LOS VIRUS & ANTIVIRUS

¿Qué son los virus informáticos?

Los Virus Informáticos son sencillamente programas maliciosos (malware**)** que "infectan" a otros archivos del sistema con la intención de modificarlo o dañarlo. Dicha infección consiste en incrustar su código malicioso en el interior del archivo "víctima" (normalmente un ejecutable) de forma que a partir de ese momento dicho ejecutable pasa a ser portador del virus y por tanto, una nueva fuente de infección.

Su nombre lo adoptan de la similitud que tienen con los virus biológicos que afectan a los humanos, donde los antibióticos en este caso serían los programas **Antivirus.**

Los **virus informáticos** tienen, básicamente, la función de propagarse a través de un software, no se replican a sí mismos porque no tienen esa facultad como los del tipo **Gusano informático** (Worm), son muy nocivos y algunos contienen además una carga dañina (payload) con distintos objetivos, desde una simple broma hasta realizar daños importantes en los sistemas, o bloquear las redes informáticas generando tráfico inútil.

Origen de los Virus

En 1949, el famoso científico matemático John Louis Von Neumann, de origen húngaro, escribió un artículo, publicado en una revista científica de New York, exponiendo su "Teoría y organización de autómatas complejos", donde demostraba la posibilidad de desarrollar pequeños programas que pudiesen tomar el control de otros, de similar estructura.

En 1959, en los laboratorios de la Bell Computer, subsidiaria de la AT&T, 3 jóvenes programadores: Robert Thomas Morris, Douglas McIlory y Victor Vysottsky, a manera de entretenimiento crearon un juego al que denominaron CoreWar, inspirados en la teoría de John Von Neumann, escrita y publicada en 1949.

Robert Thomas Morris fue el padre de Robert Tappan Morris, quien en 1988 introdujo un virus en ArpaNet, la precursora de Internet.

Puesto en la práctica, los contendores del CoreWar ejecutaban programas que iban paulatinamente disminuyendo la memoria del computador y el ganador era el que finalmente conseguía eliminarlos totalmente. Este juego fue motivo de concursos en importantes centros de investigación como el de la Xerox en California y el Massachussets Technology Institute (MIT), entre otros.

Sin embargo durante muchos años el CoreWar fue mantenido en el anonimato, debido a que por aquellos años la computación era manejada por una pequeña élite de intelectuales.

A pesar de muchos años de clandestinidad, existen reportes acerca del virus Creeper, creado en 1972 por Robert Thomas Morris, que atacaba a las IBM 360, emitiendo periódicamente en la pantalla el mensaje: "I'm a creeper... catch me if you can!" (soy una enredadera, agárrenme si pueden). Para eliminar este problema se creó el primer programa antivirus denominado Reaper (segadora), ya que por aquella época se desconocía el concepto de los software antivirus.

En 1980 la red ArpaNet del ministerio de Defensa de los Estados Unidos de América, precursora de Internet, emitió extraños mensajes que aparecían y desaparecían en forma aleatoria, asimismo algunos códigos ejecutables de los programas usados sufrían una mutación. Los altamente calificados técnicos del Pentágono se demoraron 3 largos días en desarrollar el programa antivirus correspondiente. Hoy día los desarrolladores de antivirus resuelven un problema de virus en contados minutos.

En Agosto de 1981 la International Business Machine lanza al mercado su primera computadora personal, simplemente llamada IBM PC. Un año antes, la IBM habían buscado infructuosamente a Gary Kildall, de la Digital Research, para adquirirle los derechos de su sistema operativo CP/M, pero éste se hizo de rogar, viajando a Miami donde ignoraba las continuas llamadas de los ejecutivos del "gigante azul".

Es cuando oportunamente surge Bill Gates, de la Microsoft Corporation y adquiere a la Seattle Computer Products, un sistema operativo desarrollado por Tim Paterson, que realmente era un "clone" del CP/M. Gates le hizo algunos ligeros cambios y con el nombre de PC-DOS se lo vendió a la IBM. Sin embargo, Microsoft retuvo el derecho de explotar dicho sistema, bajo el nombre de MS-DOS.

El nombre del sistema operativo de Paterson era "Quick and Dirty DOS" (Rápido y Rústico Sistema Operativo de Disco) y tenía varios errores de programación (bugs).

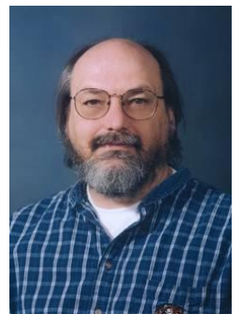
La enorme prisa con la cual se lanzó la IBM PC impidió que se le dotase de un buen sistema operativo y como resultado de esa imprevisión todas las versiones del llamado PC-DOS y posteriormente del MS-DOS fueron totalmente vulnerables a los virus, ya que fundamentalmente heredaron muchos de los conceptos de programación del antiguo sistema operativo CP/M, como por ejemplo el PSP (Program Segment Prefix), una rutina de apenas 256 bytes, que es ejecutada previamente a la ejecución de cualquier programa con extensión EXE o COM.

El creador del primer **software malintencionado** tenía sólo 15 años, en 1982, cuando decidió autocopiar los disquetes de sus amigos en su ordenador Apple II sin la autorización de éstos. El joven, que ya era conocido por alterar el funcionamiento de diversos programas insertando pequeños poemas en ellos, consiguió hacerlo, esta vez, sin tocar directamente el ordenador de sus víctimas.

El resultado de este primer **programa dañino** fue, pues, la visualización de este pequeño poema cada 50 veces que se encendía el PC:

Elk Cloner: The program with a personality
It will get on all your disks
It will infiltrate your chips
Yes it's Cloner!

1983 Keneth Thompson, quien en 1969 creó

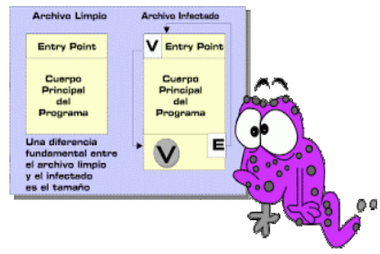


el sistema operativo UNIX, resucitó las teorías de Von Neumann y la de los tres programadores de la Bell y en 1983 siendo protagonista de una ceremonia pública presentó y demostró la forma de desarrollar un virus informático.

1984 Fred Cohen al año siguiente, el Dr. Fred Cohen al ser homenajeado en una graduación, en su discurso de agrade-cimiento incluyó las pautas para el desarrollo de un virus. Este y otros hechos posteriores lo convirtieron en el primer autor oficial de los virus, aunque hubo varios autores más que actuaron en el anonimato.

El Dr. Cohen ese mismo año escribió su libro "Virus informáticos: teoría y experimentos", donde además de definirlos los califica como un grave problema relacionado con la Seguridad Nacional. Posteriormente este investigador escribió "El evangelio según Fred" (The Gospel according to Fred), desarrolló varias especies virales y experimentó con ellas en un computador VAX 11/750 de la Universidad de California del Sur.

La verdadera voz de alarma se dio en 1984 cuando los usuarios del BIX BBS de la revista BYTE reportaron la presencia y difusión de algunos programas que actuaban como "caballos de troya", logrando infectar a otros programas. Al año siguiente los mensajes y quejas se incrementaron y fue en 1986 que se

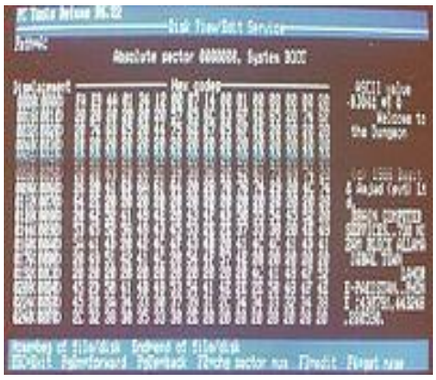


reportaron los primeros virus conocidos que ocasionaron serios daños en las IBM PC y sus clones.

