UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE CONTADURÍA Y ADMINISTRACIÓN

IMPACTO DE LOS VIRUS INFORMÁTICOS: MÁS ALLÁ DEL CÓDIGO INFECTADO

SEMINARIO DE INVESTIGACIÓN INFORMÁTICA

QUE PARA OBTENER EL TÍTULO DE:

LICENCIADO EN INFORMÁTICA

PRESENTA:

Sandra Salgado Marín

ASESOR DEL SEMINARIO:

Dra. Judith Zubieta García

México, D.F. 1995

A la memoria
de los caídos
en la lucha contra los virus...

ÍNDICE

I. INTRODUCCIÓN

Así como el desarrollo tecnológico brindó las herramientas necesarias para crear computadoras y programas que le facilitaran el trabajo al ser humano invadiendo todas las áreas del conocimiento, llegó una contraparte en donde se genera una guerra aparentemente eterna entre los creadores de virus y los creadores de antivirus. Aunque existen muchos mitos, no podemos pensar como cuando se inventó el microscopio y se descubrieron los primeros microbios, en donde el común de la gente creía que eran actos de brujería o maldiciones y que no se podían evitar, o que era chantaje de los comerciantes para vender productos medicinales.

Lo cierto es que cada vez los algoritmos de virus son más sofisticados y esto sólo se verá delimitado por la imaginación del ser humano.

Los virus informáticos son un hecho y por esta razón el presente trabajo pretende brindar una ayuda para aquellos usuarios, principalmente de computadoras PC, en cuanto a definir el concepto de virus dentro del ámbito de la Informática, hacer una clasificación, conocer cómo actúan, recomendar medidas de seguridad, saber qué efectos pueden tener dentro de un sistema, y qué hay del marco jurídico.

II. ANTECEDENTES

II.1 Concepto de virus informáticos

Los virus informáticos son programas, es decir un conjunto de instrucciones codificadas, que indican a las computadoras qué acciones se deben ejecutar. Por lo tanto, pueden realizar todas las operaciones que sean soportadas por el sistema operativo de la máquina infectada o a infectar.

La programación fue concebida originalmente con el objeto de facilitar el trabajo humano; sin embargo, este concepto se ha tornado totalmente opuesto a los fines y usos de programas denominados "virus informáticos", ya que éstos pueden reformatear discos tanto flexibles como duros, copiar, renombrar y borrar archivos, reproducirse con nueva información de configuración, modificar fechas y características de archivos, llamar a otras computadoras para telecargar archivos, etcétera[1]. Todo esto sin que el usuario lo haya solicitado y, peor aún, sin tener conocimiento previo. Por ejemplo, mientras un procesador de textos cuenta con una opción para guardar automáticamente un documento cada determinado tiempo, y evitar así la pérdida del mismo, un virus puede estar borrando información sin el consentimiento del usuario.

---

[1] Levin, B. Richard. Virus Informáticos, editorial Mc Graw Hill, Madrid, España, 1992, pág. 6.

Un virus se compone de dos partes fundamentalmente: un aparato reproductor que garantiza su propagación y un aparato ejecutor, responsable de la acción destructiva.

La mayoría de los virus de reciente aparición no son originales, sino modificaciones, generalmente ligeras, de los anteriormente existentes.

Características de un virus

Aunque en el siguiente capítulo se verá que existen varios tipos de virus, estos poseen algunas semejanzas en su forma de actuar, por lo que a continuación veremos sus principales características:

- Un virus informático es ejecutable, esto no quiere decir que el virus sea propiamente el que se ejecuta, sino que esta propiedad se le atribuye, ya que al instalarse en un archivo ejecutable, podrá lograr sus objetivos destructivos.

- Es autoduplicable, esto significa que infecta a otros programas, independientemente de la voluntad del usuario. Para esto cuenta con un "periodo de incubación", es decir, tiempo durante el cual aprovecha para infectar el mayor número de programas posibles y, una vez que termina este periodo, comienza realmente su acción dañina.

- Realiza accesos a disco sin que el usuario lo ordene, es decir, efectúa lecturas y escrituras. Como cualquier otro programa, un virus sólo está activo cuando está cargado en la memoria de la computadora.

- La acción de un virus nunca es benigna, aún cuando no destruya información y sólo emita un breve mensaje, esto distrae al usuario y ocupa memoria que podría ser utilizada a voluntad del usuario.

- Generalmente pasa desapercibido ya que su tamaño es muy pequeño. Desafortunadamente, el tamaño del virus no se corresponde con el del daño que causa cuando entra en acción, pero no por esto es menos perjudicial.

Ciclo de vida de un virus

1. *Infección*: el virus llega a la computadora por medio de un programa contaminado que se encuentra en un disco flexible, o bien vía módem o vía red, sin afectar el funcionamiento normal de los programas que infecta, por lo que será difícil percatarse de su presencia inmediatamente.

2. *Latencia*: el virus toma el control sobre el sistema operativo y comienza a infectar los archivos para los que fue creado, de tal suerte que si llegamos a copiar un archivo infectado y lo introducimos en otra máquina, el virus se propagará.

3. *Activación*: Al cumplirse una determinada condición, por ejemplo una cierta fecha, el virus se activará y comenzará su acción destructiva[2].

[2] Nombela, J. J, J. Del Pino G. y L.M. Del Pino G. Virus Informático, 2ª edición, Editorial Paraninfo, Madrid, España, 1991, pág. 23.

Métodos de infección

Cada virus tiene su forma especial de tomar el control de los archivos normales, así que lo importante es que los usuarios comprendan y practiquen las medidas de seguridad.

Existen algunos tipos generales de infección utilizados por los virus para adueñarse del control de los archivos ejecutables:

1. *Añadidura*: es cuando los virus se posicionan al final de los archivos ejecutables.

2. *Inserción*: Se da cuando los virus se sitúan dentro de los archivos ejecutables de destino. Desde el punto de vista de su diseño y desarrollo, estos virus son más difíciles de crear porque el tamaño de su código se tiene que mantener al mínimo para que no sea detectado fácilmente, y por esta razón también se reducen sus funciones.

3. *Reorientación*: es cuando los virus se introducen en alguna posición específica del disco, por ejemplo en sectores dañados o inutilizables o en archivos ocultos. Estos virus ocupan cualquiera de las dos técnicas anteriores y al activarse le dan otra orientación al flujo del programa. Además, se hacen residentes en memoria, y su código puede ser comprimido hasta dos bytes (mínimos necesarios para hacer una interrupción al MS-DOS).

4. *Sustitución*: Estos virus no infectan realmente a los archivos ejecutables, sino más bien al sistema en el que residen. Se escribe sobre los archivos destinatarios; es decir, son borrados y sustituidos por código vírico[3], en lugar de añadir o insertar.

Por esta razón, la secuencia no cambia y el virus se puede detectar casi inmediatamente después de que se haya activado. Pese a esto son muy dañinos ya que empiezan a destruir los datos desde la primera ejecución[4].

Formas de contagio

"Un virus biológico se transmite sobre todo por contacto de persona a persona o a través del aire, y hasta el momento son las vacunas las que mejor nos protegen de ellos"[5].

Cuando los usuarios de sistemas infectados por virus comparten archivos con otros usuarios, copiando, intercambiando discos o usando enlaces de telecomunicación, hay muchas posibilidades de que una copia del virus se intercale en al menos uno de los archivos compartidos. Cuando los archivos compartidos son ejecutados por sus nuevos propietarios, los virus implantados se activan instantáneamente

[3] Código vírico: conjunto de instrucciones que indican a una computadora lo que debe realizar, sin que el usuario se dé cuenta. Es sinónimo de virus informático.

[4] Levin, B. Richard. Op. Cit., págs. 31-35.

[5] Greer, William. Cazadores de virus, Editorial Toray, Barcelona, España, 1966, pág. xiii

y quedan en libertad. El ciclo de vida del virus continúa sin disminución hasta que los usuarios descubran la actividad y tomen algunas medidas en relación con sus archivos infectados.

Como cualquier otro programa, cada virus tiene su propio modo de hacer las cosas y sus propias características. Algunos virus son actualizados periódicamente para ir por delante de nuevas medidas antivirus.

Es innecesario que los usuarios se preocupen por detalles referentes a las muchas variedades de código vírico que circulan actualmente; este trabajo es mejor dejárselo a los expertos en virus.

No importa la plataforma que se esté utilizando, lo principal es darse cuenta que todas las computadoras, independientemente de su fabricante, son susceptibles de contraer infecciones víricas. Cada virus informático se crea para actuar bajo uno y sólo un sistema operativo, del mismo modo si un programa fue diseñado para Apple Macintosh, no se ejecutará en una PC IBM y viceversa. Incluso si se transfiriera un virus de la clase PC IBM a sistemas Macintosh, éstos se limitarían a las instalaciones dedicadas a IBM.

Un virus informático no se produce por casualidad; alguien tiene que emplear el tiempo necesario para crearlo. De hecho, debe existir un análisis y el código tiene que ser editado, compilado, probado y depurado. Después de que las estructuras funcionen perfectamente, el

programador tiene que crear una cubierta convincente que engañe a los usuarios para que introduzcan este programa a sus computadoras.

II.2 Origen de los virus informáticos

Gonzalo Ferreyra, en su libro "Virus en las computadoras", menciona al Dr. Fred Cohen como "El padre de los virus informáticos", ya que en 1983 el Dr. Cohen realizó un experimento en la Universidad del Sur de California, presentando el primer virus residente en una PC.

También habla de que en 1986 se difunde ampliamente un virus que fue desarrollado en Paquistán por dos hermanos que comerciaban computadoras y software. Y es en 1987 cuando los expertos de IBM tienen que diseñar un programa que desinfecte su sistema de correo interno. Este fue el primer programa antivirus desarrollado.

Aunque no existe formalmente una fecha o suceso determinado que marque el inicio de los virus informáticos, se puede afirmar que estos son descendientes de algunas especies como:

- El programa conejo
- Los gusanos
- Las bombas lógicas
- Los caballos de Troya

A continuación se presenta una breve descripción de cada uno de ellos.

Programa conejo: Se cree que un estudiante de alguna universidad estadounidense mostró su descontento a través de la creación de un programa que se autorreproducía hasta llegar a saturar el sistema; esto, a causa de la prioridad casi nula que les daban a los estudiantes de aquella Institución en la ejecución de sus actividades de cómputo. Este programa no hacía otra cosa más que reproducirse e instalarse en la cola de espera; las copias que generaba, a su vez, se ponían en la cola de espera.

Hackers y Gusanos: Un hacker es un experto de la Informática que se dedica a buscar el acceso a bancos de datos con el objeto de divertirse o bien, de obtener utilidades vendiendo a otras personas la información que obtiene. Sus únicas herramientas son un teléfono, una computadora y un módem.

Los programas que crean para el logro de sus objetivos se llaman programas gusano, los cuales realizan las siguientes actividades: introducirse en una computadora, explorar el sistema y permitir la exploración de archivos.

Aun cuando un hacker logra accesos a cierta información de una manera ilegal, regularmente no persigue fines destructivos. El gusano es autónomo; es decir, se reproduce a sí mismo como un programa independiente, en lugar de infectar y ocultarse en otros programas, como lo hacen ahora los virus. Los gusanos prevalecen más en los grandes sistemas multitareas que en una PC.

Bombas lógicas: Una bomba lógica pretende destruir información al cumplirse una determinada condición, generalmente una fecha o comando específicos. Mientras éstos no se den, el programa se mantendrá inactivo, a diferencia de los virus actuales, una bomba lógica no se reproduce ni se propaga.

Caballos de Troya: Es un programa que aparenta ser útil pero realmente su labor es destructiva. Afortunadamente, éstos no pueden autorreproducirse y una vez que se ejecuta el programa que lo contiene, es fácil detectarlo. Estos programas fueron los que dieron propiamente origen a los actuales virus informáticos[6].

