http://mundopc.net/articulos/funcionamiento-de-los-virus/

HISTORIA DE LOS VIRUS

Hacia finales de los años 60, Douglas McIlory, Víctor Vysottsky y Robert Morís idearon un juego al que llamaron Core War (Guerra en lo Central, aludiendo a la memoria de la computadora), que se convirtió en el pasatiempo de algunos de los programadores de los laboratorios Bell de AT&T.

El juego consistía en que dos jugadores escribieran cada uno un programa llamado organismo, cuyo hábitat fuera la memoria de la computadora. A partir de una señal, cada programa intentaba forzar al otro a efectuar una instrucción inválida, ganando el primero que lo consiguiera.

Al término del juego, se borraba de la memoria todo rastro de la batalla, ya que estas actividades eran severamente sancionadas por los jefes por ser un gran riesgo dejar un organismo suelto que pudiera acabar con las aplicaciones del día siguiente. De esta manera surgieron los programas destinados a dañar en la escena de la computación.

Históricamente los virus informáticos fueron descubiertos por la prensa el 12 de octubre de 1985, con una publicación del New York Times que hablaba de un virus que fue se distribuyo desde un BBS y aparentemente era para optimizar los sistemas IBM basados en tarjeta gráfica EGA, pero al ejecutarlo salía la presentación pero al mismo tiempo borraba todos los archivos del disco duro, con un mensaje al finalizar que decía “Caíste”.

Bueno en realidad este fue el nacimiento de su nombre, ya que los programas con código integrado, diseñados para hacer cosas inesperadas han existido desde que existen las computadoras. Y ha sido siempre la obra de algún programador delgado de ojos de loco.
Pero las primeras referencias de virus con fines intencionales surgieron en 1983 cuando Digital Equipament Corporation (DEC) empleó una subrutina para proteger su famoso procesador de textos Decmate II, que el 1 de abril de 1983 en caso de ser copia ilegal borraba todos los archivos de su unidad de disco.

Uno de los primeros registros que se tienen de una infección data del año 1987, cuando en la Universidad estadounidense de Delaware notaron 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 booteo 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.

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.

Actualmente, los virus son producidos en cantidades extraordinarias por muchisima gente alrededor del planeta. Algunos de ellos dicen hacerlo por divercion, 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.
Con relación a la motivación de los autores de virus para llevar a cabo su obra, existe en Internet un documento escrito por un escritor freelance Markus Salo, en el cual, entre otros, se exponen los siguientes conceptos:

Algunos de los programadores de virus, especialmente los mejores, sostienen que su interés por el tema es puramente científico, que desean averiguar todo lo que se pueda sobre virus y sus usos.

A diferencia de las compañías de software, que son organizaciones relativamente aisladas unas de otras (todas tienen secretos que no querrían que sus competidores averiguaran) y cuentan entre sus filas con mayoría de estudiantes graduados, las agrupaciones de programadores de virus están abiertas a cualquiera que se interese en ellas, ofrecen consejos, camaradería y pocas limitaciones. Además, son libres de seguir cualquier objetivo que les parezca, sin temer por la pérdida de respaldo económico.

El hecho de escribir programas vírales da al programador cierta fuerza coercitiva, lo pone fuera de las reglas convencionales de comportamiento. Este factor es uno de los más importantes, pues el sentimiento de pertenencia es algo necesario para todo

ser humano, y es probado que dicho sentimiento pareciera verse reforzado en situaciones marginales.

Por otro lado, ciertos programadores parecen intentar legalizar sus actos poniendo sus creaciones al alcance de mucha gente, (vía Internet, BBS especializadas, etc.) haciendo la salvedad de que el material es peligroso, por lo cual el usuario debería tomar las precauciones del caso.

Existen programadores, de los cuales, generalmente, provienen los virus más destructivos, que alegan que sus programas son creados para hacer notoria la falta de protección de que sufren la mayoría de los usuarios de computadoras.

La gran mayoría de estos individuos son del mismo tipo de gente que es reclutada por los grupos terroristas: hombres, adolescentes, inteligentes

QUÉ ES UN VIRUS

Un virus es simplemente un programa, elaborado accidental o intencionadamente para instalarse en la computadora de un usuario sin el conocimiento o el permiso de este.
Podríamos decir que es una secuencia de instrucciones y rutinas creadas con el único objetivo de alterar el correcto funcionamiento del sistema y, en la inmensa mayoría de los casos, corromper o destruir parte o la totalidad de los datos almacenados en el disco. De todas formas, dentro del término “virus informático” se suelen englobar varios tipos de programas.

