Virus informáticos

Los **virus informáticos** se propagan en las computadoras autocopiándose en los medios de almacenamiento de la informaciín y en la meoria RAM. Algunos entran al sistema con una imagen aparente, diferente a su cometido, y cuando menos te lo esperas, comienzan a reproducirce. Se llaman **Troyanos**, en recuerdo de la anécdota del **Caballo de Troya** de la mitología griega. Protege tu información haciendo lo siguiente:

- Realiza copias de seguridad de todos tus archivos de texto, hojas de cálculo, presentaciones, bases de datos, imágenes y música.
- Utiliza las **Herramientas de sistema** de Windows para hacer mantenimiento preventivo del sistema y de los discos de almacenamiento.
- Instala un antivirus y mantenlo actualizado diariamente a través de Internet para protejer tu información de ataques de virus y programas de **malware**.

Definición de virus

Los virus informáticos están escritos generalmente en lenguaje máquina, en ensamblador o en cualquier lenguaje de programación, y tienen algunas características especiales, de donde se puede partir a hacer una definición completa de ellos:

- Son muy pequeños, lo que los hace difíciles de detectar y eliminar.
- Se auto reproducen en la memoria de la computadora o en las unidades de almacenamiento de datos.
- Casi nunca incluyen en el código, ni nombre de autor, ni registro o copyright, ni fecha de creación.
- Al ejecutarse toman el control de la computadora y modifican otros programas.
- Ralentizan el funcionamiento de la computadora.
- Tienen la capacidad de "esconderse" para no ser descubiertos, mutando su forma, o utilizando técnicas llamadas "Stealth".
- Pueden solo causar molestias al usuario, u ocasionar graves daños a los datos almacenados en las unidades de la computadora.

Otra forma de infección se da cuando se deja una USB infectada en el área de carga. Al encender o reinicializar la computadora, en lugar de ejecutarse el programa de carga primero, el virus busca alojarse en la memoria RAM e infectar el área de carga o la tabla de particiones del disco duro.

Glosario

Virus informático. Es un programa que se ejecuta sin el consentimiento del usuario: al ser ejecutado altera el correcto funcionamiento del sistema; puede insertar copias de sí mismo en otros programas o áreas de los discos; destruye programas o datos en la memoria RAM, o en unidades de almacenamiento; marca los programas infectados para reconocer que ya han sido modificados, y se reproduce de manera infinita en la memoria y en los medios de almacenamiento.

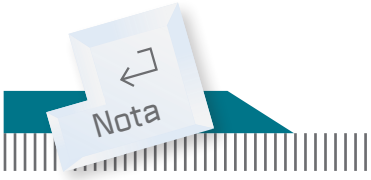
Cómo funcionan los virus informáticos

Como todos los programas, los virus informáticos necesitan que alguien los ejecute en la computadora para que realicen las tareas para las que fueron programados. De ninguna manera se pueden ejecutar solos. Al ejecutar un programa infectado, se cargan en la memoria RAM y permanecen ahí mientras se mantenga encendida la computadora. Algunos se cargan al ejecutar un programa infectado que llegó como archivo adjunto en un correo electrónico.

El virus puede actuar de inmediato, o esperar a que se den las condiciones o señales propicias que fueron programadas en su codificación. Al entrar en acción, el virus informático toma el control de la computadora desde el principio y a partir de ese momento, cualquier disco que se inserte, quedará infectado al realizar cualquier acceso de lectura o escritura. Busca infectar de inmediato alguna de las áreas críticas de los discos como el **área de carga**, la **tabla de particiones**, la **tabla de asignación de archivos**, el **directorio raíz**; o algún archivo ejecutable con extensión **.com**, **.exe**, **.dll**, .**bat**, **.ovr**, o cualquier otro.

Algunos comienzan su acción destructora de inmediato, otros esperan a que se den ciertas condiciones que se han incluido en su código, como una fecha y hora; la ejecución de alguna orden, o la realización de algún evento específico. Por último, los hay que en el momento de la infección, inician un contador que les indicará el momento de activarse. Otros virus conviven también como macros de documentos de Word, Excel, PowerPoint o correos electrónicos de Outlook.