1986 El comienzo de la gran epidemia ese año se difundieron los virus (c) Brain, Bouncing Ball y Marihuana y que fueron las primeras especies representativas de difusión masiva. Estas 3 especies virales tan sólo infectaban el sector de arranque de los disquetes. Posteriormente aparecieron los virus que infectaban los archivos con extensión EXE y COM.

También en 1986, un programador llamado Ralf Burger se dio cuenta de que un archivo podía ser creado para copiarse a sí mismo, adosando una copia de él a otros archivos. Escribió una demostración de este efecto a la que llamó VIRDEM, que podía infectar cualquier archivo con extensión **.COM**.

Esto atrajo tanto interés que se le pidió que escribiera un libro, pero, puesto que él desconocía lo que estaba ocurriendo en Paquistán, no mencionó a los virus de sector de arranque (boot sector). Para ese entonces, ya se había empezado a diseminar el virus Vienna.



Uno de los primeros registros que se tienen de una infección data del año 1987, cuando en la Universidad estadounidense de Delaware notó que tenían un virus porque comenzaron a ver "Brain" como etiqueta de los disquetes.

La causa de ello era **Brain Computer Services,** una casa de computación paquistaní que, desde 1986, vendía copias ilegales de software comercial infectadas para, según los responsables de la firma, dar una lección a los piratas. Ellos habían notado que el sector de boteo de un disquete contenía código ejecutable, y que dicho código se ejecutaba cada vez que la máquina se inicializaba desde un disquete.

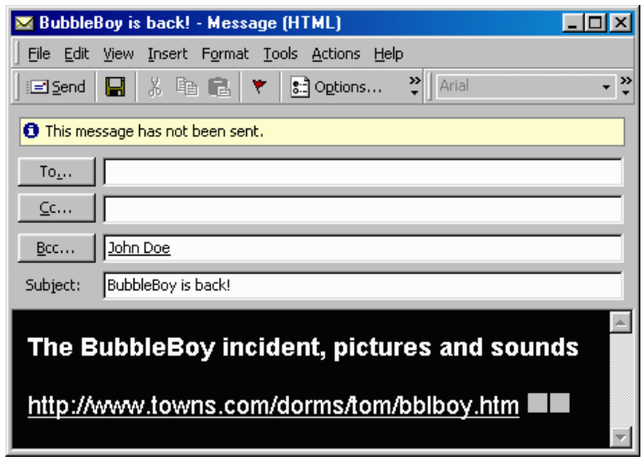
Lograron reemplazar ese código por su propio programa, residente, y que este instalara una réplica de sí mismo en cada disquete que fuera utilizado de ahí en más.

El 2 de Noviembre de 1988 Robert Tappan Morris, hijo de uno de los precursores de los virus y recién graduado en Computer Science en la Universidad de Cornell, difundió un virus a través de ArpaNet, (precursora de Internet) logrando infectar 6,000 servidores conectados a la red.

A mediados de 1995 se reportaron en diversas ciudades del mundo la aparición de una nueva familia de virus que no solamente infectaban documentos, sino que a su vez, sin ser archivos ejecutables podían auto-copiarse infectando a otros documentos. Los llamados macro virus tan sólo infectaban a los archivos de MS-Word, posteriormente apareció una especie que atacaba al Ami Pro, ambos procesadores de textos. En 1997 se disemina a través de Internet el primer macro virus que infecta hojas de cálculo de MS-Excel, denominado Laroux, y en 1998 surge otra especie de esta misma familia de virus que ataca a los archivos de bases de datos de MS-Access

A principios de 1999 se empezaron a propagar masivamente en Internet los virus anexados (adjuntos) a mensajes de correo, como el Melisa o el macro virus Papa. Ese mismo año fue difundido a través de Internet el peligroso CIH y el ExploreZip, entre otros muchos más.

Ejemplo de un mensaje de correo electónico (recibido y abierto con el programa de correo, Microsoft Outlook 97, de la empresa Microsoft), correspondiente al virus VBS /Tqll.A.



A fines de Noviembre de 1999 apareció el BubbleBoy, primer virus que infectaba los sistemas con tan sólo leer el mensaje de correo, el mismo que se muestra en formato HTML. En Junio del 2000 se reportó el VBS/Stages.SHS, primer virus oculto dentro del shell de la extensión .SHS. 2002 surge el primer virus diseñado para atacar archivos Shockwave Flash de Macromedia y aparece winux, primer virus para ejecutables tanto de Windows como de Linux.

Resultará imposible impedir que se sigan desarrollando virus en todo el mundo, por ser esencialmente una expresión cultural de "graffiti cibernético", así como los crackers jamás se detendrán en su intento de "romper" los sistemas de seguridad de las redes e irrumpir en ellas con diversas intencionalidades.

Actualmente, los virus son producidos en cantidades extraordinarias por muchísima gente alrededor del planeta. Algunos de ellos dicen hacerlo por divertimento, otros quizás para probar sus habilidades. De cualquier manera, hasta se ha llegado a notar un cierto grado de competitividad entre los autores de estos programas.

CARACTERISTICAS DE LOS VIRUS

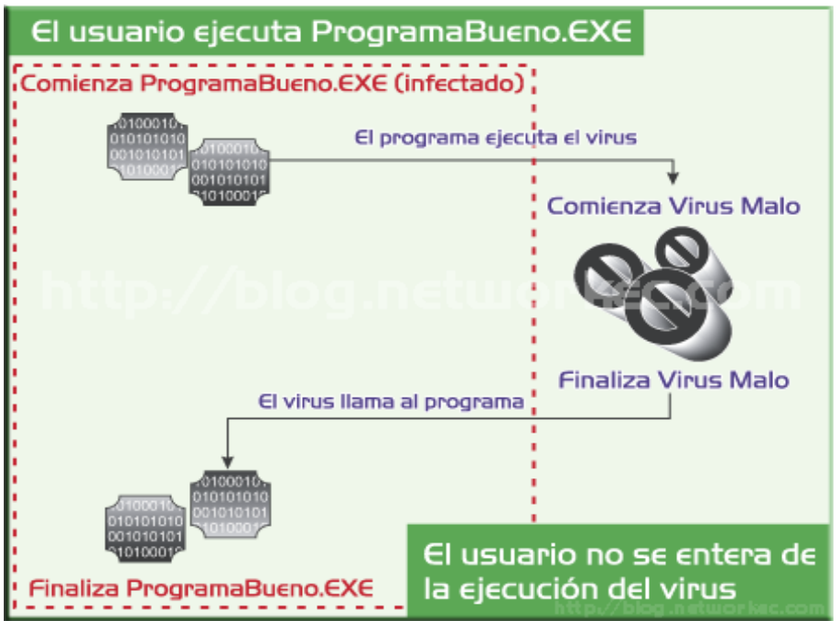
El virus es un pequeño software (cuanto más pequeño más fácil de esparcir y más difícil de detectar), que permanece inactivo hasta que un hecho externo hace que el programa sea ejecutado o el sector de "booteo" sea leído. De esa forma el programa del virus es activado y se carga en la memoria de la computadora, desde donde puede esperar un evento que dispare su sistema de destrucción o se replique a sí mismo.

Los más comunes son los residentes en la memoria que pueden replicarse fácilmente en los programas del sector de "booteo", menos comunes son los no-residentes que no permanecen en la memoria después que el programa-huésped es cerrado.