Todos estos programas tienen en común la creación de efectos perniciosos; sin embargo, no todos pueden ser considerados como virus propiamente dichos.
Decimos además que es un programa parásito porque el programa ataca a los archivos o sector es de “booteo” o arranque y se reproduce a sí mismo para continuar su esparcimiento.

Algunos se limitan solamente a multiplicarse, mientras que otros pueden producir serios daños que pueden afectar a los sistemas. Nunca se puede asumir que un virus es inofensivo y dejarlo “flotando” en el sistema.

Existen ciertas analogías entre los virus biológicos y los informáticos: mientras los primeros son agentes externos que invaden células para alterar su información genética y reproducirse, los segundos son programas-rutinas, en un sentido más estricto, capaces de infectar archivos de computadoras, reproduciéndose una y otra vez cuando se

accede a dichos archivos, dañando la información existente en la memoria o alguno de los dispositivos de almacenamiento del ordenador.
Tienen diferentes finalidades: Algunos sólo 'infectan', otros alteran datos, otros los eliminan, algunos sólo muestran mensajes. Pero el fin último de todos ellos es el mismo: PROPAGARSE.

Es importante destacar que el potencial de daño de un virus informático no depende de su complejidad sino del entorno donde actúa.
La definición más simple y completa que hay de los virus corresponde al modelo D. A. S., y se fundamenta en tres características, que se refuerzan y dependen mutuamente. Según ella, un virus es un programa que cumple las siguientes pautas:
Es dañino
Es auto reproductor
Es subrepticio u oculto

El hecho de que la definición imponga que los virus son programas no admite ningún tipo de observación; está extremadamente claro que son programas, realizados por personas. Además de ser programas tienen el fin ineludible de causar daño en cualquiera de sus formas.

CARACTERÍSTICAS 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 duplique 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-huesped es cerrado.

Los virus pueden llegar a "camuflarse" y esconderse para evitar la detección y reparación. Como lo hacen:

El virus re-orienta la lectura del disco para evitar ser detectado;

Los datos sobre el tamaño del directorio infectado son modificados en la FAT, para evitar que se descubran bytes extra que aporta el virus;

http://mundopc.net/articulos/funcionamiento-de-los-virus/

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 sobreescribirlo. 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 Windows 98).

En cambio los virus de programa, se manifiestan cuando la aplicación infectada es ejecutada, el virus se activa y se carga en la memoria, infectando a cualquier programa que se ejecute a continuación. Puede solaparse infecciones de diversos virus que pueden ser destructivos o permanecer inactivos por largos periodos de tiempo.

Asimismo, se pueden distinguir tres módulos principales de un virus informático:

Módulo de Reproducción

Módulo de Ataque

Módulo de Defensa

a) El módulo de reproducción

se encarga de manejar las rutinas de “parasitación” de entidades ejecutables (o archivos de datos, en el caso de los virus macro) a fin de que el virus pueda ejecutarse subrepticiamente. Pudiendo, de esta manera, tomar control del sistema e infectar otras entidades permitiendo se traslade de una computadora a otra a través de algunos de estos archivos.

b) El módulo de ataque

es optativo. En caso de estar presente es el encargado de manejar las rutinas de daño adicional del virus. Por ejemplo, el conocido virus Michelangelo, además de producir los daños que se detallarán más adelante, tiene un módulo de ataque que

se activa cuando el reloj de la computadora indica 6 de Marzo. En estas condiciones la rutina actúa sobre la información del disco rígido volviéndola inutilizable.

c) El módulo de defensa

Tiene, obviamente, la misión de proteger al virus y, como el de ataque, puede estar o no presente en la estructura. Sus rutinas apuntan a evitar todo aquello que provoque la remoción del virus y retardar, en todo lo posible, su detección.

SÍNTOMAS TÍPICOS DE UNA INFECCIÓN

- El sistema operativo o un programa toma mucho tiempo en cargar sin razón aparente.
- El tamaño del programa cambia sin razón aparente.
- El disco duro se queda sin espacio o reporta falta de espacio sin que esto sea necesariamente así.
- Si se corre el CHKDSK no muestra “655360 bytes available”.
- En Windows aparece “32 bit error”.
- La luz del disco duro en la CPU continua parpadeando aunque no se este trabajando ni haya protectores de pantalla activados. (Se debe tomar este síntoma con mucho cuidado, porque no siempre es así).
- No se puede “bootear” desde el Drive A, ni siquiera con los discos de rescate.
- Aparecen archivos de la nada o con nombres y extensiones extrañas.
- Suena “clicks” en el teclado (este sonido es particularmente aterrador para quien no esta advertido).
- Los caracteres de texto se caen literalmente a la parte inferior de la pantalla (especialmente en DOS).

