_LOCAL_MACHINE \Software \Microsoft \Windows \Current Versión \Run que contiene un valor string llamado ScrSvr o ScrSvrOld configurado en C:\tmp.ini.

4.1.2.4 W32.Brid.A@mm

También conocido como: PE_BRID.A [Trend], W32/Braid@mm [McAfee], W32/Braid-A [Sophos], Win32.Braid.A [CA], I-Worm.Bridex [AVP]
Tipo: Worm
Longitud de la infección: 114.687 Bytes
Sistemas afectados: Windows 95, Windows 98, Windows NT, Windows 2000, Windows XP, Windows Me
Sistemas no afectados: Windows 3.x, Macintosh, Unix, Linux

W32.Brid.A@mm es un gusano de envío masivo por correo electrónico que incluye una variante ligeramente modificada de W32.FunLove.4099. Cuando se ejecuta éste, intenta insertar varios archivos en el sistema y enviarse masivamente por correo electrónico. El gusano tiene su propio motor SMTP e intenta obtener la dirección del servidor de correo y ponerse en contacto directo con él. El mensaje de correo electrónico presenta las siguientes características:

- Asunto: [Nombre de la compañía registrado en Windows]
- Archivo adjunto: Léame.exe

Detalles técnicos.

Cuando este gusano se ejecuta, primero intenta conectarse a www.hotmail.com. Si no puede hacerlo, deja pasar un tiempo corto antes de continuar sus acciones maliciosas.

A continuación, el gusano inserta varios archivos en el sistema, modifica el Registro de Windows, ejecuta la variante ligeramente modificada de W32.Funlove.4099, y se envía a sí mismo por correo electrónico a todos los contactos en la libreta de direcciones de Microsoft Outlook.

Inserción de archivos.

El gusano agrega varios archivos en el sistema.
Copia los siguientes archivos en el escritorio de Windows:

- Help.eml
- Explorer.exe

Help.eml es un archivo de Outlook Express de Microsoft. Si se abre el archivo en un sistema en el que no se haya aplicado el parche correspondiente, el adjunto (que es el gusano) se ejecuta automáticamente. Esto sucede porque usa el fallo de seguridad: Incorrect MIME Header can cause IE to Execute E-mail attachments.

Inserción de virus.

Este gusano contiene una variante ligeramente modificada de W32.Funlove.4099. El gusano intenta ejecutar este virus. La principal diferencia entre esta variante del virus y su original W32.Funlove.4099 es el nombre de archivo que utiliza. Esta variante utiliza el nombre de archivo Bride.exe en lugar de Flcss.exe.

4.1.2.5 W32.Datom.Worm.

También conocido como: W32/Datom-A [Sophos], Win32.Datom [CA], W32/Datom.worm [McAfee], Datom [F-Secure], Worm.Win32.Datom [AVP].
Tipo: Worm.
Longitud de la infección: 58,368 bytes (Msvxd.exe), 54,784 bytes (Msvxd16.dll), 81,408 bytes (Msvxd32.dll).
Sistemas afectados: Windows 95, Windows 98, Windows NT, Windows 2000, Windows XP, Windows Me.
Sistemas no afectados: Windows 3.x, Macintosh, Unix, Linux.

W32.Datom.Worm es un gusano que se propaga a través de los recursos abiertos. Este gusano no contiene una carga útil dañina.

Detalle técnico

W32.Datom.Worm existe en la forma de tres archivos:

- Msvxd.exe
- Msvxd16.dll
- Msvxd32.dll

Los archivos se ubican en la carpeta %Windir%.

Nota: La ubicación %Windir% es una variable. El gusano ubica la carpeta de instalación principal de Windows (de forma predeterminada, C:\Windows o C:\Winnt) y se copia a sí mismo en esa ubicación.

Las tareas se han repartido entre los archivos, probablemente para tratar de evitar la detección heurística:

- Msvxd.exe sólo ejecuta Msvxd16.dll.
- Msvxd16.dll añade una referencia a Msvxd.exe en el Registro y luego ejecuta Msvxd32.dll.
- Msvxd32.dll crea una lista de los recursos abiertos y copia los tres archivos en dichos recursos en la carpeta %Windir% y añade una referencia al archivo Msvxd.exe en la línea Run= del archivo Win.ini.

4.1.2.6 W32.Lirva.A@mm.

También conocido como: W32/Avril-A [Sophos], W32/Lirva.b@MM [McAfee], WORM_LIRVA.A [Trend], Win32.Lirva.A [CA], I-Worm.Avron.c [KAV], Lirva [F-Secure]
Tipo: Worm
Longitud de la infección: 32,766 bytes
Sistemas afectados: Windows 95, Windows 98, Windows NT, Windows 2000, Windows XP, Windows Me
Sistemas no afectados: Macintosh, OS/2, UNIX, Linux

W32.Lirva.A es un gusano de envío masivo por correo electrónico que también se propaga por IRC, ICQ, KaZaA y usos compartidos de redes abiertas. El gusano intenta cerrar los productos antivirus y de firewall. También envía por correo electrónico las contraseñas de acceso telefónico a redes del caché de Windows 95/98/Me al autor del virus.

Cuando Microsoft Outlook recibe el gusano, el gusano utiliza un fallo de seguridad que permite que se ejecute el anexo del mensaje cuando usted lee o visualiza el mensaje de correo electrónico.

Si el día del mes es el 7, el 11 o el 24, el gusano conectará su navegador de Web a www.avril-lavigne.com y mostrará una animación gráfica en el escritorio de Windows.

4.1.2.7 W32.Lirva.C@mm

W32.Lirva.C@mm es un gusano de envío masivo por correo electrónico que también se propaga por IRC, ICQ, KaZaA y recursos compartidos abiertos. Es una variante de W32.Lirva.A@mm. El gusano intenta cerrar los productos antivirus y de firewall. También envía por correo electrónico las contraseñas de acceso telefónico a redes del caché de Windows 95/98/Me al autor del virus.

El gusano se conecta a un sitio Web en web.host.kz/ y descarga y ejecuta BackOrifice. W32.Lirva.C@mm también intenta descargar otro archivo, que actualmente no está presente en el sitio Web.

Cuando Microsoft Outlook recibe el gusano, el gusano utiliza un fallo de seguridad que permite que se ejecute el anexo del mensaje cuando usted lee o visualiza el mensaje de correo electrónico.

Si el día del mes es el 7, el 11 o el 24, el gusano conectará su navegador de Web a www.avril-lavigne.com y mostrará una animación gráfica en el escritorio de Windows.

4.1.2.8 W32.Sobig.A@mm

También conocido como: W32/Sobig [McAfee], WORM_SOBIG.A [Trend], W32/Sobig-A [Sophos].
Tipo: Worm
Longitud de la infección: 65,536 bytes
Sistemas afectados: Windows 95, Windows 98, Windows NT, Windows 2000, Windows XP, Windows Me
Sistemas no afectados: Macintosh, OS/2, UNIX, Linux

El gusano W32.Sobig.A@mm se envía a sí mismo a todas las direcciones que encuentre en los archivos .txt, .eml, .html, .htm, .dbx y .wab. El mensaje de correo electrónico presenta las siguientes características:

De: big@boss.com

Asunto: el asunto es uno de los siguientes:

- Re: Movies
- Re: Sample
- Re: Document
- Re: Here is that sample

Archivo adjunto: el archivo que adjunta es uno de los siguientes:

- Movie_0074.mpeg.pif
- Document003.pif
- Untitled1.pif
- Sample.pif

Antes de enviar los mensajes, W32.Sobig.A@mm envía un mensaje a una dirección en pagers.icq.com.

El gusano también intenta copiarse a sí mismo en las siguientes carpetas en todos los recursos compartidos de red abiertos:

- Windows\All Users\Menú Inicio\Programas\Inicio
- Documents and Settings\All Users\Menú Inicio\Programas\Inicio

Detalles técnicos

Cuando W32.Sobig.A@mm se ejecuta hace lo siguiente:

1. Se copia a sí mismo como %Windir%\Winmgm32.exe.

Nota: La ubicación %Windir% es una variable. El gusano ubica la carpeta de instalación de Windows (de forma predeterminada, C:\Windows o C:\Winnt) y se copia a sí mismo en esa ubicación.

2. Crea un proceso %Windir%\Winmgm32.exe con el parámetro de "inicio". El proceso Winmgm32.exe hace lo siguiente:

a) Crea una exclusión mutua con el nombre Worm.X.

b) Crea un proceso para enviar un mensaje a una dirección en pagers.icq.com.

c) Crea un proceso para descargar el contenido de un sitio Web específico en el archivo %Windir%\dwn.dat. Luego el gusano ejecuta el contenido que descargó.

d) Crea un proceso para buscar en la red todos los recursos compartidos abiertos y se copia a sí mismo en las siguientes carpetas en dichos recursos:

   - Windows\All Users\Menú Inicio\Programas\Inicio.
   - Documents and Settings\All Users\Menú Inicio\Programas\Inicio.

e) Crea un proceso para enviar mensajes de correo a todas las direcciones que encuentre en los archivos con las siguientes extensiones:

   - .txt
   - .eml
   - .html
   - .htm
   - .dbx
   - .wab

f) Después se configura a sí mismo para iniciarse cuando se inicie Windows agregando el siguiente valor: WindowsMGM %Windir%\Winmgm32.exe. Lo hace en la siguiente clave de registro:
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run

Detalles de la rutina de correo electrónico.

Los mensajes que se envían durante la rutina de correo tienen las siguientes características:

De: big@boss.com
Asunto: el asunto es uno de los siguientes:

- Re: Movies
- Re: Sample
- Re: Document
- Re: Here is that sample

Archivo adjunto: el archivo que adjunta es uno de los siguientes:

- Movie_0074.mpeg.pif
- Document003.pif
- Untitled1.pif
- Sample.pif

El gusano almacena las direcciones a las que envía un mensaje de correo electrónico en el archivo %Windir%\Sntmls.dat.

4.1.2.9 W32.SQLExp.Worm

También conocido como: SQL Slammer Worm [ISS], DDOS.SQLP1434.A [Trend], W32/SQLSlammer [McAfee], Slammer [F-Secure], Sapphire [eEye], W32/SQLSlam-A [Sophos]
Tipo: Worm
Longitud de la infección: 376 bytes
Sistemas afectados: Windows 95, Windows 98, Windows NT, Windows 2000, Windows XP, Windows Me
Sistemas no afectados: Windows 3.x, Microsoft IIS, Macintosh, OS/2, UNIX, Linux

W32.SQLExp.Worm es un gusano dirigido contra los sistemas que ejecutan Microsoft SQL Server 2000 y Microsoft Desktop Engine (MSDE) 2000. El gusano envía 376 bytes al puerto UDP 1434, el puerto de servicio de resolución de SQL Server.

El gusano tiene una carga útil indirecta que genera un ataque de negación de servicio (DoS), debido a la gran cantidad de paquetes que envía.

Detalles técnicos.

Cuando W32.SQLExp.Worm compromete un equipo, hace lo siguiente:

- Se envía repetidamente a sí mismo a todas las direcciones IP, generadas en el puerto UDP 1434, desde un puerto de origen efímero.

- Toma la ventaja de vulnerabilidad que permite sobrescribir una porción de memoria del sistema. Cuando el gusano hace esto, corre en el mismo contexto de seguridad como el servicio de SQL Server.

- Utiliza la función GetTickCount de la API de Windows, para generar una dirección IP aleatoria a la que enviar el paquete malicioso.

- De forma continua, W32.SQLExp envía paquetes a distintas direcciones IP, efectuando de hecho un ataque de negación de servicio en el host en el que se ejecuta, así como en los hosts con los que intenta conectarse.

4.1.2.10 CodeRed.F

También conocido como: CodeRed.v3, CodeRed.C, CodeRed III, W32.Bady.C, W32/CodeRed.f.worm [McAfee], Win32.CodeRed.F [CA]
Tipo: Trojan Horse , Worm
Sistemas afectados: Microsoft IIS

Esta variante difiere en sólo dos bytes del CodeRed II original. CodeRed II reiniciaba el sistema si el año era posterior a 2001. Esto ya no sucede en esta variante.

El gusano analiza las direcciones IP en busca de servidores Web Microsoft IIS 4.0 y 5.0 vulnerables y utiliza la vulnerabilidad de desbordamiento de búfer para infectar máquinas remotas.

El gusano se inyecta a sí mismo directamente en la memoria, en lugar de copiarse a sí mismo como un archivo en el sistema. Además, CodeRed.F crea un archivo detectado como Trojan.VirtualRoot. Mediante Trojan.VirtualRoot el hacker obtiene acceso remoto completo al servidor Web.

4.1.2.11 W32.Nimda.A@mm

También conocido como: W32/Nimda@mm, PE_NIMDA.A, I-Worm.Nimda, W32/Nimda-A, Win32.Nimda.A
Tipo: Virus, Worm
Longitud de la infección: 57,344 bytes
Sistemas afectados: Windows 95, Windows 98, Windows NT, Windows 2000, Windows XP, Windows Me, Microsoft IIS
Sistemas no afectados: Macintosh

W32.Nimda.A@mm es un gusano que utiliza diversos métodos para propagarse mediante el envío masivo por correo electrónico. El nombre del virus procede de la palabra admin escrita al revés.

El gusano se reenvía por correo electrónico, busca los recursos de red compartidos que se encuentren abiertos e intenta copiarse en los servidores Web de Microsoft Internet Information Server (IIS) que sean vulnerables o a los que no se les haya aplicado un parche, mientras el virus infecta tanto archivos locales como archivos remotos que se encuentran en recursos de red compartidos. El gusano utiliza el fallo de seguridad Unicode Web Traversal.

Una vez que el gusano llega por correo electrónico, un fallo de seguridad MIME permite que el virus se ejecute mediante la lectura o la vista previa del archivo.

Si visita un servidor Web que haya sido atacado, se le pedirá que descargue un archivo de correo electrónico .eml (el formato que utiliza Outlook Express), que contiene el gusano como archivo adjunto. Puede deshabilitar la opción Descarga de archivos en la zona de seguridad de Internet de Internet Explorer para impedir este ataque.

Además, el gusano crea recursos de red compartidos abiertos en el equipo infectado, lo que permite el acceso al sistema. Durante este proceso, el gusano crea una cuenta de invitado con privilegios de Administrador.

4.1.2.12 W32.Klez.H@mm

También conocido como: W32/Klez.h@MM [McAfee], WORM_KLEZ.H [Trend], I-Worm.Klez.h [AVP], Klez.H, W32/Klez-H [Sophos], Win32.Klez.H [CA], WORM_KLEZ.I [Trend]
Tipo: Worm
Sistemas afectados: Windows 95, Windows 98, Windows NT, Windows 2000, Windows XP, Windows Me
Sistemas no afectados: Macintosh, OS/2, Unix, Linux

W32.Klez.H@mm es una variante del gusano W32.Klez.E@mm capaz de propagarse por medio del correo electrónico y los recursos compartidos en red. También tiene la capacidad de infectar archivos.

4.1.2.13 W32.Bugbear@mm

También conocido como: W32/Bugbear-A [Sophos], WORM_BUGBEAR.A [Trend], Win32.Bugbear [CA], W32/Bugbear@MM [McAfee], I-Worm.Tanatos [AVP], W32/Bugbear [Panda], Tanatos [F-Secure]
Tipo: Worm
Longitud de la infección: 50,688 bytes
Sistemas afectados: Windows 95, Windows 98, Windows NT, Windows 2000, Windows XP, Windows Me
Sistemas no afectados: Macintosh, Unix, Linux

W32.Bugbear@mm es un virus enviado en masa por correo electrónico. También puede esparcirse a través de redes compartidas. Tiene capacidad de capturar las pulsaciones del teclado y de invadir sistemas a través de una puerta trasera . El virus también intentará desligar los procesos de varios antivirus y programas de firewall.

Debido al maltratamiento de recursos de redes, el worm puede inundar recursos compartidos de impresión, causando mal funcionamiento e impresiones irregulares.

Está grabado en el lenguaje de programación C++ 6 de Microsoft Visual y compactado en UPX v0.76.1-1.22.

CAPÍTULO V

FUNCIONAMIENTO LÓGICO DE LOS ANTIVIRUS

PREÁMBULO.

INTRODUCCIÓN.

Este capitulo tiene como función dar a conocer el funcionamiento lógico de los antivirus en una forma esquemática para facilitar la comprensión del lector.

Al mismo tiempo mostrar las diferencias que existen entre los diferentes antivirus del mercado.

OBJETIVOS.

- Demostrar el funcionamiento lógico de los virus y antivirus.
- Mostrar las diferencias que existen entre los antivirus.

5.1 FUNCIONAMIENTO DE LOS ANTIVIRUS

Un antivirus es un programa específicamente diseñado para detectar y eliminar virus, porque los conoce, sabe cómo actúan y cómo eliminarlos. Esto lo hace mediante una lista de virus que contiene su nombre, métodos y forma de desactivarlo.

PRELUDIO.

En este informe vamos a concentrarnos en las dificultades puramente tecnológicas del desarrollo y mantenimiento de un antivirus de primera línea, dejando de lado aspectos imprescindibles para que un antivirus pueda cumplir su misión pero que no están relacionados directamente con las tareas de programación, por ejemplo: obtener los virus aparecidos en cualquier lugar del globo, disponer de personal en línea cualificado para resolver cualquier problema relacionado con virus, buena documentación, traducciones, distribución de actualizaciones, etc.

En los siguientes apartados iremos describiendo las diversas tecnologías que se emplean en la lucha contra los virus así como las causas que han provocado el desarrollo de las mismas.

ESTUDIO DE LOS VIRUS RECIBIDOS.

