



Univ. de Concepción
Fac. de Ingeniería
Dpto. Ing. Informática

Tarea N°3

Virus Computacionales

Integrantes : Alnaldo Arias
Pedro Lazo
Mauricio Romo
Profesor : Yussef Farrán
Ayudante : Jaime Jara
Fecha : 06 de Junio de 2002

SUMARIO

Actualmente existe un peligro latente en todos y en cada uno de los computadores en todo el mundo debido a lo que se conoce como VIRUS INFORMÁTICO.

Los efectos que produce un virus pueden ser destructivos o simplemente molestos: dañar o borrar los datos almacenados en un computador, provocar el bloqueo del equipo afectado, mostrar mensajes en pantalla, etc. Además de contar con técnicas de propagación e infección, en la actualidad existen virus que también utilizan técnicas de "evasión". Esto quiere decir que el virus cuenta con técnicas o sistemas de defensa que le permiten dificultar su detección y evitar las acciones que se llevan a cabo contra él.

El nombre de virus informático es debido a su parecido con los virus biológicos. De la misma forma que los virus biológicos, los virus informáticos se introducen en el cuerpo humano (en el computador) de alguna forma concreta e infectan las células (archivos), presentando algún síntoma de esta infección. Además, ambos pueden reproducirse y propagarse, extendiendo la infección desde el sistema ya infectado a otros.

INTRODUCCION

No existe hoy en día una política contra virus que sea 100% efectiva. La forma de evitar infecciones que pueden provocar verdaderos desastres informáticos es mantenerse al tanto de las últimas novedades en seguridad existentes en el mercado en cuanto a antivirus. También es importante mantenerse al tanto de algunos métodos "caseros" de identificar mediante síntomas en la máquina y erradicar infecciones de virus descubiertas recientemente y que con seguridad no están incluidas en la lista de virus conocidos que nuestro antivirus detecta.

La creación de nuevos virus es un problema creciente, como sus homólogos biológicos, dado el crecimiento exponencial parecido al de una colonia de bacterias sin enemigos naturales, los virus no tienen otro enemigo que no sean los programas antivirus; los virus se producen en una cantidad exorbitante. Los programas antivirus crecen con una curva mucho más suavizada, es decir, lo que se observa es que los diferentes programas de antivirus se van quedando rezagados con respecto a los virus informáticos.

OBJETIVO GENERALES

Mediante el presente trabajo queremos dar a conocer que es un virus informático y que softwares están disponibles para combatirlos.

OBJETIVOS ESPECIFICOS

Conocer:

- Qué es un virus computacional.
- Cuál fue el origen de los virus.
- Qué tipos de virus existen y cuales son sus medios de propagación, infección y acción.
- Cómo podemos disminuir las posibilidades de infección en nuestro equipo.
- Qué soluciones informáticas existen contra los virus y cuál nos conviene más.

METODOLOGIA DE TRABAJO

Para lograr nuestros objetivos procedimos a buscar información a través de internet principalmente por el buscador google y paginas de empresas conocidas como Symantec, McFee, etc. para luego clasificar la información y redactar el trabajo.

¿QUE ES UN VIRUS?

Un virus un programa que se puede introducir en nuestro computador de formas muy diversas. Este tipo de programas, los virus, son especiales ya que pueden producir efectos no deseados y nocivos. Una vez el virus se ha introducido en el computador, se coloc en lugares desde los que el usuario pueda ejecutarlos de manera no intencionada. Hasta que no se ejecuta el programa infectado o se cumple una determinada condición -condición de activación (por ejemplo una fecha determinada o una acción que realiza el usuario)-, el virus no actúa. Incluso en algunas ocasiones, los efectos producidos por éste, se aprecian tiempo después de su ejecución (payload). Una característica típica de los virus es su capacidad de replicarse y propagarse a otros archivos o programas.

HISTORIA DE LOS VIRUS

No se sabe exactamente cuál fue el primer virus en la historia de los computadores, aunque sí se sabe cuál fue posiblemente el primero en una computadora con sistema operativo.

Algunos llevan este comienzo a los primeros conceptos de programas autoreplicantes, o sea programas que se reproducen, los cuales se describen en el trabajo: "Theory and Organization of Complicated Automata" de John Von Newman.

A finales de los años 50, en los laboratorios Bell, tres programadores, H. Douglas McIlroy, Víctor Vysotsky y Robert Moris inventaron un juego llamado "Core Wars", el cual consiste en elaborar "programas" para una computadora ficticia simulada. El objetivo es que los programas sobrevivan usando técnicas de ataque, ocultamiento y reproducción semejantes a los virus.

En la década del 70, aparecieron otros programas del mismo tipo.

John Shoch y Jon Hupp, investigadores de Palo Alto Research Center (PARC) de Xerox aseguran que ya en 1970 habían elaborado programas con ciertas técnicas virales de reproducción. Aunque estos programas podrían ser considerados "virus buenos", ya que controlaban continuamente la "salud" de las redes.

En 1981 apareció un programa para Apple II llamado "El Cloner" el cual se duplicaba escribiendo en la pantalla una pequeña frase. En 1982, también para microcomputadoras Apple II fue diseñado otro programa que estaba destinado solo a viajar y no a causar daños, y que fue denominado por su autor Jim Hauser, como un caminante electrónico (electronic hitchhiker) que se pegaba a programas sin ser detectado.

Tal vez el primer virus, o al menos el primero en recibir esa denominación, fue ideado en noviembre de 1983. En un seminario sobre seguridad en computadores en el que Fred Cohen se le ocurrió experimentar con un programa que "pudiera modificar otros para incluir una copia (posiblemente evolucionada) de si mismo".

En enero de 1986 aparece el virus "Brain", originario de Paquistán, el que es considerado el primer virus para PC's con sistema operativo MS-DOS. Al principio no causaba daño, sólo mostraba un mensaje de advertencia: "*Bienvenido al calabozo. (c)1986 Basit & Amjad (pvt) Ltd. BRAIN COMPUTER SERVICES*", luego la dirección y teléfono, y "*Cuidado con este virus... Contáctenos para vacunarse...*"

Comienza aquí la historia más reciente de los virus informáticos, la que continuaremos desarrollando en nuestra próxima entrega.

¿Pero cuando se usó el término virus, relacionado con estos programas de computadora ?. David Gerrold creó en 1972 una novela llamada "When HARLIE was One" (Cuando HARLIE era uno). HARLIE (que significa "Equivalentes de Entrada de Vida Robótica Análoga a la Humana" en inglés) se trataba de una computadora capaz de duplicar las funciones del cerebro humano. También podía conectarse con otras computadoras e intercambiar datos vía telefónica. Y justamente, el programa que usaba para hacer este intercambio fue llamado "virus".

También en el año 1986, un ingeniero llamado Ralf Burger creó un virus informático realmente operativo, al que llamó "VirDEM" (por "demostración de virus", al menos era esa su "inocente" intención). "VirDEM" estaba preparado para borrar gradualmente todos los archivos de la computadora huésped, causando su paulatina destrucción, pero solo luego que el mismo se hubiera reproducido en cuanto archivo encontrara. Tal vez se trató del primer virus que utilizó una de las principales características con las que hoy día los conocemos: la de reproducirse a si mismos para luego causar algún tipo de daño.

El 2 de noviembre de 1988, el caos cundió por la red ARPANET. Un "monstruo dañino" estaba comiéndose la memoria de cada computador conectado a la misma red, y hacían que funcionaran cada vez más despacio. A las tres horas todas las computadoras de costa a costa de los Estados Unidos estaban afectadas. Era el ataque del que fue llamado "Gusano de Internet", y la prensa estadounidense cubrió el tema con frases como "el mayor asalto jamás realizado contra los sistemas de la nación". Se calculó en más de 2.000 computadoras las realmente infectadas en Internet, y erradicarlo costó casi un millón de dólares, sumado a las pérdidas por haberse detenido casi toda la red.

El autor fue Robert Morris Jr, un graduado de Harvard de 23 años en ese entonces. Creó un programa con gran capacidad de reproducirse, pero jamás pensó que se propagaría tan rápida y extensamente. Morris fue acusado de acceder en forma intencional y sin autorización a computadoras "con intereses federales", impidiendo su uso y causando pérdidas de miles de dólares. El juicio fue en enero de 1990, y aunque sus abogados aseguraban que Morris "intentaba ayudar a la seguridad de Internet cuando su programa se salió de su control por accidente", la fiscalía argumentó que el gusano "no se trató de un error, sino de un ataque contra el gobierno de los Estados Unidos". Finalmente el 22 de enero, Morris fue declarado culpable por un jurado federal, lo que se convirtió en la primer condena por la ley de fraudes informáticos de 1986. Sin embargo, se lo sentenció a tres años de libertad condicional, una multa de 10.000 dólares y 400 horas de servicio a la comunidad.

En el año 1987, cuando se tuvo noticias del primer caso de un "Caballo de Troya". Ello ocurrió en Alemania, y también tuvo mucho que ver el la difusión de correo electrónico. El día 9 de diciembre, varios estudiantes de la Universidad de Clausthal-Zellerfeld, recibieron en un mensaje de Navidad unas líneas de código de un programa. El mensaje los invitaba a ejecutarlo, y les deseaba "una Feliz Navidad y un Próspero Año Nuevo". Las instrucciones decían que debían teclear la palabra "Christmas" No sospechaban que al ejecutar el programa que mostraba la imagen del árbol de Navidad, este programa también leía las direcciones electrónicas de todos los estudiantes guardadas en el computador, y se había encargado también de enviar una copia de si mismo a cada uno de esas direcciones. El mensaje se distribuyó por toda esa red con su programa infeccioso. Los usuarios de IBM tenían

más nombres en sus agendas, que los existentes en la universidad de Alemania donde se originó todo, por lo que a los 6 días de la primera infección, miles de mensajes y copias del archivo estaban dando la vuelta al mundo, llegando incluso al Japón. Cada vez que el programa se ejecutaba, podía generar entre cincuenta y cien copias o más de si mismo. El virus fue llamado por supuesto "Arbol de Navidad de IBM", pero como necesitaba la acción de un usuario para poder funcionar (se debía escribir la palabra "Christmas" para accionarlo), no se podía considerar exactamente como un virus. Y debido al disfraz que presentaba, se le ocurrió a alguien asociarlo con el famoso "Caballo de Troya". Había nacido así el primer "Caballo de Troya" en la historia de los virus

En la década de los 90, no sólo existían virus, sino una completa variedad de gusanos, caballos de troya y bombas informáticas.

Al comienzo había sido un simple programa capaz de autoreproducirse, pero ya era una verdadera amenaza para el mundo informático. Sin embargo, no fue hasta unos años después, cuando la aparición del "Michelangelo", un virus de sector de booteo que debía activarse un 23 de marzo, fecha del nacimiento del famoso artista, en que el manejo casi sensacionalista de la prensa logró que mucha gente tomara conciencia de su peligrosidad, si no se tomaban las mínimas precauciones. Es que las historias de los "gusanos" y otros virus de Internet, tan lejanos para muchos aún, ya estaba en cualquier simple computador, aunque aún no estuviera conectada a la red.

Desde entonces la industria de los antivirus también tuvo su gran auge

CLASIFICACION DE VIRUS

Los virus que existen en la actualidad, se pueden clasificar o agrupar en función de unas determinadas características. Dependiendo de éstas, algunos de ellos pertenecerán a un determinado grupo, pero otros podrán incluirse en varios de ellos. Algunos de los criterios que se tienen en cuenta a la hora de clasificar a los virus, son los siguientes:

- Medio a través del cual realizan su infección.
- Técnicas utilizadas para infectar.
- Técnicas utilizadas para ocultarse y evitar a los antivirus.
- Tipos de archivos que infectan.
- Lugares en los que se esconden, tras la infección.
- Plataforma o sistema operativo al que atacan.
- Acciones que realizan.

