VIRUS INFORMATICOS

ÍNDICE DE CONTENIDOS

INTRODUCCIÓN

Actualmente los virus informáticos representan una gran amenaza para los equipos de cómputo. El problema se agudiza en los equipos conectados en una red local y/o a Internet debido a la capacidad de propagación de estos a través de los sistemas redes de computadoras. Es por esto que el objetivo que persigue este trabajo se centra en proporcionar una definición plausible de lo qué es un virus, diferenciar los diferentes tipos de virus que se pueden encontrar, medidas de prevención que se pueden tomar, etc.

¿QUÉ ES UN VIRUS?

Con el término "**virus**" se designa un programa de ordenador, generalmente anónimo y escrito en lenguaje ensamblador, que lleva a cabo acciones que resultan nocivas para el sistema informático y cuyo funcionamiento queda definido por las propiedades que se indican a continuación:

1. Es capaz de generar **copias de sí mismo** de forma homogénea o en partes discretas, en un fichero, disco u ordenador distinto al que ocupa.
2. **Modifica** los programas ejecutables a los que se adosa, o entre cuyas instrucciones de código se introduce, consiguiendo así una ejecución parasitaria. Esto implica que se pueda activar de forma involuntaria por el usuario cuando éste ejecute el programa que lo porta. Los programas

portadores pueden ser de uso común del usuario o programas ejecutables del sistema operativo, siendo estos últimos el objetivo esencial del virus.

3. El **efecto** que produce un virus puede comprender acciones tales como un simple mensaje en la pantalla, la ralentización de la velocidad de proceso del ordenador o el formateo de una unidad de disco, pero no se debe olvidar que su funcionamiento intrínseco coincide con el de cualquier programa ejecutable. Esta característica supone que para que un programa de este tipo ejerza sus acciones nocivas es necesario que se active, es decir, que el código que lo conforma se ejecute. Por otro lado, debe permanecer en memoria para poder obtener así el control permanente de la unidad central de proceso (CPU), centro neurálgico del ordenador.

Generalmente, su funcionamiento comprende dos fases bien diferenciadas. Durante un período el programa permanece oculto al usuario, en espera de una acción,

como la introducción de una cadena especial de caracteres por el teclado, una fecha determinada o un tope de autocopias del virus almacenado en un contador interno. En esta fase el programa realiza una acción de esparcimiento cuyo objetivo fundamental consiste en realizar el mayor número posible de copias de sí mismo en otros soportes distintos o en el mismo que él ocupa. Una vez que se produce este hecho, el virus realiza la acción nociva para la que ha sido programado, completando así la segunda fase de funcionamiento. Por último, cabe destacar que un virus se diseña intentando disfrazar su presencia ante el sistema y ante el usuario. Generalmente no es descubierto hasta que, en la segunda fase del ciclo de funcionamiento del programa, surge un hecho anormal derivado de su ejecución que da la señal de alarma.

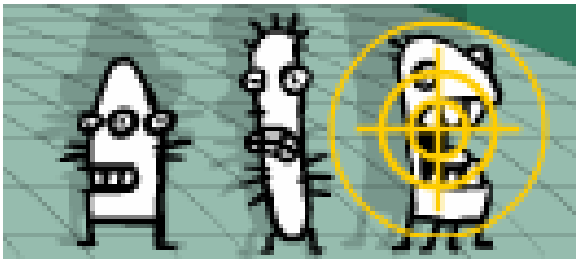
La denominación de virus informático corresponde a una metáfora que asocia este tipo de programas con sus homónimos biológicos. Ciertos autores han querido en encontrar en las características

de los virus biológicos ciertas similitudes con los programas de sabotaje. Así ha nacido una nueva jerga informática que incluye términos como "epidemia", "contagio", "infección", "vacuna", "antídoto", "tiempo de incubación", etc.

Ciertamente podría existir una similitud en lo que se refiere al fenómeno autorreproductor del *virus biológico* con su metáfora informática. Incluso sería aceptable comparar el tiempo de latencia o incubación de un germen con la espera ante un hecho que desencadene el virus informático.

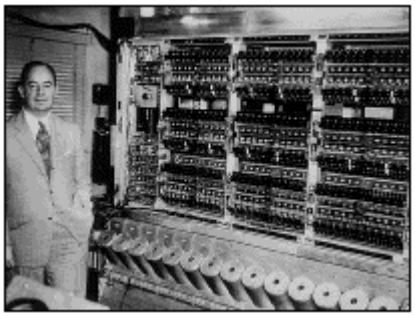
Aunque resulte simple la aclaración, se hace necesario destacar que el “contagio” del virus se realiza de forma lógica a través de operaciones e entrada y salida sobre soportes magnéticos, estando el programa contaminante en ejecución y residente en le memoria.

No se debe olvidar que el origen de todo virus es un programa "padre" desarrollado por un programador experto, encargado de iniciar la epidemia de acciones perjudiciales. Este punto es fundamental, ya que puede suponer la única prueba fehaciente cuando se trata de ejercer acciones legales contra el responsable de una "infección vírica".



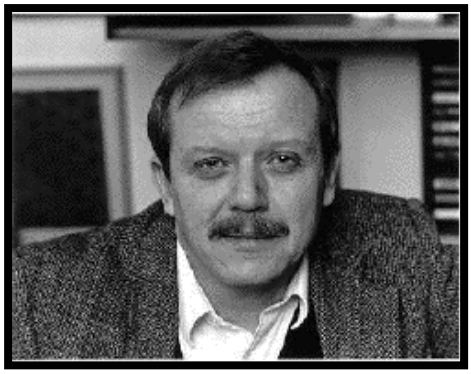
La **moraleja** aplicable de esta definición es que no hay virus benigno. Cualquier funcionamiento anómalo de un sistema de información supone un perjuicio para el usuario que implica una pérdida importante de tiempo y, por tanto, de dinero.

ORIGEN DE LOS VIRUS



Los articulistas más escrupulosos han pretendido otorgar a **John Von Newmann** la paternidad de los virus. Von Newmann, matemático brillante, hizo importantes contribuciones a la física cuántica, la lógica, la meteorología y la teoría de ordenadores. En un artículo titulado "*Theory and Organization of Complicated Automata*", de 1949, Newmann expone la idea de una porción de código que se reproduce y por tanto está "vivo". Años más tarde, en 1955, en su obra *The Computer and the Brain* (publicado en español en 1980 con el título *El ordenador y el cerebro*), hace una disertación teórica sobre la posibilidad de crear un autómata capaz de reproducirse a sí mismo. Estos primeros indicios teóricos de autorreproducción del software y del hardware no parecen ser lo bastante sólidos para establecer el origen.

La clave en el origen de la difusión del fenómeno vírico se ha querido situar en una serie de artículos publicados en la revista americana *Scientific American*, firmados por **A. K. Dewdney**. El primero de la serie, fechado en mayo de 1984 y traducido en *Investigación y Ciencia*, versión castellana de la revista americana, en julio de 1984, se tituló "*Juegos de ordenador: en el juego de la «**Guerra Nuclear**» los programas hostiles entablan, sin ayuda externa, batallas de bits*"[1]. En este primer artículo, Dewdney explica el programa llamado Guerra Nuclear, juego en el que no intervienen activamente los usuarios. En él, dos programas hostiles se enzarzan en una lucha para obtener el control de la memoria atacando abiertamente al contrario. Estos dos programas se ponen en marcha mediante un programa ejecutor llamado **MARS** (Memory Array Redcode Simulator), que va ejecutando alternativamente las instrucciones de que constan los programas de



[1] El nombre original del juego es Core War, cuya traducción técnica es “Guerras de toros de ferrita”; la expresión hace referencia a los núcleos de ferrita en forma de tiroides que componían en un principio las memorias de los ordenadores. No se entiende el origen del término “nuclear”, que seguramente será una desfiguración del término “núcleo”.

combate, una instrucción de cada programa, de modo similar a un sistema caracterizado por compartir tiempos.