[6] Nombela, J. J, et al. Op. Cit., págs. 15-21.

III. CLASIFICACIÓN DE LOS VIRUS

"La mayoría de los virus son muy exigentes en la elección del ser vivo que van a infectar y además saben en qué células de ese ser deben continuar su vida"[7].

Los virus informáticos se ubican en regiones a las que se puede acceder fácilmente desde el sistema operativo, sin despertar la atención del usuario; además, deben ser lugares que puedan encontrarse en todos los sistemas para que puedan contaminar la mayor cantidad de equipos. Todas las computadoras que trabajan con el sistema operativo MS-DOS poseen los siguientes archivos:

- IO.SYS
- MSDOS.SYS
- COMMAND.COM

Además, los discos, tanto duros como flexibles, poseen un área denominada sector de arranque (boot sector). Hay virus residentes en memoria que permanecen activos en todo momento; virus de sector de arranque que se almacenan en el registro de arranque de un disco y son ejecutados sólo cuando el disco se carga; virus predadores que buscan y destruyen archivos concretos; y, virus genéricos, que se reproducen en cada archivo ejecutable que encuentran.

---

[7] Greer, William. Op. Cit., pág. xiii

A continuación se muestra una clasificación de virus de acuerdo a la parte que infectan:[8]

III.1. De acuerdo a la parte que infectan

1. Virus del sector de arranque

Al darle formato a un disco, el sistema operativo reserva el sector cero en la pista cero como el sector de arranque (Boot sector), donde se aloja un pequeño programa escrito en lenguaje de máquina; dicho programa toma el control del sistema operativo desde que ésta se enciende, y se encarga de buscar y cargar los archivos del sistema operativo. Estos archivos ordenan a la computadora cómo realizar sus operaciones rutinarias, desde las tareas de gestión de bajo nivel, tales como el manejo de funciones básicas de entrada/salida, hasta tareas de nivel superior, como dirigir la copia de archivos y borrar solicitudes recibidas de las aplicaciones del usuario final. Estos servicios se solicitan por medio del sistema operativo, el cual los efectúa y luego informa a la aplicación correspondiente del éxito o fracaso de las acciones.

Los virus informáticos que se alojan en esta área son llamados "Contaminadores del Sector de Arranque". Por lo tanto, son cargados inmediatamente al arrancar el sistema, cuando normalmente se cargan los archivos del sistema operativo. Antes de cargarse el procesador de las órdenes, los contaminadores de sector de arranque asumen el

[8] Levin, Richard B. Op. Cit., pág. 23.

control total, por lo que pueden permanecer residentes y activos, lo cual implica el riesgo de perder información en cualquier momento: pueden contaminar discos no infectados; pueden controlar todas las acciones de los usuarios, manteniendo el dominio sobre las medidas de software antivirus; pueden cambiar listados de directorios para mostrar tamaños incorrectos de los archivos cuando en realidad estos han cambiado a consecuencia del código vírico añadido. Este tipo de virus puede presentar un tamaño falso del archivo ante los programas de software antivirus, los cuales comparan los tamaños de archivos infectados con copias buenas que se conocen.

2. Virus del procesador de órdenes.

Los archivos DOS pueden ser esencialmente divididos en dos amplias categorías: archivos de apoyo al sistema de bajo nivel y archivos de programas de interfase de usuario de alto nivel.

Los archivos ocultos del sistema operativo son llamados IO.SYS y MSDOS.SYS, los cuales no pueden ser ejecutados directamente por el usuario, ni pueden ser fácilmente borrados, renombrados, copiados o trasladados sin la ayuda de potentes programas de utilidad, diseñados concretamente para modificar estos archivos.

La interfase básica del usuario o programas centrales del procesador de órdenes están contenidos en un archivo llamado COMMAND.COM, el cual se carga después de que una computadora haya terminado su proceso de arranque. Esto significa que los dos archivos de arranque

IO.SYS y MSDOS.SYS ya han sido cargados y ejecutados, y que la computadora está preparada para empezar a actuar sobre las órdenes del usuario. Una vez que aparece el mensaje indicador A> ó C>, el COMMAND.COM ha sido cargado, está activo y listo para aceptar la entrada del usuario Cuando las órdenes son introducidas mediante el teclado, el COMMAND.COM las interpreta e intenta determinar exactamente qué es lo que el usuario pide a la computadora que haga.

Si el COMMAND.COM no puede interpretar lo que desean los usuarios, es presentado el mensaje <<Orden o nombre de archivo incorrecto>>; en caso contrario, se realizan las funciones requeridas y se vuelve a presentar el mensaje indicador (A> ó C>) y espera instrucciones adicionales.

Como muchas órdenes que se introducen pasan por el COMMAND.COM, los contaminadores de procesadores de órdenes pueden explorar las oportunidades para esconderse tras accesos normales de disco mientras se ejecutan órdenes internas COMMAND.COM por ejemplo: DIR o COPY.

Antes de que las órdenes DIR sean en realidad procesadas, los contaminadores del procesador de órdenes se introducen, buscan e 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 aquéllas de las

no infectadas. Pese a ello, la mayoría de los usuarios no nota la diferencia.

Estos dos tipos de virus son cargados al momento del arranque, permanecen residentes a lo largo de las sesiones de cálculo y tienen la capacidad de supervisar y controlar casi toda la interacción entre usuarios y máquinas.

La diferencia básica entre estos dos es que los contaminadores de sector de arranque se instalan primero, a nivel mucho más bajo que los contaminadores de procesos de órdenes, por lo que los últimos tienen menor acceso a las interacciones del sistema.

Estos dos tipos de virus se eliminan volviendo a instalar el sistema y los archivos procesadores de órdenes.

3. Virus de propósito general

Generalmente no pueden contaminar archivos de bajo nivel de sistema operativo. Los contaminadores de propósito general utilizan el mismo camino que los dos anteriores, pero en vez de buscar archivos de bajo nivel o de atacar a los procesadores de órdenes, infectan cualquier archivo ejecutable (.COM o .EXE). Lo mismo pueden infectar el comando DISKCOPY que una Hoja de cálculo y convertirlos en transmisores de virus.

Sobresalen por saturar totalmente el sistema, por lo que son uno de los tipos de virus de propagación más rápida, se mueven velozmente entre los archivos, infectándolos fácilmente. Son más difíciles de erradicar que los dos anteriores.

4. Virus con múltiples propósitos

Están diseñados para integrar las características más activas de los tres tipos anteriores. Pueden infectar inicialmente los sectores de arranque, procesadores de órdenes o ambos. Logran un nivel de supervivencia más alto y se reproducen con mayor facilidad.

Una vez que obtienen el control, durante los tiempos de ejecución, van en busca de marcas víricas. Los bytes codificados reveladores que identifican marcas víricas continúan con la infección de archivos no marcados. Cuando se encuentran estas marcas, los contaminadores avanzan para encontrar otros archivos ejecutables a infectar. Sin embargo, en ocasiones los virus infectarán igualmente archivos con marcas víricas.

5. Contaminadores de archivos específicos

Atacan a un número fijo o un tipo fijo de archivo. Como norma, son escritos por alguien que tiene "cuentas pendientes", quizá un exempleado o alguna persona o compañía con la que el programador ha tenido problemas. Están programados para buscar y destruir los archivos y algunas de sus propiedades específicas.

Se introducen en los sistemas no infectados. El infectar archivos individuales faculta a los contaminadores de archivos específicos para entrar en directorios, realizar búsquedas rápidas y salirse cuando las búsquedas no tienen éxito. Los pequeños retrasos que esto ocasiona, generalmente de uno o dos segundos, no serán advertidos por el usuario.

El infectar archivos no relacionados también proporciona oportunidades para permanecer en los sistemas mucho tiempo después de que los archivos de destino hayan sido destruidos. Esto sucede puesto que los archivos dañados con certeza serán puestos otra vez en el sistema y necesitarán ser destruidos una vez más. Los archivos no relacionados disimulan el daño hecho a los archivos destinatarios. Puede tratarse de una destrucción total o parcial, progresiva con el transcurso del tiempo.

6. Virus 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 permanecen cargados y activos en la memoria de la computadora cuando se ejecutan. Sin embargo, al contrario de las legítimas utilidades TSR (Terminate and Stay Resident), que son programas que una vez cargados y ejecutados por primera vez, permanecen en memoria para ser ejecutados varias veces, los virus residentes en memoria no tienen ninguna ejecución rápida para que los usuarios los llamen; ellos atacan inmediatamente al cargar el sistema y permanecen activos a lo largo de las sesiones de cálculo.

Puesto que están siempre cargados y activos, pueden interferir en la mayoría de las actividades informáticas. Las órdenes de teclado pueden ser interceptadas, la salida de pantalla puede ser falseada y los datos de disco pueden ser controlados e incluso modificados. Además, pueden inspeccionar continuamente los sistemas, en busca de archivos no infectados e infectarlos tranquilamente durante operaciones informáticas normales.

III.2 De acuerdo a su nombre

Existen alrededor de 3 mil virus diferentes en todo el mundo, que fueron generados para que actúen bajo el ambiente MS-DOS. Cada uno de ellos posee un nombre y en ocasiones también uno o varios *alias*. A continuación se muestra otra clasificación de los virus más conocidos en nuestro país, donde también se menciona el lugar y fecha de aparición y una breve descripción de lo que el virus realiza:

Brain: De origen pakistaní, fue descubierto en 1986, fue elaborado por dos hermanos pakistaníes (Basit y Amjads) para evitar las copias ilegales de sus programas. También se conoce bajo los nombres de *Pakistaní*, *Shoe_Virus*, *Ashar*, *UIUC*, etcétera.

Cambia la etiqueta de volumen de los discos infectados por "(c) Brain" o "(c) Ashar". Se instala en el sector de arranque de los discos flexibles, ocupando adicionalmente tres clusters que marcará como defectuosos y a donde moverá el sector de arranque original. Este virus

sólo infectaba discos de 360 Kb, pero una posterior modificación infecta también el disco duro. En memoria se instala en los últimos 7 Kb.[9]

Cascade: de origen alemán, surge en el año de 1987; también es denominado *Fall*, *Otoño*, *Letras caídas*, *Tears*, *1701* y *1704*. Originalmente, este virus era un caballo de Troya, disfrazado como un programa que se suponía que apagaba la luz de NUM-LOCK cuando se arrancaba el sistema. En vez de eso, el caballo de Troya hacía que todos los caracteres de la pantalla "cayeran" en una pila en la parte inferior de la pantalla. A finales de 1987, el caballo de Troya fue transformado por alguien en un virus residente en memoria. Mientras que el virus original tenía una longitud de 1701 bytes y contaminaba tanto PC's IBM verdaderos como compatibles, existe una variación que es 3 bytes más grande que el virus original y no contamina PC's IBM verdaderos. Ambos virus son funcionalmente idénticos en todo lo demás.

Ambos utilizan un algoritmo de codificación para evitar la detección y para complicar cualquier intento de análisis del virus. Los mecanismos de activación están basados en un sofisticado algoritmo de aleatoriedad

[9] Nombela, J. J. et al. Op. Cit., pág. 75.

que incorpora comprobaciones de la máquina, tipos de monitor, presencia o ausencia de una tarjeta de control y la hora o estación del año.

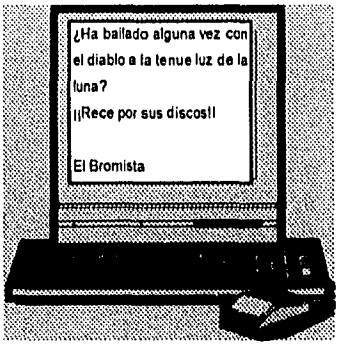
Los virus se archivaban en cualquier máquina con un monitor CGA o VGA en los meses de septiembre, octubre, noviembre o diciembre en los años 1980 y 1988.