El hecho de haber conseguido un virus, en muchos casos difícil de por sí, no significa que se detecte por arte de magia, hace falta disponer de un equipo de programadores, expertos en lenguaje máquina, que generen múltiples copias del virus, desensamblen el código del virus para conocer su funcionamiento y obtengan toda la información necesaria para su detección y desinfección. El ritmo de aparición de nuevos virus asegura trabajo continuo para este equipo de auténticos expertos en la estructura y comportamiento de más de 20000 virus informáticos.

ANÁLISIS RÁPIDO.

Como ya hemos comentado, actualmente se calcula que existen en el mundo alrededor de 20000 virus informáticos. Con este panorama uno de los primeros problemas con los que se encuentra un desarrollador de antivirus es conseguir buscar 20000 virus en cada fichero en un tiempo mínimo. Lógicamente no se puede leer los archivos a analizar de una forma minuciosa, porque el análisis de un disco duro o un servidor de archivos sería eterno. Esto exige un conocimiento exhaustivo de todos los formatos de archivo potencialmente infectables y de todas las formas de infección que los desarrolladores de virus hayan podido diseñar. Con este conocimiento los antivirus pueden buscar allá donde hay que buscar ahorrando un tiempo precioso. No obstante esto no es suficiente para conseguir una velocidad competitiva y se hace necesario además el desarrollo de un sistema de búsqueda de cadenas mediante árboles de sufijos y prefijos. Otra técnica que permite acelerar el análisis, es una clasificación de los virus por tipos y familias que permita descartar la búsqueda de determinados virus en determinados archivos o partes de archivos. Esta última técnica obliga al equipo que estudia los virus recibidos a realizar y mantener esta clasificación.

DESINFECCIÓN FIABLE.

Cuando un usuario desinfecta un archivo, espera que éste siga funcionando con normalidad. Un antivirus, no solo tiene que detectar los virus, además debe desinfectarlos y con fiabilidad.

De nuevo el desarrollador de antivirus debe andar con pies de plomo para no confundir variantes del mismo virus a la hora de desinfectar. Por ejemplo, existen más de 10 variantes del conocido Barrotes que tienen un tamaño diferente. Cada una de estas variantes debe ser desinfectada con un procedimiento diferente.

ANÁLISIS DE ARCHIVOS COMPRIMIDOS.

Otra dificultad añadida a los procedimientos de análisis es la capacidad de buscar archivos infectados dentro de los archivos comprimidos. Lógicamente esta operación de descompresión es realizada automáticamente en memoria por el antivirus, que debe conocer cómo se descomprimen los formatos de archivos comprimidos más utilizados (ZIP, ARJ, LHA, MSCOMPRESS, etc). La operación se realiza en memoria porque es impensable descomprimir el archivo en disco ya que la velocidad de análisis caería en picado y porque no se puede asegurar la existencia de espacio suficiente en disco para realizar la descompresión.

ANÁLISIS EN MODO AISLADO.

En los sistemas operativos como el DOS, los virus tienen la posibilidad de engañar a los antivirus cuando éstos leen un archivo infectado. El engaño es tan sutil que el antivirus no detectará nada en el archivo infectado porque el virus le ha dado gato por liebre. Los antivirus han desarrollado una técnica (originalmente usada por un virus, todo hay que decirlo) que permite la localización exacta de las rutinas de servicio del sistema operativo. Al disponer de esta localización los antivirus pueden ponerse en contacto con el sistema operativo directamente desactivando virtualmente cualquier programa residente y por tanto virus que pudiera estar activo en la memoria. De esta forma el virus nunca podrá engañar al antivirus.

GDE (Generic Decryption Engine).

Los buenos tiempos en los que para detectar un virus bastaba con buscar una cadena de bytes en un lugar determinado se han acabado. Cuando hicieron su aparición los virus encriptados todavía quedaba una parte fija del virus que podía usarse como patrón de búsqueda, esta era la propia rutina de encriptación/desencriptación. Hoy en día la gran mayoría de los virus que aparecen son virus polimórficos.

Esto significa que cada vez que el virus se replica, la nueva copia es completamente diferente de la anterior. Tan diferente que no se puede encontrar ni un byte coincidente (en valor y posición se entiende). La rutina del virus que se encarga de encriptarlo y desencriptarlo también cambia completamente de generación en generación, por lo que en teoría los antivirus no tienen por donde detener la infección del virus.

Esta situación ha obligado a los antivirus a desarrollar un método que permita desencriptar cualquier virus sin conocer su rutina de encriptación, para poder buscar, ahora sí, una cadena identificadora dentro del núcleo desencriptado del virus. Esto se dice fácil, pero supone el desarrollo de un emulador de instrucciones en lenguaje máquina que hace que el antivirus trabaje sin ejecutar realmente el código de desencriptación del virus. Esto es lo que en los antivirus Panda llaman Motor Genérico de Desencriptación (Generic Decryption Engine) o GDE.

ANÁLISIS HEURÍSTICO.

La rápida aparición de virus hace que algunos usuarios no dispongan de la última revisión del antivirus cuando llega a sus manos un archivo infectado con un nuevo virus. En estos casos el antivirus suministra un método para la detección de virus nuevos llamado método heurístico.

Esa forma de análisis no busca virus conocidos sino que busca secuencias de instrucciones comúnmente utilizadas por los virus y otras situaciones sospechosas generadas normalmente por la presencia de un virus.

MÉTODO DE INVESTIGACIÓN

Otro método que emplea los antivirus para detectar y capturar virus nuevos es la generación de archivos ejecutables de las más diversas formas y tamaños para su uso como carnada.

El antivirus ejecuta, abre, y opera con estos archivos generados por él para descubrir a un posible virus en memoria que se lance a infectar éstos archivos carnada.

VDL (Virus Description Language)

La gran cantidad de virus que aparecen día a día hacen que sea inviable el mantenimiento de un antivirus como un programa puramente ejecutable. Tradicionalmente las rutinas de limpieza y algunas rutinas para detectar virus estaban codificadas dentro del ejecutable principal de la aplicación antivirus. Este esquema exige la compilación del antivirus de cada una de las plataformas disponibles cada vez que se quería incluir la rutina de desinfección de un nuevo virus. Una de las consecuencias de esto es que las actualizaciones del antivirus debían de incluir la totalidad del antivirus.

Para solventar este problema se ha desarrollado un lenguaje especial interpretado, una especie de "Virus Basic", que permite codificar las rutinas de detección y desinfección de una forma independiente de plataforma, sin necesidad de compilar ninguna aplicación y con un tamaño de actualización mínimo.

INTEGRACIÓN CON LOS SISTEMAS OPERATIVOS

Aparte de las técnicas puramente relacionadas con la lucha antivirus, este tipo de productos necesitan estar perfectamente integrados con los sistemas operativos para proteger de forma efectiva a los usuarios.

Por ejemplo, todos los buenos antivirus suministran un programa antivirus residente. Esto significa que el antivirus está cargado en la memoria permanentemente y recibe notificaciones del sistema operativo cuando se producen operaciones como la ejecución o apertura de un archivo. De esta manera, el antivirus residente tiene la oportunidad de analizar el archivo en busca de virus y cancelar la operación en caso de que el archivo esté efectivamente infectado.

Dependiendo del sistema operativo hay que desarrollar un antivirus residente específico para este sistema operativo. A continuación presentamos una tabla de equivalencia entre algunos sistemas operativos y el tipo de programa residente que hay que desarrollar:

- DOS / Windows 3.x Residente tradicional (como el SMARTDRV)
- Windows 95 Driver virtual (VxD)
- Windows NT Driver en modo Kernel
- Netware Módulo cargable de Netware (NLM)

No existe duda que estas son las aplicaciones más complejas de desarrollar con la que un programador se puede encontrar. Un ejemplo, según Novell, Panda Software es la única empresa en España que desarrolla NLMs.

INTEGRACIÓN CON NUEVAS APLICACIONES

No sólo un antivirus debe seguir la pista a los virus que van saliendo. El antivirus debe estar atento a la aparición de nuevas aplicaciones o características de aplicaciones existentes que pudieran ser usadas por los desarrolladores de virus para crear nuevos tipos de virus.

La aparición del WORD BASIC y seguido de los virus de WORD, obligó a los antivirus a estudiar a fondo el formato de los documentos de WORD para poder localizar las macros infecciosas. Otras aplicaciones que deben ser monitorizadas son: Lotus Notes, cc:Mail, Microsoft Exchange.

SERVICIOS DE EMERGENCIA.

Como ya hemos comentado un antivirus no es técnica pura únicamente sino que debe de suministrar un servicio posventa adecuado que sea capaz, como por ejemplo lo es el de Panda Software, de resolver una incidencia con virus en menos de 48 horas.

A continuación se muestra en forma de diagrama los dos métodos más comunes (bajo demanda y heurística) que utilizan los antivirus para la detección de virus.

Método bajo demanda

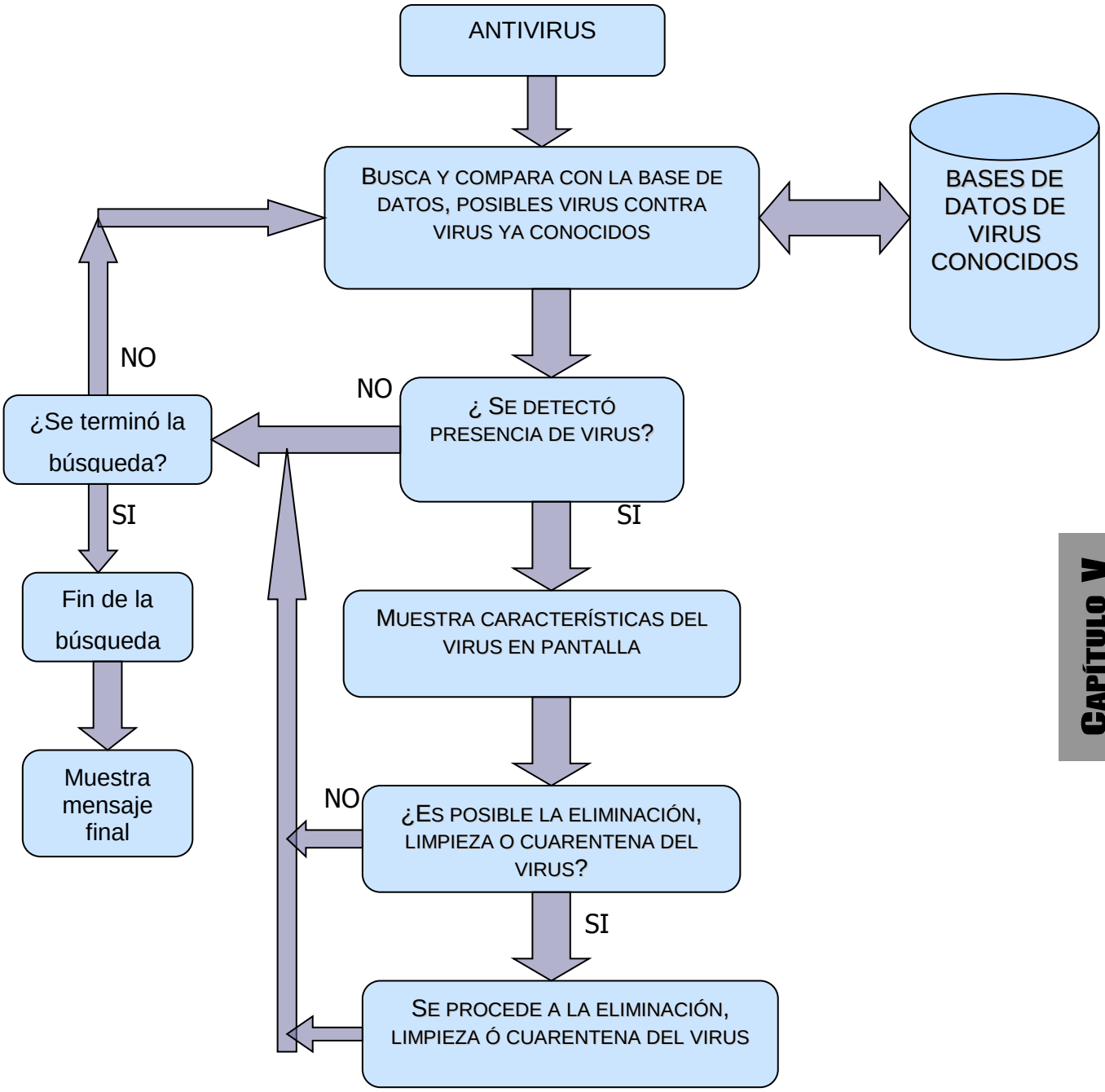


Figura 5.1

Método Heurístico

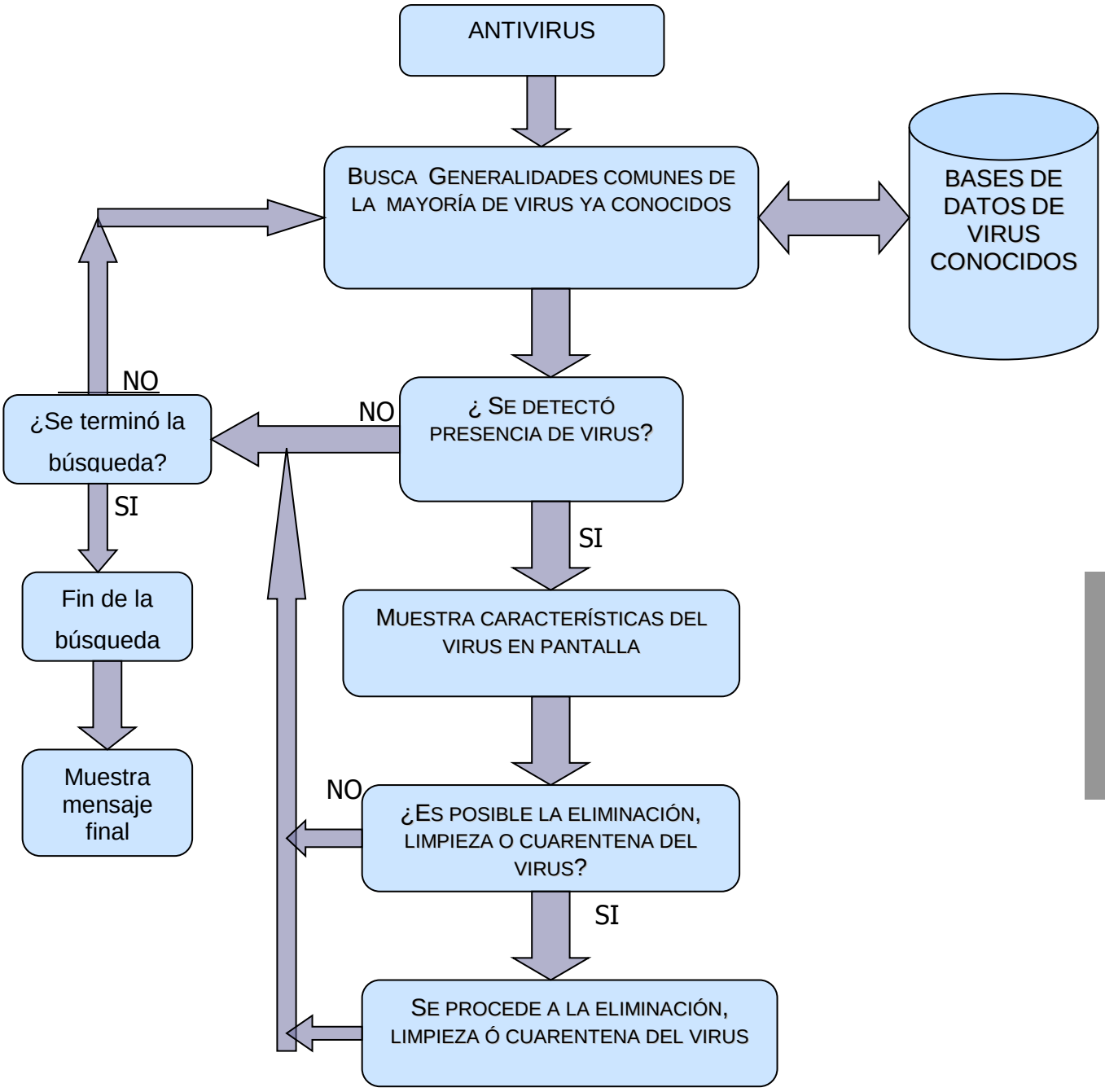


Figura 5.2

5.1.1 TIPOS DE ANTIVIRUS

Clasificación A, por acción:

- Solo detección.
- Detección y desinfección.
- Detección y aborto de la acción.
- Detección y eliminación del archivo / objeto.

Clasificación B, por método de detección:

- Comparación directa.
- Comparación por signatura.
- Comparación de signatura de archivo (detección por comparación con atributos guardados).
- Por métodos heurísticos.

Clasificación C, por instante de activación:

- Invocado por el/la usuario/a.
- Invocado por actividad del sistema (abrir, ejecutar, copiar, guardar archivo).

Clasificación D, por Objeto infectado:

- Sector de Arranque.
- Archivo Ejecutable.
- MacroVirus (Excel, Word).
- Java.

5.1.2 CARACTERÍSTICAS DE LOS ANTIVIRUS.

- La mayoría de antivirus son necesarios en sistemas y aplicaciones de la empresa Microsoft.

- La efectividad de un antivirus reside, en gran medida, en su capacidad de actualización, preferentemente diaria. Eso significa que cuanto más posibilidades de actualización nos brinde nuestro software mejor podrá eliminar los nuevos virus que circulan por la red.

- El soporte técnico proporciona una gran ayuda ante cualquier problema o duda que pueda surgir relacionado con un virus o con su funcionamiento. Estar protegido contra los virus requiere un monitoreo permanente, tanto de archivos como de correo electrónico, navegador web, etc , por lo que el sistema antivirus debe estar activo en memoria como una tarea más de las que habitualmente realiza la PC.