Los que infectan el **área de carga**, se posicionan en la memoria de la computadora desde el momento de encenderla, porque al iniciar, en lugar de leer el programa de carga, se lee primero el código del virus. Para no alertar a la computadora con un mal funcionamiento, el virus manda leer el programa de carga, que se encuentra en otro sector, donde lo envió el propio virus. De esta manera, el virus ya está en la memoria, y el usuario ni se entera, porque aparentemente no hay problemas. Norton Editor versión 7.0 muestra el sector **0** de un disco duro "sano". Observa que el primer valor hexadecimal es **FA**.



Desde antes de 1990 el problema de los virus informáticos se extendía en el cada vez más creciente número de computadoras PC. Para contrarrestar a los virus se crea la *Computer Virus Industry Association*, CVIA, comandada entonces por **John McAfee**, en donde se detectan más de 500 programas virales, que ya habían infectado a unas 200 000 computadoras solo en Estados Unidos.

Algunos virus esperan una fecha y hora para comenzar a destruir la información que se guarda en las unidades de almacenamiento.

Cuando el virus **Michelangelo** infecta un disco duro la **tabla de particiones** o Master Boot Record (MBR) se desplaza a la dirección física: **Cilindro 0**, **Lado 0**, **Sector 7**, y el virus se aloja en el lugar del **MBR**. **Michelangelo** cabe en un sector, ya que su longitud es de solo **429** bytes (los sectores contienen un total de **512**). Si el programa de carga inicial no está alojado en el **área de carga inicial** (*Boot sector*), puede suponerse que un virus lo ha desplazado a otro sector, y ha tomado su lugar en el sector de arranque. El sector **0** del mismo disco cuando ha sido infectado por el virus **Michelangelo**. Mira cómo el primer valor hexadecimal cambió a **E9**

Nota

Los virus de las computadoras son programas como todos los que conoces. Así como hay programas para las diferentes plataformas de computadoras, también se crean virus para cada una de ellas.

Clasificación de los virus de computadoras

Existen muchas clasificaciones de los virus informáticos. Cada compañía fabricante de **antivirus** y cada investigador hacen una clasificación que desde su punto de vista, debe considerarse como la adecuada. Lo cierto es que los virus se pueden clasificar según diversos criterios.

De acuerdo con el área que infectan:

- **Infectores del área de carga inicial**: infectan a las unidades de almacenamiento, alojándose en el área de carga, que se encuentra en el sector 0. Cambian de lugar al programa de carga, enviándolo a otro sector del disco. Desde el encendido de la computadora toman el control del sistema.
- **Infectores de sistema**: infectan a los programas de sistema, que son de los primeros que se cargan en la memoria de la computadora, junto con el virus, obviamente.
- **Infectores de programas ejecutables**: insertan una copia de sí mismos en el código de los programas ejecutables, que tienen extensiones **.com**, **.exe**, **.dll** y otros. Son muy peligrosos porque realizan una búsqueda de archivos ejecutables para infectarlos a todos; cuando estos archivos se desinfectan con un programa antivirus, generalmente quedan inservibles, por lo que hay que instalar nuevamente los programas y hasta restaurar el sistema operativo.
- **Infectores de documentos**: infectan a los documentos de Word, Excel y PowerPoint, alojándose en el área de **macros**. Infectan a todos los archivos que tienen las extensiones de los documentos de Office.

De acuerdo con su forma de operación:

- **Caballos de Troya**: programas que se introducen al sistema mostrando una apariencia diferente a la de su objetivo final. Muchos investigadores no con-

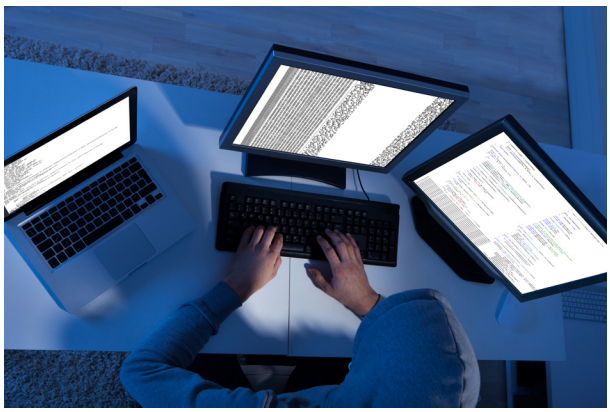
Glosario

Antivirus. Programa que protege y ayuda a eliminar los virus informáticos que se introducen en las computadoras, rastreando la memoria y las unidades de almacenamiento.