SÍNTOMAS QUE INDICAN LA PRESENCIA DE VIRUS

- Cambios en la longitud de los programas
- Cambios en la fecha y / u hora de los archivos
- Retardos al cargar un programa
- Operación más lenta del sistema
- Reducción de la capacidad en memoria y / o disco rígido
- Sectores defectuosos en los disquetes
- Mensajes de error inusuales
- Actividad extraña en la pantalla
- Fallas en la ejecución de los programas

http://mundopc.net/articulos/funcionamiento-de-los-virus/

- Fallas al bootear el equipo
- Escrituras fuera de tiempo en el disco
- En la pantalla del monitor pueden aparecen mensajes absurdos tales como “Tengo hambre. Introduce un Big Mac en el Drive A“.

RIESGOS

¿Mi computadora puede contraer una infección cuando navego por internet?

Por el simple hecho de estar conectado a Internet no se transfiere ningun tipo de virus informático. Existe quizá algún peligro, examinando páginas web o “bajando” archivos de la red.

Las páginas web que utilizan objetos ActiveX pueden contener virus, puesto que ellos son realmente ficheros ejecutables, recogidos por nuestro navegador y ejecutados en nuestras PC. Podrían eventualmente ser utilizados inescrupulosamente para propagar un virus.

La “seguridad” de los objetos ActiveX consiste simplemente en un certificado digital de autenticidad, “firmado” por quien ha creado el objeto. Pero un simple certificado de autenticidad no puede garantizar que no esté un virus presente.

También podemos recibir páginas que utilizan Applets de Java. Estos programas no llegan a ser descargados por nuestro navegador, se ejecutan en un entorno muy restringido, y no hay acceso a la PC, o al disco duro, con lo que resulta prácticamente imposible infectarnos con applets (al menos hoy por hoy).

Durante el proceso de descarga de ficheros, también es muy difícil recoger un virus, tenemos las mismas condiciones que con los applets de java, pero una vez que el fichero ha llegado completamente a nuestro PC, debe ser chequeado antes de ejecutarse, ya que podria contener un virus.

b. ¿Qué hacer con los virus del correo electrónico?

Con estos podemos estar tranquilos, ya que un virus no puede copiarse ni romper nuestro disco duro tan solo por leer un correo electrónico, porque se trata simplemente de un archivo de texto (no ejecutable).

http://mundopc.net/articulos/funcionamiento-de-los-virus/

Una cosa muy diferente, son los ficheros adjuntos (attachments), ya que podemos recibir un fichero ejecutable que podria contener un virus. Lo mejor es no ejecutar directamente los archivos desde nuestro navegador, sino almacenarlos en nuestro disco duro y antes de ejecutarlos, chequearlos con un anti-virus confiable.

Es recomendable por lo mismo, abstenerse en lo posible de enviar archivos adjuntos, por idéntico riesgo que representa para nuestros corresponsales.

Si su programa de correo electrónico esta configurado para leer los mensajes automáticamente con Microsoft Word, es posible recibir un virus-macro e infectar a nuestro Ms-Word. Si tiene esta opción activada; desactívala, y chequea los ficheros recibidos antes de ejecutarlos.

Finalmente, y por si quedara alguna duda, lo mejor es tomar por norma eliminar los ficheros recibidos por corresponsales desconocidos, aquellos que no hemos solicitado. No exponga sus datos a un riesgo innecesario por abrir (o ejecutar) un archivo desconocido.

¿Qué es un ANTIVIRUS?

No para toda enfermedad existe cura, como tampoco existe una forma de erradicar todos y cada uno de los virus existentes.

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

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

El modelo más primario de las funciones de un programa antivirus es la detección de su presencia y, en lo posible, su identificación. La primera técnica que se popularizó para la detección de virus informáticos, y que todavía se sigue

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

La técnica de scanning fue bastante eficaz en los primeros tiempos de los virus informáticos, cuando había pocos y su producción era pequeña. Este relativamente pequeño volumen de virus informáticos permitía que los desarrolladores de antivirus escaneadores tuvieran tiempo de analizar el virus, extraer el pequeño trozo de código que lo iba a identificar y agregarlo a la base de datos del programa para lanzar una nueva versión. Sin embargo, la obsolescencia de este mecanismo de identificación como una solución antivirus completa se encontró en su mismo modelo.