- A pesar de una actualización constante no se puede garantizar una protección completa, ya que una vacuna puede ser desarrollada solo después de descubrir la enfermedad.

5.2 Diferencias entre los Distintos Antivirus más Conocidos.

En estos días de proliferación masiva de ataques de nuevos virus (algunos no tan nuevos, pero si ampliamente difundidos, aprovechándose de múltiples circunstancias, muchos usuarios de computadoras, se habrán preguntado si ellos tienen la protección adecuada en sus equipos, o dicho de otro modo, si los antivirus que acostumbran usar, los protegen adecuadamente.

Muchas veces se ha dicho, que ningún antivirus tiene toda la capacidad de detectar y proteger contra todas las variantes conocidas y por conocer de virus. Pero también insistimos en lo vital que es mantener al día sus bases de datos.

La idea de este tema es mostrar comparativamente la habilidad de cada programa antivirus para descubrir y quitar este código malicioso que no solo involucra a los virus, sino a todo tipo de malware (software con capacidades destructivas) de nuestro PC. El usuario podrá evaluar luego si estas características son las mejores para su uso personal, ya que a este mercado está enfocada la tabla comparativa.
Para determinar cuál es el programa antivirus más completo y por ende seguro, se requieren muchos datos de pruebas en las que se puedan confiar, y realizadas a través de un periodo determinado de tiempo.

Para la confección de este reporte se han tomado las siguientes referencias:

Primero, los resultados obtenidos por expertos, ninguno de ellos relacionado directamente con ninguna empresa de antivirus, y que además ofrecen certificaciones mundiales en el tema, como ICSA.net, Virus Bulletin, West Coast Labs, HackFix, y Virus Test Center de la Universidad de Hamburgo, Alemania.

Segundo, la excelente comparativa de virus realizada por Hispasec (http://www.hispasec.com/comparativa2000.asp).

Y finalmente, la experiencia de video Soft BBS, a través de instalaciones realizadas a clientes individuales de los diferentes productos.

Se ha tomado como referencia el artículo publicado en About.com, pero hemos preferido enfocarlo hacia el usuario final, y no al corporativo, ya que ese siempre fue nuestro punto de vista. O como decimos comúnmente, esto pretende estar dirigido al ciudadano "común", y no al experto o a las empresas.

En concreto, lo que se ha hecho es extrapolar las distintas comparativas y pruebas realizados por los citados expertos, para crear una tabla de puntajes, y utilizar también la propia experiencia para definir ciertas condiciones no tocadas en las pruebas originales. Por ejemplo, una característica que ninguna de las pruebas mencionadas ha incluido es que tan compatible es determinado producto con el sistema operativo. Dicho en otras palabras, un producto capaz de descubrir cuanto virus anda en la vuelta, necesariamente debería ser considerado con cierta reticencia a la hora final antes de elegirlo, si ese producto causa una lentitud u otros efectos no deseados en el resto del software.

5.2.1 ¿POR QUÉ UN ANTIVIRUS ES MEJOR QUE OTRO?

La expresión "cuál es el mejor antivirus", puede variar de un usuario a otro. Es evidente que para un usuario inexperto el término define casi con seguridad al software que más fácil de instalar y usar se le presenta. Algo totalmente intranscendente para usuarios expertos, administradores de redes, etc.

Sin embargo, los usuarios sin experiencia también son muy propensos a dejarse convencer por lo que las publicaciones especializadas les indican. El tema aquí es que muchas veces este tipo de evaluación no es tan cristalino.

No estamos diciendo que necesariamente algunos medios puedan verse influenciados en sus "Selecciones del editor" por el hecho de que ciertos antivirus son sus clientes y contratan publicidad en ellos, pero es un tema delicado que de por si le quita transparencia a estas pruebas, por decirlo de algún modo.

También existe el hecho de que algunos de los reporteros que escriben dichos artículos, no son precisamente expertos en el tema, y por lo tanto sus apreciaciones pueden estar enviciadas por aquello de las apariencias puramente estéticas del producto evaluado, sin entrar en las verdaderas condiciones de un antivirus.

En definitiva, el mejor antivirus debería ser aquel capaz de descubrir y eliminar al 100% de los virus activos ("In-The-Wild"). Esto es lo ideal, pero depende también del usuario, ya que para ello mantener el antivirus actualizado es fundamental. Otro punto a tener en cuenta, es la habilidad de un antivirus para proteger nuestro PC de otras amenazas como los caballos de Troya, componentes Web maliciosos, scripts, etc.

La posibilidad de limpiar o desinfectar también es muy importante, pero desde el punto de vista de la seguridad la capacidad de detener estas amenazas debe estar en primer término, y luego la de "limpiar" los archivos infectados, teniendo en cuenta que la detección deberá hacerse antes que infecte otros elementos de nuestro PC, y que cuando hablamos de archivos infectados, nos referimos a aquellos que ya recibimos en esas condiciones, y son los que luego podrían propagar la infección en nuestra computadora si no son descubiertos y bloqueados por el antivirus.

La habilidad de poder actualizarse lo más automáticamente posible, es algo que depende mucho del nivel del usuario. Para alguien inexperto, tal vez sea algo fundamental, pero nuestra opinión personal es que debemos crear "conciencia de mantener actualizado el antivirus".

Es como si nos entregaran una libreta de conducir para nuestro PC. Deberíamos saber algo más que "arrancar y andar". Y eso incluye como primordial lo de reconocer que mantener actualizado este software es vital.

Sobre la comparativa antivirus 2000 de Hispasec

Hispasec (http://www.hispasec.com), realizó en el año 2000, por segunda vez, la que se consideró la comparativa antivirus más exhaustiva, seria y honesta, realizada por cualquier otra organización o publicación en nuestro idioma.

La primera comparativa realizada el año anterior por supuesto generó algunos descontentos entre ciertos fabricantes de antivirus, pero no hizo más que mostrar con pruebas contundentes, los resultados de un riguroso análisis.

Este año, se volvieron a generar pruebas sumamente extensas y detalladas, que no dejan lugar a dudas o confusiones. Además se corrigieron otras para afinar aún más sus resultados finales.

Como en otras oportunidades, se creó un virus totalmente desconocido, que fue enviado en forma anónima a más de 30 fabricantes de antivirus, como si de un usuario común se tratara. Se evaluó la respuesta de estas empresas, la velocidad para crear un antídoto, y el servicio prestado al cliente. Algo que jamás había sido tenido en cuenta por evaluaciones de otros expertos hasta ese momento.

Compartimos con Hispasec la importancia dada a esta prueba. Y aunque reiteramos que nuestro tema está dedicado al usuario común, también en este caso la atención personalizada del fabricante del antivirus que este usa es muy importante ante la aparición de dudas o de nuevos virus, como también lo es la velocidad de respuesta.
Las demás pruebas, fueron divididas en diferentes pruebas (puede ver una descripción detallada de éstas, así como los resultados finales y por prueba en: http://www.hispasec.com/comparativa2000.asp).

Test ITW (In The Wild). Con esta prueba salió a la luz la capacidad de los 30 productos evaluados para detectar virus que aparecen en la lista de igual nombre mensualmente, donde se reflejan los virus en actividad en el mundo entero, punto fundamental como argumentábamos más arriba.

Test MACRO, donde se evaluaron virus de macros para Word, Excel, Access, PowerPoint, AmiPro, WordPro, Lotus 1-2-3 y CorelDraw.

Test TROYA. Se seleccionaron y probaron las respuestas a 150 troyanos y backdoors, desde los más conocidos como BackOrifice, NetBus, SubSeven, hasta otros de más reciente creación.

Test BIN-BOOT, es el que incluye desde los ya poco comunes virus de arranque, hasta los más sofisticados creados para Win32, pasando por los clásicos virus que afectan ejecutables bajo MS-DOS o Win16, en un total de más de 14.000.

Test Archivos de Internet. Involucra sin dudas a la generación más reciente de virus, tanto los infectores de código HTML, como a los applets de Java, controles ActiveX (OCX), gusanos de IRC, de e-mail y de diversos scripts (VBS, etc.)

También se tuvo en cuenta la capacidad de detectar virus en formatos comprimidos (y sus encadenados, o sea comprimidos dentro de otros comprimidos, etc.). Un talón de Aquiles que solo dos antivirus lograron superar casi en un 100%, menos en algunos formatos poco conocidos (AIN, ARC, HA, PAK, ZOO) que no fueron soportados por ninguno de los productos evaluados.

La evaluación de Hispasec, sumada a la de los otros expertos mencionados, debería ser suficiente. Pero nosotros considerábamos que un punto muy importante no fue tenido en cuenta. Esto es la relación del antivirus con nuestro sistema operativo.

Como se extrapolaron los resultados.

Tanto la comparativa de Hispasec, como la de los sitios mencionados al comienzo, han sido desglosados en un orden de mayor a menor, de acuerdo a los resultados obtenidos.

Cada coincidencia suma otro punto, y el total de puntos decide cuál producto está en primer lugar. Un desglose simple, pero que genera la tabla que a continuación mostramos. No es un juicio de valores en el sentido que 2 puntos significa simplemente 2 coincidencias (en otras palabras, para dos expertos al menos, el producto reúne todas las condiciones expuestas en este artículo, pero para el resto no). Lo que usted puede decidir con esto es con cuál antivirus quedarse, si desea tener en cuenta la opinión de una mayor cantidad de expertos.

Antivirus	Sistemas Operativos probados	Puntaje
Antivirus Toolkit Pro (AVP)	DOS/95/98/NT	14
Panda Antivirus (Platinum)	3.x/95/98/2000/NT	12
McAfee (VirusScan)	DOS/95/98/2000/NT	11
Norton Antivirus	DOS/3.x/95/98/2000/NT	10
InoculateIT	3.x/95/98/2000/NT	9
Command Software Antivirus	DOS/95/98/NT	7
Norman Antivirus	DOS/95/98/NT	4
PC-Cillin	95/98/NT	3
F-Secure	95/98	3
Sophos Anti-Virus	DOS/3.x/95/98/NT	3
InoculateIT Personal Edition	95/98	2

Tabla 1

Consideraciones finales.

Finalmente, debemos hacer notar que esta tabla representa condiciones dadas en un determinado momento (mayo/junio del 2000). Recuerde que la evolución de cada producto es una constante en la mayoría de los fabricantes de antivirus, y que este artículo solo pretende ser una referencia para aquellos usuarios dubitativos y sin experiencia.

También es importante resaltar que algunos productos no aparecen en la lista, simplemente porque no fueron evaluados por los expertos, o porque su uso está restringido a un mayor conocimiento del sistema operativo por parte del usuario. Un ejemplo de esto es la versión para DOS del F-Prot (producto gratuito si es para uso personal), que sigue siendo una excelente opción como segundo antivirus para revisar nuestra máquina, incluso desde un disquete.

Y finalmente, es evidente que lo más importante en este tema es mantener un antivirus actualizado.

Pero insistimos en que igual de recomendable es no confiar en un solo antivirus. Sin embargo, jamás mantenga dos antivirus monitoreando. Las consecuencias en estos casos serían imprevisibles para su sistema operativo. Lo ideal sería un antivirus para monitorear, y otro a mano para revisar archivos y carpetas antes de ejecutar algún software por primera vez. Algo así como la segunda opinión de un médico.

5.2.2 ANTIVIRUS COMERCIALES.

En el mundo de la informática existen varias empresas que se dedican a la fabricación de antivirus. Dichas empresas desde sus comienzos han tratado de crear unos sistemas estables que le brinden seguridad y tranquilidad a los usuarios. Día a día ellas tienen la encomienda de reconocer nuevos virus y crear los antídotos y vacunas para que la infección no se propague como plagas en el mundo de las telecomunicaciones.

Entre los antivirus existente en el mercado se pueden mencionar:

- Panda Antivirus
- Norton Antivirus
- McAfee VirusScan
- Dr. Solomon's Tool Kit
- Esafe
- F-Prot
- IBM Antivirus
- PcCillin
- Bitdefender
- Inoculate

5.3 ¿ Se Puede Sobrevivir Sin Antivirus?

Casi todos los expertos coinciden en que uno de los programas más necesarios hoy en día es un buen antivirus residente, pero todavía hay usuarios que no lo consideran imprescindible, e incluso hay alguno que recomienda no utilizarlo, por diversos motivos, entre los cuales están:

- Ningún antivirus ofrece garantías totales. Podemos infectarnos por un fallo o por la aparición de un virus muy nuevo que todavía no esté controlado por el antivirus que tengamos.
- Teniendo en cuenta lo anterior, tampoco puede olvidarse que el antivirus puede crear una falsa sensación de seguridad absoluta, que es inadecuada. Quien tiene antivirus suele confiarse demasiado y olvidar otras precauciones personales que debería de adoptar como gesto de responsabilidad personal.
- El antivirus vuelve lento el rendimiento del sistema.
- El antivirus también puede modificar el funcionamiento del sistema, en algunos detalles o aspectos que no nos interesan.
- El antivirus puede incorporar fallos que añadan más inestabilidad al sistema, o puede provocar conflictos con otros programas.

A continuación se describen las precauciones adicionales que debería tomar quien renuncia al antivirus, y cuales factores pueden colaborar en el éxito o en el fracaso de esta estrategia.

Para empezar, hay que tomar algunas precauciones adicionales respecto al correo electrónico recibido. Se puede comenzar a considerar sospechoso cualquier mensaje recibido que resulte inesperado o extraño. Concretamente, se puede guiar de características del tipo siguiente:

- Si se recibe un mensaje remitido por alguien desconocido, se puede comenzar a sospechar de ese mensaje, salvo que existan otras razones que puedan justificar la recepción de ese mensaje procedente de un desconocido.
- El mensaje tiene un título que no se entiende (o que no se sabe a qué viene, o que parece sorprendente por cualquier otro motivo).
- El mensaje va dirigido a alguien que no es el dueño del correo, o a una dirección que no es la del propietario. También se puede considerar un tanto sospechoso cualquier mensaje que vaya dirigido a la dirección correcta, pero que omita la especificación del nombre habitual.
- El mensaje tiene algún archivo adjunto.
- El mensaje tiene un tamaño mucho más grande de lo habitual (más de 20 Kb, por ejemplo).

Por supuesto, puede haber mensajes que aporten más de una de estas características descritas, y esos mensajes tienen mucha más probabilidad de ser infecciosos: **seguramente hay que proceder a borrarlos directamente.**

Respecto a aquellos mensajes que puedan parecer solo "un poco sospechosos", tal vez merezca la pena no borrarlos directamente. Una opción puede consistir en tratar de echar un vistazo al interior del mensaje, pero sin abrirlo normalmente para que no pueda infectarnos. Si se usa Oultook Express se puede hacer usando el menú ARCHIVO, PROPIEDADES, ficha DETALLES, botón ORIGEN DEL MENSAJE (con otros programas seguramente haya que variar el método, pero casi todos te permiten hacer algo similar, con lo que se accede al "código interno" del mensaje). Así se puede ver el texto del mensaje, su cabecera, y los posibles archivos adjuntos que contenga. Si se tiene buenos conocimientos de informática también se podrá distinguir cuáles de esos ficheros son potencialmente peligrosos, según el tipo de contenido y/o la extensión que tengan esos archivos.

Si esta verificación confirma el peligro de virus, se puede borrar el mensaje sin abrirlo; en otro caso, se sabe que se puede abrir el mensaje sin peligro. Este procedimiento es un poco tedioso, pero puede ser eficaz si se tiene pocos mensajes "dudosos". Además hay que tener buenos conocimientos técnicos para hacer un diagnóstico respecto a la peligrosidad de lo que incluya el mensaje, y eso tampoco es algo que esté al alcance de cualquiera.

Dependiendo del programa de correo que se tenga, se podrán crear mecanismos automáticos que ayuden a distinguir estos mensajes sospechosos. Por ejemplo, se puede crear una regla de clasificación que lleve todos los mensajes mayores de 20 Kb a una carpeta de "sospechosos". Pero también se puede crear mecanismos que clasifiquen inversamente; por ejemplo, crear una carpeta "personal" y hacer que ahí sean llevados todos los mensajes dirigidos al usuario, y luego añadir otra regla posterior que lleve a "sospechosos" todos los mensajes restantes; de esta forma se tendrá en "sospechosos" todos los mensajes que no van dirigidos al usuario. Luego, se tendrá que revisar con precaución todos los mensajes, pero ya se está mentalizado para ser más prudente con los mensajes que automáticamente hayan sido clasificados como "sospechosos".

Todo lo anterior tampoco es un método perfecto ni infalible. Conviene complementarlo con otras actuaciones:

- Configurar el programa de correo para que no abra los mensajes automáticamente, al seleccionarlos. Desactivar la opción de "vista previa".

- Incrementar la configuración de seguridad del programa de correo, para que no use posibilidades Java, Javascript, ActiveX y otras opciones peligrosas que puedan ser incluidas en mensajes HTML. Mejor aún si se puede desactivar las funciones HTML de los mensajes recibidos, y que esos mensajes sean manejados como si hubieran sido escritos en texto plano.

- Aún mejor si se usa un programa distinto del OExpess, y también si no se usa Windows. No es cierto que este programa y este sistema operativo estén peor hechos; lo que sucede es que este software es el utilizado por la mayoría de los usuarios, y eso hace que los creadores de virus suelan fabricar sus bichos para que ataquen precisamente a quienes utilizan ese software. Por ese motivo, si se usa otro programa de correo y/u otro sistema operativo muchos virus no podrán atacar.

- Desactivar la posible ejecución de ficheros VBS. Windows incorpora de serie esta posibilidad que no es necesitada por la mayoría de usuarios. Pero esa característica también es aprovechada por muchos virus. Si se desactiva el VBS, ocurrirá que esos virus no podrán funcionar en el sistema.