Macros. Macroinstrucciones. Pequeños programas de tipo "script", que realizan los usuarios de aplicaciones de oficina, para llevar a cabo tareas repetitivas relacionadas con procesadores de textos, hojas de cálculo y presentaciones.

sideran a los troyanos como virus, aunque la mayoría actúa como tales. Su nombre recuerda el episodio del Caballo de Troya, que permitió el rescate de Helena por las huestes de Menelao

- **Gusanos:** programas auto replicables, que se diseminan a través de las redes y en la memoria de las computadoras, sin la ayuda de un programa anfitrión ejecutable. Se arrastran literalmente por las áreas de la memoria borrando los datos de programas e información, produciendo fallas que parecieran ser del sistema.
- **Bombas de tiempo:** son programas ocultos en la memoria del sistema, en algunas áreas de los discos o en programas ejecutables, que esperan una fecha y hora determinadas, para *explotar*, es decir, para comenzar con su actividad virulenta. Algunos no son destructivos, y solo exhiben mensajes en la pantalla en el momento de la explosión, otros son bastante perjudiciales.
- **Autorreplicables:** son los programas que realizan las funciones más parecidas a los virus biológicos, ya que se auto reproducen e infectan los programas ejecutables que encuentran en el disco. Se ejecutan en un determinado momento programado, cada determinado tiempo, al llegar un contador a su fin, o cuando "sienten" que se les trata de detectar.
- **Mutantes:** programas que se ocultan y engañan a los antivirus modificando su código mediante esquemas de **encriptación** o *codificación*. Utilizan técnicas llamadas **sigilosas** (*Stealth*) o invisibles, para escabullirse de la vista de los antivirus.
- **Macrovirus:** son macros de programas como Word, Excel o PowerPoint, que se reproducen en el sistema al abrir un documento infectado.
- **Virus de correo electrónico o Internet:** se introducen a las computadoras al acceder a páginas web que ofrecen archivos y programas gratuitos, o mediante el correo electrónico, como archivos adjuntos.
- **Secuestradores:** *hijackers*. Los nuevos programas de malware, actúan sobre las aplicaciones de redes e Internet, como los navegadores o los programas de mensajería instantánea, secuestrándolos literalmente. Cuando eso sucede, no puedes cambiar de página inicial, se presentan ventanas indeseables (Pop-ups) y se bloquean direcciones de páginas web de empresas de antivirus.



Nota

Los gusanos (*Worms*) se cargan en la memoria de la computadora y se posicionan en una determinada dirección, luego se copian en otro lugar y se borran del que ocupaban, y así sucesivamente, esto hace que se borren los programas o la información que se encuentren a su paso, causando problemas de operación o pérdida de datos.

Glosario

Encriptación. Codificación que se lleva a cabo en archivos, cambiando cadenas de caracteres por símbolos equivalentes, para evitar que sean entendidos por extraños. Para descifrarlos, generalmente se requiere de una contraseña.

- **Caza contraseñas:** *keyLoggers*. Programas que se introducen a las computadoras, residen en la memoria, y envían a sus creadores cada una de las pulsaciones que hace el usuario en el teclado. De esta manera, roban contraseñas y números de cuentas.
- **Espías:** *spyware*. Programas que recopilan información importante acerca de la identidad de los usuarios, y de las actividades que realizan en la computadora, para crear bases de datos y venderlas a empresas que utilizan estos datos para llenar los buzones con **correo electrónico "basura"** (**Spam**).
- **Esquemas de protección:** código que puede ser dañino, introducido en algunos programas comerciales, que detectan si se realizan copias del disco original. Al cabo de algún tiempo, cuando se han creado bastantes archivos importantes, modifica su estructura y no permite que la computadora siga funcionando correctamente, lo que obliga al usuario a comprar el programa original para recuperarlos. Un ejemplo claro de este tipo de virus es el **Pakistán**, como verás más adelante.