Los virus se transportan a través de programas tomados de BBS (Bulletin Boards) o copias de software no original, infectadas a propósito o accidentalmente. También cualquier archivo que contenga "ejecutables" o "macros" puede ser portador de un virus: downloads de programas de lugares inseguros; e-mail con "attachments", archivos de MS-Word y MS-Excel con macros. Inclusive ya existen virus que se distribuyen con MS-Power Point. Los archivos de datos, texto o Html **NO PUEDEN** contener virus, aunque pueden ser dañados por estos.

Los virus de sectores de "booteo" se instalan en esos sectores y desde allí van saltando a los sectores equivalentes de cada uno de los drivers de la PC. Pueden dañar el sector o sobrescribirlo. Lamentablemente obligan al formateo del disco del drive infectado. Incluyendo discos de 3.5" y todos los tipos de Zip de Iomega, Sony y 3M. (No crean vamos a caer en el chiste fácil de decir que el más extendido de los virus de este tipo se llama MS

CÓMO FUNCIONA UN VIRUS



Cuando un virus lleva a cabo la acción para la que había sido creado, se dice que se ejecuta la carga, pueden ser bastante maliciosos e intentan producir un daño irreparable al ordenador personal destrozando archivos, desplazando/sobrescribiendo el sector de arranque principal, borrando los contenidos del disco duro o incluso escribiendo sobre la BIOS, dejando inutilizable el equipo. La mayoría de los virus no borran todos los archivos del disco duro. La razón de esto es que una vez que el disco duro se borra, se eliminará el virus, terminando así el problema.

✔ Se ejecuta un programa que está infectado, en la mayoría de las ocasiones, por desconocimiento del usuario.

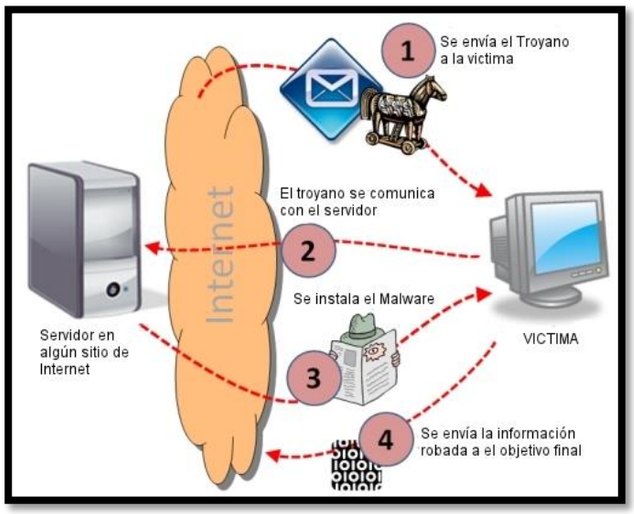
✔ El código del virus queda residente (alojado) en la memoria RAM de la computadora, aun cuando el programa que lo contenía haya terminado de ejecutarse.

✔ El virus toma entonces el control de los servicios básicos del sistema operativo, infectando, de manera posterior, archivos ejecutables (.exe., .com, .scr, etc) que sean llamados para su ejecución.

✔ Finalmente se añade el código del virus al programa infectado y se graba en el disco, con lo cual el proceso de replicado se completa.

.

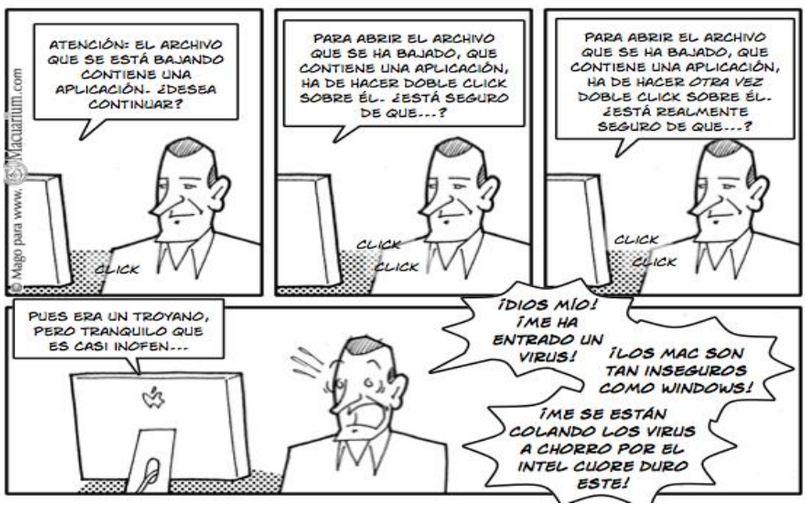
CÓMO SE TRANSMITEN LOS VIRUS



La forma más común en que se transmiten los virus es por transferencia de archivos, descarga o ejecución de archivos adjuntos a correos. Tambien usted puede encontrarse con un virus simplemente visitando ciertos tipos de páginas web que utilizan un componente llamado ActiveX o Java Applet. Además, usted puede ser infectado por un virus simplemente leyendo un e-mail dentro de ciertos tipos de programas de e-mail como Outlook o Outlook Express.

Para propagar sus creaciones y lograr sus fines, quienes se dedican a fabricar Virus frecuentemente apelan a inclinaciones emocionales profundas de sus posibles víctimas como: el miedo, la curiosidad, el deseo, el sexo, la codicia, la compasión o incluso la bondad natural, para lograr sus fines.

Muchas veces advierten a su víctima mediante un correo electrónico en el que le comunican que tiene infectado el computador con un peligroso virus que borrará toda la información contenida en el disco duro. Muy amablemente ofrecen el software que solucionará el problema o una dirección de Internet desde la cual éste se puede descargar. Lo cierto es que cuando la víctima ejecuta esos programas, se activa el verdadero virus o queda desprotegido el computador para que ingresen los 'crackers' quienes lo puedan utilizar, sin ser descubiertos, para atacar sistemas de terceros.



En otros casos se aprovechan de la curiosidad e ignorancia de su víctima para lograr que ésta abra un mensaje de correo electrónico infectado, con argumentos como que al abrirlo podrá ver fotos de alguna actriz famosa desnuda o las últimas imágenes de alguna noticia de actualidad. Muchos de estos mensajes provienen de personas conocidas, que ya tienen infectado su computador; de esta forma se evita la desconfianza sobre la autenticidad del mensaje.

Por ejemplo, un gusano [2] llamado "Prestige" se propaga mediante un correo electrónico en cuyo asunto (subject) dice: "fotos INEDITAS del PRESTIGE en el fondo del Atlántico". Sin embargo, lo que realmente incluye el archivo adjunto no son fotos, sino un virus informático. El Virus "SirCam" es otro ejemplo que ha engañado miles de usuarios en todo el mundo. Viene en un archivo adjunto (attachement) a un mensaje de correo electrónico cuyo asunto (subject) dice: "Hola, ¿cómo estás?"; además, se puede leer en el cuerpo del mensaje: "Te mando este archivo para que me des tu punto de vista. Nos vemos pronto". Cuando el usuario abre el archivo para revisarlo y poder así dar una opinión, el virus infecta el computador y se reenvía automáticamente a quienes aparecen en la libreta de direcciones del usuario infectado. Por este motivo, el virus llega remitido regularmente por una persona conocida.

FASES DE INFECCION DE UN VIRUS

Primera Fase (Infección)
El virus pasa a la memoria del computador, tomando el control del mismo, después de intentar inicializar el sistema con un disco, o con el sector de arranque infectado o de ejecutar un archivo infectado.