- Desactivar la ejecución automática de macros en Word y otros programas similares.

Lo peor de ese método es que requiere bastante frialdad a la hora de manejar (analizar) el correo recibido. Se tiene más posibilidades de hacerlo bien si se abre el correo a diario y solo se recibe 10 o 15 mensajes; si cada día llegan más de 100 mensajes, entonces se tiene mucho más riesgo, pero además también es probable que se terminen equivocando con algún mensaje. Si el usuario es una persona serena y poco impulsiva, también es un punto a su favor. Si se tiene pocos meses de presencia en Internet también es más fácil, porque luego se empieza a recibir más y más mensajes (de internautas que se conoció hace años y que quizá no se recuerde bien). Un último apunte en este sentido, para no abrumar con muchas más posibilidades: Si se tiene algún cargo público también es posible que se reciba mensajes "inofensivos" de gente que no se conoce y que se dirige al usuario por el cargo que ocupa; sería muy irresponsable borrar esos mensajes sin abrirlos.

Por otro lado, hasta ahora solo hemos hablado de correo electrónico, cuando la realidad es que los virus pueden entrar también por otras vías que vamos a comentar a continuación:

- **Navegación web.** El simple hecho de navegar puede llevar a páginas infecciosas. Si el navegador esta configurado para que maneje Java, Javascript o ActiveX, podría infectarse solo por el hecho de visitar una página. Para aminorar ese riesgo solo se puede hacer dos cosas:
  - Incrementar la configuración de seguridad del navegador, para que no ejecute ese tipo de tecnologías peligrosas. Esto tiene el inconveniente de que algunas páginas no funcionarán, o funcionarán mal.
  - Tratar de navegar solo por sitios web que aporten algunas garantías. Los sitios de grandes empresas y grandes organismos conllevan menos riesgo de este tipo. Evitar las páginas personales y los sitios web de usuarios particulares. Las páginas que no identifiquen a un responsable (páginas anónimas y/o que promuevan actividades dudosas como el "cracking") son especialmente peligrosas).

- **Descargas de archivos** (en páginas web o en servidores FTP). Antes de descargar un archivo, se debe reflexionar por segunda vez sobre lo dicho en el apartado anterior: ¿Hasta qué punto parece fiable el sitio que aloja este archivo que voy a descargar? Posteriormente a la descarga, se puede usar un antivirus en línea para chequear el fichero obtenido, antes de utilizarlo.

- **Programas de intercambio de archivos.** Estos programas se utilizan solo para descargar ficheros de datos (MP3, AVI, etc) que no sean ejecutables. De todas formas, tras descargar el archivo, y antes de utilizarlo, también se puede usar un antivirus en línea, como se ha indicado antes, para verificar el fichero obtenido.

- **IRC.** No utilizar el programa mIRC, que es el más popular y que -por ello- es atacado por más virus. Hay que rechazar cualquier archivo que sea transmitido por un desconocido, o sin venir a cuento: cancelar la recepción de ese fichero.

- Por motivos similares a los del punto anterior, también se debería prescindir del Messenger y/o rechazar cualquier archivo que pueda entrar por un programa de ese tipo.

- Disquetes o CDs. Antes de usar los ficheros de un disquete o un CD también se debería reflexionar sobre la fiabilidad de quien ha confeccionado ese disco. Igualmente conviene analizar esos archivos con un antivirus en línea, antes de usarlos.

Igual que antes se mencionó con el correo, también es necesario mantener la calma y la serenidad usando todos estos sistemas que conllevan peligros evidentes. Todo esto puede resultar extremadamente tedioso, y quizá solo resulte eficaz para quien no se vea sometido a estas situaciones diariamente.

Concluyendo: prescindir del antivirus es inadecuado para la mayoría de usuarios, por unas u otras razones. No es adecuado para quien recibe cientos de mensajes diarios, tampoco para quien descargue muchos archivos o utilice muchos CDs, etc, etc, Así pues, no parece "razonable" como recomendación general, y solamente podría ser una opción a considerar para quienes hagan un uso muy limitado (o muy concreto) del ordenador. Es posible sobrevivir con este método, pero las precauciones seguramente lleven a borrar algún mensaje que no entrañe peligro, a prescindir de ficheros que se podría obtener con más facilidad si se tuvieran antivirus.

No hay que olvidar que los virus cada día son más "listos" (nos engañan mejor), y que tampoco estamos a salvo -como humanos- de tener un desliz o un error con consecuencias fatales.

Hay otro detalle a considerar: ¿Se tienen copias de seguridad? ¿Hasta que punto saldrían perjudicado si tuvieran que formatear en el momento más inesperado? Algunos usuarios hacen una copia de seguridad (en CD) tras instalar el sistema operativo y los programas, y haber configurado adecuadamente todo eso. Luego van haciendo copias de seguridad regulares de los archivos de datos que usan, incluyendo los nuevos favoritos, los mensajes de correo-e, y los documentos que han generado o recibido. Así, en caso de infección saben que pueden formatear y recuperar su operatividad fácilmente. El único perjuicio importante es que necesitarán una hora para completar esa tarea, pero eso les garantiza una solución "razonable" en caso de infección.

Quien no tenga copias de seguridad seguramente saldrá mucho más perjudicado: En caso de infección es posible que pierda documentos importantes y necesitará mucho más tiempo y esfuerzo para reinstalar y configurar todo lo que necesita usar. Por este motivo, quien no tenga copias de seguridad nunca debería prescindir de un buen antivirus actualizado. Pero tener un antivirus no es justificación para prescindir de las copias de seguridad: Hay que recordar que se pueden perder los datos por muchas otras razones, aparte de los virus.

Otro detalle importante, para quien no tiene antivirus, es evitar que otras personas usen el ordenador, o que lo hagan de una forma responsable. Pueda que el propietario sea una persona cuidadosa y prudente, pero quizá los demás no lo sean y eso provoque una infección que perjudicaría seriamente.

En conclusión, la solución más sencilla y eficaz es tener un buen antivirus residente y actualizado. Esa es la primera y más importante prevención, aunque también se haría bien en tomar otras precauciones adicionales, algunas de las cuales ya se han comentado: nunca debemos creer que el antivirus es infalible.

Por ejemplo, aunque se tenga un buen antivirus es un poco "suicida" abrir el archivo adjunto que se recibe en un correo electrónico remitido por alguien desconocido (salvo que exista otra razón que lo justifique).

Está comprobado que la mayoría de las infecciones (y problemas similares) se producen porque los usuarios se comportan como unos verdaderos irresponsables: tienen muy pocos conocimientos técnicos, además tienen mal configurados sus sistemas... y edemas van abriendo cualquier mensaje o archivo sin pararse a pensar en lo que hacen. Muchos, además, no tienen antivirus, o tienen un antivirus obsoleto, o lo tienen mal configurado, etc.

CAPÍTULO VI

PROCEDIMIENTOS DE SEGURIDAD

PREÁMBULO.

INTRODUCCIÓN.

A continuación se muestran las medidas de prevención y seguridad contra ataques de virus informáticos que debería de existir para las computadoras personales así como para las redes informáticas. Todo con el objetivo de garantizar la estabilidad y seguridad de la información y al mismo tiempo minimizar al máximo los riesgos que conllevan un ataque de código malicioso.

OBJETIVOS.

- Brindar un manual de políticas de seguridad y prevención contra virus informáticos para redes de computadoras.

- Dar a conocer los beneficios que brinda la prevención de daños.

- Proporcionar las medidas básicas de desinfección y recuperación de datos.

6.1 ADMINISTRACIÓN DE LA SEGURIDAD.

Si la naturaleza misma de la seguridad de una empresa parece compleja, probablemente lo sea. Posiblemente el entorno computacional es heterogéneo, como la mayoría de ellos, y tiene gran cantidad de productos de seguridad de distintos proveedores. Es posible que se tenga usuarios remotos que se conectan a la red u oficinas en ubicaciones geográficas distantes. En estas circunstancias, los problemas potenciales se encuentran fácilmente. Sin una visión general de la estructura actual de seguridad, ¿cómo puede administrar la seguridad? Las herramientas de seguridad, tales como firewalls(cortafuegos), detección de intrusos y software antivirus funcionan bien, individualmente , pero ¿funcionan bien entre sí para proteger la red? y ¿cómo monitorear su rendimiento?

6.1.1 CUMPLIMIENTO DE LAS POLÍTICAS Y NORMATIVAS DE SEGURIDAD.

Las empresas necesitan establecer políticas, estándares y procedimientos de seguridad para hacer cumplir la seguridad de la información de forma estructurada. Una evaluación de riesgos ayudaría a identificar y administrar las vulnerabilidades del entorno. Con base en este análisis, el administrador puede desarrollar un marco de políticas apropiado y empezar a construir un conjunto de políticas adaptadas a su empresa.

Una cosa es adoptar una política de seguridad y otra muy diferente es administrarla y cumplirla eficazmente. Actualizar los controles de acceso, y las medidas de autenticación y autorización en todos los niveles de la red es una necesidad imperiosa para una política de seguridad eficaz. La omisión de esta información puede incrementar la exposición a riesgos. Las compañías pueden contar con políticas de seguridad de la información para proteger los activos importantes y los datos críticos, pero muy rara vez cuentan con los medios para monitorear eficazmente el cumplimiento de esta política.

Puede ser difícil obtener información en tiempo real acerca de lo que sucede en una red empresarial. Si se ha instalado varios dispositivos de seguridad en la red, el administrador sabe que se necesita tiempo para ordenar los datos que ingresan con millones de eventos y que encontrar los problemas más importantes a tiempo para poder actuar es todo un reto. Más aún, se necesita empleados calificados que posean la experiencia necesaria para interpretar dichos datos, independientemente de que se trate de un análisis de tendencias o de simplemente separar una serie de eventos importantes de los que son irrelevantes.

Una situación típica es cuando el usuario instala los componentes de seguridad por separado y cada uno de ellos viene equipado con su propia consola de administración el usuario sabe que el tiempo es vital puesto que los incidentes de seguridad no esperan a que el personal los descubra. Como el administrador no cuenta con una sola visualización de los eventos en todo el perímetro de la red, sucesos como los intentos de ingresar al servidor corporativo, o una amenaza combinada que se atraviese en la red, pueden estar sucediendo sin darnos cuenta.

6.1.2 CONTROL DE LAS AMENAZAS COMBINADAS.

El año pasado se tuvo conocimiento de las amenazas combinadas, como CodeRed y Nimda. Lo que diferencia a estas sofisticadas amenazas de los otros gusanos de Internet es que utilizan múltiples métodos de ataque o propagación., Aparte de esto, estas amenazas nos han enseñado que es anticuado el enfoque de "para cada amenaza, hay una cura". Para defender a la empresa de las amenazas combinadas, se requiere protección de toda la red y una capacidad de respuesta en los niveles del gateway, del servidor y de los clientes. Generalmente las amenazas combinadas se aprovechan de las vulnerabilidades conocidas, como los desbordamientos de búfer, las vulnerabilidades de la validación de entrada de http, las contraseñas predeterminadas conocidas, entre otras.

6.1.3 PERMITIR QUE EL PERSONAL DE SEGURIDAD RINDA AL MÁXIMO

Hoy en día, la administración de la seguridad empresarial es un proceso difícil que se realiza a través de una combinación de productos comerciales dispares de distintos proveedores sin integración ni interoperabilidad. El resultado es un alto grado de complejidad y un aumento de los costos operacionales. Los administradores invierten mucho tiempo realizando tareas redundantes, pero necesarias para administrar la compleja infraestructura de seguridad de la red. En el clima económico actual, existe presión para producir más con menos, tanto desde el punto de vista financiero como de los recursos. Hay que pensar en las posibilidades. Si se le permite al personal concentrarse en actividades de más valor, se obtendrá una seguridad mejorada y más proactiva para la empresa.

6.2 Políticas de Seguridad y Prevención Para Usuarios de La Red.

A pesar del tiempo, energía y dinero que las compañías invierten en productos para mantener la seguridad de la red, la principal amenaza a su red proviene con frecuencia del interior de la compañía. Además de tener las medidas básicas de seguridad como cortafuegos, protección antivirus y de códigos móviles y filtrado de contenidos, las compañías también necesitan concentrarse en la capacitación a los empleados a fin de reducir el impacto de la amenaza humana.

De acuerdo a la encuesta de 1999 sobre la Seguridad y Delitos a las Computadoras del Instituto de Seguridad de Computadoras y del FBI, un 38 por ciento de los demandados cometió una de cada cinco violaciones a la seguridad originadas dentro de sus organizaciones, mientras que el 16 por ciento cometió seis de cada diez. Muchas violaciones a la seguridad han ocurrido porque los empleados no capacitados no sabían como el uso de la computadora, correo electrónico o Internet influyen en la seguridad de la compañía. Los empleados puede ser presa de las tácticas de ingeniería social cuando descargan inadvertidamente códigos maliciosos o los empleados descontentos pueden intentar causarle daño a la compañía premeditadamente.

6.2.1 Amenazas Al Correo Electrónico

El correo electrónico de los usuarios o empleados puede causar varios tipos de violaciones a la seguridad. Si los empleados abren archivos adjuntos no solicitados del correo electrónico o no analizan los documentos adjuntos en busca de virus antes de abrirlos, entonces la empresa es vulnerable a los ataques de virus.

También si las compañías confían en los empleados para mantener sus definiciones de virus actualizadas, en lugar de promover automáticamente nuevas definiciones de virus a fin de asegurar el cumplimiento de la política, son susceptibles a infecciones incluso si se hace un análisis en los archivos adjuntos en busca de virus antes de abrirlos. Al permitir inadvertidamente correo electrónico inadecuado, de naturaleza sexual u ofensiva para ser enviado dentro de la oficina, las compañías son vulnerables a las acciones jurídicas.

6.2.2 LOS PELIGROS DE LA NAVEGACIÓN.

Los empleados que pasan tiempo navegando para uso personal también afectan la seguridad de la red. La mayor preocupación es el tiempo que pierden los empleados. Sin embargo, existen otras consideraciones. Así como con el correo electrónico, la navegación inadecuada por la Web puede conllevar a demandas jurídicas cuando un empleado consulta en línea material sexualmente explícito o discriminatorio. Los empleados que descargan muchos archivos MPEG o MP3 ponen en peligro la red al bloquearla o ponerla a funcionar con lentitud.

La navegación que no está relacionada con el trabajo también aumenta las probabilidades de que un empleado visite un sitio usando ActiveX o Java. Estos lenguajes se pueden utilizar para crear códigos maliciosos que se pueden comunicar directamente con el equipo del usuario, dándole acceso a los hackers a la información y potencialmente a la red.

Si los empleados descargan software o protectores de pantalla gratuitos de sitios desconocidos, el sistema se podrá infectar con un virus o caballo troyano, lo que puede causar daños que van desde el borrado de archivos hasta el hurto de contraseñas. Sin embargo, los expertos dicen que los sitios más grandes y famosos que usan estos lenguajes son bastante seguros porque utilizan medidas de seguridad.

6.2.3 EL RETO DE LAS CONTRASEÑAS

Las contraseñas son la mayor vulnerabilidad que tiene la mayoría de empresas. No resulta extraño que las personas comparten las contraseñas o utilicen una contraseña simple para ahorrar tiempo. Las contraseñas poco elaboradas facilitan el acceso de usuarios no autorizados. Un aspecto potencialmente débil de la red no puede ser las contraseñas de usuario sino los usuarios. Una actitud despreocupada hacia las contraseñas es en lo que confían los ingenieros sociales puesto que facilita que se engañe a un empleado para que dé sus contraseñas por teléfono o por el correo electrónico.

6.2.4 TÁCTICAS DE INGENIERÍA SOCIAL

Los empleados que no saben cómo responder a las violaciones potenciales de seguridad, como las tácticas de ingeniería social, dejan la compañía vulnerable a ataques de seguridad. Los empleados que no están capacitados adecuadamente o que no están contentos con su trabajo son los que tienen mayor probabilidad de divulgar la propiedad o información importante a individuos no autorizados como los competidores.

6.2.5 PROTEGIENDO LA RED

Se puede evitar las violaciones a la seguridad por factores humanos siguiendo los siguientes pasos:

- **Establecer una política para el uso de Internet.** Informando a los empleados el reglamento de la compañía acerca del uso personal del correo electrónico e Internet. El desarrollo de políticas para el uso de Internet también le ayuda a los gerentes de la tecnología de la información a configurar y monitorear las soluciones de seguridad para la red con más eficiencia.

- Usar tecnología que analice el correo electrónico en busca de contenidos inadecuados y registre la actividad en Internet que no sigue los parámetros establecidos por la gerencia.
- Los expertos jurídicos dicen que monitorear el correo electrónico de los empleados y el uso de Internet puede ayudar a proteger la compañía en caso de una demanda. Hay que tener una política y solución adecuada para monitorear el contenido con el fin de demostrarles a los empleados que se está haciendo esfuerzos por protegerlos del acoso de la siguiente forma:

    - Capacitar a los usuarios para que sepan cuándo y cómo descargar las últimas actualizaciones de antivirus y cómo detectar un virus potencial. Enseñarles a los empleados cómo analizar documentos antes de abrirlos.
    - Reparar los agujeros conocidos en el software para reducir las posibilidades de que un virus entre por las páginas web o el correo electrónico.
    - Desarrollar una política para las contraseñas, requiriendo cambios frecuentes de contraseñas y capacitando a los usuarios en las tácticas de ingeniería social y reforzar la posición de que nunca deben revelar una contraseña. El software para descifrar las contraseñas está disponible para ayudar a encontrar contraseñas débiles de usuarios en la red. Sin embargo, el software no protegerá a la compañía contra la negligencia de los empleados. Con frecuencia basta con capacitarlos.
    - Determine las necesidades del empleado para acceder a la información importante y restrinja el acceso sólo cuando sea estrictamente necesario para su desempeño en la compañía.
    - Avise a los empleados sobre los peligros de descargar software y protectores de pantalla gratuitos.