Adicionalmente, pueden existir otras características que permitan a agrupar a los virus por en otras categorías (medio de propagación, condiciones de activación, etc).

Aunque bastantes de ellos tendrán una característica especial por la que se asociarán a un tipo concreto dentro de esta clasificación, otros podrán formar parte de varios grupos diferentes.

A continuación se muestra una clasificación que agrupa parte de los tipos de virus más habituales:

- | | |
|----------------------------------|-------------------------|
| ▪ Virus de Archivos | ▪ Gusanos |
| ▪ Virus Residentes | ▪ Troyanos |
| ▪ Virus de Acción Directa | ▪ Bombas Lógicas |
| ▪ Virus de Sobreescritura | ▪ Encriptados |
| ▪ Virus de Compañía | ▪ Multipartites |
| ▪ Virus de Boot | ▪ Residentes |
| ▪ Virus de Macro | ▪ Polimórficos |
| ▪ | |

Virus de Archivos.

Este tipo de virus se encarga de infectar programas o archivos ejecutables (archivos con extensiones EXE o COM). Al realizar la ejecución de uno de estos programas, de forma directa o indirecta, el virus se activa produciendo los efectos dañinos que le caractericen en cada caso. La mayoría de los virus existentes son de este tipo, pudiéndose clasificar cada uno de ellos en función de las acciones que realizan cada uno de ellos en cada caso.

Virus Residentes.

Su característica principal es la de colocarse en la memoria RAM, de forma permanente, cuando es ejecutado. El motivo de esta acción es controlar e interceptar todas las ejecuciones de programas u operaciones llevadas a cabo por el sistema operativo. De este modo podrá infectar todos aquellos archivos y/o programas que sean ejecutados, abiertos, cerrados, renombrados o copiados.

Cuando se ponen en marcha o activan, la primera acción que realizan consiste en comprobar si se cumplen todas las condiciones (fecha, hora, etc.) para atacar. De no ser así, se colocan en la memoria RAM, esperando que se ejecute algún programa. Ocuparán un espacio en memoria de 200 a 5000 bytes. Si en alguna de las operaciones que realiza el sistema operativo, éste trabaja con un archivo ejecutable (programa) no infectado, el virus lo infectará. Para ello, el virus se añadirá al programa que infecta, añadiendo su código al propio código del archivo ejecutable o programa. Esto implica que el virus residente se ejecutará siempre que un programa necesite y acceda a los servicios del sistema operativo.

Cuando el virus consigue colocarse en la memoria como residente, intentará permanecer en ella hasta que se apague o reinicie el computador. Algunos virus de este tipo realizan modificaciones en la configuración del sistema (en el Registro de Windows, entre otros), para volver a colocarse en la memoria como residentes, siempre que se vuelva a encender o reiniciar el computador.

Estos virus permanecen en la memoria hasta que, de algún modo, se eliminan de ella. Esto sólo es posible eliminando el proceso activo correspondiente al virus (mediante la combinación de teclas CTRL+ALT+SUPR), siempre y cuando sea posible (en raras ocasiones lo es). Por tratarse de un virus que se coloca en la memoria RAM, éste desaparecerá de ella siempre que se apague o reinicie el computador. Esto es así porque la memoria RAM es volátil (cuando se elimina la alimentación - corriente eléctrica-, desaparece todo lo que hay en ella). Sin embargo, existen virus residentes que toman las medidas oportunas para volver a colocarse en la memoria, cuando el computador arranque. El virus puede llevar a cabo sus acciones cuando se cumple su condición de activación, o continuar en la memoria de forma permanente, hasta que esta tenga lugar.

Algunos ejemplos de virus residentes son:

AntiCMOS
Viernes 13

AntiEXE
Babylonia

Barrotes
CIH (Chernobyl)

Virus de Acción Directa.

En el momento de su ejecución, el virus trata de replicarse, o reproducirse. Esto quiere decir que creará copias de sí mismo. Cumpliéndose unas determinadas condiciones, particulares y específicas en cada caso, se activará y pasará a realizar infecciones dentro del directorio o carpeta en el que nos encontremos y dentro de los directorios que se encuentran especificados en la línea PATH (camino o ruta de directorios) dentro del archivo AUTOEXEC.BAT. Es posible llevar a cabo la desinfección, de los archivos afectados por el virus, dejándolos en un estado correcto.

Este tipo de virus puede ser considerado como un virus de archivo ya que buscan archivos que puedan ser sus víctimas, para infectarlos. El motivo de que estos virus realicen copias de sí mismos o se reproduzcan, es debido a que no son residentes y por lo tanto no permanecen ejecutándose en memoria. Esto les obliga a reproducirse y actuar directamente.

A continuación puede consultar la información sobre algunos de estos tipos de virus. Si desea obtener más información acceda a las listas de virus de la Enciclopedia, donde puede encontrar las descripciones de un gran número de ellos.

Algunos ejemplos de virus de acción directa son:

Aristotle
Trojan/Win32.TPS

Intruder
VBS/ColdApe.A

W32/HTM.H4
W98/Corvinus.A

Virus de Sobreescritura.

Este tipo de virus se caracteriza por no respetar la información contenida en los archivos que infecta, haciendo que estos queden inservibles posteriormente. Pueden encontrarse virus de sobreescritura que además son residentes y otros que no lo son. Aunque la desinfección es posible, no existe posibilidad de recuperar los archivos infectados, siendo la única alternativa posible la eliminación de éstos. Este tipo de virus puede ser considerado como virus de archivo.

Una característica interesante es que los archivos infectados por virus de sobreescritura, no aumentan de tamaño, a no ser que el virus ocupe más espacio que el propio archivo infectado. Esto es debido a que dicho tipo de virus se coloca encima del contenido del archivo infectado, no se incluye de forma adicional en una sección del mismo.

El efecto que producen estos virus sobre los archivos infectados, es la pérdida parcial o total de su contenido. Éste será irrecuperable.

Algunos ejemplos de virus de sobreescritura son:

Trivial.37.D

Trivial.88.B
Ulodozen

Trivial.88.D

Virus de Compañía.

Los virus de compañía pueden considerarse como virus de archivo, pudiendo además ser residentes o de acción directa. Su nombre es debido a que "acompañan" a otros archivos que ya existían en el sistema, cuando el virus llega a él. Es decir, para efectuar sus operaciones de infección, los virus de compañía pueden esperar en la memoria hasta que se lleve a cabo la ejecución de algún programa (virus residentes) o actuar directamente haciendo copias de sí mismos (virus de acción directa).

Al contrario que los virus de sobreescritura o que los residentes, los virus de compañía no modifican los archivos que infectan. Cuando el sistema operativo está trabajando (ejecutando programas) puede ocurrir que éste (el sistema operativo) tenga que ejecutar un programa con un nombre determinado. Si existen dos archivos ejecutables con el mismo nombre pero con diferentes extensiones (uno con extensión EXE y otro con extensión COM), el sistema operativo ejecutará en primer lugar el que lleve la extensión COM. Esta peculiaridad del sistema operativo es aprovechada por los virus de compañía.

En caso de existir un archivo ejecutable con un determinado nombre y extensión EXE, el virus se encargará de crear otro archivo con el mismo nombre pero con extensión COM haciéndolo invisible (oculto) al usuario para evitar levantar sospechas. Este archivo que crea será el propio virus y el sistema operativo, al encontrarse con dos archivos que llevan el mismo nombre, ejecutará en primer lugar el de extensión COM, siendo éste el virus que en ese preciso instante realizará la infección. Tras realizarse la ejecución del archivo COM correspondiente al virus, éste devuelve el control al sistema operativo para que ejecute el archivo EXE. De esta forma el usuario no tendrá conocimiento de la infección que en ese preciso instante ha tenido lugar. En definitiva, un virus de compañía, seguirá los siguientes pasos:

1. Elige como víctima de su infección a un determinado archivo, con extensión EXE.
2. Crea un archivo con el mismo nombre que el archivo víctima, pero con extensión COM.
3. Se incluye a sí mismo en el archivo con extensión COM (éste será el propio virus).
4. Oculta o esconde el archivo que acaba de crear (el COM), para no levantar sospechas.

A partir de este punto, cuando se intente ejecutar el archivo con extensión EXE, ocurrirá lo siguiente:

1. El sistema operativo intentará ejecutar el archivo con extensión EXE.
2. El sistema operativo será consciente de que existe otro archivo con el mismo nombre, pero con extensión COM.
3. El sistema operativo ejecutará el archivo con extensión COM, que será el virus.

Por estos motivos, pueden existir diferentes formatos correspondientes a los virus de compañía:

- o *Virus de compañía en MS-DOS.* Aprovechan la característica del intérprete de comandos de MS-DOS y ejecutan en primer lugar los archivos COM, antes que los EXE (si en un directorio existen dos archivos con el mismo nombre, pero uno con extensión COM y otro con extensión EXE).
- o *Virus de compañía en Windows.* Funcionan de forma similar a los virus de compañía en MS-DOS. La única diferencia es que éstos no crean un archivo con extensión COM y el mismo nombre que el archivo víctima. Por el contrario, cambian la extensión del archivo víctima, de EXE a COM. Posteriormente, el virus puede quedar como residente en memoria e infectar todos los programas que son ejecutados.

Algunos ejemplos de virus de compañía son:

DeDouble

Little Brother

W95/HLLC.4096.C

Virus de Boot (sector de arranque).

El término Boot o Boot Sector representa lo que también se denomina "sector de arranque". Se trata de una sección muy importante en un disco (disquete o disco duro), en la cual se guarda la información sobre las características de ese disco, además de incluir un programa que permite arrancar el computador con ese disco, determinando previamente si existe sistema operativo en el mismo.

Este tipo de virus de Boot no afectan a los archivos por lo que el contenido del disco no estará en peligro a no ser que se intente arrancar el computador con dicho disco. Si esto ocurre, el virus realizará la infección siguiendo una serie de pasos habituales:

1. Se oculta en un determinado sector del disco infectado.
2. Reserva un determinado espacio en memoria para que éste no sea ocupado por ningún otro programa.

3. Se coloca en esa zona reservada de la memoria.
4. Desde esa posición de memoria, intercepta servicios del sistema operativo.

A partir de este momento, ocurrirá lo siguiente:

1. Siempre que una aplicación del sistema operativo llame a una función de acceso a archivos, el virus toma el control.
2. Se comprueba si el disco al que se accede está infectado. Si no lo está, lo infecta.
3. El virus vuelve a colocar el sector de arranque original (sin infectar).
4. Se modifica el boot original, escribiendo el código del virus en él.

De esta forma el virus cede el control al sistema operativo. Así parecerá no haber ocurrido nada. No obstante el virus seguirá actuando.

Las infecciones de virus de Boot se suelen realizar mediante disquetes siendo la protección contra escritura en él, el mejor método de protección.

Si introducimos un disquete infectado por un virus de Boot en la disquetera de un computador, la infección podría extenderse o propagarse al disco duro. En tal caso, se vería afectado el MBR (Master Boot Record) del disco duro (o de los discos duros existentes en el equipo). Esto implica que todos los tipos de discos (disquete, CD-ROM, unidades Zip, Unidades Jazz,...) que utilicemos posteriormente en el computador infectado, serán igualmente infectados.