Segunda Fase (Latencia)
Durante esta fase el virus, intenta replicarse infectando otros archivos del sistema cuando son ejecutados o atacando el sector de arranque del disco duro. Si

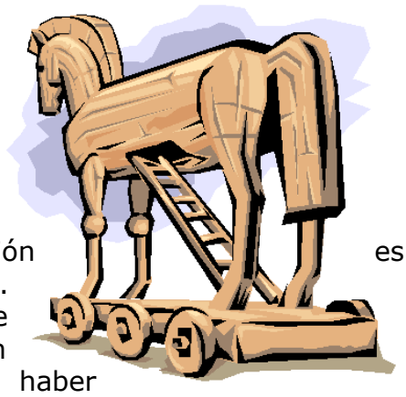
durante esta fase utilizamos discos flexibles no protegidos contra escritura, dichos discos quedan infectados y listos para pasar el virus a otro computador e infectar el sistema.
Tercera Fase (Activación) Esta es la última fase de la vida de un virus y es la fase en donde el virus se hace presente._La activación del virus trae como consecuencia el despliegue de todo su potencial destructivo.

La mayoría de los virus se activan mediante el reloj del sistema para comprobar la fecha y activar el virus.

Las principales vías de infección son:

- Redes Sociales.
- Sitios webs fraudulentos.
- Redes P2P (descargas con regalo)
- Dispositivos USB/CDs/DVDs infectados.
- Sitios webs legítimos pero infectados.
- Adjuntos en Correos no solicitados (Spam)

CLASES DE VIRUS



VIRUS POLIMORFICOS Ò MUTANTES Muy difíciles de detectar y eliminar, debido a que cada copia del virus es diferente de otras copias.
VIRUS ESTATICOS: Tipo de virus más antiguos y poco frecuentes. Su medio de propagación es a través de programas ejecutables.
VIRUS RESIDENTES: Virus que permanecen indefinidamente en memoria incluso después de haber finalizado el programa portador del virus.
VIRUS DESTRUCTIVOS: Microprogramas muy peligrosos para la integridad de nuestro sistema y nuestros datos. Su finalidad es destruir, corromper, eliminar, borrar, aniquilar datos del disco duro.
VIRUS BIPARTIDOS: Es un virus poco frecuente. Son virus incompletos, ejemplo, a veces a un virus le falta la parte de su código (el algoritmo destructivo), de este modo el virus es totalmente inofensivo. Pero puede haber otra versión del mismo virus que incorpore ese algoritmo. Si ambos virus coinciden en nuestro computador, y se unen en uno sólo, se convierten en un virus destructivo.
VIRUS COMPAÑEROS Son los virus más sencillos de hacer. Cuando en un mismo directorio existen dos programas ejecutables con el mismo nombre pero uno con extensión .COM y el otro con extensión .EXE,.
VIRUS DE BOOT (SECTOR DE ARRANQUE): Como su nombre lo indica, infecta el sector de arranque del disco duro. Dicha infección se produce cuando se intenta cargar el sistema operativo desde un disco infectado.
VIRUS AUTOREPLICABLES: Realizan funciones parecidas a los virus biológicos. Ya que se auto replican e infectan los programas ejecutables que se encuentren en el disco.
VIRUS INVISIBLES: Este tipo de virus intenta esconderse del Sistema Operativo mediante varias técnicas. Pueden modificar el tamaño del archivo infectado, para que no se note que se le ha añadido un virus.

PROGRAMAS MALIGNOS:

Son programas que deliberadamente borran archivos o software eliminándose así mismo cuando terminan de destruir la información. Entre los principales programas malignos tenemos:

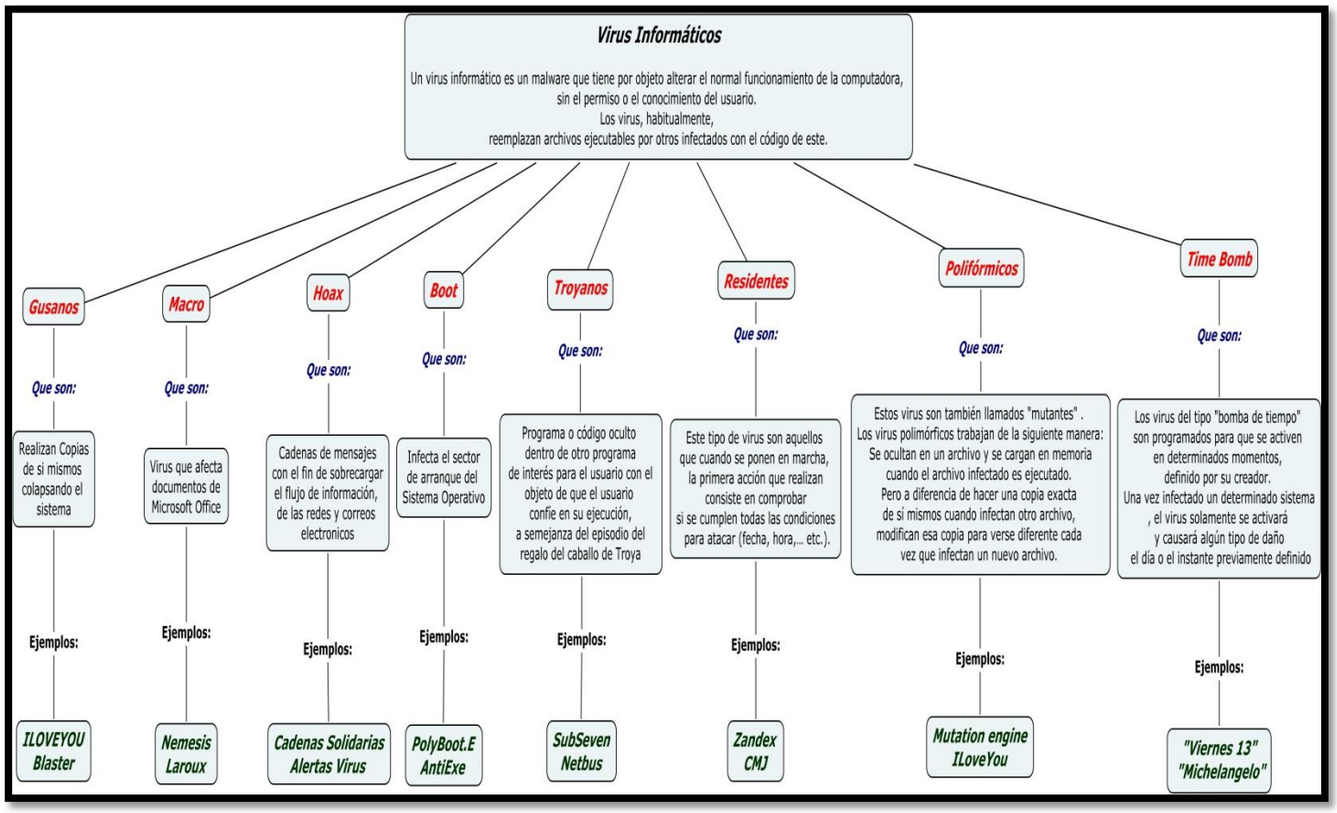
Troyano: que consiste en robar información o alterar el sistema del hardware o en un caso extremo permite que un usuario externo pueda controlar el equipo.

Gusano: tiene la propiedad de duplicarse a sí mismo. Los gusanos utilizan las partes automáticas de un sistema operativo que generalmente son invisibles al usuario.