Ayudado por **David Jones**, alumno de su departamento, va desarrollando programas cada vez mejor equipados para destruir a su contrario. Una de las versiones, denominada **Gemini**, tenía como única función producir una copia de sí mismo cien unidades de memoria más allá de su posición actual, transfiriendo después el control a la nueva copia. Dewdney comenta en este artículo que el origen de su Guerra Nuclear está en una tecnología de construcción de memorias. Cita el autor dos precedentes de su juego:

- ✓ Por un lado**, M. Douglas McIlroy**, de los laboratorios americanos Telephon & Telegraph, diseñó un programa llamado **Darwin**. En él, cada jugador presenta cierto número de programas en lenguaje ensamblador llamados "organismos", que habitan conjuntamente en la memoria central con los organismos presentados por los demás contendientes. Los programas creados por cada jugador, pertenecientes a una misma especie, tratan de aniquilar a los de otra especie. Gana la partida el jugador con más organismos al acabar el tiempo de combate.
- ✓ Por otro lado, **John F. Scoch y John Hupp**, del Centro de Investigación de **Xerox** en Palo Alto, Estados Unidos, crean **WORM**. Este programa experimental fue ideado para obtener el máximo rendimiento de una red de miniordenadores interconectados de Xerox. Un programa supervisor se encargaba de cargar el "gusano" en máquinas inactivas para asumir el control de la máquina y, en combinación con otros gusanos residentes en otras máquinas inactivas, hacer funcionar grandes programas de aplicación en el sistema multiprocesador resultante. Se suponía que lo iban a probar simplemente en los seis equipos que tenían en su laboratorio, y que se crearía una única copia en cada uno. Al día siguiente, todos lo s equipos del centro estaban “infectados” y habían en ellos tantas copias que muchos estaban bloqueados por falta de memoria. Cuando intentaron reactivar el sistema, el gusano volvió a reproducirse y se expandió de nuevo por el sistema. Como consecuencia, tuvieron que crear el primer antivirus de la historia.

En el texto de este primer artículo, **Dewdney** insta a los lectores a que reflejen sus ideas de programas autoprotectores y autorreparadores y establece las normas y reglas del juego.

En el transcurso del mismo año se define por primera vez, de forma pública, el término "***virus de ordenador***". Durante la conferencia IFIC/SEC'84, en septiembre de 1984, el doctor **Fred Cohen**, en su exposición de la ponencia "*Computer Viruses: Theory and Experiments*", explica este tipo de programas como software maligno capaz de reproducirse a sí mismo. Este hecho hizo que se le considerara mayoritariamente como el **padre de la teoría vírica**. A partir de este momento, ya se tenía una idea muy clara sobre líneas de diseño.

El segundo artículo de Dewdney en Scientific American, en marzo de 1985 (mayo de 1985 en Investigación y Ciencia), se titula "*Juegos de ordenador: virus, gusanos y otras plagas de la Guerra Nuclear atentan contra la memoria de los ordenadores*". En él Dewdney pone de manifiesto las consecuencias que puede acarrear su juego gracias a los testimonios escritos de sus lectores.

Comenta el autor: "... *Cuando en julio del año pasado apareció el artículo dedicado a la «Guerra Nuclear», no se me ocurrió que pudiera estar tocando un tema tan serio. Las descripciones de programas escritos en lenguaje máquina que entonces di, capaces de desplazarse de uno a otro lugar de la memoria, al acecho, dispuestos a aniquilarse el uno al otro, pulsaron una cuerda resonante*". Continúa diciendo el autor: "... *según muchos lectores cuyas historias y anécdotas referiré, existen multitud de gusanos, virus y otros organismos «programáticos», que moran en todo ambiente informático concebible. Tan horripilantes son algunas de las posibilidades, que dudo si transcribirlas*".

No debe interpretarse que fue **A. K. Dewdney** el inventor de los virus, más bien se debe ver como un impulsor involuntario de este tipo de programas al difundir un inocente y creativo juego. No se trata de debatir la transparencia informativa del fenómeno, lo que no cabe duda es que el autor colaboró inocentemente en dar a

conocer el fenómeno vírico cuando decidió transcribir alguna de las "horripilantes posibilidades".

En 1981 aparece ya un programa diseñado par un sistema en particular, concretamente para Apple II. Se trataba del **ELK CLONER**. Este programa sacaba versos por pantalla y se duplicaba. Un año después, **Jim Hauser y Williarn R. Buckley**, de la Universidad Politécnica de California, crearon el **APPLE WORM o ELECTRONIC HITCHNICKER**, gusano de los ordenadores de la marca Apple que sacaba copias de sí mismo en un viaje a través de la memoria del Apple II con un procesador 6502.

Otra de las plagas informáticas fue concebida por **Roberto Cerruti y Marco Morocutti** en la ciudad de Brescia. Los dos italianos buscaron el medio de infectar el **Apple II**, pero no con un gusano sino con un **virus**. Las conclusiones que sacaron fueron que el programa tendría que infectar los discos y utilizar los ordenadores como medio de transmisión de un disco a otro. El virus era una alteración del sistema operativo contenido en cada diskette del Apple. Comenta Dewdney la intención, no llevada a cabo, de los programadores latinos de convertir el virus en maligno. La ocurrencia consistía en que al cabo de dieciséis ciclos autorreproductores contados en el disco contagiado, el programa decidiera reinicializar el disco inmediatamente después del primer arranque. Incluso se les ocurrió colocar sus virus en los discos utilizados en la principal tienda de informática de su ciudad. La razón triunfó y no llevaron adelante su idea.

En 1986, el ingeniero **Ralf Burger**, basándse en las tesis de Fred Cohen, diseña un virus denominado **VIRDEM**. Este virus borraba gradualmente los archivos de la computadora destruyéndose después de grabar copias de sí mismo en los archivos.

En el *artículo de Scientific American de enero de 1987* (Investigación y Ciencia, en marzo del mismo año), Dewdney abandona completamente cualquier relación de su juego con los virus y se dedica a narrar el primer campeonato del polémico juego Guerra Nuclear. En este mismo año se produjeron varias infecciones importantes por parte de copias del **VIENNA** y del **BRAIN**.

En 1988 **dos nuevos virus** aparecen para el sistema Apple Macintosh. El primero de ellos sacaba un mensaje de paz, así como un pequeño dibujo del planeta Tierra firmado por **Drew Davidson** (supuesto autor del virus). Estaba programado para

ejecutarse el 2 de marzo de 1988 coincidiendo con el aniversario de Macintosh II. El autor lo repartió en la reunión de un club de usuarios y uno de ellos, **Marc Canter**, consultor de la empresa **Aldus Corp**., contaminó sin querer su ordenador. Posteriormente, la probar el programa maestro del **Aldus Freehand**, lo contaminó a su vez, y de ese modo se extendió la epidemia quedando más de cinco mil copias repartidas inadvertidamente.

El segundo virus fue el **SCORES.** El 19 de abril de 1988, una filial de **General Motors** de Dallas (EEUU), anunció que 24 de sus computadoras estaban infectadas. A partir de lo sucedido, comenzaron a aparecer programas antivirus y especialistas en seguridad, de hecho, es en este mimo año cuando sale al mercado uno de los primeros antivirus denominado **FLU SHOT**, creado por el programador Ross Greenberg. Además, también aparece el **VIRUSCAN** de John McAfee.

El 9 de diciembre de 1987, en la Universidad de **Clausthal-Zellerfeld**, varias personas recibieron un mensaje felicitándoles la Navidad. Debían escribir la palabra "*Christmas*" y saldría el mensaje. Así lo hicieron varios usuarios y pudieron ver un árbol de Navidad. Lo que no vieron era que su sistema de correo estaba lleno de copias del mensaje. El programa, una vez ejecutado, leía las direcciones electrónicas de todos los estudiantes y mandaba copias de sí mismo a dichas direcciones. Se trataba del primer Caballo de Troya de la historia. La infección fue de tal envergadura que en seis días miles de ordenadores de todo el mundo estaban dañados.

Al mismo tiempo, seguían apareciendo gusanos en las redes. Sin ir más lejos, en 1989, los ordenadores **VAX** de la **NASA**, fueron bloqueados por un nuevo gusano con mensajes antinucleares.

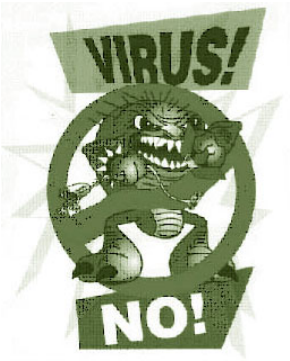
Los virus producían el 13 de mayo de 1988 su miembro más famoso: el **JERUSALEM o VIERNES 13**. Coincidiendo con el cuarenta aniversario de la fundación del estado de Israel, miles de ordenadores fueron infectados, incluyendo los del ejército y los ministerios. Finalmente, la aparición del **MICHELANGELO** hizo tomar conciencia a los usuarios de que algo muy serio se había destapado.