Estos virus se encargan de guardar una copia del Boot original, pero cada uno de ellos lo puede hacer de una forma diferente. Algunos los copiarán en una determinada sección del disco y la marcarán como defectuosa. Otros lo almacenan en una sección del disco donde ya hubiese información, perdiéndose esta (y siendo imposible de recuperar dicha información). Finalmente los más agresivos o peligrosos sobrescriben el boot original, impidiendo el arranque del computador con dicho disco.

A continuación puede consultar la información sobre algunos de estos tipos de virus. Si desea obtener más información acceda a las listas de virus de la Enciclopedia, donde puede encontrar las descripciones de un gran número de ellos.

Algunos ejemplos de virus de Boot son:

Anti-Telefónica
Diablo
Michelangelo

CMOS.Erase
Empire
Parity Boot

Cruel
Form
Tequila

Virus de Macro.

A diferencia de los tipos de virus anteriores, los cuales infectan programas (archivos EXE o COM) o aplicaciones, los virus de macro realizan infecciones sobre los archivos (documentos, libros, presentaciones y/o bases de datos) que se han creado con determinadas aplicaciones o programas. Cada uno de estos tipos de archivos puede tener adicionalmente unos pequeños programas, denominados macros.

Una macro no es más que un microprograma que el usuario asocia al archivo que ha creado con determinadas aplicaciones. Éste no depende del sistema operativo, sino de acciones determinadas que el usuario puede realizar dentro del documento que la contiene. Mediante ellos es posible automatizar conjuntos de operaciones para que se lleven a cabo como una sola acción del usuario de forma independiente sin necesidad de realizarlas una a una manualmente.

Por tanto, estas macros podrían estar infectadas o infectarse, lo que significa que los virus (más concretamente los de macro) pueden fijar sus objetivos de infección en ellas. En este caso, al abrir un documento que contenga macros, éstas se cargarán de forma automática (ejecutándose o esperando que el usuario decida ejecutarlas). En ese instante o posteriormente, el virus actuará realizando cualquier tipo de operación perjudicial. Al diferencia de lo que se piensa habitualmente, los virus de macro pueden realizar acciones dañinas de bastante importancia, propagándose en poco tiempo de forma muy rápida.

Por otra parte, estos virus pueden infectar las plantillas genéricas o globales (a través de las macros) que las herramientas (como procesadores de texto, hojas de cálculo) utilizan. Al abrir un documento, hoja de cálculo o base de datos con la plantilla infectada, éstos se infectarán. Este es el método más habitual que emplean los virus de macro para extender sus infecciones.

Este tipo de virus, como ya hemos comentado, actúan sobre los documentos, hojas de cálculo o libros, bases de datos y/o presentaciones con macros. Por lo tanto, su objetivo serán los archivos creados con herramientas que permiten utilizar macros. Esto quiere decir que no existe un sólo tipo de virus de macro, sino uno para cada tipo de herramienta:

- **Virus de macro para Microsoft Word**
- **Virus de macro para Microsoft Excel**
- **Virus de macro para Microsoft Access.**
- **Virus de macro para Microsoft PowerPoint**
- **Virus de macro Multiprograma o Multi Macro Partite**
- **Virus de macro en archivos .RTF**
- **Virus de macro para Lotus Ami Pro.**
- **Virus de macro para Corel Draw.**

No obstante, no todos los programas o herramientas que permitan la gestión de macros serán objetivo de este tipo de virus. Las herramientas que son atacadas por los virus de macro, deben cumplir una serie de condiciones:

Las macros pueden transportarse (a través de cualquier medio) de un computador a otro, por estar incluidas en el propio archivo infectado (documento, hoja de cálculo, presentación, base de datos).

Se pueden obtener, incluir y utilizar en un archivo las macros que se han creado e incluido en otros.

Las macros pueden ejecutarse automáticamente (al abrir o cerrar el archivo, por ejemplo), sin que esto dependa del usuario.

Algunos ejemplos de virus de macro son:

Virus de macro para Microsoft Word.

**Bablas
Melissa**

**Class
Marker**

**Lewinsky
Elecciones2000**

Virus de macro para Microsoft Excel.

**Barisada
Oblivion**

**Laroux
Sugar**

**Manalo
Totaler**

Virus de enlace o de directorio.

El sistema operativo debe conocer en todo momento información sobre un determinado archivo, como el nombre que tiene y el lugar (carpeta o directorio) en el que se encuentra (en el que se ha guardado). Para ello le asignará una dirección a la que se debería acceder en caso de desear utilizar ese determinado archivo. Los virus de enlace o directorio se encargan de alterar estas direcciones para provocar la infección de un determinado archivo. Si un programa (archivo con extensión EXE o COM) se encuentra en una dirección concreta, para ejecutarlo habrá que acceder a dicha dirección. Sin embargo, el virus de enlace o directorio la habrá modificado con anterioridad. Lo que hace es alterar esta dirección (dentro de la FAT) para que apunte al lugar en el que se encuentra el virus, guardando en otro lugar la dirección de acceso correcta. De esta forma, cuando se pretenda ejecutar el archivo, lo que se hará realmente es ejecutar el virus. En definitiva, este tipo de virus funcionan del siguiente modo:

1. Modifican la dirección que hace referencia al lugar en el que se encuentra el archivo infectado. Ésta apuntará ahora al lugar en el que se encuentra el virus.
2. Cuando se pretende ejecutar el archivo, realmente se ejecutará el virus (ya que la dirección de acceso al mismo, se habrá modificado para que apunte a la del virus).

Ya que este tipo de virus puede modificar las direcciones donde se encuentran todos los archivos del disco (disco duro), su capacidad para infectar TODOS éstos es real.

De este modo, los virus de enlace o directorio pueden infectar toda la información contenida en un disco, pero les es imposible realizar infecciones en unidades de red o agregarse a los archivos infectados. En caso de realizar un análisis del disco en busca de errores (mediante programas como SCANDISK o CHKDSK), se detectarán grandes cantidades de errores que identifican todos los enlaces a los archivos que el virus ha modificado. No obstante, en este caso sería mejor no recuperarlos ya que podría producirse un caos en lo que al sistema de almacenamiento de la información se refiere, que sería más perjudicial si cabe.

A continuación puede consultar la información sobre algunos de estos tipos de virus. Si desea obtener más información acceda a las listas de virus de la Enciclopedia, donde puede encontrar las descripciones de un gran número de ellos.

Un ejemplo de este virus es el **Byway**

Gusanos (Worms).

Los gusanos se diferencian de los virus en que no intentan infectar otros archivos. Su único objetivo es propagarse o expandirse a otros computadores de la forma más rápida posible. Por otra parte, emplean técnicas para replicarse (propagarse). En realidad su objetivo es crear copias de sí mismos y con ellas realizar infecciones en otros computadores. Las infecciones producidas o reproducciones que éstos realizan casi siempre a través de medios como el correo electrónico, las redes de computadores y los canales de IRC en Internet. También es posible que se multipliquen dentro de la memoria del PC.

Cuando un gusano es ejecutado, permanece así hasta que se apaga o se reinicia el computador. No obstante cada uno de ellos utiliza técnicas diferentes para asegurar su ejecución siempre que se arranca el computador y se entra en Windows. Por ejemplo la modificación del Registro de Windows.

Los gusanos que centran sus infecciones en otros computadores, copian el programa que utilizan para realizar la infección en un determinado directorio de dicho equipo. Esto lo conseguirán propagándose a través de cualquiera de las vías que permitan el acceso a otros PC's (red, correo electrónico, unidades de disco, Internet). Por otra parte, podría darse en caso de que el gusano estuviese compuesto por varios programas. En tal caso, cada uno de ellos actuará de forma subordinada a uno de éstos que se considerará principal. Esta variación, suele ser denominado como gusano de red.

Los pasos que sigue generalmente un gusano para realizar sus infecciones se pueden resumir en:

1. Alguien (generalmente un hacker), aprovechando los posibles fallos de seguridad en el sistema o en una determinada herramienta software, introduce el gusano en una red de computadores.
2. El gusano entra en los equipos a los que pueda acceder a través de un hueco de seguridad.
3. Una vez allí, el gusano crea una copia de sí mismo.

4. Después de esto, intenta introducirse en todos los computadores a los que pueda tener acceso.

Dependiendo del lenguaje en el que estén escritos, las técnicas utilizadas para propagarse y otras características, los gusanos pueden ser de varios tipos:

Gusanos de correo electrónico: son gusanos que se propagan a través de mensajes de correo electrónico, mediante la utilización de programas clientes de correo.

Gusanos de IRC (gusanos de mIRC): son gusanos que se propagan a través de canales de IRC (Chat). Los programas de IRC que emplean habitualmente para ello, son mIRC y Pirch.

Gusanos de VBS (Visual Basic Script). son gusanos escritos o creados en Visual Basic Script.

Gusanos de Windows32

Son gusanos que se propagan a través de las API de Windows (las funciones pertenecientes a un determinado protocolo de Internet).

Algunos ejemplos de virus gusano son:

Disemboweler
Happy99
Navidad

ExploreZip
I Love You
Pretty

Fix2001
Mandragore
Park The Fly

Troyanos (Caballos de Troya).

Los troyanos no se pueden considerar dentro de la categoría de virus. Recogen su nombre de la mitología (el famoso caballo de madera en el que se escondieron los soldados para entrar a la ciudad de forma aparentemente inofensiva, cuando lo que pretendían era realmente hacerse con ella). Del mismo modo funcionan los troyanos. Éstos parecen ser programas inofensivos que llegan a nuestro computador por cualquier medio. Cuando ejecutamos este programa (llevarán nombres o tendrán características que nos incitarán a ello), se instalará en nuestro computador otro programa que podrá producir efectos destructivos.

En un principio, el troyano podría no activar sus efectos. De todas formas, cuando esto ocurra (cuando se cumple la condición de activación), se podrán eliminar archivos, perder la información del disco duro, o abrirse los posibles huecos de seguridad a modo de puertas traseras (backdoor) por las que nuestro equipo podría ser atacado.

La mayoría de ellos se encargan de acceder a determinados puertos de comunicaciones y abrirlos o dejarlos accesibles desde el exterior. En tal caso, a través de una conexión (en una red local o a través de Internet) alguien podría acceder a toda la información contenida en nuestro equipo (contraseñas, claves personales, direcciones de correo electrónico), enviar esta información a otras direcciones (a otros computadores, generalmente los del atacante) y realizar cualquier tipo de operación sin nuestro consentimiento.

Algunos ejemplos de virus troyanos son:

Subseven
Back Orifice
Extacis

Netbus
DonaldDick
KillCMOS

Win32/HLLP
Crack2000
Asylum Bck

Bombas Lógicas.

Estos se encargan de activarse y producir destrozos de consideración en el equipo al que han infectado, sólo cuando se cumple/n una/s determinada/s condición/es. No se consideran virus como tales, ya que no se reproducen, sino que dependen de las acciones realizadas que lleve a cabo el usuario (éste debe copiarlos y/o ejecutarlos, de forma generalmente no intencionada).

A continuación puede consultar la información sobre algunos de estos tipos de virus. Si desea obtener más información acceda a las listas de virus de la Enciclopedia, donde puede encontrar las descripciones de un gran número de ellos.

Un ejemplo de este tipo de virus es el Restart

Encriptados.