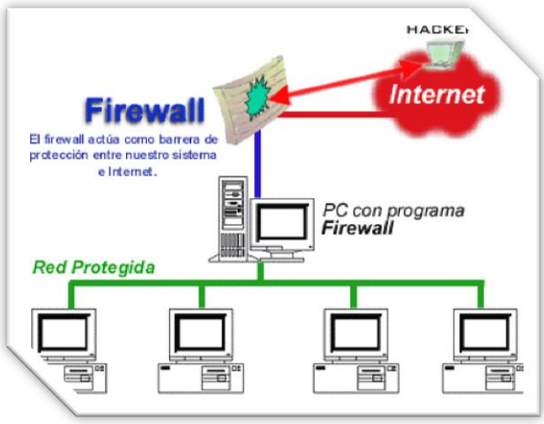
Bombas Lógicas o de Tiempo: son programas que se activan al producirse un acontecimiento determinado. La condición suele ser una fecha (Bombas de Tiempo), una combinación de teclas, o ciertas condiciones técnicas (Bombas Lógicas). Si no se produce la condición permanece oculto al usuario.

Hoax: Los hoax no son virus ni tienen capacidad de reproducirse por sí solos. Son mensajes de contenido falso que incitan al usuario a hacer copias y enviarla a sus contactos. Suelen apelar a los sentimientos morales ("Ayuda a un niño enfermo de cáncer") o al espíritu de solidaridad ("Aviso de un nuevo virus peligrosísimo")

y, en cualquier caso, tratan de aprovecharse de la falta de experiencia de los ínter nautas novatos.



CÓMO ELIMINAR UN VIRUS INFORMÁTICOS



La prevención consiste en un punto vital a la hora de proteger nuestros equipos ante la posible infección de algún tipo de virus y para esto hay tres puntos vitales que son:

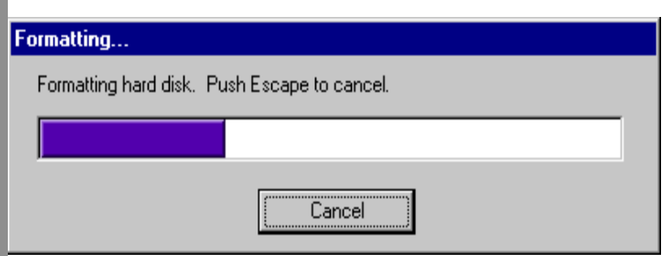
- **Un programa Antivirus.**
- **Un programa Cortafuegos.**
- **Un "poco" de sentido común.**

Para su información, seguidamente listamos una serie de normas básicas que le ayudarán a protegerse de los virus informáticos:

- Instale en su computador un software Antivirus confiable (ver lista de opciones en la siguiente sección).
- Actualice con frecuencia su software Antivirus (mínimo dos veces al mes).
- Analice con un software Antivirus actualizado, cualquier correo electrónico antes de abrirlo, así conozca usted al remitente.
- Analice siempre con un software Antivirus los archivos en disquete o Cd-Rom antes de abrirlos o copiarlos a su computador.
- No descargue, ni mucho menos ejecute, archivos adjuntos (attachement) a un mensaje de correo electrónico sin antes verificar con la persona que supuestamente envió el mensaje, si efectivamente lo hizo.
- No ejecute nunca un programa de procedencia desconocida, aun cuando el software Antivirus indique que no está infectado. Dicho programa puede contener un troyano [3] o un sniffer [4] que reenvíe a otra persona su clave de acceso u otra información.
- Instale los parches [5] de actualización de software que publican las compañías fabricantes para solucionar vulnerabilidades de sus programas. De esta manera se puede hacer frente a los efectos que puede provocar la ejecución de archivos con códigos maliciosos.
- Tenga cuidado con los mensajes alusivos a situaciones eróticas (versión erótica del cuento de Blancanieves y los Siete Enanitos, fotos de mujeres desnudas, fotos de artistas o deportistas famosos, etc.).
- Nunca abra archivos adjuntos a un mensaje de correo electrónico cuya extensión [6] sea ".exe", ".vbs", ".pif", ".bat" o ".bak".
- Cerciórese que el archivo adjunto no tenga doble extensión. Por ejemplo: "NombreArchivo.php.exe".
- Evite el intercambio por correo electrónico de archivos con chistes, imágenes o fotografías.

- Visite con cierta frecuencia sitios que ofrecen información sobre los últimos virus aparecidos: (http://esp.sophos.com/, http://www.pandasoftware.es/,http://www.deltaasesores.com/recu/RECVirus.html, etc).
- Haga una copia de seguridad de los datos de su computador con la frecuencia que estime más conveniente. De esta forma, si se produce un ataque vírico, es fácil recuperar copias seguras de todos los archivos.
- Suscríbase a un servicio de notificación por correo electrónico de nuevos virus. Enterarse a tiempo de su existencia y de la forma como se comportan es una de los modos más efectivos de evitar un contagio (http://esp.sophos.com/virusinfo/notifications/, http://www.trendmicro.com).

- Si su computador tiene comportamientos extraños y usted sospecha que ha sido infectado por un Virus, visite los sitios Web de los fabricantes de software Antivirus y busque información sobre los nuevos Virus; generalmente, allí se indica como desinfectar el computador.
- La mayoría de las aplicaciones que aceptan código de macro [7] tienen valores de seguridad que se pueden configurar. Si usted usa Internet Explorer, escoja [Herramientas/Opciones de Internet], pulse la pestaña de "Seguridad" y entonces seleccione la "zona de Internet". Pulse el botón de "Nivel de Seguridad" para examinar las opciones de seguridad, o pulse el botón de "Nivel Prefijado" para asegurar que el nivel de seguridad esté puesto en Mediano. Para encontrar los valores de seguridad de Netscape Navigator, escoja [Editar/Preferencias], y seleccione "Avanzado" en la ventana de Categoría. No olvide los valores de seguridad de macro de su aplicación. En Word, Excel o Outlook 2000, escoja [Herramientas/Macro/Seguridad] y asegúrese de que su valor esté en "Mediano" o "Alto".
- No comparta los disquetes. Incluso un amigo bien intencionado puede, sin saberlo, contagiarlo con un virus, un caballo troyano o un gusano. Etiquete sus discos flexibles claramente para que distinga los suyos y no los preste. Si un amigo le presta un disquete que no es suyo, sugiérale un método alternativo para compartir archivos.
- Cuando no entienda algún término utilizado por los expertos en Virus, acuda a los sitios de fabricantes de software Antivirus donde podrá encontrar glosarios de las palabras utilizadas en este sector de la industria informática.
- Desconfíe de mensajes de correo electrónico no solicitados que le ofrecen la oportunidad de descargar software para intercambiar música, programas antivirus o fotografías.
- No haga caso a los mensajes tipo cadena que ofrecen instrucciones para borrar un archivo de su computador argumentando que se trata de un peligroso virus que se activará dentro de muy pocos días. Generalmente, el supuesto archivo infectado no es un virus sino un archivo del sistema operativo.
- Nunca acepte asesoría no solicitada para desinfectar su computador de algún peligroso virus. Si alguien le advierte que su computador está infectado, actualice su programa Antivirus y realice una revisión de todos los archivos del computador.
- Desconfíe de las Páginas Web desconocidas dónde podrá encontrar software gratuito o promociones de artículos con precios increíblemente bajos.



POR QUÉ LA GENTE CREA VIRUS

Actualmente, los virus son producidos en cantidades extraordinarias por muchísima gente alrededor del planeta. Algunos de ellos dicen hacerlo por divertimento, otros quizás para probar sus habilidades. De cualquier manera, hasta se ha llegado a notar un cierto grado de competitividad entre los autores de estos programas.

Algunos virus se crean por el desafío que implica crear una amenaza que sea única, no detectable, o simplemente devastadora para su víctima. El creador espera que el virus se propague de tal manera que le haga famoso. La notoriedad aumenta cuando el virus es considerado tal amenaza que los fabricantes de antivirus tienen que diseñar una solución.