Ante la actualidad y notoriedad del fenómeno vírico y el rosario de informaciones que surgían al respecto, Dewdney retorna el tema en un nuevo artículo en Scientific American, en marzo de 1989 (Investigación y Ciencia, en abril del mismo año). Bajo el título "Juegos de ordenador: sobre gusanos, virus y Guerra Nuclear", el autor se

defiende de las reiteradas insinuaciones sobre la presunta relación existente entre Guerra Nuclear y los programas víricos. Justifica Dewdney su postura de transparencia informativa ante el fenómeno como un factor constructivo en el sentido de estimular los esfuerzos para la protección de sistemas. Recrimina a la prensa sensacionalista que por medio de artículos incompletos y distorsionados, escritos por columnistas que desconocen el funcionamiento interno del ordenador, ha conducido al desconcierto. Utiliza además otro argumento de peso. Las descripciones de un virus, incluso las más detalladas, no pueden utilizarse en la reconstrucción de un programa nocivo, excepto por un experto. Una persona con tal nivel de conocimientos no necesita de la lectura de revistas para crear un código que destruya los programas y los datos de otros.

Después de sentar estas bases y sin encontrar un motivo para no hacerlo, Dewdney realiza una detallada explicación del funcionamiento de los programas víricos. Se manifiesta de acuerdo con las teorías de Cohen referentes a la imposibilidad de construir un programa que detecte todo tipo de virus. Concluye este último artículo de la serie con una frase que deja claro la involuntariedad e inocencia del autor en la difusión del fenómeno vírico: "Escribir y ejecutar un virus no es la obra de un profesional de la informática y sí es la de un vándalo del ordenador. Permitamos que aquellos que pudieran contemplar actos similares prueben en vez de eso a participar en la Guerra Nuclear".

Algunas hipótesis, sin confirmación, apuntan a los grandes fabricantes de software como iniciadores de la corriente vírica. La justificación se establece como mecanismo de protección contra la copia para evitar que sus productos fuesen multitudinariamente plagiados sin obtener beneficios. Es evidente el quebrante económico que este otro tipo de delito produce en la industria del software, pero parece descabellada la idea de combatir el fuego con fuego. Este tipo de guerra acabaría perjudicando a los mismos fabricantes, que tendrían que reemplazar miles de copias de sus productos. No parece sensato que quieran tirar piedras contra su propio tejado. Además, la tendencia actual en el software está acabando con las protecciones. La mayoría de las casas comerciales está desprotegiendo sus productos contra la copia. Esta justificación se refiere a los grandes diseñadores de programas, no descartándose que algún pequeño fabricante haya utilizado estas técnicas de protección.



Resulta realmente complicado establecer la verdadera procedencia de este tipo de programas. Seguramente no surgieran de forma aislada en un único lugar y como idea de un único programador, sino que son el fruto, de la ocurrencia simultánea de distintos programadores malévolos en varios países.

TIPOS DE VIRUS

La clasificación de los virus es muy variada. Pueden diferenciarse según la **entidad** que parasiten (sector de arranque, archivos ejecutables o ambos), por su grado de **dispersión** a escala mundial, por su **comportamiento**, por su **agresividad**, por sus **técnicas** de ataque o por la forma en que se **ocultan**.

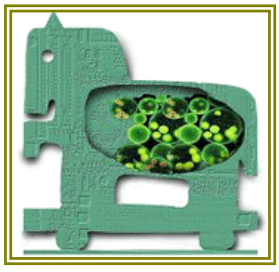
En este trabajo se hará referencia a una serie de términos que son más conocidos y utilizados de forma habitual en el lenguaje informático. Se incluyen: *Caballos de Troya, Camaleones, Gusanos, Bombas Lógicas y de Tiempo, Joke - program, Conejos, Leapfrog, Máscaras, Mockinbird, Spoofing, Back door, Tunnelling, Stealth, Variante, Polimórfico, Armouring, Killers, Spare, Dropper, Circular, Hoax, Macrovirus,* etc.

Esta agrupación es una especie de "cajón de sastre" en la que algunos de los términos **no son considerados virus** ya que no cumplen alguna de las características víricas que se han definido anteriormente. En esta clasificación se consideran como tales, ya que de un modo u otro, pueden causar daños importantes. Por tanto, esta clasificación no es estricta ni restringida. Un virus puede utilizar varias de éstas técnicas, ya que no son incompatibles entre sí.

A continuación se **definen** los distintos tipos de virus según, entre otras características, su comportamiento:

Caballos de Troya (troyan horses)

El nombre hace referencia a la historia que se narra en la **Ilíada**: los soldados griegos construyeron un caballo de madera en el que se escondieron astutamente con el fin de tomar la ciudad de Troya. Al igual que el famoso caballo de Troya, estos programas también son impostores ya que aparentemente no dañan el sistema y aparecen de forma llamativa para el usuario a modo de juegos o



anuncios. Para el diseño de estos programas existen varios métodos, uno de ellos consiste en desensamblar un programa popular y legal, añadirle determinadas instrucciones legales, ensamblarlo otra vez y redistribuirlo nuevamente.

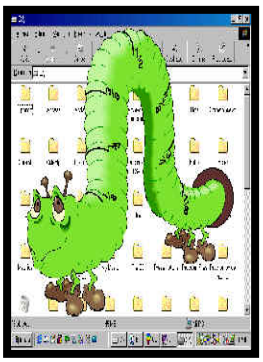
Los caballos de Troya pueden provocar pérdidas e incluso robo de datos. La principal **diferencia con los virus** es que no son capaces de autorreplicarse. Ejemplos de estos son **Pishing. gen**, uno de los más difundidos en la actualidad, y **Trojandownloader. Small.ZL.**

Camaleones

Son similares a los caballos de Troya. Se trata de programas malignos disfrazados de programas comerciales (benignos) como son los empaquetadores, los programas de demostración de productos, etc. en los que el usuario confía. Pueden almacenar logins y contraseñas (passwords) para, posteriormente, ser recuperados y utilizados ilegalmente por el creador del virus camaleón.

Gusanos (worms)

Son los más amenazantes para los sistemas con servicio de **Internet** y correo electrónico. Los gusanos, a diferencia de los virus, no necesitan un programa al que poder adherirse para reproducirse, sino que se replica por sus propios medios a través de la red. Una vez instalado en el equipo se va a copiar en otras zonas de la memoria del ordenador hasta conseguir ocupar y desbordar la capacidad total de almacenamiento de la memoria. Los gusanos pueden modificar el registro del sistema y a la vez puede contener también una serie de subprogramas que son los encargados de reproducirse.



Algunos gusanos son: **Netsky Q., Zafi B., Sober I, Mydoom R., Lovgate, Happy99, Melissa Virus (virus de macro) y Bubbleboy Worm.**

Bombas Lógicas y de Tiempo

Estos programas nocivos sólo se activan al producirse un acontecimiento determinado.

Las bombas de tiempo son virus convencionales y pueden tener una o más de las características de los demás tipos de virus pero la diferencia está dada por su módulo de ataque que se disparará en una fecha determinada. Por lo general muestran mensajes en la pantalla en alguna fecha que representa un evento importante para el programador. Su mala fama vienen de virus como el **Viernes 13** (la primera versión fue descubierta en diciembre de 1987 en los ordenadores de la Universidad Hebrea de Jerusalén) o el **Michelangelo** (causa un daño grande; se activa el 6 de marzo). Aquí también se incluye por ejemplo, el programa del moroso, que se activa pasado unos días si el cliente no ha pagado.

Las bombas lógicas se inician cuando se da una condición lógica: que se pulse una combinación de teclas o palabra determinadas, que se llene el disco duro hasta cierto nivel, que se ejecute una determinada orden del sistema, etc.

Joke – program

No suelen ser malignos. Bajo este término se agrupan todos aquellos virus que sólo resultan simpáticos. En un principio había muchos, como el **COME-COME**, el **MUSHROOM, el COOKIE**... Este virus sacaba por pantalla: “Polly wants a cracker”, o “Cookie monster is here” para desactivarlo bastaba con escribir “Cookie”. Hoy en día se diseña alguno de tarde en tarde pero no los bastantes como para reconciliarnos con los virus- maker.

Conejo (o peste)

Este tipo de técnica es muy utilizada por los **gusanos**. El código se reproduce a toda velocidad y de forma infinita llenando el disco duro del ordenador, o en caso de las redes, bloqueando el sistema al comerse literalmente toda la memoria.

Otro sistema más consiste en llenar de copias de sí mismo las colas de impresión o de correo echando a los demás usuarios e impidiendo que trabajen.