Sus variantes son *1701-B* que puede activarse en el otoño de cualquier año y el *1704-D* que funciona igual que el *1704*, excepto que la selección de IBM ha sido inutilizada de manera que pueda contaminar PC's IBM verdaderos. Otra variante es *el Cascade-B*, también conocido como *Blackjack* ó *1704-B*, que es muy similar al *Cascade*, excepto que la presentación de cascada ha sido reemplazada por un arranque del sistema que tendrá lugar a intervalos de tiempo aleatorios después que se active el virus. Una variante de este último es el *1704-C*, éste puede activarse en diciembre de cualquier año.[10]

Devil's Dance: también conocido como *Mejicano*, tiene una longitud de 941 bytes y fue encontrado en diciembre de 1989 en la ciudad de México. Este virus aumenta el tamaño de los archivos .COM; contamina un archivo múltiples veces hasta que el archivo se hace demasiado grande para caber en la memoria disponible del sistema. Una vez que se ha ejecutado un programa contaminado, cualquier rearranque en

[10]Levin, Richard B. Op. Cit., págs. 327 y 328.

caliente subsiguiente (Ctrl-Alt-Del) provocará que se presente este mensaje:



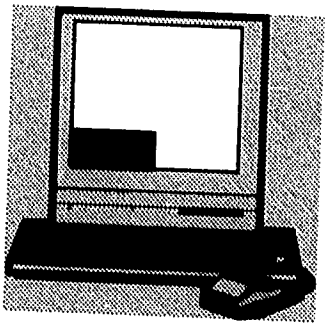
Después de las primeras 2 mil pulsaciones, el virus empieza a cambiar los colores de cualquier texto, después de las primeras 5 mil pulsaciones, borra la primera copia de la FAT. En este momento, cuando se reinicializa el sistema, despliega el mensaje anterior y destruye nuevamente la primera copia de la FAT y luego permite que continúe el arranque.[11]

Jerusalén: también llamado *Viernes 13*, *Israelíes*, *PLO*, *Rusia*, etcétera. Se cree que es una forma de inconformidad política por parte de la Organización para la Liberación de Palestina (OLP) y fue descubierto en la Universidad Hebrea de Jerusalén en diciembre de 1987. Fue escrito originalmente en Italia, como modificación del virus *Suriv 3*, y lanzado a Israel como arma de los terroristas. El plan era que el virus se difundiera hasta el día viernes 13 de mayo de 1988, en el aniversario 40 de la declaración de independencia del estado de Israel.

Cuando se ejecuta un programa infectado, el virus se carga en la memoria como un programa residente, el sistema se hace más lento y

[11] Levin, Richard B. Op. Cit., Pág. 334.

aparece una "ventana negra" o "caja negra" en la esquina inferior izquierda de la pantalla y cuando se recorre la pantalla, también se recorre la ventana negra. Una vez que el virus está activo dentro de la memoria, infecta los archivos .COM, .EXE, .SYS, .BIN, .PIF y algunos archivos overlay cuando ellos son ejecutados. Este virus no infecta al archivo COMMAND.COM.



Un archivo infectado contendrá la cadena de caracteres "sUMsDos" o una variante que depende del tipo de virus Jerusalén. Cualquier programa que intente correr el viernes 13, será destruido.[12]

Miguel Angel: Este virus se activó en el cumpleaños 517 del artista renacentista Miguel Angel Buonarotti, el 6 de marzo de 1992, en los Estados Unidos.

El 5 de marzo de 1992, los periódicos estaban llenos de predicciones de desastres, hablaban de la muchedumbre que clamaba en las tiendas de software por las últimas versiones de los antivirus. Según las estadísticas, tan sólo 2 mil computadoras fueron infectadas en todo el mundo. La República de Sudáfrica fue la más afectada, con cerca de mil PC's infectadas.

[12] Nombela, J. J, et al. Op. Cit., pág. 73.

Cuando este virus ataca, elimina la partición del disco duro.

Algunos síntomas de este virus son que al encender la máquina, la luz de la unidad de disco duro permanece activa, como si se bloqueara, y si se apaga y se vuelve a encender la máquina, aparece el siguiente mensaje.

La única forma en que se puede utilizar la computadora es haciendo otra partición y volver a dar formato al disco duro, los programas deben ser restaurados a partir de un respaldo.[13]

Natas: algunos síntomas de este virus son que la memoria convencional normalmente reportada de 640kb la reduce a 633kb cuando el virus está en memoria. Puede incrementar en 100 años la fecha de los archivos, o puede presentar el siguiente mensaje.

Daña al azar sectores del disco duro, por lo que se pierde información, además de infectar la

[13] Norton, Peter y Nielsen, Paul. Norton Antivirus. Editorial Prentice Hall, México, 1993, págs. 30, 31, 79, 80 y 81.

FAT y el sector de arranque lo que le permite tomar el control de la máquina desde que se enciende. También infecta los archivos EXE, COM, OVL, SYS y 386; incluso infecta el archivo COMMAND.COM.

Cabe mencionar que el sector de arranque de los discos flexibles se puede infectar con sólo pedir el directorio desde la máquina infectada.

El Natas es un virus mutante, lo que significa que nunca se encuentra la misma secuencia de bytes en diferentes archivos infectados, lo cual dificulta su detección por medio de secuencias ya conocidas.

Este virus incrementa 4744 bytes la longitud de los archivos que infecta pero si el virus está en memoria, ese incremento no se puede observar al pedir un directorio del disco con la instrucción DIR del DOS, debido a que dicho virus cuenta con poderosas técnicas de ocultamiento.

Los sistemas para ocultarse con los que cuenta el virus Natas son tan poderosos que pueden burlar muchas vacunas, esto es porque cuando la vacuna intenta leer el programa infectado para analizarlo, el virus lo intercepta y le muestra a la vacuna el archivo desinfectado.[14]

El Natas y el Monkey son dos virus comunes que por sí mismos son relativamente inofensivos, cuando son detectados a tiempo y se cuenta

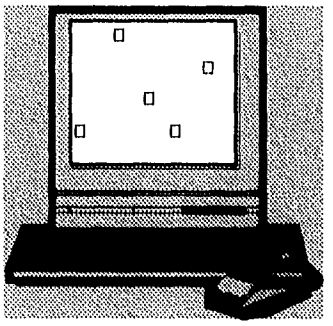
[14] Rodríguez Cárdenas, Mario. Sangre virus y rescate archivos perdidos, Editorial Rócar, México, 1995, págs. 177, 178, 179 y 180.

con el antivirus adecuado, pero en el momento que concurren a infectar un mismo sistema, las consecuencias son graves.

El Monkey toma el sector maestro de arranque del disco (MBR), lo escribe en algún otro lado del disco duro y se instala él mismo en el sitio original del MBR, cuando el usuario intenta accesar al MBR, el Monkey le presenta el MBR original haciéndole creer que todo está en orden.

El Natas procede a infectar lo que él asume que es el MBR, quedando destruido el virus Monkey y con ello, el MBR. En este punto, ya no hay Monkey, ni Natas, ni MBR, ni antivirus capaz de recuperar el MBR original.[15]

Ping Pong: Tiene algunos alias como *Pelotita saltarina*, *Italiano*, *Vera Cruz*, etcétera; fue presentado por primera vez en Italia, en marzo de 1988. La versión original *del Ping Pong* sólo contamina el sector de arranque de discos flexibles. Cuando se activa hace una base aleatoria con el caracter 7 del código ASCII (□), el cual aparece rebotando en la pantalla; este efecto se produce si se realiza algún acceso al disco, exactamente cuando se cumple el minuto 0 ó 30 de cualquier hora y sólo se puede detener reinicializando el



[15] Boletín Técnico ITASA, Monterrey, N.L, México, marzo de 1995, pág. 2.

sistema, no produce otro daño. Una vez que el virus está en memoria, se transmitirá a todos los discos que se vayan utilizando en el primer acceso que se realice a estos (lectura), por ejemplo ejecutando un simple DIR.

Ping Pong-B: También recibe el nombre de *Arranque*, es una variante del Ping Pong, la diferencia más importante es que el *Ping Pong-B* puede contaminar discos duros al igual que discos flexibles.[16]

Stoned: También se conoce como *New Zeland*, fue descubierto a principios de 1988 en Nueva Zelanda; se activa después de la octava carga inicial con el mismo disco infectado, presenta el mensaje:

Al estar contaminada una computadora con este virus, se puede infectar cualquier disco que se introduzca con sólo pedir que se visualice el directorio. De inmediato reemplaza el programa de carga inicial (Boot

[16] Levin, Richard B. Op. Cit. Pág. 349.

program) por su propio código en el sector 0 y envía el programa de carga al sector 11. Originalmente este virus no atacaba al disco duro, pero con la aparición de sus variantes: *New Zeland-B* ya ataca a los discos duros y *New Zeland-C* que además ya no produce el mensaje por lo que se hace muy difícil de detectar.[17]

[17] Ferreyra Cortés, Gonzalo. Op. Cit., págs. 7-17, 7-18, 8-10 y 8-11.

III.3 Virus en otros sistemas operativos

Aunque el acceso a otros sistemas operativos es más restringido que para el MS-DOS o el System de Macintosh, cabe la posibilidad de que alguien se ocupe en la creación de un virus para sistemas operativos no tan comunes como OS/2 o UNIX. Sin embargo, uno de los objetivos de los virus informáticos es propagarse, por lo que si se genera éste, lo más probable es que dañe información muy específica.

1. Virus en Macintosh

En Mac existen los virus y los caballos de Troya, sin embargo estos no implican un gran problema como para PC, debido a que su participación en el mercado es mucho menor que el DOS. De todas formas hay gente que se dedica a crear virus bajo esta plataforma, así que el riesgo sigue latente para los usuarios de Macintosh.

A continuación se muestra una lista de los más conocidos:[18]

Aladin: hizo su aparición en diciembre de 1987 en Hamburgo, Alemania. Se empezó a distribuir en un archivo creado por la compañía Aladin Producer Proficomp, su objetivo específico era dañar la versión pirata del software Aladin. Su tamaño varía entre 3312 y 3822 bytes.

[18] Levin, Richard B. Op. Cit., págs. 369-373

ANTI: fue descubierto en febrero de 1989, en París. Este virus se propaga a todas las aplicaciones cuyo código empieza con <<JSR>>, la mayoría de los compiladores crean este tipo de aplicación. Al instalarse este virus es llamado cada vez que se ejecuta la aplicación que lo contiene, no contamina al archivo del sistema, no hace nada más peligroso que propagarse.

Dukakis: fue escrito en el programa HyperTalk, y escondido en una pila HyperCard, descubierto a finales de 1988. La ejecución de la pila presenta un mensaje <<Dukakis para presidente>> y luego contamina la pila inicial de su aplicación HyperCard. Este virus ya no aparece con mucha frecuencia.

Hpat: es un derivado de la familia nVir, fue descubierto en diciembre de 1988. Se hicieron cambios en el código vírico para que pudiera evitar ser detectado por los antivirus. Añade un nuevo recurso sobre los programas que ya han sido contaminados.

INIT 29: descubierto en diciembre de 1988 en Los Ángeles, ataca a archivos de aplicación y de datos al igual que al archivo del sistema. Es llamado así porque coloca un recurso de 712 bytes del tipo INIT 29 en el archivo de sistema y en los archivos de datos con los que entra en contacto. Se propaga rápidamente, sin embargo no se le considera muy grave.

JUDE: fue descubierto en Bélgica en noviembre de 1989. Es una variación del nVir B; le hicieron cambios para evitar su detección y también instala nuevos recursos a los sistemas ya contaminados.
En el mismo caso se encuentran los virus nFLU, descubierto en agosto de 1989 y el nVir-f, descubierto en la Universidad de Stanford en enero de 1990.

MacMag: fue el primer virus descubierto en las Macintosh, también se conoce como virus de la Paz, fue creado para transmitir un mensaje universal de paz. Este mensaje apareció el 2 de marzo de 1988. Sólo desea a todos los usuarios una paz mundial y posteriormente se autodestruye. El virus celebraba el aniversario de las Macintosh. Por lo mismo que se autodestruye, es muy difícil encontrarlo actualmente.