CÓMO ELIMINAR EL MALWARE DE MI ORDENADOR

¿Te funciona lento el ordenador y cada día te aparecen más errores? Puede que estés sufriendo las consecuencias de haber sido infectado de **spyware**; éstos son pequeños programas espías que se dedican a utilizar nuestra conexión de Internet para robar nuestros datos e información sobre el contenido de nuestro PC o nuestro comportamiento. Todos estos **bugs**, en general, son conocidos como **malware**. Estamos seguros de que, después de conocer a ciencia cierta de qué se tratan, estás deseando deshacerte de ellos.

Si todavía no sabes **cómo eliminar el malware de tu ordenador**, en un Como.com te enseñamos a hacerlo paso por paso:

Instrucciones

- Descarga **SpyBot Search & Destroy 1.4** ¡Es completamente gratuito!
- Instala el programa pero no lo ejecutes todavía.
- Apaga el ordenador y enciéndelo nuevamente en modo a prueba de fallos (cuando tu PC esté arrancando, pulsa repetidamente F8 hasta que aparezca un menú bastante simple en el que puedas seleccionar 'Modo a prueba de fallos').
- Ejecuta SpyBot Search & Destroy 1.4 y elimina todo el **malware** que éste encuentre.
- Una vez terminada la limpieza, reinicia el ordenador de manera completamente normal y, cuando vuelva a estar encendido, analiza el PC al completo con dos antivirus diferentes. Desde unComo.com te recomendamos utilizar Avast! Free Antivirus y Avira AntiVir Free Edition.
- Ejecuta los antivirus descargados y elimina todo el **malware** que éstos encuentren.
- Reinicia el ordenador y disfruta de **un ordenador libre de virus y spyware**.
- Si deseas leer más artículos parecidos a **cómo eliminar el malware de mi ordenador**, te recomendamos que entres en nuestra categoría de Detectar y Eliminar Malware.

Necesitas

- Un ordenador con acceso a Internet.

Consejos

- Para evitar futuros problemas con el malware te recomedamos descargar un navegador seguro y rápido como, por ejemplo, Google Chrome.
- Mantén tu antivirus actualizado, al igual que tu Antyspyware.

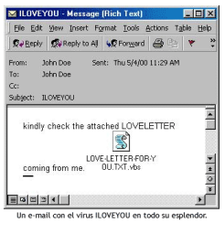
TOP 10: virus informáticos más destructivos de los últimos años

Los **virus informáticos** más famosos de estos últimos 20 años han sido más de los que nos gustarían. En el '88, por ejemplo, se creó Jerusalem, un **malware** que se instalaba en el ordenador y borraba todos los archivos cada viernes 13.

Mucho recordarán todavía el conocido 'ILoveYou', un correo electrónico que se movía por Internet como pez en el agua afectando a millones de ordenadores durante el año 2000... ¡Incluso llegó al Pentágono!

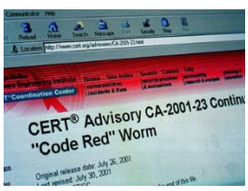
Los virus han evolucionado desde la época en que hackers adolescentes los creaban para competir entre ellos y causar un poco de desorden. Ahora, los hackers profesionales pertenecen a bandas criminales o agencias de espionaje, ya que se trata de robo de información o destrucción con un propósito, los daños son mayores y los malware son capaces de afectar la producción de industrias y el funcionamiento de bancos y agencias gubernamentales.

A continuación les presentamos una lista de los virus más dañinos de los últimos años.



Un e-mail con el virus ILOVEYOU en todo su esplendor.

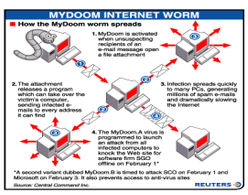
10. Carta de amor/ I LOVE YOU (2000)
En el año 2000, millones de personas cometieron el error de abrir lo que parecía ser un correo electrónico de un admirador secreto. Llevaba por título simplemente “I Love You”, pero en vez de ser una confesión amorosa, realmente era un “gusano”, que después de sobrescribir las imágenes de los usuarios se mandaba por correo electrónico a 50 contactos de la agenda Windows del usuario. En tan sólo una s horas se convirtió en una infección global.



9. Code Red (2001)
Comparado al malware moderno Code Red parece no ser tan peligroso, sin embargo en el 2001 sorprendió a expertos de seguridad en línea al utilizar una falla en el Servidor de Información de Microsoft, logrando bajar y cambiar algunos sitios web. El más memorable quizá fue el sitio de la Casa Blanca: whitehouse.gov y obligó también a otros sitios gubernamentales a bajar sus páginas momentáneamente.

8. Slammer (2003)
En enero del 2003*, Slammer* probó que tan dañino podía ser un gusano para los servicios públicos y privados. El gusano liberaba una avalancha de paquetes de red, y la cantidad de datos que transmitía a través del internet causó que varios servidores suspendieran actividades casi inmediatamente. Entre las víctimas del gusano se encontraron Bank of America, el servicio de emergencias estadounidense 911 y una planta nuclear en Ohio.

7. Fizzer (2003)
Los gusanos que se habían visto hasta el año 2004 eran principalmente para crear un poco de caos, Fizzer, iba tras el dinero. Muchos desestimaron al gusano ya que no se movía con la rapidez de Code Red, pero lo que lo hacía más peligroso es que era un gusano creado para obtener ganancias –una vez en tu correo electrónico enviaba correos no solo para propagarse, si no para enviar spam de porno y pastillas.



6. My Doom (2004)
En el 2004 logró infectar alrededor de un millón de máquinas lanzando una negación masiva del servicio de ataque, al hacer esto abruma a su objetivo al enviarle información de diversos sistemas. El gusano se propagaba por correo electrónico y lo hizo con una rapidez jamás antes vista.

5. PoisonIvy (2005)
Es la pesadilla de todo sistema de seguridad ya que permite que el virus controle la computadora que ha infectado. PoisonIvy pertenece al grupo de malware conocido como “un troyano remoto”, ya que le permite al creador del virus tener acceso completo a las máquinas que infectado usando una especie de puerta trasera, al grado que permite grabar y manipular información del equipo. Inicialmente se le consideró una herramienta de hackers principiantes, el virus ha llegado a afectar a muchas compañías de occidente.

4. Zeus (2007)
Actualmente es el malware más usado para obtener, de manera ilegal, información personal. Se puede comprar por un precio de 50 centavos de dólar en el mercado del crimen virtual y permite robar contraseñas y archivos. La información personal robada puede ser utilizada para hacer compras en línea o crear cuentas bancarias a nombre de una identidad comprometida.

3. agent.btz (2008)
Este malware fue el responsable de la creación de un nuevo departamento militar en Estados Unidos, el Cyber Command. El virus se propaga a través de memorias infectadas que instalan un malware que roba información. Cuando se encontró agent.btz en computadoras del Pentágono, sospecharon que era el trabajo de espías extranjeros.

2. Virus Conficker (2009)
En el 2009 este nuevo virus afectó a millones de máquinas con Windows en todo el mundo. Logró crear una especia de ejército global que robaba todo tipo de información. Debido a que era realmente difícil de parar se creó un grupo de expertos dedicados específicamente a detenerlo, el virus se llegó a conocer como el “súper bicho”, o “super gusano”. Lo que ha dejado a los expertos realmente perplejos es que nadie sabe para qué es exactamente, la información robada jamás se utilizó.