Más que un tipo de virus, se trata de una técnica que éstos pueden utilizar. Por este motivo, los virus que la utilizan (pudiendo pertenecer a otros tipos o categorías), se suelen denominar también encriptados. Esto es, el virus se cifra, codifica o "encripta" a sí mismo para no ser fácilmente detectado por los programas antivirus. Para realizar sus actividades, el virus se descifra a sí mismo y cuando ha finalizado, se vuelve a cifrar.

Algunos ejemplos de virus encriptados son:

DieHard
Flip

Explosion-II
Junkie

Elvira
TMC

Multipartitos.

Este tipo de virus pueden realizar múltiples infecciones y hacerlo además utilizando diferentes técnicas para ello. Su objetivo es cualquier elemento que pueda ser infectado: archivos, programas, macros, discos, etc. Se consideran bastante peligrosos por su capacidad de combinar muchas técnicas de infección y las acciones que pueden llegar a realizar.

Algunos ejemplos de virus encriptados son:

**Inca Natas
Pieck**

**One
Tequila**

Half

Polimórficos.

Son virus que emplean una nueva técnica para dificultar su detección por parte de los programas antivirus (generalmente, son los virus que más cuesta detectar). En este caso varían en cada una de las infecciones que llevan a cabo. De esta forma, generan una elevada cantidad de copias de sí mismos.

Los virus polimórficos se encriptan o cifran de forma diferente (utilizando diferentes algoritmos y claves de cifrado), en cada una de las infecciones que realizan. Esto hace que no se puedan detectar a través de la búsqueda de cadenas o firmas (ya que éstas serán diferentes en cada cifrado).

A continuación puede consultar la información sobre algunos de estos tipos de virus. Si desea obtener más información acceda a las listas de virus de la Enciclopedia, donde puede encontrar las descripciones de un gran número de ellos.

Algunos ejemplos de virus encriptados son:

**Cocaine
Neuroquila**

**Kriz
Satan Bug**

**Marburg
Tuareg**

METODOS DE INFECCION

Algunos posibles medios de entrada para los virus

- Unidades de disco extraíbles
- Redes de computadores
- Internet
 - ◊ Correo electrónico
 - ◊ Páginas web
 - ◊ Transferencia de archivos (FTP)
 - ◊ Descargas
 - ◊ Grupos de noticias

Unidades de disco extraíbles.

Las unidades de disco son aquellos medios de almacenamiento en los que se guarda información, mediante archivos, documentos, o archivos. Con ellos se puede trabajar en un computador para, posteriormente, utilizarlos en otro diferente. Algunos de estos medios de almacenamiento pueden ser los disquetes, CD-ROM's, unidades Zip y Unidades Jazz.

Los virus pueden llegar a nuestro computador mediante disquete, CD-ROM y otras unidades de disco extraíbles

Los disquetes (u otras unidades de disco extraíbles), pueden almacenar programas, archivos, páginas web (HTML), mensajes de correo que incluyen archivos infectados, archivos comprimidos. Cualquiera de estos elementos podría estar infectado. De la misma forma, el disco podría tener infectado el denominado "sector de arranque", debido a un virus de Boot . Aunque todavía tienen lugar, hoy en día las infecciones producidas a través de disquetes han disminuido considerablemente hasta un 10%. Éste medio de propagación ha dejado paso a otros mucho más rápidos, como el correo electrónico.

Redes de computadores.

Una red es un conjunto o sistema de computadores conectados entre sí físicamente (a través de cable, módem), para facilitar el trabajo de varios usuarios. De este modo es posible transferir información entre ellos y/o acceder a la información que contiene uno de ellos, desde los restantes. Si la información (programas, archivos, documentos) a la que se accede de un computador a otro estuviese infectada, los computadores que acceden a ella, podrían infectarse igualmente.

Internet.

Cada día más se utilizan las posibilidades que brinda Internet para obtener información, realizar envíos y recepciones de archivos, recibir y publicar noticias, o descargar archivos. Internet se ha convertido en la mayor vía de entrada de virus. Todas estas operaciones se basan en la transferencia de información, así como en la conexión de diferentes computadores en cualquier parte del mundo. Por tanto, cualquier virus puede introducirse en nuestro computador al mismo tiempo que la

información recibida. A través de Internet la infección podría realizarse empleando diferentes caminos como los siguientes:

- Correo electrónico
- Páginas web
- Transferencia de archivos (FTP)
- Downloads (descargas)
- Grupos de noticias

Correo electrónico: en un mensaje enviado o recibido se pueden incluir documentos o archivos (archivo adjunto o attachment) y por ende estos archivos podrían estar infectados. Al abrir el mensaje y ejecutar o abrir el archivo incluido en él, el computador del destinatario del mensaje sería infectado. Las características más importantes de las infecciones a través de correo electrónico son:

1. *Elevada capacidad de replicación y propagación.* El virus se puede extender a miles de computadores de todo el mundo, en cuestión de minutos.
2. *Almacenamiento de mensajes.* Éstos se guardan en bases de datos especiales, difíciles de analizar con antivirus que no están especialmente diseñados para sistemas de correo electrónico.
3. *Elevada capacidad de conexión.* Es posible enviar y recibir mensajes entre casi cualquier tipo de computador/plataforma.

A diario se intercambian millones y millones de mensajes de correo en todo el mundo. El tiempo transcurrido entre el envío de un mensaje y su recepción, es mínimo. Además, un mismo mensaje de correo electrónico puede tener un número elevado de destinatarios. Esto confiere al correo electrónico las condiciones más apetecibles para los creadores de virus: extrema rapidez de propagación y un gran número de destinatarios.

Por otra parte, los virus actuales pueden producir la infección y tienen capacidad para volver enviarse a sí mismos (autoenviarse) a otros computadores (sin que el usuario infectado sea consciente de ello). En este caso los nuevos destinatarios del virus podrán ser todas las personas que el usuario infectado tenga incluidas en su Libreta de Direcciones de correo.

En la gran mayoría de las ocasiones, las infecciones a través de e-mail no ocurren cuando se abre el mensaje correspondiente, sino cuando se ejecuta o abre el archivo incluido en él, no obstante existen excepciones. Algunos virus, la minoría, pueden producir su infección cuando se abre el mensaje de correo (sin necesidad de ejecutar el archivo adjunto).

Ejemplo de virus que se propaga por un mensaje de correo electrónico es el **VBS/TqII.A.**

Páginas Web: la mayoría de las páginas que visitamos en Internet son archivos de texto o imágenes escritos en un lenguaje denominado HTML. No obstante también pueden contener programas denominados Controles ActiveX y Applets de Java, que son programas. Éstos sí pueden estar infectados y podrían infectar al usuario que se encuentre visitando esa página. Si una de estas páginas incluye un virus de código HTML que incluye secciones de código dinámico (que ejecuta programas, o realiza determinadas acciones), sólo con visitarla podríamos infectarnos.

La navegación por páginas Web puede aprovechar las deficiencias de nuestro navegador, mediante los Controles Active-X, los Applets de Java, el código HTML y/o JavaScript, además de otros métodos. De esta forma los virus podrían "colarse" en nuestro computador.

Transferencia de archivos (FTP): Mediante este mecanismo se pueden colocar documentos en computadores que se encuentran en cualquier parte del mundo (upload) o copiar archivos de estos computadores al nuestro (download). En la descarga, un archivo se copia directamente desde un determinado lugar, hasta nuestro computador. Estos archivos pueden contener virus que infectarán nuestro computador.

Grupos de noticias (News o Newsgroups): mediante las denominadas "News" es posible debatir sobre un determinado tema con cualquier otra persona del mundo y recibir correo electrónico con nuevas noticias sobre ese tema. Cada usuario va dejando sus comentarios, dudas, o notas sobre determinados temas y otros usuarios pueden responderle, opinar, resolver dudas,.etc. Estos mensajes con noticias pueden tener documentación adjunta infectada que permita la introducción de virus en nuestro computador.

TABLA N°1. EVOLUCIÓN DE LOS MEDIOS DE INFECCIÓN USADOS POR VIRUS DURANTE 4 AÑOS.

Vías de infección	1996 (%)	1997 (%)	1998 (%)	1999 (%)
Archivos adjuntos en e-mail	9	96	32	56
Disquete: casa	36	42	46	25
Download: BBS/IPP/Internet	10	16	9	11
Disquete :otros	21	27	21	9
NS/ NC	15	7	5	7
Navegación WEB	-	5	2	3
Disquete: demo	11	8	4	2
Disquete: servicio técnico	3	3	3	2
Download sistemas internos	2	2	3	2
Sin especificar	-	-	-	2
Otros	0	5	1	1
Distribución autom. Software	0	2	1	0
CD Distribución de Software	0	1	2	0
Disquete: Encargado de Red	1	3	1	0
Disquete persona mal intencionada	0	1	1	0
Disquete: Software Comprimido	2	4	2	0

Según la evolución en los últimos años resulta evidente que el medio de propagación preferido por los creadores de virus, es el correo electrónico.

LUGARES DE RESIDENCIA

Un virus utiliza sus propias medidas de ocultamiento, pudiendo "escondarse" de los antivirus en diferentes lugares y utilizando diferentes técnicas para ello. Algunos de estos escondites, podrían ser los siguientes:

- **En memoria principal:** en este caso el virus se colocará automáticamente en la memoria principal (memoria RAM) esperando que se ejecute algún programa (archivo con extensión EXE o COM) para infectarlo. Ese tipo de virus, se denomina residente.
- **Documentos con macros:** por regla general, los archivos que no sean programas, no son infectados por ningún tipo de virus. Sin embargo, existen determinados tipos de documentos o archivos con los que el usuario puede trabajar, o que puede crear, que permiten incluir en ellos lo que se denomina macro. Una macro es un conjunto de instrucciones o acciones que otro programa puede llevar a cabo. Pues bien, estas macros pueden formar parte del documento (texto, hoja de cálculo o base de datos) y por tratarse de programas pueden ser infectados por los virus (virus de macro).
- **Sector de arranque (Boot y Master Boot):** el sector de arranque es una sección concreta de un disco (disquete o disco duro) en la que se guarda la información sobre las características de disco y sobre el contenido del mismo. Cuando hablamos del sector de arranque de un disquete utilizamos el término BOOT, mientras que si se trata del sector de arranque de un disco duro, emplearemos el término Master BOOT (MBR). En ocasiones, esta sección de un disco contiene un programa que permite arrancar el computador. Algunos virus (los virus de Boot) se esconden en este lugar infectando ese programa y haciendo, en el arranque del computador, que se ejecute el virus.
- **Archivos adjuntos a los mensajes de correo electrónico:** cada vez más se utiliza el correo electrónico para el envío de archivos. Estos archivos acompañan al mensaje (archivos adjuntos o attachments) de texto que se envía, pudiendo estar infectados. Generalmente, al recibirlos, el destinatario no sospecha que el archivo recibido puede contener un virus o serlo, pero al abrir el mensaje y posteriormente abrir el archivo que dentro de él se incluye podría llevarse una sorpresa desagradable.
- **Páginas Web en Internet:** las páginas que se visitan a través de la navegación por Internet, son archivos que por regla general no deberían estar infectados ya que se trata de documentos de texto (texto, imágenes, sonido). Sin embargo éstas pueden incluir otros elementos denominados Applets de Java o Controles ActiveX. Estos son programas que dotan a la página Web de mayor dinamismo, presentaciones y en definitiva, posibilidades. Por tratarse de programas pueden estar infectados e infectar al usuario que visita la página que los contiene.