MEV#: fue descubierto en Bélgica en abril de 1989; es otra variación del nVir B. También se hicieron cambios en el código para evitar su detección por los antivirus. Instala un nuevo recurso sobre los sistemas ya contaminados.

Nvir: es un tipo de varios virus y sus clones, todos derivados del nVir original. Este fue creado por un programador alemán; se dice que esperaba inspirar la creación de vacunas antivíricas. Algunos síntomas del nVir son:

- Caída del sistema;
- Las aplicaciones pitan algunas veces cuando se abren;
- La aplicación y los archivos de sistema aumentan de tamaño.

Hay dos tipos de virus nVir: nVir A, que mide 372 bytes y nVir B de 422 bytes.

Scores: es uno de los más dañinos; se rumora que fue escrito por un programador despedido de Electronic Data Systems. Fue descubierto en abril de 1988 y toma su nombre de un archivo oculto del System Folder (Carpeta del sistema). Cuando se activa el virus contamina inmediatamente el Archivo del sistema, además contamina los archivos ScrapBook (Album de recortes) y Note Pad (Block de notas) y crea dos archivos invisibles llamados Scores y Desktop. Dos días después de contaminar el sistema, el virus empieza a contaminar otras aplicaciones, dos días posteriores a esto, busca dos programas creados por Electronic Data Systems y tres días después trata de dañar esos dos programas.

Algunos de los síntomas del virus Scores son:

- Los íconos de los archivos ScrapBook y Note Pad paracen páginas muy maltratadas;
- Dos archivos invisibles (Scores y Desktop) están en el sistema;
- Las aplicaciones se estropean frecuentemente el arrancar;
- El tiempo del proceso de aplicación se reduce considerablemente;
- Los archivos sobresalientes se corrompen;
- El sistema entero reduce la velocidad; y,
- Los archivos de aplicación y de sistema aumentan de tamaño.

Sida: fue descubierto en Holanda en marzo de 1989; es una variación del nVir B, e infecta aplicaciones y al archivo de sistema; también fue creado para poder burlar a los programas antivirus. Añade un nuevo recurso a los sistemas que ya hayan sido contaminados.

2. Virus en redes

Uno de los mejores medios de distribución de virus son las redes locales, y peor aún, las remotas. En una red, es suficiente con que una de las máquinas esté contaminada para que toda la red pueda en un momento dado también contaminarse.

Por tal motivo, antes de conectarse lógicamente, cada una de las terminales debe revisarse. También es necesario, como medida de seguridad, utilizar un sistema antivirus en cada terminal.

Algunos virus fueron diseñados específicamente para infectar redes, por ejemplo el virus Internet.

Internet es una extensa red de computadoras, la cual une centros de cómputo de agencias federales, universidades, laboratorios de investigación y otras dependencias gubernamentales de todo el mundo. Esta red permite enviar y recibir información a nivel mundial. Aproximadamente 3 millones de computadoras están conectadas a esta red. El virus Internet utiliza un programa de correo electrónico llamado Send.mail para sobrecargar la red. Fue escrito aprovechando una falla

Sida: fue descubierto en Holanda en marzo de 1989; es una variación del nVir B, e infecta aplicaciones y al archivo de sistema; también fue creado para poder burlar a los programas antivirus. Añade un nuevo recurso a los sistemas que ya hayan sido contaminados.

2. Virus en redes

Uno de los mejores medios de distribución de virus son las redes locales, y peor aún, las remotas. En una red, es suficiente con que una de las máquinas esté contaminada para que toda la red pueda en un momento dado también contaminarse.

Por tal motivo, antes de conectarse lógicamente, cada una de las terminales debe revisarse. También es necesario, como medida de seguridad, utilizar un sistema antivirus en cada terminal.

Algunos virus fueron diseñados específicamente para infectar redes, por ejemplo el virus Internet.

Internet es una extensa red de computadoras, la cual une centros de cómputo de agencias federales, universidades, laboratorios de investigación y otras dependencias gubernamentales de todo el mundo. Esta red permite enviar y recibir información a nivel mundial. Aproximadamente 3 millones de computadoras están conectadas a esta red. El virus Internet utiliza un programa de correo electrónico llamado Send.mail para sobrecargar la red. Fue escrito aprovechando una falla

en el programa Send.mail, para tomar el control de la red. Reproduce al virus y transmite copias a otras computadoras, captura rápidamente la mayoría de la capacidad de procesamiento de la computadora.

Este virus puede atravesar rápidamente un país, invadiendo otras redes de computadoras que estén conectadas a Internet. Cuando los reportes de infección empiezan, algunos centros de computadoras no infectados comienzan a desconectarse de Internet, las computadoras infectadas tienen que ser restauradas, después de que el virus sea limpiado; el proceso puede llevar varios días. Este virus se activó por primera vez en noviembre de 1988.[19]

[19] Mayo, Jonathan L. What they are, how they work, how to avoid them, E.U., págs. 14.

IV. ACTUACIÓN DE LOS VIRUS Y MEDIDAS DE SEGURIDAD

IV.1 Cómo actúa un virus

El autor Juan José Nombela, en su libro Virus Informático (1991), divide en siete las fases por las que puede atravesar un virus, a continuación se muestra una descripción de la manera en que actúa un virus en cada una de esas fases:

1. Llegada al sistema

Un virus llega al sistema a través de las vías de comunicación con el exterior, que puede ser desde el puerto de comunicaciones o por medio de los discos flexibles.

a) *Llegada desde el puerto de comunicaciones*: un programa puede pasar a través del puerto de comunicaciones, siempre que consiga traspasar el control que imponen las palabras de acceso y los protocolos de intercambio de información, utilizados por un módem.

En este punto también se deben considerar las redes locales, aunque su conexión no se realiza exactamente a través del puerto de comunicaciones, el mecanismo de intercambio de información entre los nodos de la red es muy similar al intercambio de información a través de un módem.

Existen algoritmos, basados principalmente en la persistencia, que son capaces de quebrantar las claves de acceso, intentando una y otra vez el acceso con diversas claves. A estos algoritmos se les denomina: gusanos.

b) *Llegada por medio de discos flexibles*: la llegada de un virus se puede producir por la ejecución de algún programa contaminado contenido en un disco flexible, ya sea para copiar o correr algún programa.

2. Instalación

Esta es la fase de infección. En este momento el virus empieza a vivir dentro de su huésped, pero mientras no se ejecute el código vírico, éste no tendrá ningún efecto.

Si llegó a través de un disco flexible, la secuencia se ejecuta al correrse el programa que le sirve de huésped y si llegó a través del puerto de comunicaciones, se deben dar algunas circunstancias adicionales para que el código se ejecute.

El virus ha de almacenar una copia de sí mismo en el disco, es decir en algún lugar permanente del sistema con el fin de ser ejecutado varias veces.

Al virus le interesa mezclar su código con el de los programas del sistema operativo que se ejecutan en las primeras fases de arranque.

a) *Contaminación del Boot*:

1. Localizar uno o varios sectores libres del disco donde almacenar el sector 0 original y el grueso del programa del virus.
2. Leer el sector 0.
3. Guardar el contenido del sector 0 original y el programa del virus en los sectores reservados para ello.
4. Marcar dichos clusters como defectuosos.
5. Escribir el nuevo sector 0, que contendrá el código de inicialización del virus.

b) *Contaminación de un archivo .COM*:

1. Abrir el archivo para que sea de lectura/escritura.
2. Añadir el programa del virus al principio o al final del archivo
3. Guardar los primeros bytes en algún lugar apropiado del programa del virus, para que puedan ser sustituidos al final de la ejecución de éste.
4. Sustituir los primeros bytes del archivo por la llamada al código del virus.
5. Cerrar el archivo.

c) *Contaminación de archivos .EXE*: los archivos EXE contienen en su cabecera información que necesita el DOS para el cálculo de las direcciones correctas de algunas instrucciones. Se componen de dos partes: una cabecera que contiene información de control y reubicación, y un módulo de carga, que contiene el código del programa.

La cabecera contiene los datos necesarios para localizar la primera instrucción del programa. Un virus se puede aprovechar de esta circunstancia y sustituir unos pocos bytes de la cabecera por los necesarios para que la dirección de comienzo de ejecución del programa sea la del código del virus, que se añadirá al final del módulo de carga. La última instrucción del código vírico será una de salto a la primera instrucción del programa original.

El proceso de contaminación consistirá en:

1. Añadir el código del virus a continuación del código del programa.
2. Guardar determinados valores contenidos en la cabecera en alguna variable dentro del código del virus.
3. Sustituir los valores anteriores por los necesarios para que la primera instrucción que se ejecute cuando se transfiera el control al módulo, sea la de inicio del código del virus.
4. Dentro del programa del virus deberá haber alguna rutina que permita realizar los cálculos necesarios para deducir los valores adecuados que se tendrán que colocar en los registros del procesador inmediatamente antes de ceder el control al programa original. Para estos cálculos es necesario utilizar los valores originales contenidos en la cabecera y que se guardaron durante el proceso de contaminación.

Los archivos .COM no pueden tener una longitud mayor de 64K, lo que impide que sean muy sofisticados. La contaminación de archivos .EXE es

la más difícil de realizar y detectar, ya que se suelen ejecutar con poca frecuencia dentro de una misma sesión, pero son los mejores para la propagación, dado que los archivos de aplicación son los que más suelen compartirse.

Generalmente se utiliza una técnica mixta: contaminar los archivos .EXE para facilitar la propagación y el COMMAND.COM para asegurarse la toma de control de la máquina siempre que ésta se encienda.

3. Ocultamiento

Para evitar ser descubierto y eliminado, y poder seguir realizando sus acciones nocivas, el virus necesita ocultarse a los ojos del usuario. El código del virus está mezclado con el código del programa que le sirve de huésped. Pero muchas veces el virus tiene un tamaño voluminoso y ocupa demasiado espacio dentro del archivo, por lo que necesita dividirse, es decir dejar una parte pequeña dentro del huésped y guardar, en algún lugar oculto, la parte más grande del programa.

Para ocultar su código en el disco, el virus puede utilizar básicamente una de las siguientes tres técnicas:

a) *Archivos ocultos*: marcar el archivo donde está almacenado con el atributo de archivo oculto, lo que hará que no pueda ser listado con el comando DIR. Tampoco podrá ser leído ni modificado desde el intérprete de comandos.

Entre los datos de un archivo, almacenados en el directorio, existe un byte de atributo que indica qué propiedades tiene el archivo. Una de ellas permite caracterizarle como oculto, de forma que no aparezca en los listados de directorio.

b) *Ocultamiento en sectores marcados como defectuosos*: almacenar el código en uno o varios sectores libres del disco, marcándolos como defectuosos en la FAT (del inglés File Allocation Table).

Los datos se organizan físicamente en sectores en el disco y se agrupan en clusters que generalmente se componen de 4 sectores consecutivos. La organización lógica del disco agrupa los datos en archivos que ocupan uno o varios sectores cada uno, y utiliza un mapa, llamado FAT, y un directorio para localizar los datos en los sectores apropiados del disco.

El agrupamiento de los datos en archivos libera al usuario de la preocupación de los detalles de la organización física de los datos. El sistema operativo se encarga de asignar los clusters que sean necesarios a cada archivo, y mantiene un mapa del disco, la FAT, para saber a qué archivo pertenece cada cluster. Los directorios contienen información sobre cuál es el primer cluster de la cadena y la FAT contiene la información de cuáles son los restantes clusters de un archivo.

Un cluster en la FAT se marca como libre y disponible poniendo un 0 en su correspondiente entrada. Un cluster defectuoso contiene en su entrada correspondiente el valor FFF7H (-9 en decimal), y cualquier otro valor significará que el cluster está ocupado por los datos de un archivo.