6.2.6 POLÍTICAS PARA EL USO ADECUADO DE INTERNET.

El método más efectivo aunque a menudo rechazado para encausar el "factor humano" es establecer una política de capacitación constante y consistente al usuario con énfasis en los objetivos de la seguridad para la compañía. Comenzando por determinar las necesidades en relación con la política y el nivel de capacitación que requiere cada departamento. Por ejemplo, el personal de seguridad de la tecnología de la información necesita tener un conocimiento profundo de los productos y sistemas de seguridad que utiliza la compañía mientras que el personal diferente al técnico y de administración debe tener una comprensión general de las políticas adoptadas.

6.2.7 EDUCANDO A LOS USUARIOS.

Existen varias opciones de capacitación, como aprendizaje práctico, capacitación basada en la Web, capacitación en el aula de clase o por medio de seminarios. Hay que tener en cuenta que los empleados necesitan aprender y luego determinar los métodos de capacitación que serán más efectivos. Según los expertos, para enfatizar el sentido de cultura empresarial y reforzar la importancia de mantener la confidencialidad, quizás es más efectivo una capacitación en el aula de clase o por medio de seminarios presénciales. Si se necesita instruir a los empleados sobre el uso del nuevo software de seguridad , sería mejor un método práctico. Capacitar a los profesionales puede ayudar a determinar el método más efectivo que se debe adoptar.

6.2.8 HACER CUMPLIR LAS POLÍTICAS.

Determinar quién formulará y hará cumplir la política. El departamento de recursos humanos debe informar a todo el personal sobre la política durante la orientación al personal, hacer que firmen copias de las políticas como constancia de que las comprenden y aceptan y hacer cumplir la política mediante un seguimiento junto con las consecuencias establecidas cuando sea necesario. Se deben establecer claramente las consecuencias de la política. Por lo general, los administradores de la red y del sistema de seguridad deben implementar las medidas de seguridad, conformar un equipo de respuesta a los incidentes para resolver violaciones potenciales y trabajar conjuntamente con el departamento de recursos humanos para informar sobre problemas potenciales.

6.2.9 MEJORAMIENTO DEL FACTOR HUMANO.

A medida que la dependencia de Internet continúa y las amenazas a la red empresarial siguen evolucionando, es importante implementar soluciones de seguridad en especial a nivel del usuario final. A pesar de que la protección antivirus, cortafuegos y tecnologías para el filtrado de contenidos ayudan a controlar las amenazas, el comportamiento del usuario final puede comprometer la seguridad de la red. La capacitación a los empleados es una medida de seguridad importante y proactiva para complementar la estrategia para la seguridad de la red.

6.2.10 CINCO MEDIDAS BÁSICAS CONTRA LOS VIRUS

1. **No abrir ficheros adjuntos en mensajes de correo no solicitados aunque procedan de personas conocidas.** Desde la aparición del Loveletter proliferan los virus que utilizan la libreta de direcciones o los mensajes del buzón de entrada para difundirse, de modo que parezcan procedentes de personas conocidas o de presuntos "administradores del sistema". Si se ha ejecutado un virus por error desconecte inmediatamente el cable de red y contacte con soporte.

2. **Utilice Software legal y no descargue ficheros de sitios poco recomendables.** Debido a la facilidad con la que pasa de "mano en mano" el software ilegal es una fuente frecuente de virus. También los programas que se pueden descargar de sitios web que rozan la ilegalidad son causa frecuente de virus.

3. **No admita ficheros no solicitados ni de personas desconocidas en Chats, listas de distribución y servidores de noticias.** El chat IRC presenta muchos problemas de seguridad y gracias a sus facilidades para intercambiar ficheros suele ser utilizado para contaminar a incautos usuarios. También los servidores de noticias y las listas de distribución son un método habitual para difundir rápidamente un virus.

4. **Utilice y mantenga actualizado el antivirus.** Un antivirus es poco eficaz si no se mantiene actualizado. Además hay que mantener la protección permanente (residente) activada. Si se decide no tener activada la protección permanente hay que analizar todos los disquetes, los ficheros que se descarguen y los ficheros adjuntos al correo.

5. **Realice copias de seguridad de su información.** No confiar en el disco duro. Hacer copias de seguridad de todos aquellos documentos importantes generados por el o los usuarios y que de otra forma serían irrecuperables en caso de desastre.

6.3 Soluciones Para una Red Segura

Una red segura requiere dedicación y acción proactiva. Es recomendable que el administrador cree una red menos susceptible a cada uno de los problemas de la seguridad. La seguridad de la red es un tema extenso en su conjunto, pero no lo es si se divide. Se sugiere que se vea la situación desde otra perspectiva y se analice todos los aspectos de la red que necesitan protección y cómo construir la red de manera que cada capa esté protegida por su respectiva capa de seguridad.

6.3.1 Diseño y Arquitectura De La Red

Conocer lo que se tiene y lo que se necesita para protegerse. Las necesidades de la empresa y el valor de la información guardada en la red determinarán la arquitectura de la red y las soluciones que se emplearán. Cuando se construya la red, hay que separar todos los servicios para que cada uno tenga sus propias medidas de seguridad.

6.3.2 Separación Preliminar De Los Servicios De Red

Es importante separar cada servicio de los demás en la red, así como suministrar una capa de seguridad para cada servicio. Se puede comenzar a proteger la red de la siguiente manera:

1. Utilizando un cortafuego para proteger la red empresarial de Internet.
2. Usando un cortafuego para separar la Intranet empresarial de los clientes externos o servidores / servicios públicos.

Una vez implementando estas medidas de protección, se obtendrán dos redes distintas como las siguientes:

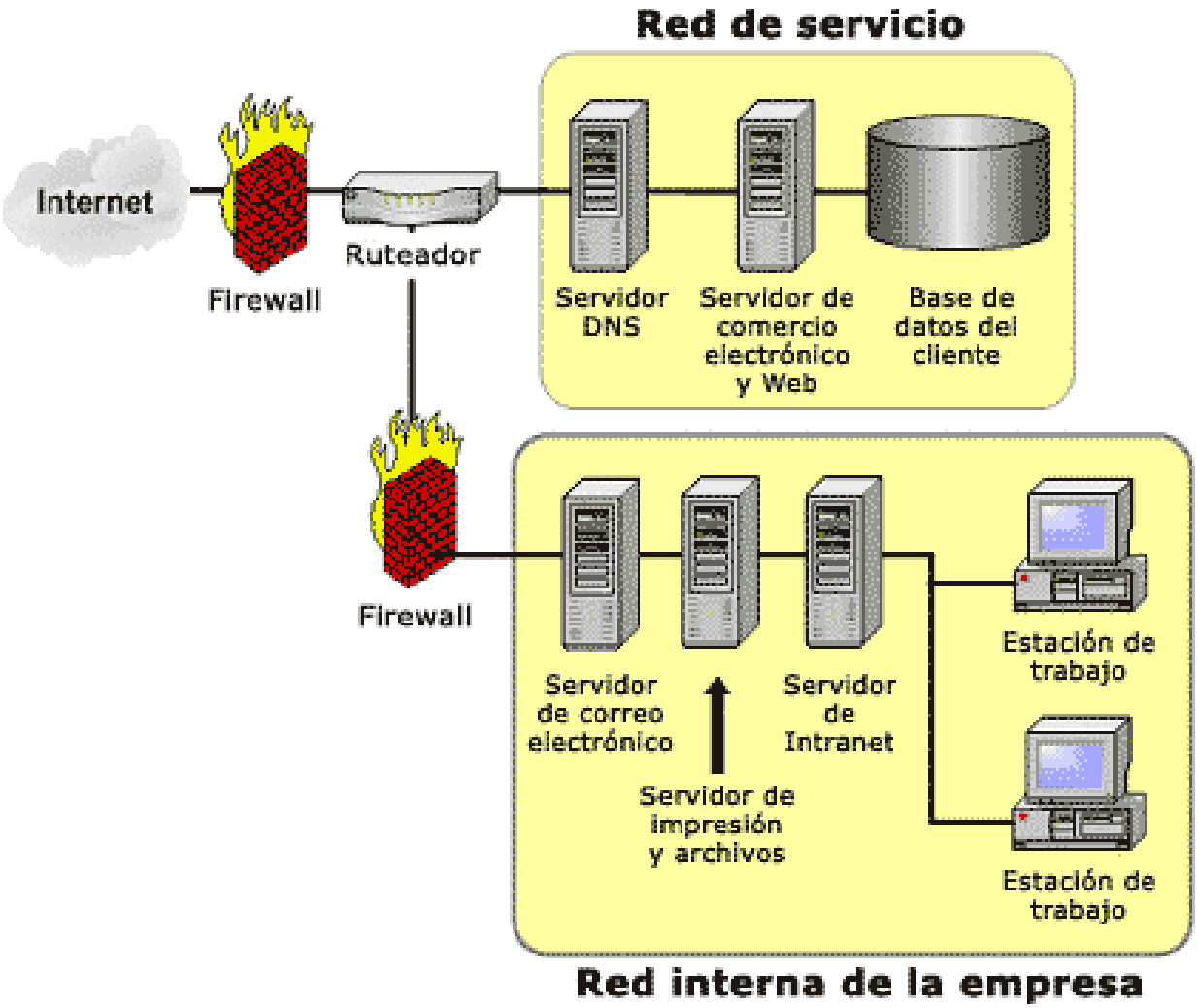


Figura 6.1

Hay que observar que la división de la red en dos grupos separados está determinada por los dos recuadros. Estos grupos son:

- **Intranet** - La Intranet contiene todos los servidores y las aplicaciones que son internos de la compañía. Este segmento de la red ahora está separado de la Internet pública por dos cortafuegos para brindar mayor protección.
- **Red de servicio o de perímetro** - También conocida como "DMZ" o Zona Neutral. La(s) red(es) de perímetro está(n) entre Internet e Intranet y contiene(n) todos los servicios e información pública o de los clientes. Se pueden definir reglas para acceder a esta red específica.

Estas categorías pueden ser muy pequeñas o grandes dependiendo de una situación específica. La protección para cada categoría debe escalarse con muchas capas de seguridad en toda la red. Todos los componentes de la red pueden dividirse esencialmente en estas dos categorías principales, lo que es un buen comienzo para las medidas de seguridad de la red.

Otras recomendaciones podrían ser estas tres medidas de seguridad específicas que el administrador puede adoptar para implementar la seguridad como la que aparece en el diagrama anterior:

- Instalar un sistema de detección de intrusos (IDS) basado en host en el servidor comercial para salvaguardar información como los nombres de clientes, las direcciones, el registro de compras y lo más importante, la información de las tarjetas de crédito.

- Implementar la conversión de dirección de red (NAT - Network Address Translation) para proteger las direcciones IP de los equipos en todas las redes.

- Insertar un sistema IDS basado en red en la red de perímetro para poder identificar los intentos de ataque de los intrusos.

Estas mejoras de seguridad adicionales han aumentado la complejidad de la red. Sin embargo, también limitan el control en la aplicación de los controles de seguridad y otorgan acceso únicamente a aquellos servicios para los cuales están autorizados los usuarios y las aplicaciones. Por esta razón, muchas compañías utilizarán un sistema IDS cliente / administrador que permita la aplicación de las reglas y políticas en toda la red. Otra posibilidad es obtener con un proveedor de seguridad una solución completamente administrable.

6.3.3 AGREGAR REDES DE SERVICIO POR SEPARADO.

La última recomendación para el diseño de red es agregar redes adicionales para los siguientes servicios:

- Copias de respaldo.
- Mantenimiento del sistema.
- Servidores proxy.
- Directorios FTP.

Establecer redes separadas dentro de la compañía permite mayor control sobre el acceso a estos servidores y servicios.

6.3.4 PROTECCIÓN FÍSICA Y AMBIENTAL DEL HARDWARE

La protección del hardware no siempre es una prioridad importante para los gerentes de la seguridad, aunque no debería pasarse por alto. La protección incluye satisfacer necesidades específicas de seguridad como las siguientes:

- **Equipo de red** - Todo el equipo de la red debe mantenerse en el mismo tipo de entorno controlado que el de los sistemas de computación de la compañía, el cual incluye:
    - Acceso limitado al equipo por parte de los empleados.
    - Temperatura y humedad controladas.
    - Extintores tipo Halon.

- **Cableado** - Asegurarse de que el cableado de la red esté protegido contra la interceptación o las averías. El uso de los cables de fibra óptica evitará la unión en general, aunque si no es posible, tenga un conducto alrededor del cable y cajillas de seguridad en los puntos de inspección y terminación.

6.3.5 ESTANDARIZAR TODAS LAS CONFIGURACIONES.

Bien sea que se tenga una pequeña red con un ruteador y unas pocas máquinas (hosts) o una red global que se extiende a múltiples puentes, conmutadores y gateways, es importante que las configuraciones de todo el equipo similar sean parecidas. Por ejemplo, los cortafuegos, Telnet y FTP, cada uno debe tener un conjunto de reglas de acceso.

6.3.6 ANÁLISIS CONSISTENTE DE LOS ARCHIVOS DE REGISTRO.

Es importante evaluar continuamente los archivos de registro del equipo de red. Con frecuencia, los archivos de registro revelan los primeros indicios de que algo inusual está sucediendo.

6.3.7 CONTROL DE ACCESO A LA RED.

El administrador de red debe saber quien tiene acceso a su red e implementar los mecanismos para controlar el acceso. Hay que tener en cuenta lo siguiente cuando se distribuye el acceso a la red:

- Restringir el acceso a aquellos servicios que han sido autorizados específicamente para los usuarios y las aplicaciones.
- No olvidar tener mecanismos de autenticación para las conexiones remotas, con base en el "valor" de la información valiosa que está disponible a través de la conexión.
- Si las "relaciones de confianza" con personas externas les permite acceso a la red, asegurarse de que únicamente tengan acceso a los servicios específicos requeridos.
- Los usuarios necesitan con frecuencia acceder a la información con diferentes niveles de valor. Cuando se establezcan los niveles de acceso múltiple, asegurarse de que un nivel de protección no comprometa la información más valiosa.

6.3.8 AMENAZAS COMUNES A LA RED.

A continuación se presenta un resumen general de algunas amenazas comunes a la seguridad de la red y las recomendaciones para evitar ser víctima de ellas:

- **Análisis en el puerto** - Los hackers utilizan herramientas de análisis para buscar en los hosts que están conectados a una red en busca de puertos que estén activados o abiertos. Los hackers comparan esta información con las vulnerabilidades conocidas de la seguridad para ver si pueden obtener acceso a los hosts identificados.

  Cómo reducir la amenaza: Active únicamente los servicios que se necesitan y utilice la conversión de dirección de red (NAT) para evitar que las direcciones estén a disposición del público en Internet.

- **Negación de servicio (DoS) -** Diseñado para negar el acceso a los recursos de computación o interconexión al sobrecargar el host o la red con solicitudes continuas. Es decir que los ataques DoS envían más solicitudes de lo que la máquina o red pueden manejar.

  Cómo reducir la amenaza: Asegurarse de que los servidores en la red de perímetro no funcionen al límite de su capacidad y que utilicen los cortafuegos de filtrado de paquetes para evitar que los paquetes falsificados entren en la red de perímetro. Además, actualizar todos los hosts y servidores con parches y soluciones de seguridad.

- **Falsificación de la dirección IP -** Los hackers encuentran una dirección IP confiable y la modifican para que parezca que proviene de un host confiable cuando en realidad no es así.

  Cómo reducir la amenaza: Configurar los ruteadores y cortafuegos para rechazar todo paquete que ingrese y afirme haberse originado en un host de la red interna. De esta manera, la máquina externa no puede aprovecharse de las relaciones de confianza de la red interna.

- **Husmeo de la dirección IP -** Los intrusos potenciales "husmean" (monitorean) una red para captar información valiosa, como las direcciones IP, los nombres de usuario y las contraseñas mientras los usuarios registran un sistema remoto.
  Cómo reducir la amenaza: Hacer obligatorio el uso de una contraseña y el uso de los servidores proxy y NAT para reducir el husmeo de la dirección IP.

- **Virus, caballos de Troya y gusanos** - Aunque son diferentes, cada uno de estos programas maliciosos puede tener un efecto devastador en las computadoras de la empresa y posiblemente en toda la red.
  Cómo reducir la amenaza: Siempre ejecutar el software antivirus con un archivo actualizado de definiciones de virus y nunca ejecutar un programa no solicitado sin primero ensayarlo en un host de prueba aislado. Capacitar a todos los empleados para que tengan cuidado al abrir correo electrónico sospechoso que provenga de fuentes desconocidas.

6.4 PROCEDIMIENTOS DE DESINFECCIÓN

Tener el sistema infectado por un virus es un factor que puede suceder en cualquier momento. Se trata de un grave problema que requiere una atención y acción inmediata. A continuación se presenta una lista de los procedimientos a seguir para desinfectar un sistema que contiene un virus.

Antes que nada, se debe identificar el tipo de virus que infecta el sistema. Para ello, puede ser de utilidad un buen programa antivirus.

En caso de no poseer un antivirus en el momento de la infección, puede utilizar un antivirus en línea, gratuito, el cual serviría para detectar si la maquina ha sido infectada por un virus. Cabe mencionar que dependiendo del ancho de banda que se tenga para acceder al Internet así es el tiempo que se toma el antivirus en para realizar un diagnostico de la computadora.