Cuando los ordenadores de tipo medio estaban extendidos especialmente en ambientes universitarios funcionaban como multiusuario con un nivel de prioridad. El ordenador ejecutaba los programas de cada usuario dependiendo de su prioridad y tiempo de espera. Si se estaba ejecutando un programa y llegaba otro de prioridad superior, atendía al recién llegado y al acabar continuaba con lo que hacía con anterioridad. Como por regla general, los estudiantes tenían prioridad mínima, a alguno de ellos se le ocurrió la idea de crear este virus. El programa se colocaba en la cola de espera y cuando llegaba su turno se ejecutaba haciendo una copia de sí mismo, agregándola también en la cola de espera. Los procesos al ser ejecutados iban multiplicándose hasta consumir toda la memoria de la computadora central interrumpiendo todos los procesamientos.

Leapfrog (o rana)

Lo usan los gusanos cuando desean conocer las claves de acceso o las cuentas de correo. El sistema más obvio es leer las listas de correo del usuario y enviar copias a las mismas.

Máscara

Para entrar en un sistema restringido, el virus adopta la personalidad de un usuario autorizado haciéndose pasar por él. No es muy utilizado.

Mockinbird

El virus se queda fuera del sistema en estado de espera, y cuando un usuario autorizado entra, se fija en el proceso de entrada aprendiendo la clave de acceso, nombre de usuario y cualquier otro dato interesante. Puede aprovechar el hueco para entrar y actuar. Normalmente no causa daños para no revelar su existencia.

Spoofing

Una variación del anterior. En éste caso al entrar en el sistema, lo bloquea. Podemos decir que el spoofing es un mockinbird con mala uva.

Back Door

Usada por algunos Gusanos y Caballos de Troya. Se crea una "puerta trasera" o agujero en el sistema, por el que el diseñador podrá entrar más tarde sin que lo detecten.

Tunnelling

Es una técnica usada por programadores de virus y antivirus para evitar todas las rutinas al servicio de una interrupción y tener así el control directo sobre esta. Los virus utilizan el **tunneling** para protegerse de los módulos residentes de los antivirus que, monitorean todo lo que sucede en la máquina para interceptar todas la actividades "típicas" de los virus. Requiere una programación compleja: se necesitan conocimientos amplios de programación en lenguaje máquina. No suelen durar mucho, pues más pronto o más tarde se descubre el truco y se aumentan los puntos de vigilancia.

Stealth (o silencioso)

Oculta síntomas de la infección que todo virus realiza inevitablemente al actuar sobre un fichero. En general capturan determinadas interrupciones del PC para ocultar la presencia de un virus, como mantener la fecha original del archivo, evitar que se muestren los errores de escritura cuando el virus escribe en discos protegidos...El problema para ellos es que el sistema stealth funciona cuando el virus está activo en la memoria, y arrancando desde disquetera esto se evita y queda a merced del antivirus.

El virus **Brain** es un ejemplo de este tipo de virus. Se aloja en el sector de arranque del disco e intercepta cualquier operación de entrada o salida que se intente hacer en esa zona.

Variante

Se usa un virus idéntico al original, pero que presenta pequeños cambios, normalmente en los mensajes que pueda llevar el código vírico. Hoy en día aparecen muchas variantes de virus para los cuales existen programas generadores. El usuario sólo debe escribir un texto distinto y ensamblar el virus. En lo demás, suelen actuar como el original. Otro sistema puede ser el cambio de las fecha de activación para confundir a los investigadores.

Polimórfico (o mutante)

Un virus polimórfico intenta escapar de los antivirus produciendo mutaciones de sí mismo cuando se copia en el fichero. Este es el método más logrado por los programadores de virus. La técnica básica usada es la de inserción del código viral en un archivo ejecutable, pero para evitar el aumento de tamaño del archivo infectado, el virus compacta parte de su código y del código del archivo anfitrión de manera que la suma de ambos sea igual al tamaño original del archivo. Es una técnica para impedir ser detectados la de variar el método de encriptación de copia en copia. Esto obliga a los antivirus a usar técnicas heurísticas ya que como el virus cambia en cada infección es imposible localizarlo buscándolo por cadenas de código. Esto se consigue utilizando un algoritmo de encriptación que ponga las cosas muy difíciles a los antivirus. No obstante no se puede codificar todo el código del virus, siempre debe quedar una parte sin mutar que toma el control y esa es la parte más vulnerable al antivirus.

Al ejecutar el programa infectado el único que actúa es el virus. En cada infección se eliminan archivos de programas válidos, los cuales son reemplazados por nuevas copias del virus.

En un principio este sistema era peligrosísimo, e incluso aparecieron virus con millones de mutaciones posibles. Sin embargo hoy en día los antivirus son muy

efectivos. Hay varios tipos según el sistema de encriptación que usen. Aquí se incluyen por ejemplo los virus oligomórficos que poseen un conjunto reducido de funciones de encriptación y eligen una de ellas aleatoriamente. Requieren distintos patrones para su detección.

Armouring

Usan trucos para evitar la búsqueda, desensamblaje y lectura de su código. Mediante esta técnica el virus impide que se examinen los archivos que él mismo ha infectado. Para conocer más datos sobre cada uno de ellos, éstos deben ser abiertos (para su estudio) como ficheros que son, utilizando programas especiales (debuger) que permiten descubrir cada una de las líneas del código (lenguaje de programación en el que están escritos). Pues bien, en un virus que utilice la técnica de armouring no se podrá leer el código.

Killers (o retrovirus)

Un retrovirus intenta como método de defensa atacar directamente al programa antivirus incluído en el ordenador. Precisamente de una forma de ver la fama o perfección de un antivirus es comprobar cuántos retrovirus se diseñan contra él.

Spare

Llevan una **bomba de tiempo** aleatoria. No se sabe cuándo se activarán. Se cree que hay más de cincuenta Spare creados en los últimos cinco años que aún no se han activado. De todas formas, cuanto más aumenta el tiempo de ocultamiento más aumentan las posibilidades de descubrirlo. Hoy en día muchas vacunas llevan sistemas para detectar virus desconocidos.

Dropper (o comadronas)

Un programa que al ser ejecutado, lanza el virus. Todos los virus suelen comenzar su vida operativa como Droppers. Puede resultar interesante, porque a veces son difíciles de detectar en ese estado.

Circular (o redundante)

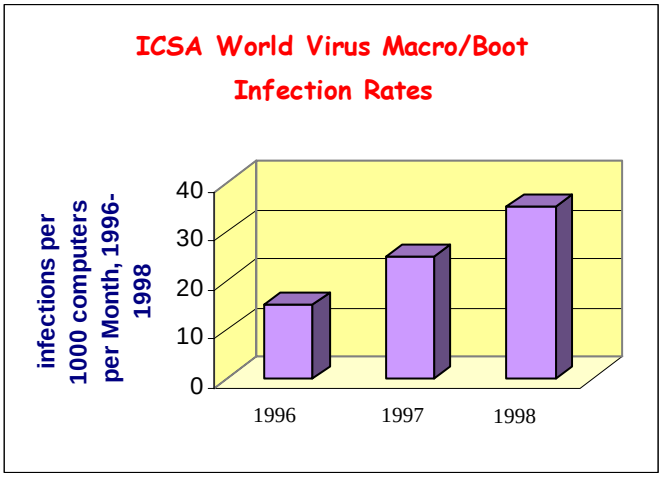
Cuando dos virus infectan a la vez el sector de arranque del disco. Lo normal es que un virus no infecte si el objetivo está ya infectado, pero los hay que se diseñan para poner las cosa más difíciles permitiendo varias infecciones en el sector de arranque. Al borrar uno, queda el otro y viceversa. Si no se limpia con cuidado, el virus que queda puede aprovechar para intentar incluso la infección de la vacuna.

Hoax

No es un virus. Se trata de un falso mensaje sobre el descubrimiento de un troyano o un gusano en Internet.

Macrovirus

Representan una de las amenazas más importantes para la red y también para los ordenadores independientes. Actualmente son los virus que más se están extendiendo a través de Internet. Su máximo peligro reside en que son completamente independientes del sistema operativo o de la plataforma. Es más, ni siquiera son programas ejecutables sino que son pequeños programas escritos en el lenguaje propio de un programa. La mayoría de los macrovirus se han escrito en lenguaje de intérprete como el WordBasic o incluso en la última versión de Visual Basic para Aplicaciones (VBA), ambos de Microsoft. Actualmente hay macrovirus que infectan ficheros de CorelDraw, Microsoft Word, Microsoft Excel, Microsoft Access, Microsoft Powerpoint, etc. Para detectarlos y borrarlos se necesitan antivirus específicos.