TECNICAS USADAS POR LOS VIRUS PARA INFECCIÓN Y OCULTAMIENTO

Cada uno de los miles de virus existentes utiliza diferentes mecanismos, tanto para realizar la infección como para ocultarse y pasar desapercibido. Estas técnicas evolucionan con el tiempo, como las técnicas utilizadas por los programas antivirus para detectarlos. los mecanismos utilizados por los virus con más frecuencia son:

- Ocultamiento (Stealth)
- Sobrepasamiento (Tunneling)
- Autoencriptación
- Polimorfismo
- Armouring

Ocultamiento (Stealth)

Los virus que utilizan este tipo de métodos intentan pasar desapercibidos ante los ojos del usuario, no levantando ninguna sospecha sobre la infección que ya ha tenido lugar. Los virus residentes son los que más la utilizan, aunque no es exclusivamente este tipo de virus quienes la aplican, otros tipos de virus también la utilizan. Por otra parte, Las técnicas de ocultamiento o stealth pueden ser varias, el término ocultamiento no se refiere a una sola forma de realizar esta práctica. No obstante, los programas antivirus, también utilizan técnicas especiales anti-ocultamiento para realizar las detecciones de estos tipos de virus.

El virus se encargará de que cada las señales que puede dejar en el momento de la infección no puedan ser visualizadas. Para ello vigilará peticiones de información que requiere el sistema operativo acerca de estas características, interceptándolas y ofreciendo un información falseada e irreal. Los virus que utilizan técnicas de ocultamiento o stealth, suelen realizar ciertas acciones para que no se aprecien sus efectos. Entre alguna de éstas, podemos destacar las siguientes:

- Cuando un virus infecta un determinado archivo, suele dejar signos evidentes de su actuación, como los siguientes: aumento de tamaño en el archivo infectado, modificación de la fecha y hora de creación en el archivo infectado, secciones marcadas como defectuosas, disminución de la capacidad en la memoria.
- Los archivos infectados aumentarán de tamaño cuando se produce la infección, ya que el virus se introduce dentro del mismo. Sin embargo, este tipo de virus impide que se muestre el nuevo tamaño del archivo, para no levantar sospechas.
- Cuando infectan a un archivo, no modifican su fecha, ni su hora. Es decir, no permiten que el archivo tenga la fecha y hora de la última modificación (las del momento en el que se produjo la infección).
- Si se colocan en memoria, lo suelen hacer por encima de los primeros 640 Kbytes.

Sobrepasamiento (Tunneling)

Se trata de una técnica especialmente diseñada para imposibilitar la protección antivirus en cualquier momento. Mientras el análisis permanente, o residente, del programa antivirus que se encuentre instalado intenta realizar detecciones, el virus actúa en su contra. Todas las operaciones que se realizan sobre cualquiera de los archivos son inspeccionadas por el antivirus mediante la interceptación de las acciones que el sistema operativo lleva a cabo para hacerlas posibles. De la misma manera, el virus interceptará estas peticiones o servicios del sistema operativo, obteniendo las direcciones de memoria en las que se encuentran. Así el antivirus no detectará la presencia del virus.

No obstante, existen técnicas antivirus alternativas que permiten la detección de virus que realicen este tipo de operaciones.

Autoencriptación

Los antivirus se encargan de buscar determinadas cadenas de caracteres (lo que se denomina la firma del virus) propias de cada uno de los posibles virus. Estos, por su parte y mediante la técnica de autoencriptación, podrían infectar de forma diferente en cada ocasión (polimórficos).

Esto significa que el virus utilizará una cadena concreta para realizar una infección, mientras que en la siguiente infección utilizará otra distinta. Por otro lado, el virus codifica o cifra sus cadenas para que al antivirus le sea difícil encontrarlo. Sin embargo, los virus que utilizan este tipo de técnicas, emplean siempre la misma rutina o algoritmo de encriptación, con lo que es posible su detección.

Es decir, mediante una clave de cifrado y una serie de operaciones matemáticas, el virus se puede codificar a sí mismo. Esto dificulta la decodificación del virus para su análisis y/o detección. El virus también puede descifrarse a sí mismo. Generalmente, utilizan la misma clave para el cifrado que para el descifrado.

Polimorfismo: basándose en la técnica de autoencriptación, los virus polimórficos se codifican o cifran, de manera diferente en cada infección que realizan (su firma variará de una infección a otra). Si sólo fuese así estaríamos hablando de virus que utilizan la encriptación, pero adicionalmente dichos virus cifrarán también el modo (rutina o algoritmo) mediante el cual realizan el cifrado de su firma. Todo esto hace posible que un virus polimórfico sea capaz de crear ejemplares de sí mismo diferentes, de una infección a la siguiente, cambiando de "forma" en cada una de ellas.

Para su detección, los programas antivirus emplean técnicas de simulación de descifrado. En un principio, éstos tratarán de localizar a los virus buscando su firma o patrón (cadena de caracteres que lo identifica de manera única). Si el virus está codificado y además esta codificación se hace de forma diferente en cada una de las infecciones, resultará muy difícil su detección.

Sin embargo, el virus no puede codificarse completamente a sí mismo, ya que necesita contar con una parte (no cifrada) que le permita realizar su propia

decodificación. Esto es utilizado por los programas antivirus para realizar la detección de los virus polimórficos. Para ello el antivirus intentará localizar la rutina o algoritmo que permite al virus decodificarse automáticamente.

Armouring

Corresponde a una técnica en la cual el virus impide que se pueda estudiar su código, haciendo imposible su desensamblado o traseado. De ahí el nombre de armouring (acorazado, con armadura). De todas formas, existen programas antivirus que utilizan técnicas heurísticas para detectar a este tipo de virus.

CLASIFICACIÓN DE DAÑOS OCASIONADOS POR VIRUS

Sin daños: en este caso los virus no realizan ninguna acción tras la infección. Generalmente, suelen ser virus que solamente se dedican a propagarse e infectar otros elementos y/o equipos (se envían a sí mismos por correo electrónico, IRC, o a través de la red).

Daño mínimo: solamente realizan acciones que son molestas al usuario, sin afectar a la integridad de la información, ni de otras áreas del equipo (presentación mensajes por pantalla, animaciones en pantalla).

Daño moderado-escaso: en este caso pueden presentarse modificaciones de archivos o pérdidas moderadas de información, pero nunca serán totalmente destructivas (desaparecen algunos archivos, o el contenido de parte de ellos). Las posibles acciones realizadas por el virus, serían reparables.

Daño grave: pérdida de grandes cantidades de información y/o archivos. Aun así, parte de los datos podrían ser recuperables, aunque el proceso sería algo complicado.

Daño muy grave-irreparable: en este caso se podría perder toda la información contenida en las unidades de disco infectadas (incluidas las unidades de red). Se podría además perder la estructura de cada una de las unidades de disco (por lo menos de la principal), mediante el formateo de éstas. Estos daños son muy difícilmente reparables y algunos de ellos irreparables. Además, se atacan también otros sistemas de memoria como la RAM, la CMOS y la BIOS, así como los sistemas de arranque y todos los archivos propios del sistema.

Daños imprevisibles: son aquellos que generalmente causan los troyanos. Éstos son programas que pueden estar manipulados de forma remota (desde otro computador) por una persona que está produciendo un ataque (atacante o hacker).

Este tipo de programas cada vez son más complejos y cuentan con más utilidades y funciones de ataque. Con el programa cliente -en el computador del atacante-, el programa servidor -en el computador de la víctima- y una conexión a través de un puerto de comunicaciones en el computador de la víctima, es posible realizar cualquier acción en éste último.

SINTOMAS DE INFECCIÓN

Cuando se produce una infección posibles síntomas que podemos apreciar, cuando algún virus, gusano o troyano ha producido una infección o se ha activado en nuestro computador. Algunos de los síntomas o efectos que podemos apreciar en nuestro computador, cuando el virus ha producido su infección o se ha activado (en función de la condición de activación), podrían ser los siguientes:

Lentitud: se puede apreciar que el computador trabaja mucho más despacio de lo habitual. Tarda mucho más en abrir las aplicaciones o programas que utilizamos. Incluso el propio sistema operativo emplea mucho más tiempo en realizar operaciones sencillas que antes no le llevaban tanto tiempo.

Ejecución-Apertura: cuando tratamos de poner en marcha un determinado programa o abrir un determinado archivo, este no se ejecuta o no se abre.

Desaparición de archivos y carpetas: los archivos contenidos en algunas carpetas (generalmente aquellas que pertenecen al sistema operativo o a ciertas aplicaciones), han desaparecido porque el virus las ha borrado. También podrían desaparecer directorios o carpetas completas.

Imposible acceder al contenido de archivos: al abrir un archivo se muestra un mensaje de error, o simplemente esto es imposible. Puede ser que el virus haya modificado la Tabla de Asignación de Archivos, perdiéndose así las direcciones en las que éstos comienzan.

Mensajes de error inesperados y no habituales: aparecen cuadros de diálogo con mensajes absurdos, hirientes o agresivos que generalmente no aparecen en situaciones normales.

Disminución de espacio en la memoria y el disco duro: el tamaño libre en el disco duro disminuye considerablemente. Esto podría indicar que el virus ha infectado una gran cantidad de archivos y que se está extendiendo dentro del computador. Cuando ejecutamos algún programa, además aparecen mensajes indicando que no tenemos memoria suficiente para hacerlo (aunque esto no sea cierto, pues no tenemos apenas programas abiertos).

Sectores defectuosos: se indica que alguna sección del disco en el que estamos trabajando, tiene errores y que es imposible guardar un archivo, o realizar cualquier tipo de operación en ella.

Alteración en las propiedades de los archivos: el virus modifica alguna o todas las características del archivo al que infecta. De esta manera, podremos apreciar, que la fecha/hora asociada a él (la de su creación o última modificación) es incorrecta, se han modificado sus atributos o el tamaño ha cambiado.

Errores del sistema operativo: al realizar ciertas operaciones -normales y soportables por el sistema operativo en otro tipo de circunstancias- aparecen mensajes de error, se realizan otras acciones no deseadas, o simplemente no ocurre nada.

Archivos duplicados: si existe un archivo con extensión EXE, aparecerá otro con el mismo nombre que éste, pero con extensión COM (también programa). El archivo con extensión COM será el virus. El virus lo hace así porque, si existen dos archivos con el mismo nombre, el sistema operativo ejecutaría siempre en primer lugar el que tenga extensión COM.

Archivos renombrados: el virus habrá cambiado el nombre de los archivos a los que ha infectados y/o a otros concretos.

Problemas en el arranque del computador: el computador no arranca, o no lo hace de la forma habitual. Sería conveniente arrancar el computador con un disco de sistema o arranque y analizar todas las áreas del computador con un antivirus n línea de comandos.

Bloqueo del computador: en situaciones donde tenemos pocos programas abiertos (o ninguno) y la carga del sistema no es elevada, éste se bloquea (se queda "colgado") y nos impide continuar trabajando. Será necesario utilizar la combinación de teclas CTRL+ALT+SUPR. para poder eliminar la tarea que se ha bloqueado, o reiniciar el sistema.

El computador se apaga (se reinicia): sin realizar ninguna operación extraña y mientras estamos trabajando normalmente con el computador, éste se apaga automáticamente y se vuelve a encender (se reinicia).

El programa se cierra: mientras estamos trabajando con una aplicación o programa, ésta se cierra sin haber realizado ninguna operación indebida o alguna que debería haber producido esta acción.

Se abre y cierra la bandeja del CD-ROM: sin que intervengamos para nada en el equipo, la bandeja de la unidad lectora de CD-ROM, se abre y se cierra de forma autónoma. Esta acción es muy típica de los troyanos.