6.4.1 CUANDO EL VIRUS ES UN MACROVIRUS

Aproximadamente el 80% de las infecciones causadas por virus que se conocen son de macrovirus. Estos virus suelen propagarse al abrir un documento de Word o Excel que se ha creado en el sistema infectado de otro usuario y que se envía al destinatario por correo electrónico, se descarga o se abre desde un servidor, un disquete compartido o un disco comprimido. Si abre un documento infectado en su sistema, todos los documentos del sistema son susceptibles de contener el virus e infectar a quien los abra. No suele aparecer ninguna indicación que señale que el documento está infectado o que se está propagando el virus.

Este tipo de virus es más fácil de eliminar que un virus que infecte el sector de inicio, exe o com, pero suele ser mucho más infeccioso. Una vez desinfectadas las unidades de disco duro, también se debe explorar todos los soportes extraíbles y las unidades de todos los servidores a los que se conecta normalmente. Asimismo, es de vital importancia notificar a todos los usuarios con los que se suele intercambiar archivos de Word o Excel que su sistema está infectado y que puede haberlos contagiado.

6.4.2 CUANDO EL VIRUS ES INFECTANTE DEL SECTOR DE INICIO EXE Ó COM

Aunque estos virus son menos frecuentes, suelen ser más difíciles de eliminar que los macrovirus. Es muy importante que se entienda y se siga las directrices siguientes para desinfectar el sistema. Con una limpieza rápida del sistema lo único que hará será propagar el virus a más archivos todavía.

El problema con este tipo de virus es que en ordenadores con Win95/98 puede hallarse en la memoria, unido a las interrupciones del sistema operativo. Esto le permite controlar todo lo que el sistema ejecuta y protegerse de los programas antivirus que intentan eliminarlo. Algunos de los creadores de estos programas de virus son programadores muy astutos, para los cuales mantener el virus con vida en su sistema constituye un reto. No hay que subestimar su inteligencia.

A grandes rasgos, el proceso a seguir es: mantener el sistema en un estado seguro y, a partir de aquí, desinfectar sus partes desconocidas. Procediendo de la siguiente manera:

- **Paso nº 1**: Aislar el sistema. Desconectar de las redes a las que esté conectado. Incluyendo Internet.

- **Paso nº 2**: Comprobar que no haya ningún virus en la memoria. Para llegar a este estado, se debe iniciar el sistema desde un disquete limpio. Sin embargo, es posible que el virus haya modificado el CMOS para inhabilitar el inicio desde el disquete. Por ello, se debe comprobar antes que el CMOS está configurado para iniciar desde el disquete.
- **Paso nº 3**: Comprobar que el sector de inicio del disco duro esté limpio. Para llegar a este estado, se debe ejecutar un detector antivirus para explorar la unidad de disco duro después de iniciar el sistema en el segundo paso con el disquete seguro.
- **Paso nº 4**: Desinfectar los archivos de la unidad de disco duro. Una vez se haya comprobado que los archivos y los sectores de inicio del disco duro del sistema no están infectados, se puede iniciar el sistema siguiendo el procedimiento habitual. Seguidamente, se deberá explorar con detalle todos los archivos del sistema para asegurarse de que ninguno contiene un virus. Se debe explorar y limpiar los archivos hasta que no se detecten más virus. Cuando se crea que el sistema está limpio, es aconsejable volver al paso nº 1 y repetir todo el proceso una vez más, por razones de seguridad.
- **Paso nº 5**: Desinfectar los soportes extraíbles. Ahora que el sistema está limpio, se puede explorar los soportes. Explorar los disquetes, discos de compresión, CDROM y cintas de copias de seguridad. Hay que tomar en cuenta que el virus puede haber infectado el sistema hace tiempo y haberse propagado por todas partes.
- **Paso nº 6**: Desinfectar la red. Hay que observar que no se dice "servidor". El servidor es sólo un componente de la red. A pesar del trabajo que comporta, si realmente se desea eliminar un virus nocivo, se debe eliminar de todas partes para evitar que vuelva a reproducirse. Todos los usuarios de la red deben garantizar que sus máquinas están limpias y, evidentemente, el administrador del sistema debe desinfectar los servidores.

- **Paso nº 7**: Desinfectar el entorno. El sistema se ha infectado con este virus de algún modo. Es posible que el virus provenga de una fuente externa a la red. Se debe comunicar a todas las personas que trabajan con la red que el sistema está infectado. Si no se hace, es posible que se vuelva a transmitir el virus.
- **Paso nº 8**: Mantener el sistema limpio. Examinar el ordenador con la ayuda de el software antivirus. Esto permitirá detectar nuevas infecciones antes de que se propaguen y comunicará si existen archivos infectados que, de no utilizar el programa, no habría detectado.
- **Paso nº 9**: Cada día aparecen nuevos virus. Se debe actualizar el software antivirus con frecuencia. Si no se hace, es posible que el programa antivirus no detecte los virus nuevos, de modo que otros usuarios pueden resultar infectados involuntariamente antes de que se detecte el virus.
- **Paso nº 10**: Algunas veces los virus son tan nuevos que los antivirus no logran limpiarlos o eliminarlos, pero se logran detectar y se sabe que la computadora posee un virus. En estos casos normalmente las compañías creadoras de antivirus, como por ejemplo Symantec, publican en su portal Web las herramientas y soluciones para eliminar dicho virus, llamados parches, en los cuales proporcionan todas las instrucciones a seguir para la desinfección, por lo que es una alternativa más para poder desinfectar una computadora o Red.
- **Paso nº 11**: Este es el paso que se debería de tomar en una ultima instancia, y es que si no funcionara ninguna de los procedimientos anteriores para desinfectar las computadoras, se tendría que formatear disco por disco, computadora por computadora y luego instalarles los diferentes programas necesarios para el funcionamiento. Cabe mencionar que este es el ultimo recurso al cual recurrir.

Los procedimientos vistos anteriormente no están sujeto a un orden especifico, ya que las formas de infección son distintas y algunos procedimientos de desinfección son más fáciles que otros. Por lo que se debe realizar un análisis de la situación en que se encuentra la computadora o red.

6.5 Métodos Básicos Para La Recuperación De Datos

Un Plan de Contingencia de Seguridad Informática consiste en los pasos que se deben seguir, luego de un desastre, para recuperar, al menos en parte, la capacidad funcional del sistema aunque, y por lo general, constan de reemplazos de dichos sistemas. Se entiende por Recuperación, tanto la capacidad de seguir trabajando en un plazo mínimo después de que se haya producido el problema, como la posibilidad de volver a la situación anterior al mismo, habiendo reemplazado o recuperado el máximo posible de los recursos e información.

Así, la recuperación de la información se basa en el uso de una política de copias de seguridad (Backup) adecuada. La realidad indica que al no respetarse este enunciado, en la práctica, sólo existe un motivo por el que se pierde información: la falta de copias de seguridad.

El Respaldo de archivos permite tener disponible e íntegra la información para cuando sucedan los accidentes. Sin un backup, prácticamente, es imposible volver la información al estado anterior al desastre.

La falta de concientización de los usuarios en este sentido es muy alta. Más allá de lo que cabe esperar, y de lo que sería normal; un alto porcentaje de usuarios sabe lo que es un Backup o Copia de Seguridad pero nadie sabe como hacerlo, o peor aún: saben como hacerlo pero NADIE LO HACE.

Los motivos para esto son muy variados pero siempre podemos concluir que hacer una copia de seguridad es molesto, tedioso e involucra aparente pérdida de tiempo que nadie está dispuesto a afrontar.

Estos son motivos válidos, pero entonces el usuario pierde su disco y su preciada carpeta "mis documentos" y no la puede recuperar por lo que pensamos que ya aprendió la lección.

Como se indicaba más arriba los motivos por los cuales no hacer backup pueden ser muchos y muy variados pero nunca superarán al beneficio de tener un backup funcional en el momento de perder la información (cosa que siempre ocurrirá, tarde o temprano).

Hay que observar que se dice backup funcional; porque también es muy normal hacer backups en lugares en los cuales no se está 100% seguros que podemos recuperarlos. Esto es:

- Hacer copias en disquetes o cintas que pueden estar dañados;
- Hacer copias en CD "más baratos". Recordar que lo barato sale caro.
- Hacer copias de respaldo parciales porque "creo que eso ya lo copie";
- Hacer copias de respaldo "cada 6 meses mas o menos";
- Hacer copias de respaldo y guardarlo en "lugar seguro" más allá de lo que cualquiera entienda por lugar seguro.
- Hacer copias de respaldo no es una tarea trivial, e involucra recursos y costos que generalmente ni los usuarios finales ni las empresas consideran.

En el caso de los usuarios es relativamente fácil hacer copias de respaldo, pero como ya se mencionó lo difícil es crear una concientización adecuada.

Las posibilidades para realizar una copia de respaldo son muchas, si bien unas mas adecuadas que otras según se considere el caso:

- Se puede realizar una simple copia con el viejo conocido COPY/CP de DOS/UNIX.
- Se puede grabar un CD.
- Se puede grabar una cinta.
- Se puede copiar la información a un disco removible/PC espejo del original.
- Se puede subir la información a la web en hostings que cuenten con copias de respaldo.

Aunque parezca obvio, todas estas posibilidades SIEMPRE deben contemplar que la copia se realizó correctamente y como requisito extra esta verificación debe realizarse cada cierto tiempo prudencial.

En lo que respecta a empresas las acciones a realizar son un poco más complejas pero el concepto es el mismo: hacer copias de respaldo es ahorrar tiempo y dinero.
En este caso será necesario realizar un análisis costo/beneficio para determinar qué información será almacenada, los espacios de almacenamiento destinados a tal fin, la forma de realización, las estaciones de trabajo que cubrirán las copias de respaldo, etc.

Para una correcta realización y seguridad de las copias de respaldo se deberán tener en cuenta estos puntos:

- Se debe contar con un procedimiento de respaldo de los sistemas operativos y de la información de los usuarios, para poder reinstalar fácilmente en caso de sufrir un accidente.
- Se debe determinar el medio y las herramientas correctas para realizar las copias, basándose en análisis de espacios, tiempos de lectura/escritura, tipo de copia a realizar, etc.

- El almacenamiento de las Copias de Respaldo debe realizarse en locales diferentes de donde reside la información primaria. De este modo se evita la pérdida si el desastre alcanza todo el edificio o local.
- Se debe verificar, periódicamente, la integridad de los respaldos que se están almacenando. No hay que esperar hasta el momento en que se necesitan para darse cuenta de que están incompletos, dañados, mal almacenados, etc.
- Se debe contar con un procedimiento para garantizar la integridad física de los respaldos, en previsión de robo o destrucción.
- Se debe contar con una política para garantizar la privacidad de la información que se respalda en medios de almacenamiento secundarios. Por ejemplo, la información se puede encriptar antes de respaldarse.
- Se debe contar con un procedimiento para borrar físicamente la información de los medios de almacenamiento, antes de desecharlos.
- Mantener equipos de hardware, de características similares a los utilizados para el proceso normal, en condiciones para comenzar a procesar en caso de desastres físicos. Puede optarse por:
    - ***Modalidad Externa*****:** otra organización tiene los equipos similares que brindan la seguridad de poder procesar la información, al ocurrir una contingencia, mientras se busca una solución definitiva al siniestro producido.
    - ***Modalidad Interna*****:** se tiene más de un local, en donde uno es espejo del otro en cuanto a equipamiento, características técnicas y capacidades físicas. Ambos son susceptibles de ser usados como equipos de emergencia.

En todos los casos se debe asegurar reproducir toda la información necesaria para la posterior recuperación sin pasos secundarios ni operación que dificulte o imposibilite la recuperación.

6.5.1 RECUPERANDO ARCHIVOS BORRADOS

En muchas ocasiones, debido al ataque de un virus o simplemente por un error, borramos archivos importantes que luego no podemos recuperar, ya que tampoco se conservan en la papelera de reciclaje.

Drive Rescue (Unidad de rescate) es la utilidad que no debe faltar en nuestra caja de herramientas, y que nos permitirá encontrar y recuperar datos perdidos o borrados en nuestros discos duros, aún si la tabla de particiones está mal o corrupta, o ya no existe.

Esta es una herramienta gratuita (FREEWARE), que permite recuperar además, áreas críticas como la tabla de particiones, sector de arranque (boot record), FAT, etc. Soporta FAT12 (disquetes), FAT16 (DOS, Win3.x, Win95), FAT32 (Win95 OSR2, Win98, WinMe, W2000 y WinXP) y NTFS (Solo Undelete bajo W2000 y WinXP).

Incluye **Digital Image Recovery**, que permite la recuperación de imágenes de cámaras digitales borradas (Smartmedia, Compact Flash, Memory Stick y otros). Soporta los siguientes tipos de imágenes: JPEG, exif, TIFF, PNG, GIF, BMP, Canon CRW. También soporta archivos de audio y video (AVI, MOV, WAV).

El programa es muy sencillo de utilizar, simplemente navegamos con él al estilo del Explorador de Windows, mientras visualizamos archivos y carpetas borrados, y con un simple botón derecho recuperamos el o los archivos borrados (directorios y subdirectorios incluidos). Soporta entre otros lenguajes el español.

El programa nos indica la condición del archivo (god o poor, o sea recuperable, o probablemente irrecuperable o corrupto). Recordemos que cuando se borra un archivo o carpeta, el sistema operativo en realidad no lo borra físicamente, solo cambia un byte al comienzo de su nombre, dejando el espacio con una marca de disponible para guardar un nuevo archivo.

Por esa razón, las posibilidades de recuperar archivos eliminados, disminuye a medida que escribimos nuevos archivos al disco, luego de un borrado.

El programa agrega algunas utilidades extras para usuarios avanzados. En su versión más reciente, puede recuperar discos con el sector de arranque dañado.

Por supuesto, **Drive Rescue** no hace milagros, y no puede recuperar datos si los sectores del disco están físicamente dañados.

Para recuperar archivos e incluso particiones enteras, se sugiere trabajar con un segundo disco duro como esclavo, a los efectos de traspasar la información luego de recuperada. Esto aumenta las posibilidades de éxito, ya que se evita escribir algo en los discos a recuperar. Escribir datos en un disco, puede destruir datos anteriores.

Existen dos versiones de esta herramienta, una de ellas para recuperación de emergencia, si los datos de su disco duro han sido borrados y no se puede acceder a Windows.

Algunas características del programa:

- Recuperación de archivos con su antigua fecha y hora.
- Grabar los datos recuperados a una unidad de red.
- Recuperar discos con los sectores de arranque perdidos (solo FAT)
- Recuperación de archivos perdidos sin referencias a directorios (por ejemplo, después de Quick Format).
- Soporte estos archivos: ARJ, AVI, BMP, CDR, DOC, DXF, DBF, XLS, EXE, GIF, HLP, HTML, JPG, LZH, MID, MOV, (MP3), PDF, PNG, RTF, TAR, TIF, WAV, ZIP.
- Búsqueda de un archivo específico borrado.
- Visualizar archivos borrados o perdidos.

En conclusión existen varias herramientas para la recuperación de datos similares, con diferentes nombres, pero con las mismas características, que se pueden obtener en Internet, este es una medida de emergencia con la cual se puede contar para la recuperación de información perdida. Aunque ya se había mencionado anteriormente la medida más eficiente para la recuperación de información es la cultura de realizar copias de respaldo periódicamente.

CAPÍTULO VII

CASOS REALES

PREÁMBULO.

INTRODUCCIÓN.

En este capítulo se analizan ciertas empresas salvadoreñas, las cuales han sido víctimas por los daños que causan los virus informáticos.

Esto tiene como objetivo un estudio que permita mostrar los daños y costos que estos programas maliciosos efectúan en el comercio e industria de El salvador, y a su vez verificar las medidas de seguridad que las distintas empresas implementan en materia de seguridad.

OBJETIVOS.

- Conocer diferentes empresas salvadoreñas afectadas por los virus informáticos.

- Determinar los costos que conllevan los daños causados por los virus.

- Analizar las medidas de seguridad que las empresas implementan en sus sistemas.

7.1 Como Afectan los Virus Informáticos a Las Empresas y El Comercio Mundial.

Los virus informáticos causan este año (2003) unas pérdidas económicas por valor de 14.000 millones de euros, a nivel mundial.

Las epidemias de virus informáticos siguen causando estragos en la economía mundial, según un estudio de Computer Economics, que cifra las pérdidas ocasionadas por estos códigos maliciosos en 14.544 millones de euros, lejos, no obstante, de los 19.232 millones de euros del año pasado.

Durante el presente año, las epidemias provocadas por estos códigos maliciosos se han sucedido, aunque las compañías de seguridad informática cada vez reaccionan con mayor celeridad. El virus más devastador en términos económicos en 2001 ha sido el denominado 'Código Rojo', cuyos efectos han supuesto pérdidas cercanas a los 2.950 millones de euros. A continuación aparece el virus más propagado en este año, el 'Sircam', que ha provocado pérdidas por valor de 1.298 millones de euros, mientras que el coste del 'Nimda' asciende a 715 millones de euros.

Aunque las consecuencias de estos virus han sido muy elevadas, todavía permanecen muy lejos del famoso 'I love you', que en 2000 provocó por sí solo 9.856 millones de euros de pérdidas en la economía mundial, la mitad del total contabilizado en todo el año.

No obstante, no hay que olvidar que la tendencia destructiva de los códigos maliciosos proviene de 1999, cuando los virus 'Melissa' y 'Explorer' tuvieron un impacto económico de 1.238 millones de euros y 1.147 millones de euros, respectivamente.

En cualquier caso, del estudio se deduce que, a no ser que comience una nueva epidemia devastadora en la última semana del año, la tendencia alcista de los últimos seis años parece haberse estancado en 2001.

Así, después de incrementarse ininterrumpidamente desde los 564 millones de euros de pérdidas de 1995 hasta los 19.232 millones de euros del año pasado, por el momento el año se cerraría en torno a los 15.025 millones de euros de pérdidas.