Glosario

Spam. Mensajes de correo electrónico de tipo publicitario no solicitados, enviados en forma masiva a los usuarios registrados en diversos servidores de correo.

Historia de los virus de computadoras

En 1949, **John von Neumann** (1903-1957), padre de la computación, describió algunos programas que se reproducen a sí mismos en su ponencia **Teoría de Autómatas Auto reproductivos** (*Theory and Organization of Complicated Automata*). Esto, aunque no se enfocaba a la creación de programas que se diseminan sin permiso de los usuarios de computadoras, si no es el comienzo de los virus, sí es el primer indicio de código autorreproductor.

En la década de 1960, estudiantes de computación en el *Instituto Tecnológico de Massachusetts*, se reunían por las noches para elaborar **código sofisticado** de programas como **Guerra en el espacio** (*Space War*). Jugaban entre ellos bombardeando al programa contrincante. No eran propiamente virus, sino bombas que actuaban explotando al momento.

En 1972, varios científicos estadounidenses de los laboratorios de computación de la AT&T (*Bell Laboratories*): **H. Douglas Mellory**, **Robert Thomas Morris Sr.**, **Victor Vysottsky** y **Ken Thompson**, *ingeniero en sistemas*, creador de la primera versión del sistema **Unix**, para entretenerse inventaron el juego **Guerra nuclear** (*CoreWar*), inspirados en un programa escrito en lenguaje ensamblador llamado **Creeper**, el cual tenía la capacidad de reproducirse cada vez que se ejecutaba.

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

En 1983, el **Dr. Fred Cohen** presentó en la Universidad del Sur de California el primer **virus residente en una** PC, por lo que hoy se le conoce como el *Padre de los Virus Informáticos*. **Cohen** demostró que el código de programas para computadora podía autoreplicarse, introducirse a otros códigos y alterar el funcionamiento de las computadoras.

En 1986, es cuando ya se difunde ampliamente un *virus* con la finalidad de causar destrozos en la información de los usuarios. Este ataca una gran cantidad de computadoras en todo el mundo. Fue desarrollado en Lahore, Pakistán, por dos hermanos que comercializaban computadoras y software. Uno de ellos escribió un programa administrativo de gran utilidad, que vendían muy poco, porque todos lo copiaban y se lo distribuían entre sí.

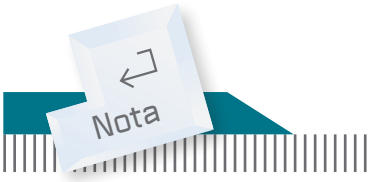
Cansados de sufrir por la **piratería**, decidieron vender copias *ilegales* de programas populares como Lotus 1-2-3, y en estos, así como en su propio programa, introdujeron un **virus benigno** con código muy elegante, el cual permitió que otros programadores lo modificaran para hacer de él, en sus nuevas versiones, uno de los virus más dañinos, conocido como virus **Brain** o **Paquistaní**, que se supone que infectó más de 30,000 computadoras solamente en Estados Unidos.

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

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

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

El 2 de noviembre del mismo año 1988, las redes ARPANET y *NSFnet* en Estados Unidos, fueron infectadas por un virus gusano que se introdujo en ellas, afectando a más de 6,000 equipos de instalaciones militares de la NASA, universidades y centros de investigación públicos y privados. También, el gusano invadió la naciente red Internet.



John von Neumann, matemático húngaro nacionalizado estadounidense, fue discípulo de **Albert Einstein** y pionero de la computación digital.

El gusano fue creado por **Robert Morris Jr.**, estudiante de Harvard de 23 años, e hijo de uno de los creadores de COREWAR. Después de un juicio, en el cual alegaba inocencia, porque no lo hizo intencionalmente, fue condenado a tres años de libertad condicional, una multa de $10,000 dólares y 400 horas de trabajo social.

