# Los virus computacionales



**Los virus Computacionales**



**Introducción**

**Un virus computacional es un programa o una serie de instrucciones que van encaminadas hacia el daño y la destrucción de la información cibernética, es decir estos virus no hacen mas que borrar información, o modificarla, también pueden reproducirse y acaparar toda la memoria disponible de la computadora ósea saturarla de información basura.**

**A lo largo de toda la historia de los virus, se desencadena una evolución tremenda en ellos, los hackers comienzan a buscar las nuevas maneras de fabricarlo hacerlos mas precisos e incluso hacerlos mas sigilosos ante los usuarios para que no se percaten de se presencia; Cada virus actúa de diferente manera y pueden ocasionar diversos daños en la información.**

**Los virus computacionales al igual que los virus biológicos, requieren de vacunas para poder eliminarse, estas vacunas son solamente programas o instrucciones contra restantes a los virus, y los eliminan de la computadora además si es posible recuperan la información, pero como cada vez existen mas virus, deben existir mas vacunas.**

**De lo anterior se desprende el gran negocio del software antivirus, ya que cada virus necesita ser estudiado de manera separada y crear su vacuna, este negocio no seria fructuoso sin el avance de los virus ya que los usuarios buscamos la tranquilidad y el resguardo debido a nuestra información, por ello se buscan los mejores antivirales como son El Norton, McAffe, Panda Sofware etc.**

**Historia de los virus computacionales.**

**A continuación se presenta una breve cronología de lo que ha sido los orígenes de los virus:**

**1949:** Se da el primer indicio de definición de virus. John Von Neumann, Expone su "Teoría y organización de un autómata complicado". donde demostraba la posibilidad de desarrollar pequeños programas que pudiesen tomar el control de otros.

**1959:** En los laboratorios AT&T Bell, se inventa el juego "Guerra Nuclear" (*Core Wars*). Basado en la idea de Neuman consistía en una batalla entre los códigos de dos programadores, en la que cada jugador desarrollaba un programa cuya misión era la de acaparar la máxima memoria posible mediante la reproducción de si mism

**1970:** El Creeper uno de los primeros virus difundidos por la red ARPANET. El virus mostraba el mensaje "SOY CREEPER...ATRAPAME SI PUEDES!". Ese mismo año es creado su antídoto: el antivirus Reaper cuya misión era buscar y destruir al Creeper.

**1980:** La red ARPANET es infectada por un "gusano" y queda 72 horas fuera de servicio. La infección fue originada por Robert T. Morris, un joven estudiante de informática de 23 años.

**1983:** Keneth Thomson siendo protagonista de una ceremonia pública presento y demostró la forma de desarrollar un virus informático.

**1986:** En ese año se difundieron los virus (c) Brain, Bouncing Ball y Marihuana y que fueron las primeras especies representativas de difusión masiva. Estas 3 especi virales tan sólo infectaban el sector de arranque de los diskettes. Posteriormente aparecieron los virus que infectaban los archivos con extensión **EXE** y **COM**.(los archivos con estas extensiones son la base de los programas)

**1988:** El virus Brain creado por los hermanos Basit y Alvi Amjad de Pakistan aparece en Estados Unidos

**1995:** 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

**1999:** 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

**VIRUS**

**Un virus es cualquier programa capaz de desarrollarse y generar daños a un ordenador.**

Virus puro

Un virus tiene como característica más importante la capacidad de copiarse a sí mismo en soportes diferentes al que se encontraba originalmente, y por supuesto hacerlo con el mayor sigilo posible y de forma transparente al usuario; a este proceso de auto réplica se le conoce como "infección", de ahí que en todo este tema se

utilice la terminología propia de la medicina: "vacuna", "tiempo de incubación", etc.

Un virus puro también debe modificar el código original del programa o soporte objeto de la infección, para poder activarse durante la ejecución de dicho código; al mismo tiempo, una vez activado, el virus suele quedar residente en memoria para poder infectar así de forma transparente al usuario.

Los virus son programas informáticos capaces de multiplicarse mediante la infección de otros programas mayores, e intentan permanecer ocultos en el sistema hasta darse a conocer. Pueden introducirse en los ordenadores de formas muy diversas, produciendo efectos molestos, nocivos e incluso destructivos e irreparables.