Sus autores los escriben para que se extiendan dentro de los documentos que crea el programa infectado. De esta forma se pueden propagar a otros ordenadores siempre que los usuarios intercambien documentos a través de archivos adjuntos de e-mail (attachements), disquetes, bajadas de Internet, transferencia de archivos y aplicaciones compartidas. Este tipo de virus alteran de tal forma la información de los documentos infectados que su recuperación resulta imposible.

→ Para finalizar es necesario definir un último término:

Bug-ware:

Es un error de diseño en un programa. Muchas veces los usuarios aducen esos daños a la actividad de virus informáticos. Los programas bug-ware no son en absoluto virus informáticos, simplemente son fragmentos de código mal implementado o bien no son bien utilizados por los usuarios produciéndose errores, dañándose el hardware o inutilizándose los datos del computador.

Se denomina así por un curioso suceso con una de las primeras computadoras de válvulas. Ésta comenzó a funcionar mal. Después de varios días, al ser desarmada, se encontró que la causa de la mal función era una polilla (bug) que se había introducido en los circuitos.

FUNCIONAMIENTO DE LOS VIRUS INFORMÁTICOS

Un virus es ante todo un código informático capaz de reproducirse a si mismo y atacar a un programa inofensivo sin conocimiento del usuario. Los virus se diseñan con intenciones malignas y destructivas.

CICLO DE VIDA DE LOS VIRUS INFORMÁTICOS

Los virus informáticos tienen un ciclo de vida determinado, que comienza cuando son creados y termina cuando son erradicados completamente. Se distinguen distintas etapas:

1. Creación: Antes para crear un virus se requería del conocimiento del lenguaje de programación assembler. Actualmente, cualquiera con un poco de conocimiento en programación puede crear un virus.

2. Gestación: Luego de que el virus es creado, el programador hace copias asegurándose de que se diseminen.

3. Fase de infección: Se subdivide en tres fases:

    a) **Primera fase (infección):** El virus pasa a la memoria del ordenador, y toma el control del mismo después de intentar inicializar el sistema con un disco, o con el sector de arranque infectado o de ejecutar un archivo infectado.

    El virus pasa a la memoria y el sistema se ejecuta, el programa funcionará aparentemente con normalidad, de esta forma el usuario no se da cuenta de que su sistema está siendo infectado.

b) **Segunda fase (latencia):** Durante esta fase el virus, intenta replicarse infectando otros archivos del sistema cuando son ejecutados o atacando el sector de arranque del disco duro. De esta forma el virus toma el control del sistema siempre que se encienda el ordenador, ya que intervendrá el sector de arranque del disco, y los archivos del sistema.
Si durante esta fase usamos discos flexibles no protegidos contra escritura, dichos discos quedan infectados y listos para pasar el virus a otro ordenador e infectar el sistema.

c) **Tercera fase (activación):** Esta es la última fase de la vida de un virus y es la fase en donde el virus se hace presente.

La activación del virus trae como consecuencia el despliegue de todo su potencial **destructivo**, y se puede producir por muchos motivos, dependiendo de cómo lo creó su autor y de la versión de virus de que se trate, debido a que en estos tiempos encontramos diversas mutaciones de los virus. La mayoría de los virus se activan mediante el reloj del sistema para comprobar la fecha y activar el virus, dependiendo de la fecha u hora del sistema, o mediante alguna conducción y por último atacan, el daño que causan depende de su autor.

Algunos virus se activan después de un cierto número de ejecuciones de un programa infectado o de encender el sistema operativo; otros simplemente esperan a que se escriba el nombre de un archivo o de un programa. Es decir, los virus que contienen rutinas dañinas, se activarán bajo ciertas condiciones, por ejemplo, en determinada fecha o cuando el usuario haga algo determinado. Los virus sin rutina dañina no se activan, pero causan daño al robar espacio en el disco.

- Descubrimiento: Esta fase por lo general viene después de la activación. Cuando se detecta y se aísla un virus, se envía al International Security Association en Washington D.C., para ser documentado y distribuido a los encargados de desarrollar los productos antivirus.

- Asimilación: Es este punto, quienes desarrollan los productos antivirus, modifican su programa para que éste pueda detectar los nuevos virus. El tiempo que tarde depende de quien lo desarrolle y del tipo de virus.

- Erradicación: Si suficiente cantidad de usuarios instalan una protección antivirus actualizada, puede erradicarse cualquier virus. Hasta ahora, ningún virus ha desaparecido completamente, pero algunos han dejado de ser una amenaza.

¿CÓMO SE PRODUCE EL CONTAGIO?

En primer lugar el virus debe entrar en el ordenador. Por ejemplo, por puertos de comunicaciones o por un disco. Existe un agente transmisor, que es el usuario; y si el ordenador está infectado es porque ha introducido el virus; lógicamente sin ser consciente de ello. El virus ya se encuentra dentro del ordenador.

Para que el virus se active, debe **ejecutarse el fichero que está infectado**. Es decir, la infección solo se produce cuando se ejecuta el fichero infectado.

Los puntos de infección son los lugares o programas del sistema en donde los virus insertan su código ejecutable para posteriormente entrar en acción cuando este punto o programa sea ejecutado, hay virus que infectan el sector de arranque, el intérprete de comandos, archivos ejecutables, drivers de dispositivos, monitores residentes en memoria, etc.

Los virus informáticos se **propagan** cuando las instrucciones que hacen funcionar los programas pasan de un ordenador a otro. Una vez que un virus está activado, puede reproducirse copiándose en discos flexibles, en el disco duro, en programas informáticos o a través de redes informáticas.

Los virus **funcionan, se reproducen y liberan** sus cargas activas sólo cuando se **ejecutan**. Por eso, si un ordenador está simplemente conectado a una red infectada o se limita a cargar un programa infectado, no se infectará probablemente. Un usuario no ejecuta conscientemente un código informático potencialmente nocivo debido a que

los virus “engañan” frecuentemente al sistema operativo del ordenador o al usuario para que lo ejecute; y esto lo consiguen usando trucos de ocultamiento.

Los virus también pueden residir en las partes del **disco duro o flexible** que cargan y ejecutan el sistema operativo cuando se arranca el ordenador, por lo que dichos virus se ejecutan automáticamente. En las **redes**, algunos virus se ocultan en el software que permite al usuario conectarse al sistema.

Para que el virus comience una infección tendrá que introducir una **copia** a partir de la cual comenzar a sacar **múltiples** copias. Es decir, lo normal es que se realice una sola copia para infectar el sistema, y luego una avalancha llenando el ordenador. Un buen lugar para dejar esa copia es en un fichero. Y otro punto interesante que en primer momento es utilizado como sitio de reproducción es la memoria RAM, ya que resultará infectado todo fichero que sea ejecutado, y que por tanto, pase por esa memoria. El problema es que la copia reproductora resultará destruida al apagar el ordenador, eso sí, tras dejar gran cantidad de ficheros infectados.

Lo más común es que un virus sea capaz de reproducirse desde cualquier tipo de memoria en que esté. Intentará infectar el máximo número de ficheros para así iniciar una propagación por todo el ordenador (por eso el virus intenta, ante todo, infectar ficheros que se sabe de antemano que van a ser ejecutados muchas veces).

Desde estos ficheros el virus tiene totalmente dominado el ordenador, pero debe tener cuidado en no destruir al fichero original. Simplemente debe añadir copias de sí mismo mientras el fichero ejecuta sus funciones normales, y a ser posible ejecutarse antes que el código verdadero.

El virus debe elegir al infectar un fichero, si añade simplemente su código al fichero, o si sustituye un trozo del mismo (overwrite). Al reemplazar el arranque del disco, actúa él mismo como arranque; asimismo elimina la zona donde se almacenan los mensajes de error del arranque. Por ejemplo, esto es lo que hacen los virus BSI o MBSI. Otro truco, es aprovechar un hueco vacío e introducirse en él. Por ejemplo, esto lo utilizan los macrovirus.

Existe una clasificación dependiendo del lugar donde resida el virus:

1) Contaminación del sector de arranque.
2) Contaminación de propósito general o de ficheros.

3) Virus residentes en memoria.
4) Contaminación por macrovirus.
5) Contaminación debido a Internet.
6) Telefonía móvil.

PUNTOS DE INFECCIÓN

1. Contaminación del sector de arranque

En este caso el código del virus se copiará en el primer sector del disco duro que el ordenador lee al arrancar. Puede que se sobrescriba el sector original o que quede una copia del mismo para ser detectado. Los virus de sector de arranque se aseguran de ser los primeros en entrar en el sistema.