El proceso a seguir para marcar un cluster como defectuoso será:

1. Localizar un cluster en buen estado que esté libre.
2. Poner en la entrada de la FAT correspondiente a dicho cluster el valor FFF7H.
3. Sustituir las dos copias de la FAT por la ya corregida.
4. Escribir en el cluster elegido el código a ocultar.

c) *Mediante técnicas de formateo no estándar*: con estas técnicas se logra introducir sectores extraños, que permanecen ocultos a los ojos del DOS porque no los puede leer.

Es imposible que el virus se oculte de forma total, pues siempre se pueden apreciar ligeros aumentos en el tamaño de los programas donde se oculta, o el aumento de sectores defectuosos en el disco, o retardos en la ejecución de los programas del usuario.

La localización, tamaño y número de sectores dentro de una pista están bajo control del software, las características de los sectores de un disco (tamaño y número por pista) se establecen cuando se da formato a cada

pista, pero existe una rutina de la BIOS que se puede utilizar para dar formato a una pista del disco.

4. Control del sistema

Para poder realizar sus acciones, el virus necesita hacerse del control de la máquina, aunque sea de forma momentánea o intermitente. Esto lo puede hacer de dos maneras:

a) *Inmediatamente antes de la ejecución de un programa de usuario*: si el virus se ha instalado en un archivo .EXE, el código del virus será ejecutado antes que el de su programa huésped. Normalmente el virus aprovechará también ese momento para instalarse en memoria y quedar residente, tomando completamente el control del sistema operativo.

b) *A intervalos cortos, aprovechando el sistema de interrupciones del procesador:* desde el punto de vista de un virus, lo deseable es actuar el mayor número de veces posible. Por eso, si se elige la opción a), es preferible emplear como huésped un programa de uso frecuente, por ejemplo el COMMAND.COM.

Existe una interrupción del DOS que permite la terminación de un programa, pero dejándolo residente en memoria y evitando por tanto que pueda ser borrado posteriormente al cargar otro programa. La interrupción a la que nos referimos es la número 27H.

La interrupción de reloj es utilizada por la PC para actualizar la hora del sistema. Dicha interrupción se activa varias veces por segundo, las mismas que se interrumpe el programa que en ese momento se está

ejecutando, para pasar a procesar las instrucciones que componen la rutina de atención a la interrupción.

Cada vez que se produce la interrupción hardware de reloj, el procesador acude a una tabla que indica la dirección de memoria donde cada rutina de interrupción comienza, extrae de ella la dirección de comienzo de la rutina de interrupción de reloj y ejecuta dicha rutina.

Lo que el virus ha de hacer es modificar dicha tabla sustituyendo la dirección de comienzo de la rutina de reloj por la dirección de su propio código, de esta forma el procesador acude a la tabla, extrae de ella la dirección y pasa el control erróneamente al virus. A esto se le llama "interceptar" una interrupción.

Para que el usuario no se dé cuenta de que algo anda mal, una vez ejecutado el código del virus, éste da un salto a la rutina de reloj auténtica, para que efectúe las tareas que le son propias.

Para que este esquema pueda funcionar, es imprescindible que el virus antes haya quedado residente en la memoria.

5. Reproducción

Una de las características fundamentales que distingue a un virus de otros programas es su capacidad para reproducirse.

La capacidad reproductora de los virus puede variar desde una única copia a una reproducción de tipo exponencial, en la que cada copia realiza varias copias de sí misma.

Para que la reproducción sea efectiva, la copia realizada ha de quedar permanente en alguna parte del sistema. Como la memoria RAM es volátil, sólo tiene sentido la copia en disco, infectando otros archivos ejecutables.

El virus, en su afán por garantizar la propagación y no dejar al azar la posibilidad de que se ejecute un programa no contaminado, intenta realizar copias de sí mismo en todos los archivos del disco susceptibles de ser ejecutados.

Para copiarse necesita, en principio, hacer una reconstrucción de sí mismo, pues muy probablemente esté esparcido en varios trozos a lo largo del disco, con objeto de ocultarse. La propagación a otro sistema requiere la recuperación de la totalidad del código. Existirá por tanto, alguna rutina recuperadora de las diversas partes, si es que está dividido.

Se puede dividir el proceso de reproducción en las siguientes fases:

a) *Búsqueda de un huésped donde instalarse*: en el caso de los contaminadores de Boot, el proceso de búsqueda es innecesario, pues el programa a contaminar está claramente localizado en el sector 0 del

disco. El proceso consistirá en buscar en el directorio archivos, traerlos a la memoria, infectarlos y volverlos a escribir en el disco.

La función del sistema operativo que permite ejecutar un programa es el servicio 4BH de la interrupción INT 21H del DOS. El programa contaminante puede simplemente cargar en memoria el programa que se solicita, modificarlo, volverlo a escribir en el disco y dar luego control a la rutina original de la función 4BH.

b) *Comprobación de copia realizada anteriormente*: instalarse varias veces en un mismo programa es inútil, y sólo incrementa la probabilidad de ser descubierto; además, es importante ahorrar tiempo, evitando realizar acciones inútiles, y ahorrar espacio. La comprobación de copia puede consistir en observar el programa huésped para ver si contiene alguna palabra clave o cadena determinada que identifique al virus.

La no inclusión de una rutina de comprobación puede hacer, en los contaminadores de archivos, que crezcan en grandes proporciones, lo que hace al virus fácilmente detectable.

6. Propagación

a) *Por medio del Boot*: la propagación a través del Boot sólo tiene sentido cuando se va a arrancar la computadora con un disco flexible. Generalmente, la mayoría de los usuarios arrancan desde el disco duro o con sus propios discos protegidos. Es cierto que casi nadie la arranca

con discos flexibles extraños, pero ¿quién no ha dejado por accidente un disco cualquiera, que no contiene sistema operativo, metido dentro de la unidad A y encender la computadora con él? Lo que sucede entonces es que la máquina no encuentra el sistema operativo y saca un mensaje de error del tipo:

<<Error en disco o disco sin DOS>>
<<Cámbielo y pulse cualquier letra>>

Lo que nosotros solemos hacer entonces es sacar el disco de la unidad A y pulsar una tecla cualquiera.

Un virus contaminador del sector de arranque no necesita que el disco en que se instala contenga el sistema operativo. Cuando encendemos el sistema con un disco introducido en la unidad A, la computadora pasa el control al programa contenido en el boot record del disco. Si éste está infectado, el virus se instalará en memoria. Si no reinicializamos, el virus permanecerá en la memoria, y el sistema quedará infectado. La única solución para evitar esto consiste en apagar y volver a encender la PC para arrancar correctamente desde el disco duro.

b) *Propagación por medio de archivos ejecutables*: la propagación a través de los archivos ejecutables es la más eficaz en su efecto negativo, por dos motivos: primero, porque los grandes programas de aplicaciones, es decir, los que realizan tareas más complejas y son por lo tanto más

útiles, son por fuerza archivos .EXE y al ser programas de mucha utilidad, estará garantizada la distribución.

7. Manifestación

Es la fase final del programa virus. Existen dos posibilidades no excluyentes:

a) *Manifestarse con el único fin de dar un susto o una sorpresa*: por ejemplo los que hacen aparecer de forma periódica mensajes o dibujos en la pantalla.

b) *Manifestarse con el fin de hacer daño*: las acciones habituales, en este caso, suelen ser darle formato a un disco (destruyendo toda la información contenida en él), el borrado del directorio o de la FAT (volviendo irrecuperables los datos del disco), o el borrado de algún archivo aislado.

IV.2 Medidas de seguridad

No existe una fórmula mágica para impedir que un virus se introduzca en una computadora. Aun los antivirus, que hasta ahora han sido la mejor opción para prevenir y eliminar virus, siguen siendo ineficaces, por lo que es necesario, además, tomar ciertas medidas que sirvan de barrera para los virus. Aplicar estas medidas puede quitarle al usuario unos minutos de su tiempo, pero puede disminuir el riesgo de perder su información; si se trabaja en una PC con el sistema operativo MS-DOS, el riesgo es mayor que en cualquier otro sistema operativo.

Cuando algún usuario llega a tener problemas serios por causa de virus informáticos, en lo primero que piensa es en aislar su computadora y su software; abstenerse de introducir discos de otros lugares y no permitir que los suyos sean utilizados en computadoras ajenas.Sin embargo, esto es casi imposible, ya que tarde o temprano tendrá que compartir algún programa o archivo y el riesgo de un ataque viral continuará, por lo que es mejor tomar algunas medidas como las que a continuación se describen:

- Establecer políticas acerca del manejo del software y hardware; debe existir una persona responsable para controlar la información que entra y sale de un centro de cómputo.

- Inculcar a los usuarios la costumbre de revisar los discos que introduzcan a la máquina, explicándoles claramente las razones. Se les debe capacitar en el manejo de los programas antivirus.

- Independientemente del sistema operativo bajo el cual se esté trabajando, es importante realizar respaldos (backups) de la información que se considere importante, ya que el riesgo de que algún virus se introduzca en una computadora está siempre latente. También se deben hacer respaldos de los discos originales, previamente protegidos contra escritura, y utilizar únicamente los respaldos para instalaciones.

- Mantener informados y actualizados tanto a los usuarios como al supervisor en cuanto al surgimiento de nuevos virus y antivirus.

- Tener sumo cuidado al ingresar a una red como supervisor, ya que la facilidad de acceso puede aumentar la propagación de los virus.

- Observar el tiempo que tarda una aplicación en cargarse, ya que un programa con virus hace que se incremente este tiempo. Dentro de la aplicación, también se puede observar si el tiempo que se lleva en realizar algún proceso es normal. En cuanto a los accesos a disco, hay que observar cuánto tiempo permanece encendida la luz del indicador del disco duro, ya que los virus pueden estar explorando los archivos durante un buen rato y esto se notará cuando el usuario no realiza

ningún acceso al disco y la luz indicadora se enciende algunos instantes.

- Es recomendable tener siempre a la mano discos flexibles inicializables o de arranque, es decir que contengan los archivos IO.SYS, MSDOS.SYS y COMMAND.COM, asegúrese de proteger sus discos de arranque contra escritura. Si se sospecha de la presencia de un virus, lo primero que se debe hacer es apagar la máquina e inicializar el sistema desde su disco de arranque y posteriormente utilizar software antivirus como el que se describe más adelante.

- No introducir discos de origen dudoso, en caso de que esto sea inevitable, se deben revisar los discos antes de trabajar con ellos en la computadora.

- Emplear una máquina exclusivamente para revisión y vacunación de discos infectados (en el caso de un centro de cómputo).

- Actualizar los antivirus en cuanto salgan nuevas versiones.

- Revisión de las máquinas con cierta periodicidad.

- Evitar que cualquier persona tenga acceso a las máquinas.

- No permitir que los empleados traigan y lleven discos de la empresa a otros lugares donde podrían contaminarse.

- Cuando se vaya a trabajar en una computadora que ya se encuentre encendida y se desconozca el trabajo que se estaba realizando, evitar introducir un disco. Es recomendable reinicializar la computadora.

- Si no tiene otro recurso más que formatear su disco duro, lo debe hacer a bajo nivel para limpiarlo totalmente. De la versión 5.0 en adelante del sistema operativo MS-DOS se puede hacer un formateo rápido, donde lo que se elimina es la FAT, por lo que con esto no se eliminarán los virus de arranque.

- Revisar discos de demostración y, una vez asegurado que no tienen virus, protegerlos físicamente contra escritura.

- Muchos virus son eliminados al borrar los programas contaminados, pero se debe ser cuidadoso con el comando DEL del MS-DOS, ya que éste no destruye al programa y con algunas utilerías se pueden recuperar dichos programas y con ellos, los virus.