Los principales virus informáticos

Diariamente se descubren nuevos tipos de virus con códigos y funcionamientos diferentes: objetos que se mueven por la pantalla, pantallas que se voltean de cabeza, cambio de los colores de las pantallas, sonidos extraños, etcétera. Esto se debe en gran parte a la facilidad de programación en el ambiente de Windows, y a su popularidad. Desde los primeros virus, los más conocidos son:

AIDS

También conocido como HAHAHA, TAUNT, SIDA O VGA2CGA, es un virus infector de archivos ejecutables. Al activarse presenta un mensaje en la pantalla: "*Your computer now has AIDS*".

El virus infecta los archivos ejecutables posicionándose en los primeros 13 kB, por lo que al eliminarlo con cualquier antivirus, los programas quedan inservibles.

AirCop

Virus residente en memoria descubierto en Estados Unidos en el año de 1990, de origen Taiwanés, infectaba el sector de arranque de los disquetes. Es un virus muy dañino, ya que destruía los datos del sector 719, que es a donde enviaba el programa de carga original. Bloqueaba y utilizaba las interrupciones 12h, 13h y 1Bh para controlar la computadora. Desplegaba el mensaje "*Red State, Germ Offensive. AIRCOP*".

Ambulance Car

Virus de archivos ejecutables que al ejecutarse presentaba una imagen de una ambulancia que barre la parte inferior de la pantalla de izquierda a derecha, mientras se escuchaba el sonido característico de una sirena.

Boot Sector

Es un virus originario de la ex Alemania Occidental que atacaba a las computadoras Atari modelo **ST**, alojándose en el sector de carga de los discos. Cuando se realizaba la carga inicial del sistema con el disco infectado, el virus se activa en la memoria de la computadora agregándose al vector de llamadas del sistema, que es el que controla todos los accesos al disco.

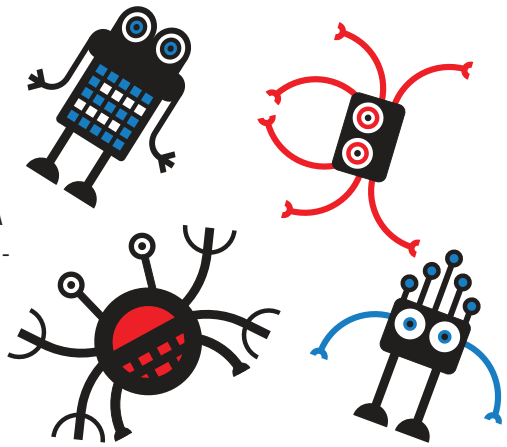
Brain o de Pakistán

Infector del *sector de arranque*, que ha sufrido una serie de mutaciones, adiciones, modificaciones. Conocido también como Paquistaní, Nipper, Mente Paquistaní, Clone, Brain Ashar y Brain Singapore, es el mismo que desarrollaron los hermanos que vendían productos de computación en Lahore, Pakistán.

Cascade (Virus de cascada)

Se le conoce también como Falling Tears, Autumn Leaves, Black- Jack, Fall, Falling Letters, 1704 y Cascade-1706. Originado a finales de 1987, es producto de un Caballo de Troya modificado y producía la caída del texto a la parte inferior de la pantalla.

Virus de la galletita (Cookie)



Se cuenta de un virus gastronómico que contagió las computadoras DECsystem 10. Este pequeño personaje permanecía latente por tiempo indefinido, y cuando se activaba presentaba en la pantalla el mensaje **I WANT A COOKIE!** (¡QUIERO UNA GALLETITA!). Al teclear la palabra *COOKIE*, se lograba desactivarlo durante algún tiempo. La versión *Cookie 2232*, incluso al recibir la palabra *COOKIE*, desplegaba en la pantalla el mensaje *BURPS*...

Dark Avenger

Virus originario de Bulgaria, conocido además como Eddie, Diana, VAN Soft, Black Avenger, Rabid Avenger, Evil Men y otros, fue descubierto en septiembre de 1989. Este virus infecta los archivos ejecutables. Cada decimosexta infección enviaba parte de su código a escribir en sectores seleccionados aleatoriamente, destruyendo los datos ahí contenidos.