El virus sustituye el sector de boot original del ordenador cambiando así la secuencia normal de boot. De esta manera, lo primero que se ejecuta al encender el sistema es el código del virus, el cual queda residente en memoria y luego carga el núcleo del sistema operativo.

Para llevar a cabo la contaminación del sector de arranque, el virus sustituye el programa de carga del DOS, que está en el sector original, por otro programa que lo que hace es cargar e inicializar el virus, eso sí, cuando acaba de ejecutarse el programa normal de arranque. Debido a su afán de ocultación el virus no borra el sector original, sino que lo traslada a otro lugar junto con el grueso del programa del virus. Un buen sitio son en los últimos sectores, porque son los últimos en llenarse: a veces incluso utiliza la Fat. Hay excepciones, por ejemplo los caballos de troya borran el sector original.

Siguiendo el proceso, el virus leerá el sector original y lo guardará junto con el programa principal del virus en los sectores antes elegidos. Una vez hecho esto, marcará como defectuosos esos clunters apuntando esos datos en la Fat. Finalmente escribirá el nuevo y especial sector original.

Resumiendo, estos virus residen en la primera parte del disco duro o flexible, conocida como sector de arranque inicial, y sustituyen los programas que almacenan información sobre el contenido del disco o los programas que arrancar el ordenador.

Estos virus suelen difundirse mediante el intercambio físico de discos flexibles.

Las principales ventajas de este tipo de infección son que, por un lado, es fácil de programar un virus de estas características y, por otro lado, al quedar el virus por debajo del sistema operativo tiene virtualmente un control total sobre las acciones del mismo e incluso puede engañar más fácilmente a muchos antivirus.

Su desventaja es que son fácilmente detectables (cuanto más fácil es hacerlos, más fácil resulta cazarlo y desactivarlos) y eliminables. Ya que si el usuario arranca el ordenador con un disquete “limpio” el virus no podrá cargarse en memoria y no tendrá el control.

Un caso menos probable es que el virus sea de “tabla de partición”. El mecanismo es muy parecido al de los de sector de arranque solo que el truco de arrancar con un disquete limpio no funciona con estos. Estos virus guardan una copia de la Fat original en otro lugar del disco que marcan como sectores defectuosos para mostrársela al usuario.

Un ejemplo de virus de sector de arranque es el virus ***Michelangelo***. Este virus activa su rutina de destrucción el 6 de marzo, la fecha de cumpleaños del artista italiano. El virus queda residente en memoria cuando se intenta arrancar desde un disquete infectado.

2. Contaminación de ficheros (virus de programas)

Este método de infección es uno de los más usados, ya que los virus de este tipo contagian todos los archivos ejecutables que encuentren en el sistema de archivos. Independientemente de la acción destructiva que realizan, son extremadamente difíciles de erradicar, ya que por lo general este tipo de virus asegura su permanencia contagiando cierta cantidad de archivos antes de iniciar sus acciones destructivas, con

lo cual, al momento de detectarlo, el virus puede haber infectado todo el sistema e incluso otros sistemas.

Al infectar un fichero como por ejemplo un fichero .COM o .EXE:

El virus debe asegurarse de que lo primero que se ejecutará será su código vírico. Para conseguir esto, el virus sustituye los tres primeros caracteres del fichero original por una instrucción JMP (salto a dirección de memoria determinada). Así, al cargarse el fichero, la secuencia de instrucciones "salta" hasta la primera instrucción vírica. Ejecuta todo el virus, y luego finaliza con los tres bytes modificados dando paso al programa original para que no se note nada. Excepcionalmente el virus se sitúa delante del código del programa a infectar.

El virus ejecutará todos los programas, pero después se copiará a sí mismo y se "pegará" al programa ejecutado "engordándolo" unos cuantos bytes. Para evitar que un usuario avanzado se de cuenta de la infección, oculta esos bytes para que parezca que siguen teniendo el mismo tamaño.

Los virus ocultan el tamaño real de los archivos que han contaminado, de forma que si hacemos un DIR la información del tamaño de los archivos puede ser falsa.

Un ejemplo de virus de programas son el *Jerusalén*, *Viernes 13* o *Chernobyl*.

3. Virus residentes en memoria

Estos virus se instalan en memoria y allí permanecen hasta que se apague el sistema.

Estando en memoria el virus puede realizar todas las acciones de contagio y destrucción que desee en cualquier momento.

4. Contaminación por macrovirus

De acuerdo con la International Security Association, los virus macro forman el 80% de todos los virus y son los que más rápidamente han crecido en toda la historia de los ordenadores en los últimos cinco años. A diferencia de otros tipos de virus, los virus macro no son exclusivos de ningún sistema operativo y se diseminan fácilmente a través de archivos adjuntos de e-mail, disquetes, bajadas de Internet, transferencia de archivos y aplicaciones compartidas.

Los virus macro son, sin embargo, aplicaciones específicas. Infectan las utilidades macro que acompañan a ciertas aplicaciones como el Microsoft Word y Excell. Gran parte de los ficheros de datos utilizados en sistemas como Windows 95/98, usan lo que se llaman macros; que son listas de órdenes programadas que ahorran tiempo y aumentan la velocidad de las operaciones. Estas macros van listadas en la cabecera del fichero de turno.

El virus macro puede o bien sustituir una macro benigna por otra con el mismo nombre pero maligna, o incluir otras macros nuevas que realicen operaciones indeseadas.

Estos virus son capaces de cambiar la configuración de Windows, borrar ficheros de nuestro disco duro, enviar por correo cualquier archivo sin que nos demos cuenta, e incluso infectar nuestro disco duro con un virus de fichero.

Estos virus no son muy complicados de diseñar como los virus convencionales. Están codificados en forma de macros del Word y por tanto pueden entrar en acción nada más cargar un documento. El Word contiene una especie de lenguaje de programación llamado WordBasic y es con este lenguaje como se diseñan. Pueden infectar diferentes puntos de un archivo en uso, por ejemplo, cuando éste se cierra o se borra. Lo primero que hacen es modificar la plantilla maestra (normal.dot) para ejecutar varias macros insertadas por el virus, así en cada documento que abramos o creemos , se incluirán las macros “víricas”.

Ejemplo de este tipo son el virus *Melissa* o el *Loveletter.*

5. Internet

La red se ha convertido en el mayor medio de transferencia de información entre ordenadores y, en consecuencia, hoy es la mayor vía de entrada de virus. La vía preferida son los e-mails, los cuales provocan más el 80% de las infecciones detectadas. Su peligrosidad deriva de su extrema capacidad de replicación y propagación, así como de su gran sofisticación técnica. Gracias a este último aspecto, son capaces de reenviarse por sí solos a todos los contactos que el usuario afectado tenga en la Libreta de direcciones, provocar infecciones con la simple lectura o apertura del mensaje, aprovecharse de posibles vulnerabilidades o agujeros de seguridad de los programas de correo, etc.

Un concepto sobre este tipo de virus debe quedar claro, no puede haber un virus de correo electrónico porque precisamente el correo no es autoejecutable. Puede ser que recibamos un programa infectado con un virus pero solo pasará a tener efecto cuando lo ejecutemos. Pero debemos ejecutarlo desde nuestro ordenador, así que todos esos rumores de que hay correos que con sólo abrirlos nos pueden destruir toda la información de nuestro disco duro, todo eso es mentira. Uno de los correos de este tipo más famoso era el "***Good Times***".

También ha cobrado una importancia creciente la navegación por páginas web, dado que algunas de las tecnologías incluidas en ellas son susceptibles de contagio y transmisión. Los grupos de noticias y los sistemas de conversación en línea (chats, messenger,etc) representan otra fuente de riesgo. Cada usuario va dejando sus mensajes, que pueden ser infectados, para que los demás los lean. Otras veces el ordenador puede quedar infectado mientras se está conectado en línea.

No se pueden dejar de mencionar la transferencia de ficheros FTP, pues al descargar uno, éste se copia directamente en el ordenador con el consiguiente peligro en caso de que contenga algún virus.

Mención aparte merecen los riesgos de ADSL y de las conexiones por cable, cuando se utiliza un módem, el procedimiento se basa en la asignación de una dirección IP dinámica que varía en cada conexión; con la banda ancha se asigna una dirección IP estática, es decir, que es la misma sea cual sea el momento en que se conecte. Ante esta dinámica el uso de un cortafuegos no es ya una recomendación sino que es incluso una obligación.