También es reseñable el impacto que ha tenido el virus 'Goner' en el tramo final de este año. Así, Computer Economics calcula que alrededor de 860.000 equipos resultaron infectados, pero su propagación no ha sido masiva debido a que las compañías de seguridad han conseguido contrarrestarlo con rapidez.

Hasta la fecha, este gusano ha provocado pérdidas por valor de 9,6 millones de euros, de los que más de 7,2 millones de euros fueron a cargo de empresas que tuvieron que limpiar sus equipos, y algo menos de 3 millones en pérdidas de productividad.

Los virus ocasionan pérdidas muy diversas que afectan la economía de toda empresa: eliminación de información valiosa, daños al hardware, costos relacionados con la reinstalación de software, descenso de la velocidad en la infraestructura informática, entre otras.

En la actualidad no existe empresa o usuario que no se haya visto afectado por este problema a pesar de que la mayoría tiene algún tipo de protección antivirus.

Se estima que actualmente el tiempo de propagación de un virus vía Internet a todo el mundo es de menos de tres horas (tiempos que obviamente serán cada vez menores). Todas las compañías dedicadas al desarrollo de antivirus pueden demorar incluso varios días en proporcionar los antivirus correspondientes.

¡De esto se deriva que ningún programa antivirus pueda darnos la solución definitiva a tan preocupante problema!.

Como la opción de dejar de estar conectados al mundo nos acarrearía más pérdidas que las ocasionadas por los propios virus, la solución más racional pasa por la conciencia y conducta de todos los usuarios, y por la seriedad global de la solución informática empleada en la empresa.

Los virus son pequeños programas de computación que se aprovechan de los agujeros de seguridad que sin saberlo o sin quererlo dejan a disposición básicamente todos los programas y sistemas operativos que usamos en nuestras computadoras. En particular, nuestros programas de correo electrónico y navegadores son hoy día los más atacados, ya que son los que permiten el contagio vía Internet. El éxito de un virus se mide por la cantidad de daño que causa en el mundo informático, por ende los programadores de virus eligen escribir dichos códigos para atacar los programas que la gente más usa. Hoy día estos son Outlook, Outlook Express, Internet Explorer, y los sistemas operativos Windows (todos ellos de la empresa Microsoft).

Tanto Outlook como Outlook Express permiten, por su propia concepción de diseño, que los virus se ejecuten con sólo ver el mensaje sin necesidad de abrir archivo adjunto alguno.

Por lo tanto, sólo mediante una estrategia global que tome en cuenta todos los temas mencionados se logrará proteger con éxito lo que es clave y preciado en toda empresa: su información.

7.2 Empresas Afectadas Por Los Virus Informáticos en El Salvador.

Los virus informáticos afectan gravemente a las empresas**.** Un estudio realizado por los laboratorios de investigación ICSA, revela que el número de virus por cada mil ordenadores fue casi estático en 2002, pero los problemas que comportaron llevaron más tiempo y más costes económicos que nunca.

El informe asegura que esto se debe a que los últimos virus tienden a borrar datos y colapsar las redes y los servidores de correo electrónico. El daño que provocan ha obligado a las compañías a instalar software y hardware específicos para combatir los virus y otros programas perjudiciales.

Las cifras señalan que los virus informáticos son tenidos muy en cuenta a la hora de utilizar Internet y el correo electrónico. Según los prestigiosos laboratorios de Investigación ICSA; el pasado año 105 equipos de cada 1000 tuvieron un contacto mensual con un virus. En 2001 la proporción fue de 103 virus mensuales por cada 1000 ordenadores, un gran aumento con respecto a cinco años atrás, con 32 contactos por cada 1000 máquinas.

Según Larry Bridwell, portavoz de ICSA y co-autor del estudio, un descenso en el número de ordenadores afectados sería un dato muy positivo. Sin embargo, ha asegurado también que los virus actuales son mucho más perjudiciales. "Los virus han pasado de ser una molestia a impedir que los usuarios puedan acceder a sus equipos mediante la pérdida de datos y productividad".

Las empresas tardan una media de 23 días en recuperarse de estos fallos de seguridad, (20 días en 2001). Este aumento se debe a que las redes actuales son mucho más complejas. Lleva más tiempo asegurarse de que el virus se ha eliminado de todos los sistemas. Las buenas noticias que recogen el estudio revelan que cada vez más compañías utilizan software antivirus y filtros para el correo electrónico.

Los detalles de esta 8ª encuesta anual sobre permanencia de los virus de ICSA se revelaron en el Information Security Show en Olympia, Londres, que se llevó a cabo del 29 de abril al 1 de mayo de 2003.

El Salvador no es la excepción, muchas empresas en el país han sido afectadas por los daños que causan los virus informáticos, muchas de estas empresas han sido víctimas de daños en los equipos y en los Software, así como pérdida de información, tiempo y dinero. Aunque en la mayor parte de los casos no se tiene un registro oficial de estos daños.

Según el estudio y las encuestas (ver anexos) realizadas, por el autor de este trabajo, se verificó que las empresas encuestadas tuvieron, al menos una vez, pérdidas y daños causados por virus informáticos, daños que se convirtieron en pérdida de información, tiempo y dinero. Cabe mencionar que existen empresas e instituciones que aun desconocen la magnitud de los daños que pueden causar los virus informáticos a sus sistemas de información, aunque la mayoría de las empresas ya han tomado cartas en el asunto y han empleado todas las medidas de seguridad pertinentes para disminuir al máximo los riesgos sobre cualquier ataque de virus informáticos.

Las razones por la cual algunas empresas carecen de medidas de seguridad son:

- Ignorancia sobre el tema
- Costos que implican las medidas de seguridad
- Tiempo
- No han sido afectadas hasta el momento

7.2.1 DAÑOS TÉCNICOS

Dentro los daños técnicos que se pudieron observar en el estudio, prevalecen los daños hacia los sistemas operativos y archivos de Office, así como el bajo rendimiento de los equipos de cómputo, todo esto debido a los efectos que producen los virus informáticos, especialmente los gusanos y troyanos.

Cabe mencionar que en la mayoría de empresas e instituciones del país existe una cultura de seguridad y la mayoría de estos institutos cuenta con medidas de prevención y seguridad como son los antivirus, factor determinante que ha contribuido a que los daños causados por los virus informáticos sean mínimos.

7.2.2 DAÑOS ECONÓMICOS

Los daños a la economía causados por los virus informáticos son variables, en especial a las empresas o instituciones salvadoreñas entrevistadas, todo esto debido a los diferentes efectos que provocaron los gusanos y troyanos, que son los códigos maliciosos más comunes en esta época. Los daños a la economía se dividen en varias partes:

- **Horas extras:** Es el costo en tiempo para la desinfección de las computadoras.
- **HW y/o SW:** Es el costo por la compra de alguna aplicación o equipo en especial que se vio dañado por causa de los virus.

- **Tiempo:** El tiempo perdido o que se deja de producir a raíz de los virus. Este tiempo es el que normalmente se invierte para corregir todos los daños que se presenta en las computadoras o en la Red.

Según el estudio de campo realizado a las empresas salvadoreñas el costo económico que conlleva un ataque de virus informáticos oscila entre $500 y $1000 dólares, todo esto distribuido en horas extras, el tiempo que se deja de producir en las empresas por la desinfección y en medidas de seguridad. El tiempo mínimo que conlleva desinfectar una máquina oscila entre 1 y 2 días por cada máquina en promedio.

Cabe mencionar que la mayoría de empresas entrevistadas invierten dinero en la compra de equipo y aplicaciones de seguridad contra virus de computadoras. Pero existe un detalle muy importante a recalcar y es que según las investigaciones realizadas la mayoría de infecciones a causa de los virus es debido al descuido e ignorancia de los usuarios finales en el momento de manipular los archivos que se envían en los correos electrónicos o manipulación de disquetes infectados. Estos descuidos por parte del personal que utiliza la red o sistema es el causante de un 60% a 80% de las infecciones en las computadoras en la red y lo curioso de esta situación es que el 99% de las empresas entrevistadas no gastan ningún centavo en capacitaciones a los usuarios acerca de la prevención de los virus y como contribuir a reducir al máximo los riesgos de una infección.

Es deber de toda empresa en capacitar al personal que utiliza el equipo de cómputo o la red sobre los riesgos de un ataque de virus informáticos así como en la seguridad y reducción de riesgos sobre los datos e información.

Así como las organizaciones invierten tiempo y dinero en otras capacitaciones necesaria también son indispensables las capacitaciones sobre este tema, ya que lo más importante que pueda poseer una empresa o institución es eso tan preciado que se llama **INFORMACIÓN.**

7.3 TRABAJO DE CAMPO

En la investigación de campo que se realizó se obtuvieron datos muy valiosos e interesantes que nos muestra el nivel de cultura, en cuanto a seguridad informática respecta, en El Salvador. Esta información se obtuvo mediante encuestas (ver anexos) y entrevistas realizadas a diferentes empresas e instituciones del país.

El trabajo de campo utilizando el método por encuesta es muy importante porque nos permite consultar la opinión ciudadana, en este caso empresas e instituciones, y conocer en la realidad concreta cual es la situación problemática que ocasionan los virus informáticos.
Es importante señalar que toda tesis de graduación lleva un trabajo de campo para poder comprobar la teoría desarrollada en los capítulos en la práctica social.

El universo de la muestra tiene las siguientes características:

- Se escogió un total de diez empresas e instituciones.
- Se seleccionaron solo aquellas empresas e instituciones que cuentan con su departamento de informática.
- De ellas se encuestaron solo las que han sido infectadas o atacadas con virus informáticos.
- Se elaboró previamente un cuestionario que contiene las situaciones problemáticas que ocasionan los virus.
- Se encuestaron ocho empresas y dos instituciones educativas haciendo un total de diez visitas.

El Salvador a pesar de ser un país subdesarrollado cuenta con medidas de seguridad de primer nivel, en cuanto a seguridad informática se refiere, así como la tecnología necesaria para la seguridad y prevención de daños a la información. A continuación se muestran en forma grafica los datos obtenidos de las encuestas realizadas en las distintas empresas e instituciones del país.

7.3.1 PROCESAMIENTO DE DATOS

A. La mayor parte de empresas o instituciones que cuentan con un departamento de informática han sido afectadas al menos una vez por los ataques de virus informáticos.

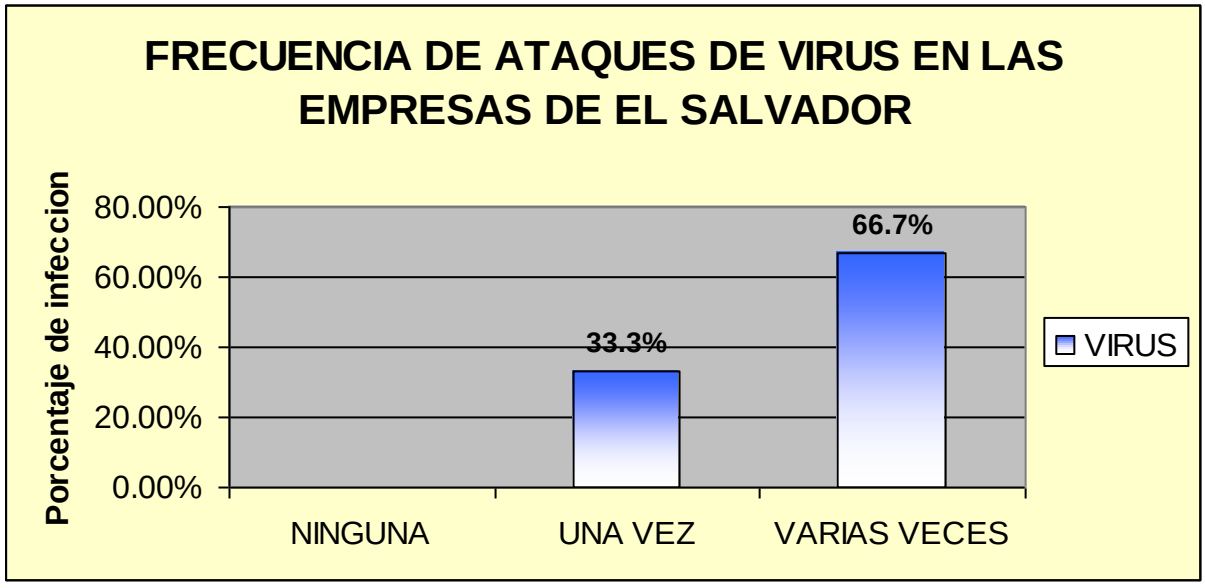


Figura 7.1

B. En la actualidad los códigos maliciosos más comunes son los gusanos y troyanos, son códigos conocidos por muchos como los macrovirus que se distribuyen en la Internet. Estos virus vinieron a reemplazar los virus antiguos que solían atacar el sector de arranque de las máquinas.

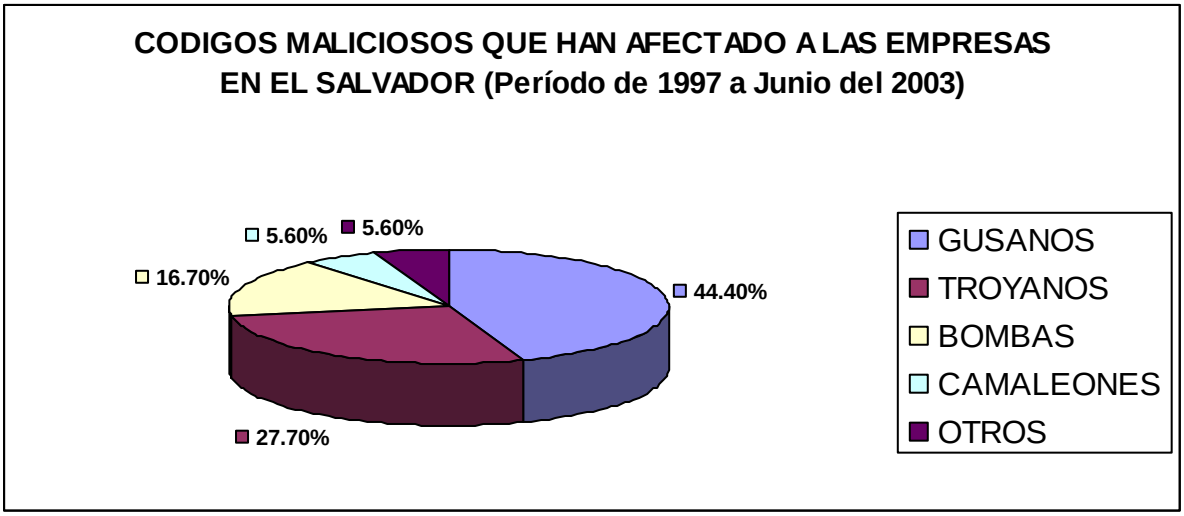


Figura 7.2

C. La mayor parte de empresas encuestadas poseen al menos un antivirus en sus sistemas lo que indica una buena cultura de prevención.

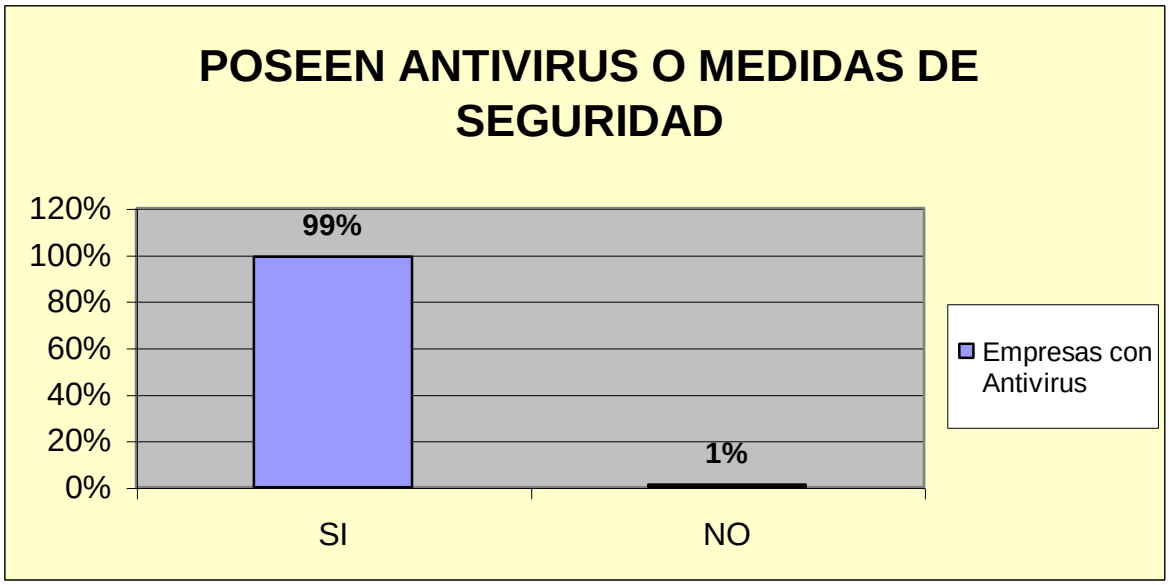


Figura 7.3

D. Todas las empresas e instituciones encuestadas poseen medidas de actualización de los antivirus, lo cual es la medida esencial para la prevención y eliminación de los nuevos virus informáticos.