**Virus residentes**

La característica principal de estos virus es que se ocultan en la memoria RAM(memoria de acceso aleatorio) de forma permanente o residente. De este modo, pueden controlar e interceptar todas las operaciones llevadas a cabo por el sistema operativo, infectando todos aquellos ficheros y/o programas que sean ejecutados, abiertos, cerrados, renombrados, copiados, etc.

Estos virus sólo atacan cuando se cumplen ciertas condiciones definidas previamente por su creador (por ejemplo, una fecha y hora determinada). Mientras tanto, permanecen ocultos en una zona de la memoria principal, ocupando un espacio de la misma, hasta que son detectados y eliminados.

**Virus de acción directa**

Al contrario que los residentes, estos virus no permanecen en memoria. Por tanto, su objetivo prioritario es reproducirse y actuar en el mismo momento de ser ejecutados. Al cumplirse una determinada condición, se activan y buscan los ficheros ubicados dentro de su mismo directorio para contagiarlos. Además, también realizan sus acciones en los directorios especificados dentro de la línea PATH (camino o ruta de directorios), dentro del fichero AUTOEXEC.BAT (fichero que siempre se encuentra en el directorio raíz del disco duro). Los virus de acción directa presentan la ventaja de que los ficheros afectados por ellos pueden ser desinfectados y restaurados completamente.

**Virus de sobreescritura**

Estos virus se caracterizan por destruir la información contenida en los ficheros que infectan. Cuando infectan un fichero, escriben dentro de su contenido, haciendo que queden total o parcialmente inservibles.

También se diferencian porque los ficheros infectados no aumentan de tamaño, a no ser que el virus ocupe más espacio que el propio fichero (esto se debe a que se colocan encima del fichero infectado, en vez de ocultarse dentro del mismo).

La única forma de limpiar un fichero infectado por un virus de sobreescritura es borrarlo, perdiéndose su contenido.

**Virus de macro**

El objetivo de estos virus es la infección de los ficheros creados usando determinadas aplicaciones que contengan macros: documentos de Word (ficheros con extensión DOC), hojas de cálculo de Excel (ficheros con extensión XLS), bases de datos de Access (ficheros con extensión MDB), presentaciones de PowerPoint (ficheros con extensión PPS), ficheros de Corel Draw, etc.

Las macros son micro-programas asociados a un fichero, que sirven para automatizar complejos conjuntos de operaciones. Al ser programas, las macros pueden ser infectadas.

Cuando se abre un fichero que contenga un virus de este tipo, las macros se cargarán de forma automática, produciéndose la infección. La mayoría de las aplicaciones que utilizan macros cuentan con una protección antivirus y de seguridad específica, pero muchos virus de macro sortean fácilmente dicha protección.

Existe un tipo diferente de virus de macro según la herramienta usada: de Word, de Excel, de Access, de PowerPoint, multiprograma o de archivos RTF. Sin embargo no todos los programas o herramientas con macros pueden ser afectadas por estos virus.

**Virus de enlace o directorio**

Los ficheros se ubican en determinadas direcciones (compuestas básicamente por unidad de disco y directorio), que el sistema operativo conoce para poder localizarlo y trabajar con ellos.

Los virus de enlace o directorio alteran las direcciones que indican donde se almacenan los ficheros. De este modo, al intentar ejecutar un programa (fichero con extensión EXE o COM) infectado por un virus de enlace, lo que se hace en realidad es ejecutar el virus, ya que éste habrá modificado la dirección donde se encontrab originalmente el programa, colocándose en su lugar.

Una vez producida la infección, resulta imposible localizar y trabajar con los ficheros originales.

**Virus encriptados**

Más que un tipo de virus, se trata de una técnica utilizada por algunos de ellos, que a su vez pueden pertenecer a otras clasificaciones.

Estos virus se cifran o encriptan a sí mismos para no ser detectados por los programas antivirus. Para realizar sus actividades, el virus se descifra a sí mismo y, cuando ha finalizado, se vuelve a cifrar.