6. Nuevas vías de propagación: Los teléfonos móviles

Los teléfonos móviles han evolucionado mucho en los últimos años y cada vez se parecen más a los ordenadores, lo que conlleva ventajas pero también inconvenientes. Uno de ellos es la aparición de virus informáticos.

Hace un año un virus se extendió rápidamente en Japón; pero el virus más común es **Cabir**, aunque hay otros.

El virus Cabir es un gusano que infecta sólo a los teléfonos móviles que presentan Bluetooth y que tienen concretamente el sistema operativo Symbian.

El virus consigue introducirse en el teléfono y enviar mensajes de forma indiscriminada a todos los contactos que estén grabados en la agenda; e incluso a otros números de alto coste, con los daños económicos para el usuario que eso conlleva y el gasto de batería, aunque no daña de ningún modo al sistema operativo.

LOS ANTIVIRUS

DEFINICIÓN Y FUNCIÓN

Los antivirus son una unas aplicaciones o programas para combatir el problema de los virus informáticos detectándolos y, en algunos casos, eliminándolos.

Es importante aclarar que todo antivirus es un programa y que, como todo programa, sólo funcionará correctamente si es adecuado y está bien configurado. Además, es una herramienta para el usuario y no sólo no será eficaz para el 100% de los casos, sino que nunca será una protección total ni definitiva. Como se dice coloquialmente: “No para toda enfermedad existe cura”.

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

Es importante tener en claro la diferencia entre "detectar" e "identificar" un virus en un ordenador. La detección es la determinación de la presencia de un virus, la identificación es la determinación de qué virus es. Aunque parezca contradictorio, lo mejor que debe tener un antivirus es su capacidad de detección, pues las capacidades de identificación están expuestas a muchos errores y sólo funcionan con virus conocidos.

TÉCNICAS DE BÚSQUEDA DE VIRUS

El modelo más primario de las funciones de un programa antivirus es la detección de su presencia y, en lo posible, su identificación.

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

La técnica de **scanning** fue bastante eficaz en los primeros tiempos de los virus informáticos, cuando había pocos y su producción era pequeña. Esto permitía que los desarrolladores de antivirus escaneadores tuvieran tiempo de analizar el virus, extraer el pequeño trozo de código que lo iba a identificar y agregarlo a la base de datos del programa para lanzar una nueva versión.

El primer problema que nos encontramos con este sistema radica en que siempre brinda una solución *a posteriori*: es necesario que un virus informático alcance un grado de dispersión considerable para que sea enviado (por usuarios capacitados, especialistas o distribuidores del producto) a los desarrolladores de antivirus. Estos lo analizarán, extraerán el trozo de código que lo identificará, y lo incluirán en la próxima versión de su programa antivirus. Este proceso puede demorar meses a partir del momento en que el virus comienza a tener una dispersión considerable, siendo el tiempo necesario en el cual puede causar graves daños sin que pueda ser identificado. Por ello es recomendable que este tipo de antivirus deben actualizarse periódicamente debido a la aparición de nuevos virus.

Se sigue utilizando debido a que permite identificar rápidamente la presencia de los virus más conocidos y, como son estos los de mayor dispersión, permite una

importante gama de posibilidades. Un ejemplo de antivirus que utiliza esta técnica es: **Viruscan de McAfee.**

Otro tipo de técnica es la que utiliza algoritmos **heurísticos.** Se creo debido al pronto agotamiento técnico de la técnica de scanning. Las novedades de esta técnica es que los desarrolladores de programas antivirus han dotado a sus creaciones de métodos para búsquedas de virus informáticos (y de sus actividades), que no identifican específicamente al virus sino a algunas de sus características generales y comportamientos universalizados. Este tipo de técnica rastrea rutinas de alteración de información que no puedan ser controladas por el usuario, modificación de sectores críticos de las unidades de almacenamiento (master boot record, boot sector, FAT, entre otras), etc.

De hecho, esta naturaleza de procedimientos busca, de manera bastante eficiente, códigos de instrucciones potencialmente pertenecientes a un virus informático. Resulta eficaz para la detección de virus conocidos y es una de las soluciones utilizadas por los antivirus para la detección de nuevos virus. El inconveniente que presenta este tipo de algoritmo radica en que puede llegar a sospecharse de muchísimas cosas que no son virus. Esto hace necesario que el usuario que lo utiliza conozca un poco acerca de la estructura del sistema operativo, a fin de poseer herramientas que le faciliten una discriminación de cualquier falsa alarma generada este modelo. Algunos de los antivirus con esta técnica son **Norton Anti Virus** y **Dr. Solomon's Toolkit**.

Otra técnica utiliza **chequeadores de integridad**. Se encarga de detectar la presencia de un virus informático en un sistema, monitoreando las actividades del PC señalando si algún proceso intenta modificar los sectores críticos de los dispositivos de almacenamiento o los archivos ejecutables.

Sobre la base de estas consideraciones, podemos consignar que **un buen sistema antivirus** debe estar compuesto por **un programa detector de virus** -que siempre esté residente en memoria- y **un programa que verifique la integridad** de los sectores críticos del disco duro y sus archivos ejecutables. Existen productos antivirus

que cubren los dos aspectos, o bien pueden combinarse productos diferentes configurados de forma que no se produzcan conflictos entre ellos.

MODELO DE ANTIVIRUS

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

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

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

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

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

2) **Módulo de respuesta:** la función **alarma** se encuentra incluida en todos los programas antivirus y consiste en detener la acción del sistema ante la sospecha de

la presencia de un virus informático, e informar la situación a través de un aviso en pantalla.

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

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

DETECCIÓN Y PREVENCIÓN

Debido a que los virus informáticos son cada vez más sofisticados, hoy en día es difícil sospechar su presencia a través de síntomas como la pérdida de performance. De todas maneras la siguiente es una lista de síntomas que pueden observarse en un ordenador que se sospeche que esta infectada por alguno de los virus más comunes:

- Operaciones de procesamiento más lentas.
- Los programas tardan más tiempo en cargarse.
- Los programas comienzan a acceder por momentos a las disqueteras y/o al disco duro.
- Disminución no justificada del espacio disponible en el disco duro y de la memoria RAM disponible, en forma constante o repentina.
- Aparición de programas residentes en memoria desconocidos.

La primera medida de prevención a ser tenida en cuenta es, como se dijo anteriormente, contar con un sistema antivirus y utilizarlo correctamente. Por lo tanto, la única forma de que se constituya un bloqueo eficaz para un virus es que se utilice con determinadas normas y procedimientos. Estas normas tienden a controlar la entrada de archivos al disco duro del ordenador, lo cual se logra revisando con el antivirus todos los disquetes o medios de almacenamiento en general y, por supuesto, disminuyendo al mínimo posible todo tipo de tráfico.

Además de utilizar un sistema antivirus y controlar el tráfico de archivos al disco duro, una forma bastante eficaz de proteger los archivos ejecutables es utilizar un programa **chequeador de integridad** que verifique que estos archivos no sean modificados, es decir, que mantengan su estructura. De esta manera, antes que puedan ser parasitados por un virus convencional, se impediría su accionar.

Para prevenir la infección con un **virus de sector de arranque**, lo más indicado es no dejar disquetes olvidados en la disquetera de arranque y contar con un antivirus. Pero, además, puede aprovecharse una característica que incorpora el setup de los ordenadores más modernos: variar la secuencia de arranque del PC a "**primero disco duro y luego disquetera**" (C, A). De esta manera, la computadora no intentará leer la disquetera en el arranque aunque tenga cargado un disquete.

En consecuencia, la detección alternativa a la de scanning y las de chequeo de actividad e integridad resultan importantes, ya que pueden detectar la presencia de un virus informático sin la necesidad de identificarlo. Y esta es la única forma disponible para el usuario de detectar virus nuevos, sean nacionales o extranjeros.

De todas maneras, **existe una forma de actualizar la técnica de scanning**. La misma consiste en incorporarle al antivirus un archivo conteniendo cadenas de caracteres ASCII que sean trozos de código (strings) significativos del sector vital de cada nuevo virus que todavía no esté incorporado en la base de datos del programa. De todas formas, esta solución será **parcial**: la nueva cadena introducida sólo *identificará* al virus, pero no será capaz de erradicarlo.

Es muy importante que los "strings" que se vayan a incorporar al antivirus provengan de una fuente confiable ya que, de lo contrario, pueden producirse falsas alarmas o ser ineficaces. Algunos de los antivirus que soportan esta cualidad de agregar strings son Viruscan, F-Prot y Thunderbyte.

La NCSA (National Computer Security Association, es la encargada de certificar productor antivirus.