1. Stuxnet (2009-2010)
Este virus fue el primero en ser creado para causar daño en el mundo real y no sólo en el mundo virtual. El malware tenía como objetivo principal dañar sistemas industriales –se cree que el virus fue responsable de causar daños al equipo que procesaba uranio en una planta de Natanz en Irán-. Basándose en información de la Agencia Internacional de Energía Atómica, los expertos creen que el virus fue responsable de causar que muchas centrifugues que procesaban uranio en Irán giraran hasta perder el control y se auto-destruyeran. El virus no se descubrió hasta el 2010 pero sospechan que infectó computadoras desde el 2009.

ANTIVIRUS

Los **antivirus** nacieron como una herramienta simple cuyo objetivo fuera detectar y eliminar virus informáticos.

Con el transcurso del tiempo, la aparición de sistemas operativos más avanzados e Internet, los antivirus han evolucionado hacia programas más avanzados que no sólo buscan detectar un Virus informáticos, sino bloquearlo, desinfectar y prevenir una infección de los mismos, así como actualmente ya son capaces de reconocer otros tipos de malware, como spyware, rootkits, etc.

El funcionamiento de un antivirus varía de uno a otro, aunque su comportamiento normal se basa en contar con una lista de virus conocidos y su formas de reconocerlos (las llamadas firmas o vacunas), y analizar contra esa lista los archivos almacenados o transmitidos desde y hacia un ordenador.

Adicionalmente, muchos de los antivirus actuales han incorporado funciones de detección proactiva, que no se basan en una lista de malware conocido, sino que analizan el comportamiento de los archivos o comunicaciones para detectar cuáles son potencialmente dañinas para el ordenador, con técnicas como Heurística, HIPS, etc.

Usualmente, un antivirus tiene un (o varios) componente residente en memoria que se encarga de analizar y verificar todos los archivos abiertos, creados, modificados, ejecutados y transmitidos en tiempo real, es decir, mientras el ordenador está en uso.

Asimismo, cuentan con un componente de análisis bajo demando (los conocidos scanners, exploradores, etc), y módulos de protección de correo electrónico, Internet, etc.

Antivirus populares

- Kaspersky Anti-virus.
- Panda Security.
- Norton antivirus.
- McAfee.
- avast! y avast! Home
- AVG Anti-Virus y AVG Anti-Virus Free.
- BitDefender.
- F-Prot.
- F-Secure.
- NOD32.
- PC-cillin.
- ZoneAlarm AntiVirus.

Tipos de antivirus

- **Cortafuegos (Firewall)**

Programa que funciona como muro de defensa, bloqueando el acceso a un sistema en particular. Se utilizan principalmente en computadoras con conexión a una red, fundamentalmente Internet. El programa controla todo el tráfico de entrada y salida, bloqueando cualquier actividad sospechosa e informando adecuadamente de cada suceso.

Antiespías (Antispyware)

Aplicación que busca, detecta y elimina programas espías (spyware) que se instalan ocultamente en el ordenador.

Los antiespías pueden instalarse de manera separada o integrado con paquete de seguridad (que incluye antivirus, cortafuegos, etc).

Antipop-ups

Utilidad que se encarga de detectar y evitar que se ejecuten las ventanas pop-ups cuando navegas por la web. Muchas veces los pop-ups apuntan a contenidos pornográficos o páginas infectadas.

Algunos navegadores web como Mozilla Firefox o Internet Explorer 7 cuentan con un sistema antipop-up integrado.

Antispam

Aplicación o herramienta que detecta y elimina el spam y los correos no deseados que circulan vía email. Funcionan mediante filtros de correo que permiten detectar los emails no deseados. Estos filtros son totalmente personalizables.

Además utilizan listas de correos amigos y enemigos, para bloquear de forma definitiva alguna casilla en particular.

Algunos sistemas de correo electrónico como Gmail, Hotmail y Yahoo implementan sistemas antispam en sus versiones web, brindando una gran herramienta en la lucha contra el correo basura.

OPCIONES DE SOFTWARE ANTIVIRUS

Los programas Antivirus detectan los virus mediante una comparación que realiza entre los archivos guardados en el computador y una biblioteca de firmas [8] que identifican a cada Virus. Esto significa que primero se debe conocer el Virus (y por tanto, alguien se debe haber infectado) antes de desarrollar la firma para ese Virus.

Es muy importante mantener actualizada la base de datos de firmas de Virus de su programa antivirus debido a que diariamente aparecen nuevos Virus.