IV.3 Antivirus

Actualmente existen múltiples programas que ayudan a la prevención, identificación y eliminación de los virus informáticos; algunos pueden quedar residentes en memoria. Cuando un antivirus encuentra actividades dudosas en el sistema operativo, entra en acción e informan al usuario lo que está ocurriendo. Sin embargo, puede ocupar un valioso espacio de la memoria RAM y muchas veces interrumpe constantemente el programa que se está ejecutando, lo cual puede resultar muy molesto para el usuario.

Desafortunadamente, algunos virus pueden detectar la presencia de los antivirus y burlarlos, pero la lucha continúa porque algunos antivirus trabajan vigilando continuamente los relojes de las computadoras, ya que para los virus no es una labor difícil el detener un reloj y volver a arrancarlo después de desactivar un sistema antivirus.

A continuación se muestra una descripción de los antivirus más conocidos:

1. Norton Antivirus (NAV)

Fue lanzado al público en diciembre de 1990, por Symantec Corporation y es compatible con DOS, Windows y LAN.

Características:

a) *Protección transparente*: lo tradicional de un antivirus es que la protección completa contra los virus estuviera acompañada de constantes alertas y advertencias que interrumpan la ejecución del programa que estuviera en pantalla en ese momento. Norton Antivirus inocula los archivos automáticamente y no hace sonar una alarma hasta que está seguro de que el problema es real.

Virus Intercept es una parte del NAV, la cual reside en memoria para activar la alarma cuando detecta un archivo infectado o existen sospechas de un virus. Para que el Virus Intercept pueda realizar esto, al instalar NAV se debe modificar el archivo CONFIG.SYS. Virus Intercept se cargará en memoria cada vez que se encienda la computadora y se desplegará el siguiente mensaje cuando el programa haya sido cargado.

<<The Norton Antivirus>>
<<Version 2.0>>
<<Comprehensive Scan>>
<<â1991, Symantec Corporation>>
<<All Rights Reserved>>

b) *Prueba recursiva*: algunos virus no verifican si ya han infectado un archivo, por lo que lo vuelven a infectar, de hecho un mismo archivo puede ser infectado por varios virus. La manera como NAV resuelve este problema es reparando los daños que hizo el primer virus y volver a

revisar el archivo las veces que sea necesario para eliminar todos los virus que tenga el disco.

c) *Protección pasiva del sector de arranque*: de manera opcional, NAV puede alertar cada vez que un programa intente escribir en el sector de arranque de un disco. La vigilancia de NAV puede evitar que un virus escriba en la tabla de partición y en el sector de arranque.[20]

Principales archivos que componen el NAV:
NAV.EXE: dentro de este programa existe la opción SCAN, la cual se va a encargar de detectar virus conocidos y que puedan ser agregados nuevos códigos de virus. Para ello el usuario deberá introducir el código hexadecimal de los mismos. La opción TOOLS permite grabar en el disco los datos acerca de la tabla de partición, el sector de arranque y los valores del Setup (CMOS). Si en un momento dado se llega a alterar alguna de estas opciones, podrán ser recuperadas. Otra opción permite al usuario bloquear con una clave el acceso a la modificación del NAV.

NAV_.SYS: este programa se utiliza para que el NAV quede residente en memoria, al cargarlo en el archivo CONFIG.SYS, consume entre 35 y 50 Kb de memoria. Su función es buscar virus en los archivos ejecutables cuando están siendo cargados, copiados o movidos. Puede detectar virus que ataquen a la tabla de partición o al sector de arranque.[21]

[20] Norton, Peter y Nielsen, Paul. Op. Cit., págs. 104 y 105.
[21] Cortés, Pedro L. Virus Manual de referencia, Editorial Métodos, México, 1994. Págs. 97-100.

2. Viruscan

Fabricado por McAfee Associates. En el laboratorio de investigación de McAfee se reciben programas virales que aparecen en todo el mundo, a través de sus agentes internacionales y usuarios. En cuanto se detecta un virus no conocido, se envía inmediatamente y se generan periódicamente actualizaciones que mantienen a los usuarios protegidos oportunamente.

VirusScan identifica el tipo de virus que esté infectando la tabla de partición, sector de arranque o los programas ejecutables. Si se usa con la opción de limpieza (/CLEAN), desinfectará el área o los archivos infectados, eliminando el código vírico. En la mayoría de los casos la información quedará completamente restaurada y libre de virus.

Es compatible con todas las redes existentes tipo IBMNET o NETBIOS, incluyendo Novell NetWare, Banyan Vines, 3COM, 3/Share, 3/Open, Artisoft Lantastic, AT&T StarLan, Dec Pathworks, IBM Lan Server, IBM Token Ring, Microsoft Lan Manager y MS-NET.

Sus principales archivos son:

V-SHIELD: es un programa tipo TSR, el cual explora la memoria de los sistemas, el sector de arranque, la tabla de partición y el sistema de archivos, buscando virus conocidos y se verifica y rastrea a sí mismo. Después queda instalado en la memoria residente, monitoreando

ejecuciones de programas y al sector de arranque de los discos flexibles accesados en operaciones de lectura y/o escritura.
Cuando se solicita la ejecución de un programa y existe alguna infección o son invocados los comandos de DOS DIR o COPY, VSHIELD mostrará un mensaje diciendo al usuario el nombre del archivo infectado y el nombre del virus en cuestión, evitando la ejecución de dicho programa, para que el virus no entre al sistema.

VSHIELD se autoinstala en memoria de la mejor manera posible, buscando ocupar incluso la memoria extendida y la memoria alta para dejar totalmente libre la memoria básica.

NETSHIELD: programa diseñado para operar en sistemas Novel 3.11, 3.12 y 4.01. Protege al servidor contra el acceso de cualquier usuario que intente entrar con alguna terminal contaminada, con todas las ventajas de VSHIELD para ser usado desde el servidor y para toda la red. La función de este programa es verificar los archivos del servidor buscando virus conocidos.[22]

3. Symantec Antivirus para Macintosh (SAM)

SAM previene, detecta y elimina virus del ambiente Macintosh, este programa cuenta principalmente con dos partes:

[22] Información proporcionada por McAfee Associates Mexico, 1995.

a) SAM Intercept: es el componente de prevención, el cual es cargado en memoria cuando se inicializa la máquina y permanece activo hasta que se apaga. Constantemente está monitoreando la posible presencia de virus en algún archivo. Cuando Intercept detecta algún virus o alguna actividad sospechosa, interviene y le notifica al usuario lo que está sucediendo.

b) *Virus clinic*: es el componente de detección y eliminación de virus, se utiliza para rastrear archivos, discos duros o volúmenes (partición de un disco) y servidores de red para detectar la posible presencia de virus conocidos; repara o borra, en caso necesario, archivos infectados, protege archivos y volúmenes desde que el virus intenta infectarlos y añade o elimina definiciones de virus para poder detectar nuevos virus.[23]

4. PC-cillin

La tecnología PC-cillin previene contra infecciones de virus. Las áreas protegidas incluyen archivos, sector de arranque, tabla de particiones y memoria. Incluye tres scanners para examinar casi cualquier tipo de archivo.

Repara automáticamente los daños en la tabla de particiones del disco duro.

[23] SAM User's Guide & Reference, CA, E.U., 1992, págs. v y vi.

Cuenta con un disco de arranque que asegura llegar al intérprete de comandos sin virus en memoria; protege antes de que se cargue en memoria el sistema operativo y cualquier virus del sector de arranque.

Permite recuperar la información del disco duro después de un ataque de virus, ya que guarda una copia de la información crítica del sector de aranque y de la tabla de particiones en un conector externo (donde está a salvo de los virus), permitiendo una recuperación instantánea.

Funciona en los ambientes: DOS, Windows 3.1, OS/2, NetWare, Banyan Vines y LAN Manager.[24]

[24] Folleto de publicidad PC-cillin, 1995.

IV.4 Mitos y realidades acerca de los virus informáticos

El crecimiento en el número de virus informáticos ha sido paralelo al aumento de popularidad y potencia de tratamiento de las computadoras personales.

Los virus informáticos son como ladrones o espías del mundo del *software* informático.

A partir de su aparición, simultáneamente han surgido innumerables mitos acerca de lo que los virus informáticos son capaces de hacer, por lo que a continuación se hacen algunas aclaraciones con el objeto de delimitar las actividades de dichos programas:

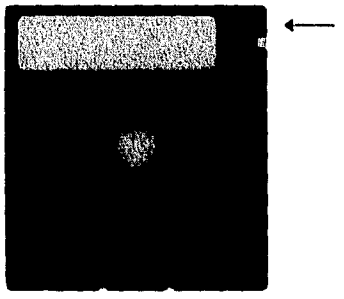
Vida electrónica: Muchos usuarios creen erróneamente que los virus informáticos contienen alguna forma de vida electrónica, o que se pueden propagar de computadora en computadora sin requerir contacto físico entre sistemas distribuidos o que pueden vivir dentro de los circuitos, incluso después de que se haya cortado la corriente eléctrica, o que si dejan un disco infectado junto a otros que no lo están , éstos se contagiarán; esto es completamente falso, ya que al contrario de sus correspondientes biológicos, éstos no pueden flotar en el aire o adherirse a la piel.

Mutación: Para los virus biológicos "La vida moderna permite la mezcla, la mutación y la revitalización de algunos virus poco estables"[25].

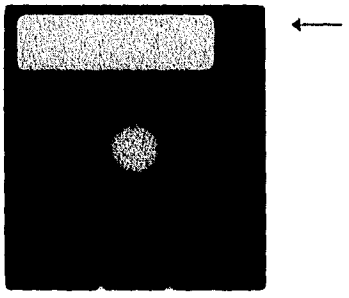
Algunos virus informáticos pueden transformarse cada vez que se instalan y se les conoce con el nombre de virus polimórficos, y también existe una especie de virus "compañeros", los cuales por sí solos pueden hacer un daño menor, pero cuando se juntan con su compañero pueden causar verdaderos desastres.

Discos: Ningún virus puede propagarse a los archivos contenidos en un disco protegido contra escritura.

Disco no protegido contra escritura



Disco protegido contra escritura



[25] Greer, William. Op. Cit., pág. xiii.

Cuando se le da formato a un disco se crea una estructura lógica en él, la cual va a servir de referencia para que el sistema operativo guarde ordenadamente los archivos. Un virus puede destruir la estructura lógica, mas no al disco.

V. EFECTOS QUE PUEDE CAUSAR UN VIRUS AL INSTALARSE EN UN SISTEMA

Un virus informático puede tener varios efectos al instalarse dentro de un sistema de cómputo, que van más allá de su definición como una serie de instrucciones o un fragmento de código. Por tal motivo, a continuación se describen un enfoque financiero, un enfoque social y un enfoque tecnológico para exponer algunos de los más importantes efectos de estos virus.

V.1 Enfoque Financiero

Desde el punto de vista financiero los virus tienen repercusiones al instalarse en un sistema de cómputo, las cuales pueden traducirse en pérdidas para una empresa, incluso para un usuario que trabaja individualmente.

Poco se ha escrito acerca de los costos que se pueden producir por la instalación de un virus informático, tomaremos como referencia, en primer lugar al Dr. Frederick Cohen, quien en su libro "A Short Course on Computer Viruses" (1990) hace un análisis comparativo de costos de las defensas contra virus

El Dr. Cohen toma en cuenta para su análisis los siguientes factores:

El costo de la licencia para un checksum y para un escudo de integridad (detectores de modificaciones) es un costo único, al contrario de los scanners y monitores, que regularmente se actualizan y fuerzan a que las licencias tengan que ser pagadas varias veces.

El costo de una revisión diaria de los sistemas es mayor que cualquier diferencia razonable en las tarifas de licencia.

Los costos de actualización más los de recuperación de nuevos ataques, más el tiempo de búsqueda de un scanner, comparado con el de un checksum, los scanners resultan ser menos caros, ya que son pocos los virus nuevos cada año.

En relación a los costos de búsqueda, los scanners y los monitores son relativamente iguales, sin embargo, el costo por limpiar un sistema (scanners) es normalmente mucho mayor que el costo por limpiar un solo archivo (monitores).