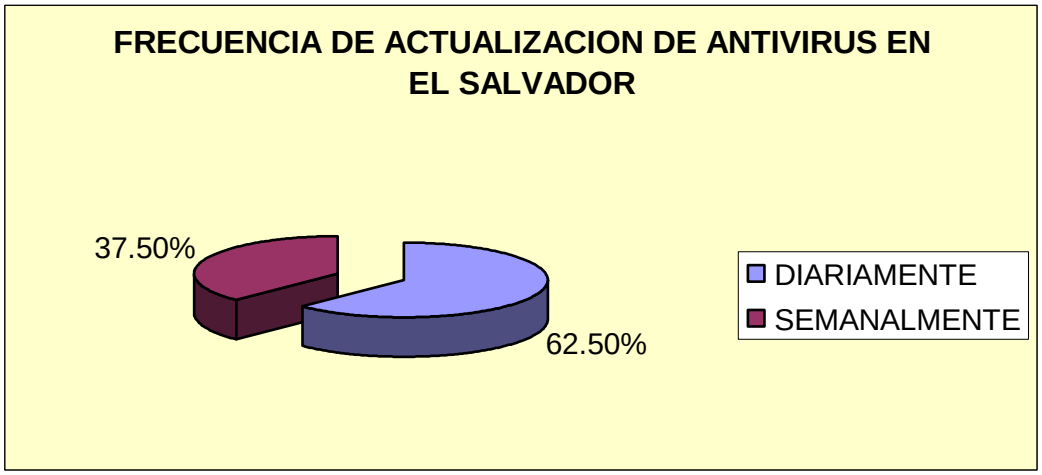


Figura 7.4

E. En la actualidad el país cuenta con una gama de productos de software antivirus en el mercado, los cuales muchos de ellos son utilizados por las diferentes empresas en El Salvador. A continuación se muestran los productos más utilizados.

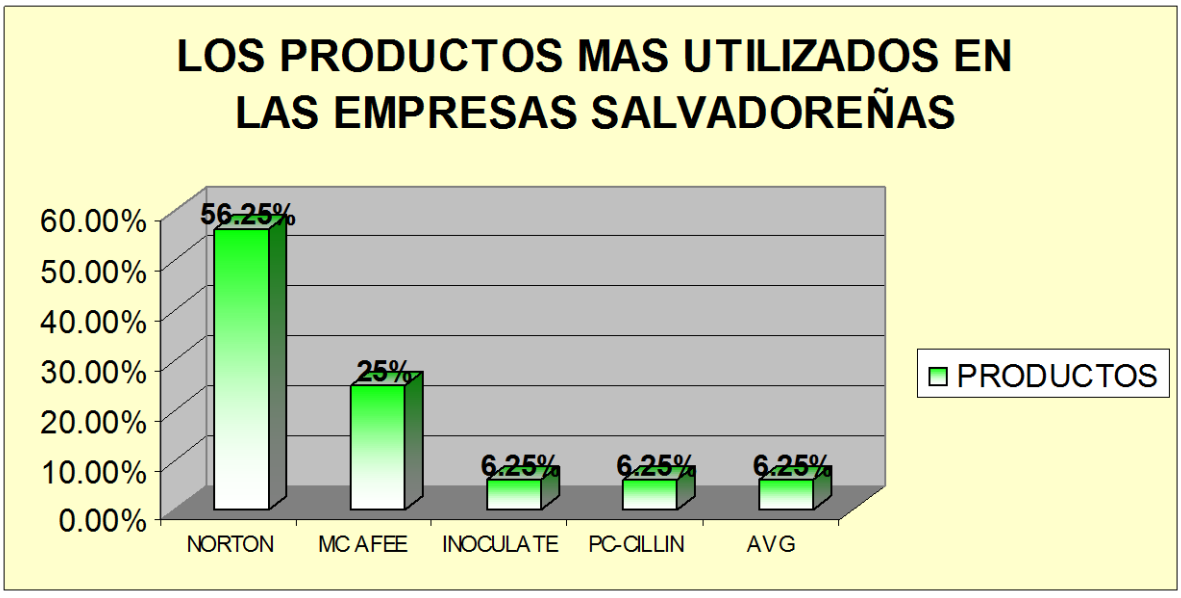


Figura 7.5

Es de mencionar que a medida que todos los usuarios nos vayamos concientizando acerca de las medidas de seguridad y prevención contra los virus, así vamos a reducir al mínimo los riesgos de sufrir un ataque o pérdida de información a causa de cualquier desastre.
El desarrollo de cualquier país depende del grado de cultura y educación que posea, y una meta que tenemos por delante es subir siempre nuestro nivel de educación y cultura, y en particular sobre las medidas de seguridad y prevención de virus.

Con los resultados obtenidos al procesar las encuestas se llegó a las siguientes conclusiones:

a) La mayor parte de las empresas o instituciones que cuentan con un departamento de informática han sido victimas, al menos una vez, de los virus informáticos.

b) En la actualidad los códigos maliciosos más comunes son los gusanos y troyanos, códigos conocidos por muchos como macrovirus que se distribuyen en el Internet.

c) La mayoría de empresas encuestadas poseen al menos un antivirus que los protege de los ataques de virus informáticos.

d) Todas las empresas e instituciones poseen medidas de actualización de los antivirus.

e) En la actualidad el país cuenta con una amplia gama de productos antivirus en el mercado, los cuales muchos de ellos son utilizados por las diferentes empresas en El Salvador.

CAPÍTULO VIII

CONCLUSIONES GENERALES Y GLOSARIO

PREÁMBULO.

INTRODUCCIÓN.

En este capitulo se exponen las aportaciones y criterios, como consecuencia de lo observado durante la realización de la investigación.
Se presentan las conclusiones que a criterio del autor de este trabajo contribuirá en el entendimiento de la investigación realizada.

Como punto final, contiene un glosario el cual ayudará al lector a comprender el significado de las terminologías extrañas que se manejan en el medio.

OBJETIVOS.

- Describir las conclusiones surgidas como consecuencia de la investigación.
- Proporcionar un glosario técnico para la comprensión de términos.

CONCLUSIONES

- La existencia de los virus informáticos es una realidad en el mundo, pero no hay que tratarlo con pánico, mas bien conocer el comportamiento y las medidas de prevención para con estos programas informáticos llamados virus de computadoras.

- Existen varios tipos de software llamados rouge que son programas dañinos para los sistemas informáticos y dentro de este software se encuentran los virus, que es un tipo de software rouge, a su vez existen varios tipos de virus que dependiendo de sus características generan diversos tipos de daños.

- Hay que tener en cuenta que no todo problema con respecto al software de las computadoras se le puede atribuir a los virus informáticos ya que algunos problemas son simplemente causados por descuidos o defectos de hardware o software.

- Cabe mencionar que los software rouge más comunes en la actualidad son los de tipo gusano, ya que los beneficios que presta el Internet son los idóneos para la diseminación de estos, y parece ser que la filosofía de los hackers es el poder infectar la mayor cantidad de maquinas en un mismo momento.

- Según estudios se cree que en la actualidad existen más de 20,000 virus informáticos registrados, y cada año existe un incremento del 175% con respecto a los años anteriores, algunos piensan que surgen entre 200 y 400 virus nuevos cada mes. Por lo que la industria de los antivirus se actualiza periódicamente.

- La mayoría de los gusanos y virus informáticos que circulan en el medio atacan sistemas Windows, algunos expertos creen que este fenómeno se debe a que los programadores de virus buscan dañar los sistemas más populares del mercado y uno de estos es Windows.

- La mayoría de las infecciones (y problemas similares) se producen porque los usuarios tienen muy pocos conocimientos técnicos, además tienen mal configurados sus sistemas y no reciben capacitaciones acerca de cómo reducir los riesgos de un ataque de virus de computadora.

- La mayoría de los antivirus pueden restaurar el archivo infectado a su estado original, aunque no siempre es posible, dado que los virus pueden haber hecho cambios no reversibles. Los antivirus pueden también borrar los archivos infectados u hacer el virus inofensivo.

- Los antivirus funcionan de varias formas: Un método es la comparación del archivo infectado con una muestra de un virus conocido.
  Hay métodos heurísticos que tratan de encontrar modificaciones típicos que producen los virus en los archivos encontrados, y existen programas que graban para cada archivo encontrado en el sistema unos atributos típicos (longitud, suma cíclica). Al revisar el sistema por virus, se vuelven a determinar estos atributos y si no coinciden con los datos guardados con los actuales se considera posiblemente infectado el archivo.

- A pesar de una actualización constante no se puede garantizar una protección completa, ya que una vacuna puede ser desarrollada solo después de descubrir la enfermedad.

- Un antivirus además de protegernos el sistema contra virus, debe permitirle al usuario hacer alguna copia del archivo infectado por si acaso se corrompe en el proceso de limpieza, también la copia es beneficiosa para intentar una segunda limpieza con otro antivirus si la primera falla en lograr su objetivo.

- La principal vía de infección es el correo electrónico y, en concreto, los archivos adjuntos que suelen acompañar a los mensajes. La navegación y la lectura de los correos no reviste mayor riesgo, mientras no se intente descargar un archivo.

- El Backup de archivos permite tener disponible e íntegra la información para cuando sucedan los accidentes. Sin un backup, simplemente, es imposible volver la información al estado anterior al desastre.

- En la actualidad no existe empresa o usuario que no se haya visto afectado por este problema (virus) a pesar de que la mayoría tiene algún tipo de protección antivirus.

- Es recomendable mantener dos antivirus diferentes en los sistemas o servidores, uno para monitorear y otro para scanear archivos y carpetas, ya que un solo antivirus no es suficiente. Además es de suma importancia mantenerlos actualizados.

- Se estima que actualmente el tiempo de propagación de un virus vía Internet a todo el mundo es de menos de tres horas (tiempos que obviamente serán cada vez menores).

- Los virus informáticos causan este año (2003) unas pérdidas económicas por valor de 14.000 millones de euros.

- Las razones por la cual algunas empresas carecen de medidas de seguridad son:
  - *Ignorancia sobre el tema*
  - *Costos que implican las medidas de seguridad*
  - *Tiempo*
  - *No han sido afectadas hasta el momento*

- Según el estudio de campo realizado a las empresas salvadoreñas el costo económico que conlleva un ataque de virus informáticos oscila entre $500 y $1000 dólares.

- El 99% de las empresas Salvadoreñas entrevistadas, no gastan ningún centavo en capacitaciones a los usuarios acerca de la prevención de los virus y como contribuir a reducir al máximo los riesgos de una infección.

- El Salvador a pesar de ser un país subdesarrollado cuenta con medidas de seguridad de primer nivel, en cuanto a seguridad informática se refiere, así como la tecnología necesaria para la seguridad y prevención de daños a la información.

GLOSARIO

Términos Generales	Descripción
Archivos Adjuntos	Termino que significa adjuntar archivos. Usado en los correos electrónicos de Internet.
Archivos Ejecutables	Archivo central del programa, responsable de iniciar el software.
Backup	Termino usado para referirse a las copias de respaldo que se realizan frecuentemente.
BBS	Servicio de tablero de boletines electrónicos. Son servicios de información en línea adaptado a las necesidades de un grupo de usuarios específicos.
Descargar	Termino que significa descarga de archivos, desde un lugar especifico como Internet.
Disco duro	Dispositivo de almacenamiento magnético fijo incluido en la mayor parte de las PC. Es una pila de platillos de aluminio o vidrio, cada uno recubierto con óxido de hierro; está encerrada dentro de una unidad de disco duro.
Encriptar	Proceso de codificar y decodificar datos.
Ensamblador	También llamado ensamblador, es un programa de cómputo que convierte las instrucciones del lenguaje ensamblador en lenguaje de maquina.
Fans	Termino utilizado para referirse a las personas fanáticas.
FAT	Tabla de asignación de archivos. En un disquete o disco duro, tabla de registro creada en el proceso de formateo lógico que registra la ubicación de cada archivo y el estado de cada sector.
Formateo	Proceso de relacionar en forma magnética un disco con una serie de pistas y sectores donde se almacenarán los datos.
Hardware	Componentes físicos de una computadora; incluyen el procesador y los chips de memoria, dispositivos de entrada y salida, cintas, discos, módems y cables.
Host	Conocido también como Anfitrión, se define típicamente en el modelo de computadora centralizada como un sistema informático de tiempo compartido con el que los terminales se comunican y sobre el que descargan el procesamiento.

Términos Generales	Descripción
Intranet	Red interna cuya interfaz y facilidad de acceso siguen el modelo de un sitio Web basado en Internet. Solo se permite a los usuarios internos tener acceso a la información o recursos en la Intranet.
MODEM	Dispositivo de entrada/salida que permite a las computadoras comunicarse a través de líneas telefónicas. Un MODEM convierte los datos digitales de salida en señales analógicas que pueden transmitirse por medio de las líneas telefónicas; además, convierte las señales acústicas entrantes en datos digitales que pueden ser procesados por la computadora; abreviatura de modulador-demodulador.
Pasatiempo	Término utilizado para describir un pasatiempo especifico.
Proxy	Un Proxy Server, es un servidor destinado a almacenar páginas del Internet, gráficos, fotos y archivos que los usuarios usan mucho.
RAM	(Random Access Memory), memoria de acceso aleatorio. Memoria de la computadora.
Sector de Arranque	También llamado sector de arranque. Parte del proceso de formateo lógico. El sector de arranque es una porción de un disco que contiene un programa que se ejecuta cuando la computadora se enciende y determina si el disco tiene los componentes básicos necesarios para ejecutar el sistema operativo con éxito.
Sitio Web	Hoja o página electrónica. Término utilizado para hacer referencia a una hoja electrónica específica.
Software	Colección de instrucciones electrónicas que indica a la CPU llevar a cabo una tarea especifica. El software por lo general reside en el área de almacenamiento.
Software Malicioso	Son programas que se cargan y se llevan a cabo sin que los usuarios les pidan la ejecución. Los virus informáticos son solo una variedad de este tipo de software.
Subrepticiamente	Término que se utiliza para describir acciones realizadas a escondidas o sin autorización.

Términos de Virus y Antivirus	Descripción
BUGS	Simplemente son fragmentos de código implementados que, debido a fallos lógicos internos, dañan el hardware o inutilizan los datos del usuario de forma accidental.
Cortafuego	Método contra la piratería para proteger a las redes. Un nodo de red actúa como una compuerta (gateway), permitiendo el acceso a secciones públicas mientras protege las áreas privadas.
Cracker	Se utiliza para nombrar a los "saboteadores", o en mejor acepción, se refiere a personas talentosas que se entretienen infiltrándose en los sistemas de las grandes empresas que presentan un reto para su inteligencia.
Gusanos	Los gusanos son programas que viajan a través de un sistema informático interconectado, de ordenador en ordenador, sin dañar necesariamente al hardware o al software.
Hackers	Experto en tecnología de computadoras que usa su destreza y técnicas innovadoras para solucionar problemas de cómputo complejos. También se les llama "piratas informáticos".
Linux	Sistema operativo.
Piratas	Es otro término que se utiliza para nombrar a los hackers. Son "asaltantes" informáticos.
Programa Vacuna	Es otra manera de referirse a los Antivirus. Programas que detectan y eliminan virus informáticos.
Tecnoterrorista	Término utilizado para describir las personas que se dedican a sabotear redes informáticas.
Troyanos	Parecen ser aplicaciones útiles, corrientes y molientes, mientras que en realidad contienen una o más órdenes informáticas destructivas.

BIBLIOGRAFÍA

- The Computer Virus Handbook Richard B. Levin.
- http://www.symantec.com
- http://www.monografias.com/trabajos/estudiovirus/estudiovirus.shtml
- http://www.monografias.com/trabajos/estudiovirus/estudiovirus.shtml
- http://www.trendmicro-la.com/vinfo/vinfo.html
- http://www.pandasoftware.es/
- http://www.sophos.com/
- http://www.avpve.com/
- http://www.perantivirus.com/sosvirus/general/histovir.htm
- http://www.uvirtual.cl/prensa/reportajes/virus.htm
- http://www.agilmic.com/cast/Seg/InfGC10.htm
- http://www.ganar.com/edicion/noticia/0,2458,90081,00.html
- http://www.stratos-ad.com/tutoriales/archivos/art%5Bcomplejidad_antivirus%5D.pdf
- http://www.caravantes.com/arti02/sinantiv.htm
- http://www.inei.gob.pe/biblioineipub/bancopub/Inf/Lib5049/cap02.htm
- Prof. Jesús Rivero. Curso de metodología e Investigación. Universidad Central de Venezuela. UCV, 1989, Fotocopiado
- O´QUIST, Prof. Paul. Los Marcos Teóricos. Caracas: Universidad Central de Venezuela (UCV). 1989.

ANEXO

ENCUESTAS DE CAMPO

QUESTIONARIO DE PREVENCION Y SEGURIDAD PARA EMPRESAS

Nombre de Institución o empresa: _____

1. Han sido victimas de virus informáticos?

   Si ☐ No ☐

2. Que tipo de virus han afectado a su empresa?

   Gusanos ☐ Troyanos ☐ Camaleones ☐ Bombas ☐ Otros ☐

3. Que efectos sucedieron?

   _____

   _____

4. Hubieron datos afectados? Si ☐ No ☐
   Explique: _____

   _____

5. Perdieron información? Si ☐ No ☐
   Explique: _____

   _____

6. Hubieron daños en el sistema o en el Hardware? Si ☐ No ☐
   Explique: _____

   _____

7. Cual fue el costo de los daños causados por los virus?

   a. Tiempo _____

   b. HW y SW _____

   c. Económico _____

   d. Horas Extras _____

8. Poseen medidas de seguridad y protección contra virus informáticos?
   Si ☐ No ☐

   Cuales son: _____

   _____

   _____

9. Con que frecuencia han sido victimas de los virus?

   Ninguna ☐ Una vez ☐ Varias veces ☐

10. Que tipos de virus han sido los mas comunes?

    Gusanos ☐ Troyanos ☐ Bombas ☐ Otros ☐

11. Cuanto dinero invierten en seguridad?

    _____

    _____

12. Que productos utilizan?

    _____

    _____

13. Cada cuanto tiempo actualizan sus antivirus?

    _____

    _____