Casino

Afortunadamente no fue un virus muy común, ya que el concepto destructivo azaroso, se prestaba para que algunos usuarios aventureros se jugaran la integridad de sus datos. El propósito de este virus era borrar la tabla de asignación de archivos del disco duro. Al activarse, hacía una copia de la FAT en la memoria RAM y borraba los datos del disco. Enseguida presentaba una pantalla con un juego de azar. Se contaba con cinco oportunidades para lograr que las tres maquinitas giratorias cayeran en **???** Sí caían tres signos **£££**, el virus cumplía su cometido; si tenías la suerte de ganarle al virus, se despliega en la pantalla un mensaje ofensivo.

Los virus más recientes distribuidos por Internet

W32.Mydoom.AI@mm

Descubierto el 16 de enero de 2005, este gusano que se distribuye de manera masiva por correo electrónico, utiliza su propio protocolo SMTP para enviarse a lodos los contactos almacenados en la computadora. Al infectar crea los archivos **lsasrv.exe**, **version.ini** y **hserv.sys**, donde almacena una copia de sí mismo, un texto y un archivo binario. Intenta desactivar los procesos de seguridad que se ejecutan en computadoras con elementos de seguridad como firewalls y antivirus.

VBS.Rowam.A

Pequeñísimo troyano de solo 2,749 bytes, que cuando infecta trata de borrar archivos alojados en el disco duro. Puede enviar mensajes de correo electrónico a todos los recipientes de la libreta de direcciones, aunque esta no es su manera de propagación. Los mensajes enviados muestran el mensaje "Free MSN Upgrade" en el campo **Asunto**.

Nimda.L

Virus infector de archivos ejecutables de origen chino, que se distribuye en la red Internet al acceder a páginas web infectadas, o a redes con recursos compartidos. Esta variante se detectó el 16 de junio de 2003, y se activa al ejecutarse los archivos **_setup.exe** y **riched20.dll**, que infectan a todos los archivos ejecutables a su paso.

W32/Bugbear.B

Esta variante del destructivo gusano Bugbear se distribuye en Internet, en los mensajes de correo electrónico. Los archivos anexos que contiene se muestran con dos extensiones que pueden ser **.scr**, **.pif**, o **.exe**. Deshabilita los antivirus y burla a los firewalls para infectar archivos de sistema. Facilita a los hackers tomar el control de un sitio, desde un lugar remoto.

Code Red (Código Rojo)

Se trata de un gusano que se auto copia de máquina en máquina a través de las redes. Se considera que este virus ha sido uno de los más destructivos de los últimos tiempos, ya que reprodujo más de 250,000 copias de sí mismo en un solo día.

I-Worm.Sircam.c

Este gusano de Internet cuyo origen se atribuye a México se ha escrito en Delphi y tiene cerca de 130K. Se distribuye mediante el correo electrónico y se reproduce a una gran velocidad, de tal manera, que en un solo día infectó a miles de usuarios de Internet, quienes vivieron una pesadilla al perder sus archivos y programas.

Net-Worm.Win32.Kido

Descubierto en enero de 2009, es un virus de riesgo moderado que tiene múltiples variantes de **Kido**. Este es un virus polimórfico que se está propagando ampliamente mediante redes locales y medios de almacenamiento extraíbles. Desactiva el modo de restauración del sistema operativo, bloquea accesos a sitios web de seguridad informática, y descarga malware adicional en los equipos infectados.

Email-Worm.Win32.Warezov.nf

El 19 de enero de 2009 apareció en Internet la nueva modificación del gusano **Warezov**, que se considera de riesgo moderado a alto. La forma de infectar es parecida al **Email- Worm.Win32.Warezov.mx**.

Zhelatin.o

En febrero de 2009 se detectó envío masivo de este virus por Internet, como archivo adjunto de mensajes de correo infectados. En el campo Asunto presenta mensajes como: I Always Knew; I Believe; I Love You Soo Much; I Love You with All I Am; I Still Love You, etcétera.

AutoRun.MXS

Troyano de bajo peligro, que llegar al sistema como archivo adjunto de correo enviado de forma masiva. Vigila las actividades del usuario en Internet Explorer e intenta descargar otros códigos maliciosos. Es posible eliminarlo con la función de restauración del sistema de Windows Me, Windows XP y Windows Vista.