Los checksums resultan ser más caros que los escudos de integración, ya que verificar cambios en cada programa justo antes de correrlos es más barato que la detección periódica de cambios en todo el sistema.

Tomando en cuenta que la diferencia en el costo anual de una licencia es pequeño comparado con el costo de actualización, se concluye que los escudos de integración son más baratos que los monitores, ya que en estos últimos se debe considerar el costo de actualización para su mantenimiento y el costo de limpieza de ataques que los monitores no detectan.

Aunque el Dr. Cohen afirma que en cuestión de costos, los escudos de integración son los más baratos, se debe de tomar en cuenta los intereses particulares del usuario para hacer una buena elección de estas herramientas o, en su caso, una combinación de ellas podría dar mejores resultados.

Otro autor que trata los costos es el Ing. Guillermo M. Mallén en su obra "Virus Computacionales" (1994), donde aborda de la diferencia de impacto que puede generar un virus debido a la variedad en el uso de equipos y a la importancia que tiene la información para cada usuario.
Menciona que no sólo se debe considerar el tiempo que invierten los empleados en generar la información que se daña o se pierde sino también los siguientes factores:

- El costo de oportunidad, es decir lo que se deja de ganar por el daño que sufrió la información.
- La existencia de copias de seguridad, lo cual reduce notablemente el impacto de un accidente.
- El costo del accidente, es decir el costo total de los recursos que se emplearon tanto para la prevención como para la recuperación de la información, está influido por los procedimientos operativos de la organización y por la naturaleza misma de la información almacenada en la computadora.
- La probabilidad de que el accidente ocurra en una máquina en cierto periodo, la cual se puede medir en términos de riesgo, como lo hacen

las compañías de seguros en relación a los accidentes automovilísticos, aunque estos datos serían muy variables como resultado de la propia dinámica de la computación, donde todo gira en torno al valor de la información.

Tomando como referencia lo anterior, propongo la siguiente fórmula para calcular el costo de un equipo infectado, sabiendo de antemano que esta fórmula no se puede generalizar para todos los casos de equipos infectados, ya que cada usuario tendrá infinidad de variables que agregar, dependiendo de las medidas de seguridad que ya tenga establecidas y el valor que le dé a su información:

Costo Total = Costo del Accidente + Costo de Medidas contra Virus
CT = CA + CV

En donde el Costo del Accidente representa la erogación que se haya hecho por los siguientes conceptos:
Costo de la Información Perdida + Pérdida de Tiempo Máquina + Pérdida Tiempo Gente + Costo Técnico + Daños al Hardware - Costo de Respaldos
CA = CIP + PTM + PTG + CT + DH - CR

El Costo de Medidas contra Virus; representa la suma de los costos de las medidas de prevención que se tengan para el caso de un ataque de virus y se compone de:

Costo de Licencia + Costo de Instalación y Mantenimiento

CV = CL + CIM

V.2 Enfoque social

Para darle un enfoque social al problema de los virus informáticos, tomaremos en cuenta algunos aspectos que generan un impacto a los usuarios de los equipos de cómputo cuando se presenta algún daño o pérdida de información:

Predisposición: Existe gente que no ha usado computadoras pero se ha enterado, ya sea por los medios masivos de comunicación o por algunos conocidos, de los daños que puede causar un virus informático. Ellos tendrán la desconfianza que causa por sí sola una computadora a primera vista, y sobre todo si en sus primeros encuentros con la computadora se pierde información, aun cuando no sea por causa de un virus.

Desconcierto: En relación a la gente que le da un uso cotidiano a una computadora, como una secretaria que no está directamente involucrada con el funcionamiento del sistema operativo, la aparición de un virus puede traer graves consecuencias.

Por ejemplo una secretaria que utiliza un único programa, un procesador de textos en una máquina PC, un día trabaja un documento de una página, el cual guardó; al día siguiente trata de abrir este documento y no lo encuentra, por lo que llama al técnico, quien le pregunta si creó algún respaldo a lo que contesta que no; el técnico trata de recuperar el

archivo, pero tal parece que sus herramientas no son suficientes, por lo que finalmente el documento no puede recuperarse.

La experiencia de la secretaria es que es muy importante contar con un respaldo actualizado de la información pero, por otro lado, existe un temor a usar la PC por lo cual, para ciertos trabajos preferirá regresar a su antigua máquina de escribir que sí le ofrece seguridad; en realidad, las computadoras no le están facilitando del todo su trabajo. Para el técnico el aprendizaje es que sus herramientas ya son obsoletas o insuficientes para ofrecer la seguridad necesaria y para el director de la empresa es que hacen falta medidas preventivas y correctivas para salvaguardar la información.

Comunicación laboral: Es necesario que los encargados de las áreas de cómputo estén actualizados en cuanto a los virus nuevos que van surgiendo y obviamente también a los antivirus, pero esta información no sólo la deben conocer ellos, sino también los usuarios de los sistemas de cómputo para poder tomar las medidas de seguridad necesarias y así buscar la fluidez de las actividades de una organización.

Por otro lado, la presencia de un virus puede provocar pérdidas en cuanto a que un empleado quede sin trabajo por ser el responsable de la información que se dañó; pueden perderse ventas, que por no poderse registrar en el momento; los clientes pueden irse y, sobre todo, se puede

perder la confianza al pensar que no haya sido un virus quien provocó daños en la información sino que se trata de una excusa.

V.3 Enfoque tecnológico

Los virus son resultado de algunos puntos débiles que tienen tanto las arquitecturas de computadoras como los sistemas operativos, y desde un punto de vista optimista diremos que de alguna manera los creadores de virus han ayudado a encontrar dichas debilidades, mas no a solucionarlas, por lo que algunas empresas han dedicado sus esfuerzos, por un lado, al desarrollo de antivirus cada vez más eficaces y, por otro, bloquearles la entrada a los virus informáticos. A continuación se describe la tecnología que existe para combatir a los virus:

Scanners: Un scanner es un programa que busca cadenas de virus conocidos o patrones, aunque algunos utilizan técnicas heurísticas para reconocer al virus.

Los scanners son actualizados regularmente, sin embargo,surgen nuevos virus en ese lapso, los cuales no se pueden detectar.

Los scanners pueden ser de comando en línea, es decir que el usuario corre el programa desde el Autoexec, por ejemplo y éste se encarga de examinar archivos ejecutables; o TSR, que tan pronto como un disco sea leído por la computadora, el scanner revisa el sector de arranque, y en cuanto se lea el archivo es revisado para buscar virus. Por ser un programa residente en memoria, existe una pequeña reducción en la memoria libre.

Este tipo de antivirus no puede detectar un pequeño porcentaje de virus (los extremadamente polimórficos).

Monitores: El software de monitoreo fue a menudo denominado "vacuna" por las casas comerciales de software, es residente en memoria y anda en busca de actividades sospechosas, pueden resultar más problemáticos que útiles, ya que están constantemente preguntando por confirmación de actividades válidas, también pueden ser evadidos por virus que estén programados en un lenguaje de bajo nivel.

Es muy difícil especificar lo que se debe revisar en el software de monitoreo, ya que los creadores de estos programas no detallan qué es lo que busca este programa.

Los monitores pueden detectar nuevos virus, pero no han demostrado ser eficaces contra el "compañerismo" vírico, en donde los virus aislados no son tan dañinos como cuando se mezclan con un compañero[26].

Checksummers: Examinan la configuración del sistema, almacenan esta información y la comparan contra la configuración más actual. La mayoría de estos programas realizan una inspección cíclica superflua que busca cambios en un archivo, aun cuando la longitud de éste permanezca igual. Por ejemplo, los archivos ejecutables no deben cambiar, excepto en contados casos.

[26]Activity monitors, dirección en Internet: http://dbweb.agora.stm.it/webforum/virus/sladerev.html

La ventaja de los checksummers es que no detectan un repertorio de virus, así que no necesitan actualizarse, las desventajas son que no previenen sino avisan después de la detección.

Algunas versiones de este software corren sólo durante el tiempo de arranque del sistema, otras revisan cada programa mientras corre.

Un factor importante entre los detectores de cambios es con respecto a la instalación y el tiempo de operación, ya que el sistema va a estar recopilando información de todos los programas seleccionados para su revisión y esto puede tomar un tiempo considerable sobre todo porque se tiene que reinstalar cada vez que se haga algún cambio en el sistema.

Estos programas antivirus también pueden producir falsas alarmas, por no saber cuándo un cambio es válido o cuándo es causado por un virus[27].

Software de restricción de operaciones: Este tipo de antivirus es similar al de monitoreo, excepto que en lugar de vigilar por actividades sospechosas, automáticamente las previene, algunos de estos paquetes permiten restringir las actividades que los programas pueden ejecutar, algunas veces en una base de archivo por archivo, sin embargo mientras más opciones permitan estos programas, más tiempo se requerirá para

[27] Frequently Asked Questions, Op. Cit.

instalarlos. El programa debe ser modificado cada vez que se haga un cambio válido al sistema, es importante que el operador del software de restricción de operaciones sea informado de cuándo un programa u operación en particular deberá ser interrumpida o detenida y por qué, ya que también se generan falsas alarmas.

Software de encriptación: El software de encriptación escribe programas o datos en los discos de una manera no estándar (encriptar) y posteriormente lo desencripta cuando se necesita utilizar. Esto significa que si un virus tratara de infectar el sistema, normalmente no concordaría con la información, por lo que sería fácilmente detectable.

El software de encriptación cambia esencialmente todo el ambiente de operación con el fin de crear un nuevo ambiente en el que los virus no puedan sobrevivir. Pero otra vez existe la necesidad de trabajar mucho en la instalación y el mantenerlo al corriente cuando se realizan cambios. Si el sistema no se configura correctamente desde el principio, existe la posibilidad de que no se pueda usar ni reparar.

Este software deja dos grandes huecos: a) una parte del sistema debe permanecer sin encriptar y por lo tanto es vulnerable a un ataque de virus, y b) si el sistema se inicia con archivos infectados, el software encriptará a los virus, junto con los demás datos y esto les permitirá producir su efecto[28].

[28] Activity monitors, Op. Cit.

De lo anterior, podemos deducir cuenta de que no existe una herramienta que por sí sola garantice una protección total contra virus, por lo que es más recomendable hacer una combinación de ellas para obtener resultados más eficaces.

VI. MARCO JURÍDICO

Actualmente no existe en México una ley que regule las actividades que se realizan con respecto a los virus informáticos, sin embargo la Cámara de Diputados y el Instituto Nacional de Estadística, Geografía e Informática (INEGI) están trabajando para que este año queden asentadas las bases para la formulación de dicha ley, por lo que empezaremos por definir algunos conceptos que nos ayudarán a cimentar el terreno donde se pueden ubicar las actividades relativas a los virus informáticos.

Derecho Informático: es una rama de las ciencias jurídicas que contempla a la Informática tanto en su papel de instrumento (Informática Jurídica) como en el de objeto de estudio (Derecho de la Informática).

Informática Jurídica: "nacida en 1959 en Estados Unidos, es la técnica interdisciplinaria que tiene por objeto el estudio e investigación de los conocimientos de la informática aplicables a la recuperación de la información jurídica, así como la elaboración y aprovechamiento de los instrumentos de análisis y tratamiento de información jurídica necesarios para lograr dicha recuperación.

Se trata de la utilización de las computadoras en el ámbito jurídico"[29].

[29] Tellez Valdes, Julio. Derecho Informático, UNAM, México, 1987, págs. 29 y 30

En sus primeros años, la Informática Jurídica se presentó en los términos de creación y recuperación de información que contenían datos principalmente jurídicos, como leyes, jurisprudencia y doctrina.

Poco a poco se empezó a vislumbrar que también se podía obtener no sólo información sino también mediante programas estudiados expresamente, verdaderos actos jurídicos como certificaciones, atribuciones de juez competente, sentencias premodeladas, naciendo a fines de los años setenta la llamada informática Jurídica de Gestión.