**Virus polimórficos**

Son virus que en cada infección que realizan se cifran o encriptan de una forma distinta (utilizando diferentes algoritmos y claves de cifrado).

A los virus se les puede dar adjetivos de acuerdo a la forma en que trabajan o como llegan a la PC.



Caballo: Este adjetivo se le da cuando el virus hace copias de sí mismo y empieza a saturar la memoria de la computadora

Caballo de Troya: Este nombre tiene como influencia la hazaña de los griegos, se introducen al sistema como programas o archivos que al ejecutarlos liberan o crean otro el troyano que es el que causa daño, la mayoría de estos virus son para recopilar información para después ser enviada a los hackers que crearon el virus, el troyano adquiere y grava todas y cada una de las pulsaciones que el usuario hace a la computadora, es así como el hackers obtiene datos, claves o passwords.

Bombas de Tiempo: Este adjetivo se da cuando el virus tiene una cierta fecha u hora para actuar uno de los mas famosos virus que actúa de esta forma es el Viernes 1 que precisamente entro en acción en esa fecha.

**Ejemplos de virus**

**Uno de los virus mas peligrosos de los ultimos tiempos I LOVE YOU**

**El proceso. La infección comienza cuando un usuario recibe un correo electrónico titulado I Love You (Te quiero), que lleva asociado un fichero llamado LOVE-LETTER-FOR-YOU.TXT.vbs. (Carta de amor para ti). Este último archivo contiene el código del virus, supuestamente firmado con el apodo spyder (araña), fechado en Manila (Filipinas) e incluye una expeditiva frase I hate go to school (Odio ir al colegio).**

**A diferencia de su predecesor, el virus Melissa, que elegía las primeras 50 direcciones de la agenda del usuario para enviar una copia del virus, I love you toma todas las direcciones, lo cual aumenta su capacidad de reproducción.**

**Aquellas personas cuya dirección de correo electrónico figuren en la agenda del ordenador infectado recibirán en su buzón electrónico una copia del virus I love you, y si alguno de estos destinatarios decide abrir el mensaje, el proceso se repetirá provocando que la expansión del virus siga una progresión geométrica.**

***love you*** **se instala en el ordenador y borra ficheros de gráficos y de sonido -extensiones JPG, JPEG, MP3 y MP2-, sustituyéndolos por otros con el mismo nombre y la extensión VBS e introduciendo el código malicioso.**

**Existen muchos virus, de todos tipos, actualmente existen paginas de internet que dan estadísticas de los ultimos virus encontrados y/o generados ademas de hacer estimación de a cuantos computadores ha dañado y su grado de peligrosidad: poe ejemplo al dia 19/09/2004 estas son las estadísticas**

Para ver el gráfico seleccione la opción "Descargar" del menú superior

**Principales medios de contagio.**

**Correo electrónico.**

**Algunos virus vienen adjuntos a los correos electrónicos o simplemente contagian al abrir el correo para la lectura.**

**Discos extraíbles:**

Los discos extraíbles son unidades físicas y externas a nuestro ordenador, que se utilizan para guardar e intercambiar información, como los disquetes, CD-ROMs, DVDs, discos duros extraíbles, etc.

Si uno de los programas, ficheros, mensajes de correo, etc. guardados en una unidad de disco está infectado, al introducirla en otro ordenador podría infectarlo también

Tradicionalmente, esta era la mayor fuente de infecciones. Hoy en día, los discos han retrocedido en importancia frente a la expansión de Internet, pero todavía continúan representando un riesgo considerable.

**Redes de ordenadores.**

Las redes de ordenadores consisten en un conjunto de ordenadores conectados físicamente entre sí (a través de cable, módem, etc.), para poder compartir información programas, Intranet, etc.) y recursos entre ellos (acceso a impresoras, escáner, etc), sin necesidad de recurrir a las unidades de disco extraíbles.

Esto es positivo y facilita el trabajo, pero también facilita la transmisión de virus: la probabilidad de infección en una red es mayor que si el ordenador no está conectado en red.

Si uno de los ordenadores de una red contiene información con virus, cuando los demás accedan a ella serán infectados a su vez, cayendo todos en cadena y paralizando la actividad de la toda red.