El teclado y/o el ratón no funcionan correctamente: cuando utilizamos el teclado, éste no escribe lo que queremos, o realiza acciones que no corresponden a la combinación de teclas que hemos pulsado. Por otra parte, el puntero del ratón se mueve de forma autónoma por toda la pantalla, sin que nosotros lo movamos (o cuando lo movemos, realiza ciertas animaciones no habituales).

Desaparecen secciones de ventanas y/o aparecen otras nuevas: determinadas secciones (botones, opciones de menú, redidentes en la barra de tareas de Windows, textos) que deberían aparecer en una determinada ventana, han desaparecido y no se muestran en ella. También sería posible que en pantallas donde no debería aparecer nada, se muestren iconos extraños o contenidos que no son habituales en ellas.

FALSAS ALARMAS DE VIRUS

Estas se pueden clasificar en 2 categorías:

Hoax

Los llamados Hoax no son virus sino falsos mensajes de alarma sobre virus inexistentes. Estos se envían por correo electrónico con la intención de extender falsos rumores por Internet. Los mensajes no suelen estar fechados, con lo que se pretende que los mensajes siempre parezcan recientes.

En ocasiones, los Hoax pretenden engañar a los usuarios mediante el uso de palabras técnicas. Por otra parte, suele ser frecuente la inclusión del nombre de ciertas agencias de prensa en el encabezamiento de estos mensajes. Con todo esto se pretende dar un aspecto verídico a los mensajes.

Ante la aparición de este tipo de mensajes no conviene ser alarmistas y lo mejor es no prestarles la más mínima atención.

Jokes

Los Jokes no son virus sino más bien bromas de mal gusto que tienen por objeto hacer pensar a los usuarios que han sido afectados por un virus. Se trata de programas que simulan los efectos de virus destructivos -por ejemplo la eliminación de los archivos de disco duro-. Ante este tipo de programas lo mejor es no perder la calma y comprobar que en realidad no han producido los efectos destructivos que el programa simulaba.

RECOMENDACIONES PARA EVITAR CONTAGIO

La principal recomendación es usar un antivirus adecuado, escanear las unidades del equipo y actualizarlo frecuentemente. Estos programas por lo general tienen opciones de seguridad, mecanismos de búsqueda y desinfección automática, por ejemplo al introducir en el equipo un disco extraíble.

Una de las actividades más realizadas por los usuarios en Internet, es la descarga de programas (shareware), documentos, etc; además de las descargas de software en lugares concretos. Por este motivo, es muy importante descargar archivos solamente de aquellos lugares o sitios que cuenten con las suficientes garantías. Es por esto que eso se recomienda bajar archivos de sitios seguros, como por ejemplo desde Tucows Inc. (<http://www.tucows.com>), desde la cual se pueden descargar utilidades y herramientas de software.

Pro lo anterior, otro aspecto a considerar es la legalidad de un programa al momento de instalarlo y ejecutarlo ya que generalmente el riesgo de infección mayor si se trata de software pirata.

También otro mecanismo de detección de un virus es estar atento ante algunos ay numerosos síntomas que podrían alertar acerca de la presencia virus: aumento del tamaño de archivos, avisos de macros en documentos Word o Excel, recepción por parte de otras personas de mensajes nuestros de correo que no hemos enviado.

Para evitar las infecciones a través de correo electrónico, podríamos tener en cuenta los siguientes criterios o consejos:

- Contar con antivirus específico para analizar correo electrónico.
- No abrir mensajes sospechosos, cuyo destinatario sea desconocido, que contengan textos extraños,... etc.
- No ejecutar ni abrir los archivos incluidos en mensajes de correo sospechosos.
- Si sospechamos que el mensaje está infectado, lo deberíamos eliminar y avisar de ello al remitente del mismo.

Para evitar contagio a través de navegación por paginas web se recomienda el uso de un navegador apropiado. La navegación por páginas Web puede aprovechar las deficiencias de nuestro navegador, mediante los Controles Active-X, los Applets de Java, el código HTML y/o JavaScript, además de otros métodos. De esta forma los virus podrían infectar nuestro computador.

ANTIVIRUS

DEFINICIÓN DE ANTIVIRUS

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

La función de un programa antivirus es detectar, de alguna manera, la presencia o el accionar de un virus informático en un computador.

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

LOS ANTIVIRUS INFORMATICOS

Un antivirus es cualquier metodología, programa o sistema para prevenir la activación de los virus, su propagación y contagio dentro de un sistema y su inmediata eliminación y la reconstrucción de archivos o de áreas afectadas por los virus informáticos.

Los antivirus permiten la detección y eliminación de virus. Un virus es identificado mediante una cadena del antivirus que busca, encuentra y elimina los distintos virus informáticos.

El software antivirus contrarresta de varias maneras los efectos de los virus informáticos para detectarlos. En resumidas cuentas, la mayoría de las soluciones se basan en tres componentes para la detección : exploración de acceso, exploración requerida, y suma de comprobación.

- **Exploración de acceso:** inicia automáticamente una exploración de virus, cuando se accede a un archivo, es decir al introducir un disco, copiar archivos, ejecutar un programa, etc.
- **Exploración requerida:** el usuario inicia la búsqueda de virus. Las exploraciones se pueden ejecutar inmediatamente, en un directorio o unidad de disco determinado
- **Suma de comprobación o comprobación de integridad:** método por el que un producto antivirus determina si se ha modificado un archivo. Como el código de virus se une físicamente a otro archivo, se puede determinar tal modificación guardando la información del archivo antes de la infección. La suma de comprobación es generalmente exacta y no necesita actualizaciones. Sin embargo la suma de comprobación no proporciona ni el nombre, ni el tipo de virus.

Los programas antivirus se componen fundamentalmente de dos partes : un programa que rastrea (SCAN), si en los dispositivos de almacenamiento se encuentra

alojado algún virus, y otro programa que desinfecta (CLEAN) a la computadora del virus detectado.

TECNICAS AVANZADAS USADAS POR LOS ANTIVIRUS

A medida que evolucionan las técnicas empleadas por los virus y éstas son investigadas, los programas antivirus incorporan medidas de búsqueda de virus y protección más avanzadas como las siguientes:

- **Búsqueda de cadenas:** cada virus contiene determinadas una cadenas de caracteres que le identifican a él exclusivamente, de forma unívoca. Ésta es las denominada firma del virus. Los programas antivirus incorporan un archivo denominado "*Archivo de Identificadores de Virus*", en el que guardan todas las cadenas correspondientes a cada uno de los virus que detectan. De esta forma, para encontrarlos, se analizarán todos los archivos especificados comprobando si alguno contiene alguna de dichas cadenas. Si un archivo no contiene ninguna de ellas, se considera limpio, mientras que si el programa antivirus la detecta en el interior del archivo avisará acerca de la posibilidad de que éste se encuentre infectado.

Esto implica que los antivirus tengan que realizar las búsquedas de dichas cadenas en secciones concretas y no muy extensas del archivo analizado. Del mismo modo deben tener en cuenta que pueden existir dos variantes de un mismo virus, con la misma cadena a buscar, o pueden aparecer nuevos virus cuyas firmas aun no se conocen. Esto hace necesario que los programas antivirus combinen la técnica de Búsqueda de Cadenas, con otras técnicas más precisas.

- **Búsqueda deductiva:** como la búsqueda de cadenas puede no ser demasiado confiable en determinadas ocasiones, los programas antivirus utilizan adicionalmente otras técnicas. Una de ellas, de características similares a la búsqueda de cadenas, es la búsqueda deductiva. Ésta consiste en la observación de ciertas propiedades concretas en cada uno de los archivos que son analizados. Existen propiedades que siempre se dan en los archivos infectados. Cuando la búsqueda deductiva detecte alguna de ellas, confirmará que el archivo se encuentra infectado.

Este tipo de búsqueda tiene en cuenta la estructura interna de los archivos que analiza, la fecha, la hora de dicho archivo y los atributos que tiene asociados (sólo lectura, escritura, sistema, oculto).

- **Excepciones:** una alternativa a la búsqueda de cadenas y a la búsqueda deductiva, es la búsqueda de excepciones. Cuando un virus utiliza una determinada cadena (firma) para realizar una infección, pero en la siguiente emplea otra distinta, es difícil detectarlo mediante la búsqueda de cadenas. Si esto ocurra, el programa antivirus consigue es realizar la búsqueda de un determinado virus, en concreto.

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

Debido a su gran potencia de análisis y sospecha de situaciones extrañas, este tipo de técnica antivirus podría presentar alarmas (falsas alarmas) que hagan referencia a posibles virus, cuando realmente éstos no existen. Esto es debido a que el análisis de cada archivo se realiza mediante la inspección de secciones del mismo que tengan características o realicen funciones que no son habituales.

Este tipo de análisis puede detectar tanto virus conocidos, como virus desconocidos. Esto es así ya que el análisis no se basa en características particulares de ningún virus, sino a características comunes que todos los virus pueden tener (todos los virus utilizan grupos de técnicas similares, que sí pueden ser detectadas). Por esto es aconsejable que el resultado de los análisis heurísticos se tome con precaución. Esto quiere decir que debemos analizar las acciones que deseamos llevar a cabo en consecuencia. Existen antivirus que permiten el envío de archivos sospechosos al para que sean analizados por expertos, mediante un análisis heurístico.

Protección permanente (residente): aunque no se trata de una técnica como tal, la mayoría de los programas antivirus utilizan esta característica adicional. Durante todo el tiempo que el computador permanezca encendido, el programa antivirus se encargará de analizar todos los archivos implicados en todas las operaciones que se realicen (en el sistema y a través de Internet). El antivirus coloca su programa de análisis en la memoria, de forma permanente y cuando, se abren, se cierran, o se ejecutan archivos, etc., el antivirus los analiza. En caso de haberse detectado un virus se muestra un aviso desde el cual es posible realizar la desinfección. Si no se encuentra nada extraño, el proceso de análisis continúa.

Por lo tanto, podemos decir que la protección permanente es quien se encarga de vigilar constantemente todo, sin que el usuario tenga que hacerlo por su cuenta. Esto reduce considerablemente el riesgo de infección ya que el programa antivirus está siempre realizando análisis sobre cualquier área del computador en la que se llevan a cabo acciones y evitando que se ejecuten los archivos o programas infectados en ellas.

Aunque es aconsejable contar siempre con la protección permanente, los antivirus que cuentan con esta posibilidad permiten al usuario activarla o desactivarla. Además, también será posible indicar o configurar cada una de sus características (elementos a analizar, acciones a llevar a cabo en caso de detección, elementos que no deberían ser analizados, indicar cómo deben ser los avisos del antivirus).

- **Vacunación:** mediante esta técnica, el programa antivirus almacenan información sobre las características de cada uno de los archivos que ya ha analizado (los archivos son vacunados). Si en un nuevo análisis de esos archivos se detecta algún cambio entre la información guardada y la información actual del archivo, el antivirus avisa de lo ocurrido. Esta técnica facilita además la reconstrucción del archivo, en el caso de que éste haya sido infectado.