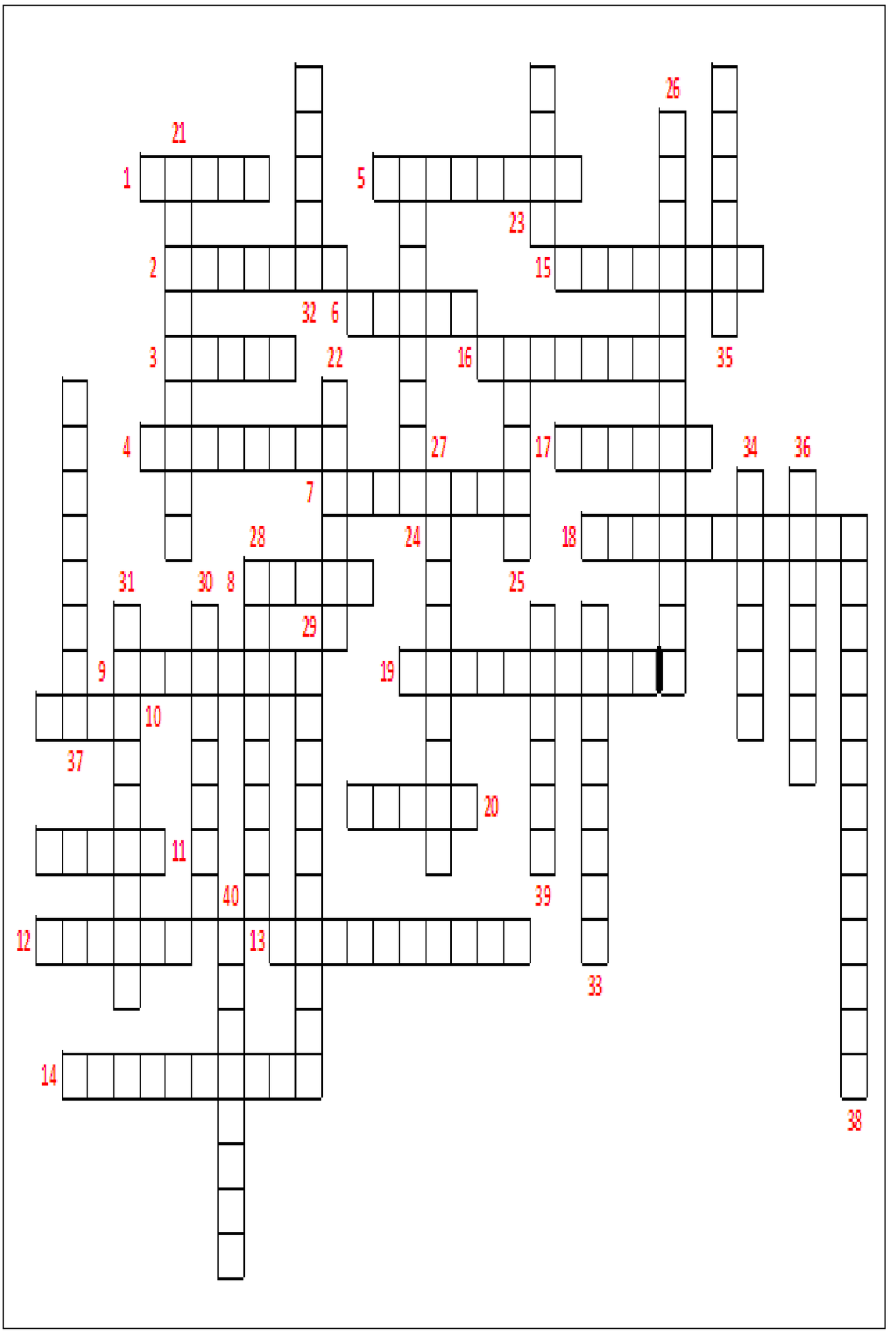
ANALIZADORES ANTIVIRUS	CALIFICACIï¿½N	COMENTARIOS
Symantec Norton Antivirus 2003 9.0 http://www.symantec.com/region/mx/	Muy Bueno ** (Shareware 15 dï¿½as)	Uno de los de mejor desempeï¿½o. Tambiï¿½n es el que tiene la interfaz mï¿½s clara e intuitiva de los productos probados. No detectï¿½ algunos virus de guiï¿½n ni pudo escanear algunos archivos guardados en las pruebas de zoovirus [9] **
Panda Antivirus Platinum 7.0 http://www.pandasoftware.es/	Bueno * (Shareware 30 dï¿½as)	Se integra con el cliente de correo electrï¿½nico de Microsoft Outlook y analiza las bases de datos Lotus Notes. No detectï¿½ 20 por ciento de los zoovirus [9] polimorfos en las evaluaciones. *
Trend Micro PC-Cillin 2003 10.0 http://www.trendmicro-la.com/index-e.html	Bueno ** (Shareware 30 dï¿½as)	Este software ha ganado numerosos premios en publicaciones de prestigio, ha sido retocado para estar al dï¿½a con las nuevas amenazas de virus, en la ï¿½poca de Internet. Es uno de los programas que ofrece la mejor protecciï¿½n posible para un computador personal. **
Network Associates McAfee VirusScan 7.0 http://es.mcafee.com/	Pobre * (Shareware 30 dï¿½as)	Fuerte anï¿½lisis de Virus, pero no detectï¿½ algunos de los Virus ï¿½Salvajesï¿½ en el sector de arranque durante anï¿½lisis totales. Incluye un cortafuegos, asï¿½ como un anï¿½lisis de virus para PDAs (Personal Digital Asistant ï¿½ Asistente Personal Digital). *
Computer associates Etrust EZ Antivirus 5.4 http://www.my-etrust.com/TrialReg	Muy Bueno * (Shareware 30 dï¿½as)	Tiene una interfaz limpia e intuitiva pero su desempeï¿½o deja mucho que desear. No detectï¿½ algunas aplicaciones maliciosas ni virus de guiï¿½n, y tuvo problemas en analizar archivos guardados en pruebas de zoovirus [9]. *
Sophos Anti-Virus http://esp.sophos.com/	Bueno ** (Shareware 30 dï¿½as)	Protï¿½gete contra mï¿½s de 68.000 virus, troyanos y gusanos. Detecta y elimina virus polimï¿½rficos, macros, ubicados en el sector de arranque y los que se trasmiten a travï¿½s de ejecutables. **
AVG Anti-Virus System Free Edition 6.0.404 http://www.grisoft.com/html/us_downl.htm	Muy Bueno ** (Gratuito)	Potente antivirus gratuito. Permite pausar una revisiï¿½n en curso para reanudarlo en otro momento. Monitoriza constante del sistema, revisa el correo electrï¿½nico, la actualizaciï¿½n de la base de datos de virus es gratuita que incluye actualizaciï¿½n automï¿½tica. **
AntiVir Personal Edition 6.17.03.54 http://www.free-av.com/	Muy Bueno ** (Gratuito)	Antivirus potente, eficaz y gratuito. Capaz de detectar y eliminar mï¿½s de 50.000 virus, incluyendo los de macro y sector de arranque, y es ademï¿½s muy fï¿½cil de usar. Vigila en todo momento el sistema con un Virus Guard residente que controla los movimientos de archivos. Incluye un asistente que actualiza automï¿½ticamente las bases de datos de virus. **
Avast! 4.0 http://www.avast.com/avad1.htm	Bueno ** (Gratuito)	Un antivirus eficaz, eficiente y ademï¿½s gratuito. Capaz de detectar una larga lista de virus, gusanos, troyanos e incluso virus capaces de modificarse a sï¿½ mismos. Comprueba la integridad de datos a fin de poder recuperar esos archivos mï¿½s fï¿½cilmente en caso de infecciï¿½n. Incorpora una interfaz para usuarios novatos que no quieren complicarse la vida con demasiadas opciones de configuraciï¿½n. Protege de virus de macros y virus residentes. Se integra con el Explorador de Windows y actualiza la base de datos de virus cada mes. **

CASILLERO SOBRE LOS VIRUS & ANTIVIRUS

PREGUNTAS DEL CASILLERO

HORIZONTALES	**VERTICALES**
1. Antivirus cuyo logo es un oso. **2. Tipo de virus que se camufla como un archivo inofensivo y después se activa y muestra su verdadera cara.** **3. Programa que tiene la capacidad de reproducirse a si mismo y realiza acciones con mala intención en el computador.** **4. Principal acción que realizan los antivirus sobre la información.** **5. Una de las características de los virus.** **6. Tipo de antivirus que tienen como logo una sombrilla.** **7. Acción que realizan los antivirus cuando detectan un virus informático.** **8. Antivirus con el siguiente logo:**  **9. Propósito principal que tienen los virus al ingresar a la computadora.** **10. Riesgo que hay con los datos cuando hay virus en el pc.** **11. Dispositivo de la computadora que por lo general activa los virus.** **12. Un virus es un programa o c… que altera el normal funcionamiento de la computadora.** **13. Tipo de virus que intenta esconderse en el sistema operativo.** **14. Virus que consiste que en un mismo directorio existan dos programas ejecutables con el mismo nombre.** **15. Así se les conoce a los programas que deliberadamente borran archivos.** **16. Fase en la que el virus intenta replicarse infectando otros archivos del sistema.** **17. Tipo de virus que se activa en una fecha determinada.** **18. Elemento importante de la computadora al cual los virus buscan atacar e infectar.** **19. Así se le llama a la última fase de un virus.** **20. Un tipo de programa maligno.**	**21. Programas diseñados para eliminar los virus.** **22. Nombre del primer virus que se hizo.** **23. Tipo de virus que se aloja en el sector de arranque.** **24. Tipo de virus que resulta de la combinación de varios virus.** **25. Virus inofensivos que por lo general causan molestias en el pc.** **26. Personas que hacen los virus.** **27. Efecto de propagarse un virus en toda la computadora.** **28. Así se les llama a los virus que cambian ciertas partes de su código y que son muy difíciles de detectar y eliminar.** **29. Virus que permanecen indefinidamente en la memoria.** **30. Lugar de la computadora donde suelen alojarse los virus.** **31. Delito informático que consiste en robar información, descargar música violando los derechos de autor.** **32. Antivirus muy usado cuyo símbolo es un ojo. N..** **33. Además de eliminar los virus y desinfectar la computadora, los antivirus cumplen también con esta función. Pr…** **34. Así se le suele llamar al remedio para contrarrestar los virus informáticos y biológicos.** **35. N… antivirus que por lo general viene preinstalado con el sistema operativo Windows.** **36. Sistema operativo muy propenso a infectarse con virus.** **37. Acción que ejecutan los antivirus de no permitir que el virus ingrese al sistema. Bl…** **38. Se recomienda hacer la A… a nuestro antivirus para que esté al día y no se vuelva obsoleto.** **39. Esto se recomienda hacer constantemente con la información de la computadora para evitar pérdidas de datos.** **40. Lugar por donde más se descargan virus al computador.**

CASILLERO


1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40