**Internet**

Internet se ha convertido en el mayor medio de transferencia de información entre ordenadores, y en consecuencia, hoy es la mayor y más rápida vía de propagación d virus.

Sin embargo, Internet posibilita numerosas formas de intercambiar información, y cada una de ellas tiene unas características y un potencial de riesgo distinto.

De aquí seurgen entonces los antivirus. Los principales antivirus son el Norton Antivirus, McAffe, Panda antivirus; hay muchos antivirus, lo importante es que se esté actualizando muy seguido puede ser via internet o simplemente adquiriendo los nuevos productos actualizados. Estos antivirus presentan "vacunas" que no son masqu programas o procedimientos que borran o eliminan al virus de la computadora.

**Conclusión:**

A lo largo de este rema hemos comprendido y aprendido del grave problema de los virus computacionales, sin duda lo mejor seria erradicarlos por completo pero esto es imposible, si esto no es posible una alternativa para proteger nuestra información podría ser respaldar todos y cada uno de los archivos mas importantes, en un diskette o CD

No hay que olvidar tener instalado un Software antivirus que proteja a nuestro ordenador, este antivirus se deberá estarse actualizando con continuidad ya que los viru computacionales se generan día con día, Sin duda aquella persona que no utilice un Antivirus sera presa facil de los tantos y tantos virus que existen y que se siguen generando.

Tambien sin duda el ambiente de impotencia al terminar de leer y estudiar este texto es notable, solamente por la decisión de unos pocos otros tenemos que pagar no solo económicamente si no también laboralmente un precio, ya sea con dinero o con inversión de tiempo porque para muchos su trabajo se encuentra ahí, en un ordenador.

Resultará imposible impedir que se sigan desarrollando virus en todo el mundo, por ser esencialmente una expresión cultural de "**graffiti cibernético**", así como los hackers jamás se detendrán en su intento de "romper" los sistemas de seguridad de las redes e irrumpir en ellas con diversas intencionalidades. Podemos afirmar que eterna **lucha entre el bien y el mal** ahora se ha extendido al **ciber espacio**.

**Bibliografía:**

http://www.el-mundo.es/navegante/2000/05/05/ailofiu_virus.html

hhtt://alerta-antivirus.red.es/

http://www.zonavirus.com/Detalle_HISTORIA.asp?HISTORIA=13

http://www.perantivirus.com/sosvirus/general/wazzu.htm

http://www.perantivirus.com/sosvirus/general/fujimori.htm

http://www.perantivirus.com/sosvirus/general/histovir.htm

http://www.geocities.com/ogmg.rm/Historia.html

http://www.geocities.com/ogmg.rm/Clasifica.html

http://www.geocities.com/ogmg.rm/Funciona.html

http://trucosdeordenador.com/tipo_virus.php

http://www.trucosdeordenador.com/presenta_v.php?tipo=v&vid=54

http://www.trucosdeordenador.com/presenta_v.php?tipo=v&vid=19

http://www.trucosdeordenador.com/listvir.php?q=t&tid=3

http://www.trucosdeordenador.com/listvir.php?q=t&tid=4

http://www.trucosdeordenador.com/listvir.php?q=t&tid=6

http://www.trucosdeordenador.com/listvir.php?q=t&tid=5

http://www.trucosdeordenador.com/presenta_v.php?tipo=v&vid=49

**Salvador de la Cruz**

## Comentarios

**Para dejar un comentario, regístrese gratis o si ya está registrado, inicie sesión.**

## Trabajos relacionados

**Guía de Computación**¿Qué es Excel?. ¿Cómo se crea un libro de trabajo nuevo?. ¿Cómo se abre un libro existente?. ¿Cómo se guarda un libro de...

La realización de las actividades prácticas de la disciplina de Profilaxis, Enfermedades Infecciosas y Parasitarias de l...

**La multimedia aplicada a una clase teórico-práctica. software "dermatomicosis bovina"**
Las bases de un cuello de botellas. ¿Dónde es la Lentitud?. Aplicaciones con lentitud. Escalamiento horizontal y vertica...

**Planificación de capacidades y problemas de productividad con Solaris 2.6**

Ver mas trabajos de Software