CERTIFICACION DE ANTIVIRUS

Para obtener la certificación de antivirus los productos deben pasar una serie de rigurosas pruebas diseñadas para asegurar la adecuada protección del usuario.

Antiguamente el esquema de certificación requería que se detectara (incluyendo el número de versión) el 90 % de la librería de virus del NCSA (Asociación Nacional de Seguridad de Computadoras), y fue diseñado para asegurar óptimas capacidades de detección. Pero esta metodología no era completamente eficiente.

Actualmente, el esquema de certificación enfoca la amenaza a los ordenadores empresariales. Para ser certificado, el producto debe pasar las siguientes pruebas:

- Debe detectar el 100% de los virus encontrados comúnmente. La lista de virus comunes es actualizada periódicamente, a medida que nuevos virus son descubiertos.
- Deben detectar, como mínimo, el 90% de la librería de virus del NCSA (más de 6.000 virus)

Estas pruebas son realizadas con el producto ejecutándose con su configuración "por defecto".

Una vez que un producto ha sido certificado, la NCSA tratará de re-certificar el producto un mínimo de cuatro veces. Cada intento es realizado sin previo aviso al desarrollador del programa. Esta es una buena manera de asegurar que el producto satisface el criterio de certificación.

Si un producto no pasa la primera o segunda prueba, su distribuidor tendrá siete días para proveer de la corrección. Si este límite de tiempo es excedido, el producto será eliminado de la lista de productos certificados.

Una vez que se ha retirado la certificación a un producto la única forma de recuperarla es que el distribuidor envíe una nueva versión completa y certificable. No se aceptará sólo una reparación de la versión que falla.

Acerca de la lista de virus de la NCSA, aclaremos que ningún desarrollador de antivirus puede obtener una copia. Cuando un antivirus falla en la detección de algún virus incluido en la lista, una cadena identificatoria del virus le es enviada al productor del antivirus para su inclusión en futuras versiones. En el caso de los virus polimórficos, se incluyen múltiples copias del virus para asegurar que el producto testeado lo detecta perfectamente. Para pasar esta prueba el antivirus debe detectar cada mutación del virus.

ALGUNOS ANTIVIRUS

DR. SOLOMON'S ANTIVIRUS TOOLKIT.

Certificado por la NCSA. Detecta más de 6.500 virus gracias a su propio lenguaje de detección llamado **VirTran**, con una velocidad de detección entre 3 y 5 veces mayor que los antivirus tradicionales. Elimina virus en archivos en forma sencilla y efectiva con pocas falsas alarmas, y en sectores de buteo y tablas de partición la protección es genérica, es decir, independiente del virus encontrado.

Permite detectar modificaciones producidas tanto en archivos como en la tabla de partición del disco duro. Para ello utiliza Checksumms Criptográficos lo cual, sumado a una clave personal de cada usuario, hace casi imposible que el virus pueda descubrir la clave de encriptación.

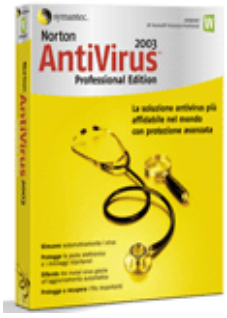
Uno de los últimos desarrollos de S&S es la tecnología G. D. E. (Generic Decription Engine, Motor de Desencriptación Genérica) que permite detectar virus polimórficos sin importar el algoritmo de encriptación utilizado.

Otras características que presenta este antivirus, son:

- Ocupa 9K de memoria extendida o expandida.

- Documentación amplia y detallada en español y una enciclopedia sobre los virus más importantes.
- Actualizaciones mensuales o trimestrales de software y manuales.
- Trabaja como residente bajo Windows.
- H. A. (Advanced Heuristic Analysis, Análisis Heurístico Avanzado).

NORTON ANTIVIRUS



Certificado por la NCSA. Posee una protección automática en segundo plano. Detiene prácticamente todos los virus conocidos y desconocidos, a través de una tecnología propia denominada **NOVI**, que implica control de las actividades típicas de un virus, protegiendo la integridad del sistema antes de que causen algún daño o pérdida de información, con una amplia línea de defensa, que combina búsqueda, detección de virus e **inoculación** (se denomina 'inoculación' al método por el cual este antivirus toma las características principales de los sectores de booteo y archivos para luego chequear su integridad). Cada vez que se detecta un cambio en dichas áreas, NAV avisa al usuario y provee las opciones de Reparar - Volver a usar la imagen guardada - Continuar - No realiza cambios - Inocular - Actualizar la imagen.

Utiliza diagnósticos propios para prevenir infecciones de sus propios archivos y de archivos comprimidos.

El escaneo puede ser lanzado manualmente o automáticamente a través de la planificación de fecha y hora. También permite reparar los archivos infectados por virus desconocidos. Incluye información sobre muchos de los virus que detecta y permite establecer una contraseña para aumentar así la seguridad.

La lista de virus conocidos puede ser actualizada periódicamente (sin cargo) a través de servicios en línea como Internet, América On Line, Compuserve, The Microsoft Network o el BBS propio de Symantec, entre otros.

VIRUSSCAN

Este antivirus de **McAfee Associates** es uno de los más famosos. Trabaja por el sistema de scanning descrito anteriormente, y es el mejor en su estilo.

Para escanear, hace uso de dos técnicas propias: CMS (Code Matrix Scanning, Escaneo de Matriz de Código) y CTS (Code Trace Scanning, Escaneo de Seguimiento de Código).

Una de las principales ventajas de este antivirus es que la actualización de los archivos de bases de datos de strings es muy fácil de realizar, lo cual, sumado a su condición de programa, lo pone al alcance de cualquier usuario. Es bastante flexible en cuanto a la configuración de cómo detectar, reportar y eliminar virus.

PANDA ANTIVIRUS

Algunas de las cualidades de este producto antivirus son:

- Actualización diaria
- La versión Platinum dispone de: 'Actualización Inteligente' y 'Actualizaciones programadas' que permiten tener actualizado el antivirus sin necesidad de prestarle atención.
- Versiones en diversos idiomas incluido el catalán.
- Servicio Técnico Personal 24 horas 365 días (y en castellano) llamando al 902 24 365 0 (este servicio es extensivo a los empleados, que podrán hacer uso de él desde su domicilio)
- Ante la aparición de un nuevo virus, Panda recogería, detectaría y eliminaría el nuevo virus en menos de 24 horas.

El nuevo **Panda Platinum 2006 Internet Security** ofrece la protección más eficaz contra virus, spyware, hackers, phishing, spam y demás amenazas, para que disfrutar de Internet con toda tranquilidad. Para mayor seguridad, ofrece una doble garantía de

protección contra virus desconocidos e intrusos a través de las **Tecnologías TruPrevent™**.

CONCLUSIONES

Si se es cuidadoso con los programas que se utilizan a diario, con la información que se introduce en la computadora y con los lugares que se visitan en Internet, así como en el intercambio de discos en la oficina, trabajos u otros dispositivos de otras personas de procedencia dudosa, es muy posible que nunca se tengan problemas con los virus pero, aún así, es indispensable tener instalado un buen Antivirus.

Además, ningún sistema de seguridad es 100% seguro. Por eso, todo usuario de ordenadores debería tratar de implementar estrategias de seguridad antivirus, no sólo para proteger su propia información sino para no convertirse en un agente de dispersión de algo que puede producir daños graves e indiscriminados.

Y por último, cabe recordar que no todo lo que afecte al funcionamiento normal de un ordenador es un virus.

BIBLIOGRAFÍA CONSULTADA

LIBROS:

- ✓ Jesús de Marcelo Rodae. "*Virus de sistemas informáticos e Internet*". Edit. Ra-Ma, 2000.

- ✓ Alfonso Mur, Pablo Nieto, Jesús Molina. "*Virus informáticos*". Edit. Anaya Multimedia S. A., 1991.

PÁGINAS WEB:

- ✓ http://www.monografías.com/trabajos5/virusinf/virusinf.shtml.
- ✓ http://es.wikipedia.or/wiki/virus_informatico.
- ✓ http://www.eumed.net/grumetes/virus.htm.
- ✓ http://www.geocities.com/ogmg.rm/Funciona.html.
- ✓ http://www.itq.edu.mx/vidatec/espacio/aisc/ARTICULOS/virus/VIRUS.htm.
- ✓ http://www.enplenitud.com/nota.asp?articuloid=8074.
- ✓ http://www.publispain.com/supertutoriales/underground/virus/cursos/1/estudiovirus.doc
- ✓ http://www.xoc.uam.mx/utilerias/saat/bol_esp.html.

.