Existen dos tipos de vacunaciones:

- *Interna (Inoculación).* La información se guarda dentro del propio archivo (se añade la vacuna al código del archivo vacunado), de tal forma que al ejecutarse él mismo comprueba si ha sufrido algún cambio.
 - *Externa.* La información que guarda en un archivo especial y desde él se contrasta la información) con al obtenida en el análisis actual.
-
- **Investigación:** existen virus que podrían haberse colocado y activado en la memoria (RAM) del computador. Éstos podrían no haber sido detectados en un análisis normal de la memoria. El mecanismo de investigación consiste en "provocar" al virus para que intente realizar una infección. De este modo se podrán descubrir también nuevos virus y averiguar las artimañas para realizar dicha tarea. Entonces el virus podrá ser detectado. En tal caso, el programa antivirus tendrá en cuenta cuáles son las actividades que lleva a cabo y cómo las realiza.

COSTOS Y DESCRIPCIÓN DE ALGUNOS ANTIVIRUS

Panda Active Scan Software (<http://www.pandasoftware.es>)

(Para el Hogar)

Características:

- No requiere de la instalación de ningún programa, sólo el computador a escanear debe estar conectado a Internet.
- Analiza, desinfecta y elimina los virus de todos los dispositivos del sistema, discos duros, archivos comprimidos y la totalidad del correo electrónico.
- Se actualiza al menos una vez al día, por lo que incorpora a cada análisis los últimos virus descubiertos.

Costo gratuito.

Panda Titanium

(Para el Hogar)

Características:

- Detecta y elimina rápidamente un gran número de virus.
- Actualizaciones automáticas contra nuevos virus.
- Utiliza una avanzada tecnología antivirus para Internet y correo electrónico.
- Utiliza además el llamado *motor UltraFast*, que entrega máxima velocidad en la revisión y mínimo consumo de recursos del sistema.
- Incluye además tecnología *SmartClean* que repara los daños del sistema.
- Soporte Técnico.
- Residente en la memoria, prácticamente pasa desapercibido.
- Tecnología heurística completamente mejorada.
- Sencilla Interfase.

Costo: US\$ 24,95 (uso doméstico, duración de licencia no definida)

Panda Platinum

Windows XP/2000/9x/3.1x/NT/MS-DOS y DOS

- Aporta una protección para Internet y correo electrónico, la principal vía de entrada de virus al sistema.
- Detecta y elimina virus en los más conocidos navegadores (Explorer, Netscape, Opera) y sistemas de correo electrónico (Outlook, Outlook Express, Eudora, Netscape Mail)
- Adicionalmente, Panda Antivirus Platinum bloquea los puertos de salida de servicios de Internet (como telnet, http, ftp...).
- Completa protección multiplataforma para PCs individuales, Panda Antivirus Platinum bloquea todos los posibles puntos de entrada de virus, eliminándolos antes de que puedan causar ningún daño e independientemente de la forma en que intenten acceder al ordenador: disquetes, CD-ROMS, correo electrónico o descargas de ficheros desde Internet.

McAfee Security Center (<http://www.mcafee.com>)

- Las Actualizaciones del Virus automáticas
- La Tecnología de Actualización incremental: Transmite sólo los archivos que han cambiado desde que la última actualización reduciendo el tamaño del archivo y el tiempo de descarga en 1/10 de las versiones anteriores
- El Análisis Heurístico para descubrir y bloquear virus desconocidos y variantes del virus
- La Cuarentena del archivo
- Disco de Rescate de emergencia
- Proporciona protección al e-mail

Costo US\$ 29,95

Norton AntiVirus™ 2002 (<http://www.norton.com>)

Windows 98/XP/2000/NT WS/Me

- Elimina automáticamente los virus sin interrumpir el trabajo
- Bloqueo de script proactivo para detener nuevos virus.
- Analiza y limpia tanto el correo que recibe como el que envía.
- Puede acceder a muchas de sus funciones instantáneamente desde la barra de herramientas del Explorador de Windows®.
- Incluye Norton AntiVirus 2001 para usuarios de Windows 95B.
- Actualizaciones automáticas a través de Internet para la protección contra nuevos virus (Live Update).
- Protege su sistema contra los códigos dañinos ActiveX®, subprogramas Java™ y los caballos de Troya.
- Cuarentena le permite transferir un archivo infectado a un área "segura" de su sistema. do.
- Analizar y enviar (Scan and Deliver) le permite enviar rápida y fácilmente archivos sospechosos o irreparables al equipo de Symantec™ Security Response (antes conocido como Centro de Investigación Antivirus de Symantec, o SARC™) para ser analizadas de inmediato.

Costo: US\$49,95

Norton Antivirus Profesional Edition 2002

- Incluye herramientas para proteger los datos en su Palm OS. Software especial lo ayuda a recuperar archivos importantes que se hayan borrado accidentalmente, y asegura la confidencialidad de sus datos eliminando los archivos que ya no utiliza.
- "Data Recovery" (recuperación de datos)
- "Data Cleaning" elimina todo rasgo de los archivos confidenciales que desea remover de su PC.
- Protección automática sin que tenga que interrumpir su trabajo
- Incluye Norton AntiVirus 2001 para usuarios de Windows 95B.
- Actualizaciones automáticas a través de Internet para la protección contra nuevos virus (LiveUpdate).
- Examina automáticamente los mensajes y adjuntos de correo electrónico de los clientes POP3 estándar, incluyendo Microsoft® Outlook®, Eudora® y Netscape® Mail.

- Protege su sistema contra los códigos dañinos ActiveX®, subprogramas Java™ y los caballos de Troya.
- Cuarentena le permite transferir un archivo infectado a un área "segura".
- Analizar y enviar (Scan and Deliver) le permite enviar rápida y fácilmente archivos sospechosos o irreparables al equipo de Symantec™ Security Response (antes conocido como Centro de Investigación Antivirus de Symantec, o SARC™) para ser analizadas de inmediato

US\$69.45

Panda PYME

- Para Estaciones, Servidores de archivos y Exchange
- Protección Internet.
- Analiza e-mails recibidos y enviados
- Incluye un año de Soporte Técnico Telefónico.
- Garantía de Calidad.
- Panda Antivirus PYME incluye la tecnología de Panda Antivirus Platinum

Costo licencias (US\$)

Nº Licencias	Años			
	1	2	3	Perpetua
5	330	262	561	728
10	594	831,60	1.009,80	1.306,80
25	1.485,00	2.079,00	2.524,50	
50	2.673,00	3.742,20	4.544,10	5.880,60

Panda Corporativo

- Protección completa para redes
- protección global y uniforme para estaciones de trabajo, servidores de archivos, plataformas de mensajería y colaboración, firewalls y proxies,
- Actualizaciones completamente automáticas.
- Blindaje de las comunicaciones vía e-mail e Internet.
- Análisis heurísticos de scripts / HTML y filtrados de contenidos) para el bloqueo preventivo de virus.
- Filtrado de contenidos.
- Notificaciones personalizables en caso de alerta de virus
- Soporte

Costo 1 Licencia (US\$)

Años			
1	2	3	Perpetua
107,85	150,99	183,84	237,27

Panda LINUX

Red Hat

- Diseñado para su manejo desde la línea de comandos o consola.
- El objetivo de Panda Antivirus para Linux es realizar análisis y desinfecciones a las estaciones Windows y DOS conectadas a un servidor Linux, así como el propio servidor Linux.

- Realiza sus análisis sobre archivos empleando búsqueda de cadenas y técnicas heurísticas.
- No se analiza el sector de arranque (boot) ni la tabla de particiones.
- No ofrece servicio de Soporte Técnico para este software.

Costo Gratuito

CONCLUSION

Según lo expresado en el presente informe, se deben tener en cuenta los siguientes aspectos en lo que a virus se refiere:

- Todo virus es un programa y, como tal, debe ser ejecutado para activarse.
- No todo lo que afecte el normal funcionamiento de una computadora es un virus.
- Es imprescindible contar con herramientas de detección y desinfección. Para esto se cuenta con programas antivirus que constituyen un elemento esencial para prevenir estos males y existe en el mercado informático una gran oferta de estos productos.
- Los virus que existen en la actualidad, se pueden clasificar o agrupar en función de unas determinadas características. Dependiendo de éstas, algunos de ellos pertenecerán a un determinado grupo, pero otros podrán incluirse en varios de ellos. Algunos de los criterios que se tienen en cuenta a la hora de clasificar a los virus,
 - Medio a través del cual realizan su infección.
 - Técnicas utilizadas para infectar.
 - Técnicas utilizadas para ocultarse y evitar a los antivirus.
 - Tipos de archivos que infectan.
 - Lugares en los que se esconden, tras la infección.
 - Plataforma o sistema operativo al que atacan.
 - Acciones que realizan.
- Algunos posibles medios de entrada para los virus
 - Unidades de disco extraíbles
 - Redes de computadores
 - Internet
 - Correo electrónico
 - Páginas web
 - Transferencia de archivos (FTP)
 - Descargas
 - Grupos de noticias
-
- Un virus utiliza sus propias medidas de ocultamiento, pudiendo "esconderse" de los antivirus en diferentes lugares y utilizando diferentes técnicas para ello. Algunos de estos escondites o lugares de residencia pueden ser:
 - En memoria principal
 - Documentos con macros
 - Sector de arranque (Boot y Master Boot)
 - Archivos adjuntos a los mensajes de correo electrónico
 - Páginas Web en Internet
-

- Ningún sistema de seguridad es 100% seguro. Por eso todo usuario de computadores debería implementar estrategias de seguridad mediante el uso de 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.

GLOSARIO

Active-X (Controles .Active-X): permiten la ejecución de programas y son muy utilizados en la actualidad, debido a sus interesantes propiedades

Análisis Heurístico: Es el método, estrategia, o criterio establecido para hacer más fácil la resolución de problemas. Este método se aplica automáticamente de forma intuitiva. Aplicado a la lucha antivirus, se trata de un análisis adicional que solamente algunos programas antivirus pueden realizar, para detectar virus que en ese momento son desconocidos.

Antivirus: son todos aquellos programas que permiten analizar memoria, unidades de disco y otros elementos de un computador, en busca de virus. Una vez el antivirus ha detectado alguno de ellos, informa al usuario procediendo inmediatamente y de forma automática a desinfectar los archivos, directorios, o discos que hayan sido víctimas del virus.

Archivo DLL: es un tipo especial de archivo, con extensión DLL. Estos archivos pueden ser utilizados por varios programas y evitan incluir en cada uno de ellos un determinado código. Es decir, hacen posible crear una sección de código que será utilizada por varios programas. Estas librerías pueden ser atacadas por los virus.

Archivos SCR: Son los denominados archivos de Script. Su extensión es SCR y sirven para determinar los parámetros con los que se deben ejecutar unos determinados programas. Permiten iniciar un programa con unas pautas fijadas de antemano.

ASP (Active Server Page): la mayoría de las páginas que generalmente visitamos en Internet, están creadas en el lenguaje HTML. No obstante, existen otras creadas en otros lenguajes, como las ASP. Las primeras se cargan y procesan directamente en el computador del usuario que las visita. Por su parte, las páginas ASP son procesadas o manipuladas en un servidor Web Microsoft, antes de que el visitante la haya cargado completamente en su computador.

BIOS: es la abreviatura de Basic Input / Output System e identifica al software o conjunto de programas que arrancan el computador (antes de encontrarse un disco de sistema) cuando se pulsa el botón de encendido. La BIOS, este programa, se encuentra siempre en la memoria principal, pero no en la RAM (Random Access Memory) pues al apagar el computador se borraría, sino en la ROM (Read Only Memory - Memoria de Sólo Lectura), cuyo almacenamiento es permanente.