Win32/Lafee.B

Se le conoce también con los nombres Win32/Lafee.B, Virus.Win32.Daum.a, Virus.Win32.Daum.a y Mal/Generic-A. Es un virus infector de archivos ejecutables con extensiones **.exe** y **.scr,** y descarga de Internet otros tipos de **malware**.

Como puedes ver, muchos de los virus antiguos infectaban, y procedían de disquetes infectados y copias piratas de programas de juegos y utilitarios. En cambio, los nuevos virus generalmente se distribuyen a través de las redes y mediante el correo electrónico, como archivos adjuntos.

Protección y Antivirus

La manera más común de adquirir un virus informático siempre fue a través de copias ilegales de programas. Por esta razón, por sentido común y por norma ética, como primer consejo: no debes copiar los programas originales para distribuirlos ilegalmente entre tus amigos; ¡y mucho menos para venderlos!

10 medidas de seguridad

- **No** utilices copias ilegales o piratas de los programas.
- **No** olvides crear respaldos o copias de seguridad de toda la información generada, diaria y semanalmente.
- **No** olvides memorias USB en las unidades lectoras. Si la USB está infectada, fácilmente se puede contagiar la computadora.
- **Protege** contra escritura las USB que tengas que introducir a una computadora extraña.
- **No** permitas que personas desconocidas introduzcan unidades USB o discos compactos de dudosa procedencia en tu computadora.
- **Protege** los accesos a la red con contraseñas (*passwords*).
- **Configura** correctamente las opciones de **Correo electrónico no deseado de Outlook.**
- **No** abras todos los correos electrónicos que te llegan, sobre todo cuando desconozcas quién te los envía, o su procedencia.
- **No** "bajes" archivos de sitios web desconocidos, sobre todo, no los ejecutes en tu computadora si no los revisas antes con un antivirus actualizado.
- **¡Instala un programa antivirus, y mantenlo siempre actualizado!**

Programas antivirus

A partir de la proliferación de los virus informáticos, se ha desarrollado también una industria dedicada a la creación de programas llamados vacunas o antivirus, que tienen como finalidad detectarlos, erradicarlos y prevenir las infecciones virales.

Los programas antivirus actuales han tenido que evolucionar, ahora ofrecen esquemas completos de seguridad que incluyen desde aplicaciones para crear copias de seguridad, hasta programas que realizan análisis de virus y software espía, protección integral tipo *firewall*, revisión de mensajes de correo electrónico y por supuesto, la función de actualización de las vacunas, que es de lo más importante.

Las siguientes direcciones de Internet son de compañías confiables, dedicadas al desarrollo de antivirus. Algunas de las empresas ofrecen versiones de evaluación o gratuitas.

También las hay que permiten revisar en línea el disco duro de tu computadora, de manera gratuita, para desinfectar el disco si contiene algún virus conocido, o amenazas de *malware.*

onecare.live.com/standard/es-us

Windows Live OneCare es un nuevo programa de protección desarrollado por Microsoft, expresamente para equipos con sistema operativo Windows Vista. Permite administrar redes domésticas, proteger el sistema contra *virus informáticos*, *Spyware*, *piratas informáticos* e *intrusos*.

En la página web puedes conseguir una versión de evaluación por 90 días, de manera gratuita. El paquete protege hasta 3 equipos. Como la mayoría de sitios antivirus, incluye una sección donde se muestran las principales amenazas del momento, que obviamente ya se incluyen en su esquema de protección.

www.symantec.com/es/mx/index.jsp

Norton Antivirus siempre ha sido uno de los mejores programas de protección de computadoras, ya que el **Dr. Peter Norton** se especializó en el trabajo interno de las computadoras, especialmente en el disco duro, con su Norton Utilities, que también ha sido una de las mejores aplicaciones de utilidades, edición y reparación lógica de discos duros.

Desde su instalación, el programa hace una revisión del sistema y descarga de Internet las actualizaciones para localizar virus y amenazas desde el principio. Además pregunta si quieres suscribirte al servicio **Norton Community Watch**, que te protege mientras estás en línea.

Cuando el antivirus detecta un virus, detiene su acción y lo elimina; siempre y cuando se hayan configurado las acciones de esa manera. Si se activó la opción en donde el usuario decide las acciones a seguir, pregunta si se elimina o lo pone en cuarentena. De cualquier manera, no deja actuar al virus o a la amenaza detectada.