Derecho de la Informática: si bien es cierto que los precursores informáticos nunca imaginaron los alcances que llegarían a tener las computadoras, aun en los campos tan aparentemente fuera de influencia como el jurídico, todavía más difícil hubiera sido el concebir que el Derecho llegaría a regular a la Informática.

"Derecho de la Informática es el conjunto de leyes, normas y principios aplicables a los hechos y actos derivados de la Informática.

Normas en virtud de aquellas que integran la llamada Política Informática.
Principios, en función de aquellos postulados emitidos por jueces, magistrados, tratadistas y estudiosos respecto al tema.
Hechos, como resultado de un fenómeno aparejado de la Informática inimputable al hombre; y,

Actos como resultado de un fenómeno directamente vinculado a la Informática y provocado por el hombre"[30].

Algunos juristas han analizado en qué rama del Derecho podría estudiarse a la Informática pero no han podido ponerse de acuerdo. Sin embargo, veremos qué régimen jurídico podría aplicarse al caso de los virus informáticos.

En cuanto al Derecho Penal, en el robo se requiere del apoderamiento físico de una cosa mueble, la cual en los términos de la información como algo intangible no configura convincentemente, ya que no es una persona la que directamente daña la información. Por otra parte, en el abuso de confianza se requiere de la disposición de una cosa ajena mueble, por lo que igual representa problemas por lo abstracto de la información.

En el fraude se requiere un engaño o aprovechamiento de un error que permita hacerse ilícitamente de alguna cosa o alcanzar un lucro indebido, ya que difícilmente el creador de un virus obtendrá la información que dañó o algún beneficio económico directamente.

Patentes y marcas: se le ha considerado como uno de los métodos más apropiados para resolver el problema de la no clasificación del Derecho Informático.

[30] Tellez Valdes, Julio. Op. Cit., pág. 60

Para que una invención sea patentable requiere denotar novedosidad, actividad inventiva, así como una aplicación industrial. En el caso de los programas de cómputo, aun cuando ya se encuentra plasmado a nivel legislativo y jurisprudencial, si se atiende a un criterio rígido, difícilmente se podría demostrar que los programas cumplen con dichos requisitos, de aquí que se recurra a un análisis de otras formas de protección. Sin embargo sólo se está contemplando el derecho que tiene el autor de un programa, más no el que tiene quien sufre daños en la información por causa de un virus informático o la sanción para quien creó dicho virus.

Existe una insuficiencia en las características necesarias de los programas para que pudieran ser susceptibles de patentarse (particularmente los algoritmos). Además, existe una variedad infinita en la forma en que se dispone la alimentación de datos a una computadora y la manera en la que se obtienen los resultados.

Derechos de autor: tiene por objeto la protección de los derechos, en beneficio de toda obra intelectual o artística y salvaguarda del acervo cultural de la nación. Esta figura es aparentemente la más viable en cuanto al problema de protección de los programas computacionales, aunque algunas autoridades señalan que sólo se pueden proteger los trabajos que se hacen con la intención de ejercer una influencia directa a los sentidos humanos. Pero esta definición no deja nada para la regulación de las actividades con respecto a virus informáticos.

Ley específica para el Derecho Informático

En el ya largo debate en torno al problema de la protección jurídica de los programas, algunos autores consideran que debido a la complejidad de los programas y de una necesaria regulación bajo las consideraciones de una nueva ley, ésta puede llegar a darse tomando los elementos más significativos por parte de las instituciones jurídicas y en especial en materia de patentes y derechos de autor, a fin de integrarlos en una nueva estructura que constituya un derecho particular acorde a las consideraciones específicas de los programas.

Cabe hacer notar que el problema puede ser percibido de una manera diferente dependiendo del contexto, por lo que la solución no puede ser la misma para cada caso.

Existe una herramienta que puede ser muy útil para la formulación de esta nueva ley, que es la Política Informática, la cual pretende lograr un desarrollo informático adecuado mediante una planificación a través de normas que a su vez conforman una política diferente de una legislación en cuanto que esta última se refiere a aspectos más específicos.

Así tenemos que dentro de esta política informática algunos de los principales puntos contemplados son el adecuado desarrollo de la industria de construcción de equipos de cómputo y de programación; por otra parte, la planeación, difusión y aplicación del fenómeno informático, la contratación gubernamental de bienes y servicios informáticos, formulación de normas y estándares en materia informática, control de

importaciones y exportaciones sobre equipos, accesorios y programas de computadoras; sin embargo esto no es suficiente para mantener a la informática en los términos idóneos de crecimiento.

A continuación menciono algunos puntos que pueden servir para dar solución a los problemas jurídicos en el campo de la informática[31]:

- Recurrir a las leyes ya existentes mediante una aplicación analógica frente a las situaciones concretas que se presenten.
- Hacer aplicaciones jurisprudenciales dado el desarrollo de casos que en este campo se están presentando en los estrados judiciales.
- Expedir un conjunto de reglas que puedan completar las ya existentes capaces de dar soluciones adecuadas.
- Crear una nueva ley de carácter específico que regule todos los aspectos del mundo informático.

Puntos específicos para tratar el problema de los virus informáticos:

- Destinar los recursos necesarios para el desarrollo de sistemas antivirus y no invertirlos en la búsqueda de los creadores de virus.
- La falta de protección legal ha provocado que las empresas creadoras de software antivirus destinen sumas considerables de dinero para desarrollar programas cuyo único propósito es detectar y eliminar virus, ya que no hay una forma de frenar a los creadores de virus.

[31] Sandoval Ruiz, Justo Evelio. Derecho Informático, una nueva perspectiva jurídica, UNAM, Tesis Doctoral, 1994, págs. 83 y 84.

- Hacer conciencia en las escuelas donde se imparten carreras o se brindan las herramientas que pueden fomentar la creación de virus.
- Regular las precauciones que deben tener los fabricantes de software cuando los programas originales contengan virus.
- Que exista un centro especializado para analizar virus, donde se puedan remitir virus que los usuarios puedan entregar al detectarlos.
- Evitar que los vendedores de hardware y software regalen copias "piratas" a sus clientes.
- Al no existir una ley la gente no puede delimitar qué procedimientos son válidos y cuáles no.

Concepto de "piratería"

"En las esferas del derecho de autor y de los derechos conexos se entiende generalmente por piratería la reproducción de obras publicadas o de fonogramas por cualquier medio adecuado con miras a la transmisión (distribución) al público y también la reemisión de una radiodifusión de otra persona sin la correspondiente autorización. La fijación ilegal de representaciones o ejecuciones en directo se denomina en lenguaje común contrabando"[32].

Establecimiento de un código de ética

Otra forma de regular las actividades informáticas es a través de un código de ética, donde se proponen los siguientes puntos[33]:

[32] Glosario de derecho de autor y derechos conexos de la Organización Mundial de la Propiedad Intelectual (ONPI).
[33] Sandoval Ruiz, Justo Evelio. Op. Cit., págs. 205, 206.

- Responsabilidades y deberes de las personas que intervienen en los diferentes niveles de tratamiento de la información.
- Acceso a la información personal.
- Seguridad de la información
- Respeto a la privacidad e intimidad de las personas. Definición del carácter confidencial de la información y aplicación de las reglas sobre secreto profesional.
- Normas sobre obtención, suministro y modificación de datos.

Puntos específicos enfocados al tratamiento de los virus informáticos:

- Hacer énfasis en la prohibición del acceso a la información sin previa autorización.
- Hacer notar que no existen virus benignos.
- Describir la relación que puede existir entre virus y piratería.
- Responsabilidades que tiene un proveedor cuyo software "original" contiene virus.
- Enunciar las consecuencias que trae esta lucha de antivirus contra virus, como el despilfarro de recursos.

VII. CONCLUSIONES

Cuando se dieron a conocer los primeros virus informáticos no se pensó en que pudieran existir virus polimórficos o amigos que son actualmente los más dañinos, y ya que la lucha de antivirus contra virus puede resultar eterna, lo mejor es tener un respaldo actualizado de la información.

Después de un respaldo actualizado no debe faltar uno o la combinación de algunos antivirus para la protección, detección y erradicación de virus.

Mucho se ha temido que algún fabricante de software considere introducir virus en sus productos para controlar la piratería. Esto sería lo mismo que decir que, de alguna manera, la piratería fomenta la creación de virus. Sin embargo, en nuestro país al restringir las posibilidades de obtener copias a bajo costo, seguramente se detendría el desarrollo informático y la formación de recursos humanos altamente capacitados.

Aunque algunos autores clasifican a ciertos virus como "benignos" por que no dañan información sino sólo emiten algún mensaje, prácticamente no existe virus que no implique pérdida de tiempo. En el mundo de los negocios se traduce en dinero.

Es muy difícil evaluar de manera general el costo de un virus, ya que en éste influyen factores como el valor de la información dañada o perdida que varía mucho en cada caso. Sin embargo, con sólo traducir esto en tiempo, siempre será una pérdida, como tal, podemos afirmar que desde el surgimiento de los virus, los costos asociados a la Informática se han elevado, ya sea por la adquisición de antivirus o por remediar el daño causado, las empresas e individuos usuarios de las computadoras han tenido que pagar un precio que nunca antes se hubiera previsto.

Es necesario tener ya una ley que controle los actos relacionados a la informática, contemplando también las actividades relacionadas con virus, ya que actualmente los usuarios no saben hasta dónde están permitidos dichos actos; y aunado a esto, la construcción de un código de ética.

Lo que está detrás de un virus es la búsqueda de los puntos débiles o de las fallas de los sistemas operativos, y de alguna manera los creadores de virus al detectar dichas fallas han fomentado que se les hagan mejoras, sin embargo es en los usuarios de dichos sistemas en quienes repercuten las consecuencias que ocasionan estos huecos que ha dejado el avance tecnológico. Estos recursos humanos que han detectado las debilidades de los sistemas operativos o de las arquitecturas de las computadoras, bien podrían trabajar en favor de las empresas fabricantes de software.

BIBLIOGRAFÍA

1. B. Levin, Richard. Virus Informáticos, Editorial Mc-Graw-Hill, México, 1992.

2. Ferreyra Cortés, Gonzalo Virus en las computadoras, 2ª edición, Editorial Macrobit, México, 1991.

3. Norton, Peter y Nielsen, Paul. Norton Antivirus, Editorial Prentice Hall, México, 1992.

4. Cortés, Pedro Luis. Virus manual de referencia, Editorial Ventura, México, 1994.

5. Nombela, Juan José y Del pino González, Javier. Virus Informático, 2ª edición, Editorial Paraninfo, Madrid, España, 1991.

6. Greer, William. Cazadores de virus, Editorial Toray, Barcelona, España, 1966.

7. Rodríguez Cárdenas, Mario. Saque virus y rescate archivos perdidos, Editorial Rócar, México,1995.

8. Mallén, Guillermo M. Virus computacionales, CONACYT-Sirius, México, 1994.

9. Cohen, Frederick B. A short course on computer viruses, Editorial ASP Press, Pittsburgh, USA, 1990.

10. Sandoval Ruiz, Justo Evelio. Derecho Informático, una perspectiva jurídica, Tesis doctorado, Facultad de Derecho, UNAM, 1994.

11. Boletín Técnico ITASA, Monterrey, N.L., México, 1995.

12. User's Gulde & Reference-SAM, CA, E.U., 1992.

13. Mayo, Jonathan. What they are, how they work, how to avoid them, E.U.. 1989.

Direcciones de Internet

1. http://www.cis.ohio-st...ter-virus-faq/faq.html

2. http://dbweb.agora.stm.it/webforum/virus/viruinfo.html

3. http://dbweb.agora.stm.it/webforum/virus/solomhis.htm#H04

4. http://dbweb.agora.stm.it/webforum/virus/sladerev.html