BOOT, MASTER BOOT (Sector de Arranque): todos los discos (disquetes y discos duros) tienen una sección muy importante, denominada "sector de arranque". En ella se almacena la información acerca de las características del disco, además de poder albergar un programa con el que es posible arrancar el computador, mediante la utilización de ese disco. Aunque tanto para los disquetes como para los discos duros se habla de sector de arranque, éstos son diferentes y se denominan de forma diferente.

Cifrado-Encriptado: es una de las técnicas que, algunos de los virus existentes, utilizan para que los antivirus no los encuentren. El virus se cifra, codifica o

"encripta" automáticamente cuando realiza una infección. Esta operación de cifrado, consiste en realizar operaciones matemáticas sobre cada de las secciones del código del virus. El resultado es la modificación del código del virus, que dificulta la detección del mismo por parte del antivirus.

Condición de Activación (Tigger): indica las condiciones bajo las cuales el virus se activa o comienza a realizar sus acciones en el computador infectado. Estas condiciones pueden ser de fecha, de acciones, o combinaciones de éstas. Es decir, un virus se puede activar en una determinada fecha, cuando la fecha y la hora del sistema cumple una determinada condición, cuando el usuario infectado realiza ciertas operaciones,... etc. En definitiva, se trata de la condición que activa el payload o carga dañina de los virus.

Cookie: es un archivo de texto que, en ocasiones el servidor envía al usuario cuando éste visita una página web. El objetivo de estos archivos es registrar la visita del usuario a la página e incluir en él información como la identificación del computador visitante, su sistema operativo, el navegador que utiliza, dirección de correo electrónico,... etc. Una de sus utilidades puede consistir en recordar la clave de acceso anteriormente utilizada para acceder a una determinada sección de la web, cuando dicha página vuelve a ser visitada.

Desinfección: es la acción que realizan los programas antivirus cuando, tras detectar un virus, lo eliminan del sistema y, en la medida de lo posible, recuperan la información infectada y restablecen la configuración del sistema (si ésta fue modificada por el virus)

DOS (MS-DOS): estas siglas significan Disk Operating System (DOS). Se refieren al sistema operativo (S.O.) anterior a Windows que, en su momento, creó la empresa Microsoft.

Familia-Grupo: cada uno de los virus existentes, puede contar con diferentes variantes. Esto quiere decir que puede existir un virus que tenga una determinadas características, pero también otros (creados a partir de él), con las mismas o muy similares características. Dicho virus y cada una de sus variantes, constituyen lo que se denomina una familia. Por ejemplo la familia de virus Marker cuenta con las siguientes variantes, entre otras: W97M/Marker.C, W97M/Marker.B.

Falsa Alarma o Falso Positivo: es el fenómeno por el cual un antivirus detecta virus en un elemento (archivo, mensaje de correo) que no está infectado. Esto puede ocurrir, en determinadas ocasiones, debido a la aplicación de técnicas especiales y alternativas para la búsqueda de nuevos virus.

Falso Negativo: es el fenómeno por el cual un antivirus no detecta virus en un elemento (archivo, mensaje de correo) que está infectado. Esto puede ocurrir, en determinadas ocasiones, cuando se trata de un nuevo virus y las técnicas especiales para la detección, no han sido suficientes para detectarlo.

FAT: también denominada Tabla de Asignación de Archivos (File Allocation Table). Representa una sección del disco en la cual se almacenan las direcciones donde se encuentran los archivos contenidos o guardados en dicho disco y el formato, estructura o secciones del mismo. Es decir, el Boot o Master Boot Record forma parte de la FAT, pero no son lo mismo.

Firma- Identificador: la firma de un virus es una cadena alfanumérica (conjunto de letras y/o números consecutivos) que está asociada a un determinado virus, y sólo a él. Por lo tanto es quien identifica al virus, como si de un código o DNI se tratase.

HTTP (HyperText Transfer Protocol): es un protocolo de comunicación que permite el acceso a los documentos de hipertexto, creados en formato HTML (lenguaje HTML de las páginas web). En realidad se trata del protocolo que nos permite visualizar páginas Web a través de nuestro navegador habitual.

Infección: es la acción que realiza un virus al introducirse, empleando cualquier medio (disquete, CD-ROM, conexión en red, mensajes de correo electrónico, FTP,...), en nuestro computador (o en dispositivos de almacenamiento) para poder realizar sus acciones dañinas. Las infecciones pueden ser de dos tipos:

Rápidas. La infección no se produce simplemente cuando se ejecuta el archivo infectado, sino que puede tener lugar por hacer una referencia a dicho archivo.

Lentas. Cuando se trabaja con un archivo (apertura, grabación, copiado, movimientos,...), el virus actúa sobre él infectándolo.

IRC: es una de las posibilidades que permite Internet. Mediante el IRC se pueden mantener conversaciones escritas, en tiempo real, entre varios usuarios conectados a un canal de comunicaciones disponible en Internet.

Java: es uno de los lenguajes de programación con el que se pueden crear páginas Web, componentes que se pueden incluir en éstas, y otros tipos de programas o aplicaciones.

Macro (Virus de macro): una macro es una secuencia de operaciones o instrucciones que definimos para que un programa (por ejemplo, Word, Excel, o Access) las realice de forma automática y secuencial. Estas son "microprogramas" que pueden ser infectados por los virus. Los documentos de texto, las bases de datos o las hojas de cálculo de, no son programas y por ello no deberían ser infectados por ningún virus. No obstante, en cada uno de los archivos creados con este tipo de aplicaciones se pueden definir macros y éstas sí son susceptibles de ser infectadas. Los virus de macro son aquellos que infectan exclusivamente documentos, hojas de cálculo o bases de datos que tienen macros definidas.

Método de Infección: es una de las características más importantes de un virus. A través de ella conocemos cada una de las operaciones que realiza el virus para llevar a cabo su infección. Nos informa sobre las modificaciones en la configuración en el Registro de Windows, que el virus debe realizar en el computador atacado, para llevar a buen término su infección.

Método de Propagación: es una de las características más importantes de un virus. Ésta nos informa de "cómo" y "por qué medio" produce el virus su infección. No solamente se trata de indicar cual es el medio que el virus emplea (disquetes, CD-ROM, redes de computadores, mensajes de correo electrónico, FTP, Internet,...); sino también cómo lo hace y cuales son las características más destacables en este sentido.

Nivel de Riesgo: es una forma de medir lo peligroso que puede llegar a ser un virus. Este valor se asigna a un virus, teniendo en cuenta una serie de factores como los siguientes: las acciones que puede realizar, cómo y a qué velocidad se puede propagar a otros computadores, cuántas infecciones ha producido en todo el mundo.

Nivel de Daños: indica el grado de efectos y/o payload que el virus puede producir en un computador infectado.

Nivel de Distribución: este valor indica cómo se puede extender o se ha extendido el virus por todo el mundo.

Nuke: aunque una determinada familia de virus hace referencia a este nombre, la definición real del término es la caída o pérdida de una conexión del tipo TCP/IP (Internet Protocol), provocada por alguna persona (un hacker, por ejemplo).

Payload: este término se refiere a los efectos destructivos, nocivos o molestos que cualquier virus puede producir cuando ya ha tenido lugar su infección, además de los efectos secundarios de dicha infección (cambios en la configuración del sistema, reenvío de e-mail, ejecución del virus en el arranque del sistema o de Windows).

Plantilla (Plantilla Global): una plantilla global es un determinado archivo que una aplicación concreta utiliza para iniciar su sesión de trabajo con unos valores o parámetros establecidos por defecto. Por ejemplo, el procesador de textos Microsoft Word (que forma parte de Microsoft Office) tiene asociada una plantilla cuyo archivo se denomina NORMAL.DOT.

POP (Post Office Protocol): se trata de un protocolo para recibir u obtener los mensajes de correo electrónico.

RAM (Random Access Memory): es la memoria principal del computador, también conocida como memoria de acceso aleatorio. Todos los programas que se estén ejecutando en un determinado instante, estarán situados en ella. Por ejemplo, si ejecutamos un programa (o abrimos un documento) que está en una unidad de disco (disquete, disco duro), éste se colocará automáticamente en la memoria principal para ser ejecutado.

Redireccionar: esta acción permite aplicar un nuevo destino. En el caso de los virus, se puede hablar de éste término cuando un virus es capaz (por ejemplo) de hacer que el sistema en lugar de acceder a una dirección en la que debería encontrar determinados componentes, es obligado por el virus a saltar o acceder a otra dirección diferente.

Réplica: se define como réplica la acción por la cual los virus se propagan o hacen copias de sí mismos, con el único objetivo de realizar posteriores infecciones.

ROM (Read Only Memory): es un tipo de memoria que se caracteriza porque, desde un computador normal, no es posible guardar o escribir información en ella. Solamente es posible leer su contenido (Memoria de Sólo Lectura). Existen máquinas especiales para grabar contenido en las memorias ROM.

Script (Virus de Script): los virus de script están escritos en lenguajes de programación como Visual Basic Script (VBScript) y JavaScript. Estos virus utilizan el Scripting Host de Windows para activarse e infectar otros archivos. Los virus se activarán de modo automático al hacer doble clic en los archivos VBS y JS infectados. Estos virus suelen incluir en su nombre y/o alias, las letras que así lo indican: VBS o JS. Por ejemplo: VBS/LoveLetter.D.

Síntomas de Infección: son cada una de las acciones o efectos que el virus puede realizar cuando ha producido su infección y se reúnen las condiciones de activación (si éste cuenta con ellas).

SMTP (Simple Mail Transfer Protocol): es el protocolo que se utiliza en Internet para el envío (y sólo para el envío) de correo electrónico. Además también se puede utilizar para conectar servidores de correo que no son compatibles entre sí. Otros protocolos de correo electrónico como el POP serán los utilizados para la recepción de mensajes de correo.

Spam: éste es un conocido fenómeno que tiene como centro de actividad el correo electrónico. Aunque no se trata de ningún tipo de virus, tiene relación con ellos debido a la proliferación de aquellos que se envían por correo electrónico. En definitiva el spam consiste en el envío masivo de mensajes. También puede estar relacionado con los hoax o jokes, ya que éstos se centran en este medio. A diario es habitual recibir un gran número de correos electrónicos que no hemos solicitado, conteniendo publicidad, noticias, comentarios, cadenas de solidaridad que no deberíamos romper.. Este es el fenómeno conocido como spam.

Vacunación: mediante esta técnica, el programa antivirus almacena información sobre cada uno de los archivos. En caso de haberse detectado algún cambio entre la información guardada y la información actual del archivo, el antivirus avisa de lo ocurrido. Existen dos tipos de vacunaciones:

Interna. La información se guarda dentro del propio archivo, de tal forma que al ejecutarse él mismo comprueba si ha sufrido algún cambio.

Externa. La información que guarda en un archivo especial y desde él se contrasta la información.

Virus: los virus son programas que se pueden introducir en nuestros computadores de formas muy diversas. Este tipo de programas son especiales ya que pueden producir efectos no deseados y nocivos. Una vez el virus se ha introducido en el computador, se colocará en lugares donde el usuario pueda ejecutarlos de manera no intencionada.

Zip: existen varias herramientas que permiten comprimir archivos, para que el conjunto de todos ellos (o alguno de ellos individualmente) ocupen menos espacio. Los archivos comprimidos mediante la herramienta WinZip, tendrán extensión .ZIP, aunque existen otros formatos de compresión como ARJ, LZH, LHA, RAR.. Los archivos comprimidos (en cualquier formato) contendrán a otros archivos en su interior. Si alguno de éstos estuviese infectado, podrían producirse infecciones al descomprimir o trabajar con el archivo comprimido.