Si el virus se encuentra en un disquete protegido contra escritura o en un CD-ROM, no lo puede eliminar, pero no dejará que el virus contagie el disco duro. El antivirus reconoce el virus y despliega su nombre en una ventana, Al pulsar en el nombre del virus, se abre una página de la compañía con todos los datos del virus encontrado, como se muestra en la figura.

Cuando el antivirus, detiene su acción y lo elimina; siempre y cuando se hayan configurado sus acciones de esa manera. Si se activó la opción en donde el usuario decide las acciones a tomar, pregunta si se elimina o pone en cuarentena. De cualquier manera, no deja actuar al virus o a la amenaza detectada

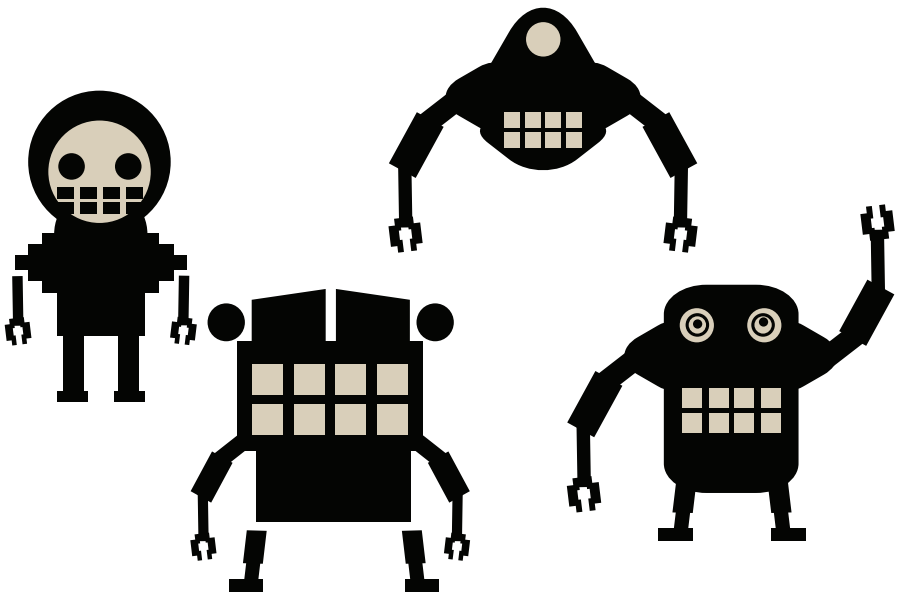
Nota

Para que un programa antivirus tenga buenos resultados en la lucha contra los virus, no basta instalarlo y olvidarse de él. ¡Debes mantenerlo actualizado! Afortunadamente, casi todos ofrecen el servicio de actualización mediante Internet, de manera automática, por lo que una vez configurado de esta manera, entonces sí, tú has tus trabajos escolares y que el antivirus te proteja.

Otro de los antivirus más antiguos y confiables es **McAfee**.

www.mcafee.com/mx/

Este antivirus estuvo bajo la dirección de **John McAfee**, quien fue también director de la *Computer Virus Industry Association*, una asociación de empresas dedicadas a la detección y eliminación de virus informáticos desde el siglo pasado, que luchaba contra los **hackers** y los **crackers**.



latam.kaspersky.com/

Otro pionero de la lucha contra los virus informáticos es **Eugene Kaspersky**, programador ruso, que se interesó por los virus informáticos desde muy joven. En la actualidad es el dueño de su propia empresa; *Kaspersky Antivirus*, con más de 900 empleados en varios países.

Otras empresas de programas antivirus son:

www.f-secure.com/
www.norman.com/es
www.pandasecurity.com/mexico/
la.trendmicro.com/la/home/

Glosario

Hackers. Expertos en computación que ingresan a sitios conectados a las redes, con la finalidad de demostrar su superioridad tecnológica; es decir, superar el reto de "romper" la seguridad de los sitios web.

Crackers. Expertos en computación que disfrutan destrozando y robando la información de sitios y páginas web conectadas a Internet.