El primer punto grave de este sistema radica en que siempre brinda una solución a posteriori: es necesario que un virus informático alcance un grado de dispersión considerable para que sea enviado (por usuarios capacitados, especialistas o distribuidores del producto) a los desarrolladores de antivirus. Estos lo analizarán, extraerán el trozo de código que lo identificará, y lo incluirán en la próxima versión de su programa antivirus. Este proceso puede demorar meses a partir del momento en que el virus comienza a tener una dispersión considerable, lapso en el cual puede causar graves daños sin que pueda ser identificado.

Además, este modelo consiste en una sucesión infinita de soluciones parciales y momentáneas (cuya sumatoria jamás constituirá una solución definitiva), que deben actualizarse periódicamente debido a la aparición de nuevos virus.

En síntesis, la técnica de scanning es altamente ineficiente, pero se sigue utilizando debido a que permite identificar rápidamente la presencia de los virus más conocidos y, como son estos los de mayor dispersión, permite una importante gama de posibilidades.

Un ejemplo típico de un antivirus de esta clase es el Viruscan de McAfee, que se verá más adelante.

http://mundopc.net/articulos/funcionamiento-de-los-virus/

En virtud del pronto agotamiento técnico de la técnica de scanning, los desarrolladores de programas antivirus han dotado a sus creaciones de métodos para búsquedas de virus informáticos (y de sus actividades), que no identifican específicamente al virus sino a algunas de sus características generales y comportamientos universalizados.

Este tipo de método rastrea rutinas de alteración de información que no puedan ser controladas por el usuario, modificación de sectores críticos de las unidades de almacenamiento (master boot record, boot sector, FAT, entre otras), etc.

Un ejemplo de este tipo de métodos es el que utiliza algoritmos heurísticos.

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

Algunos de los antivirus de esta clase son F-Prot, Norton Anti Virus y Dr. Solomon’s Toolkit.

Ahora bien, otra forma de detectar la presencia de un virus informático en un sistema consiste en monitorear las actividades de la PC señalando si algún proceso intenta modificar los sectores críticos de los dispositivos de almacenamiento o los archivos ejecutables. Los programas que realizan esta tarea se denominan chequeadores de integridad.

Sobre la base de estas consideraciones, podemos consignar que un buen sistema antivirus debe estar compuesto por un programa detector de virus -que siempre esté residente en memoria- y un programa que verifique la integridad de los sectores críticos del disco rígido y sus archivos ejecutables. Existen productos antivirus que cubren los dos aspectos, o bien pueden combinarse productos diferentes configurados de forma que no se produzcan conflictos entre ellos.

http://mundopc.net/articulos/funcionamiento-de-los-virus/

UNA FORMA DE EVITAR LOS VIRUS DE PENDRIVE

Una buena parte de los virus de computador, hacen uso de características propias de Windows, para hacer de las suyas. Una de esas características es la ejecución del archivo autorun.inf en CD-ROM DVD-ROM o memorias USB incluyendo una gran cantidad de dispositivos USB. Este método es el más efectivo para controlarlo…

La mayor parte de bloqueadores de autorun.inf utilizan una variable policies que evita la autoejecución en determinados dispositivos. Pero en el momento en el que uno abre descuidadamente el dispositivo, de todas maneras se ejecuta el archivo autorun.inf, con el consiguiente virus infectado del dispositivo.

Este método a continuación deshabilita permanente y totalmente la capacidad de autoejecución de autorun.inf (Es probable que pueda llegarse al mismo resultado por alguna configuración recóndita de Windows).

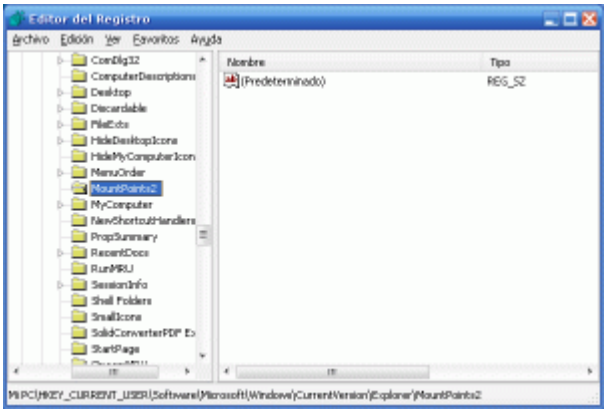
Se trata de Eliminar las subclaves en el registro de configuración de regedit, y "congelarlo".

Procedimiento:

1. Inicio -> Ejecutar -> regedit.
2. Buscar la siguiente clave del registro:

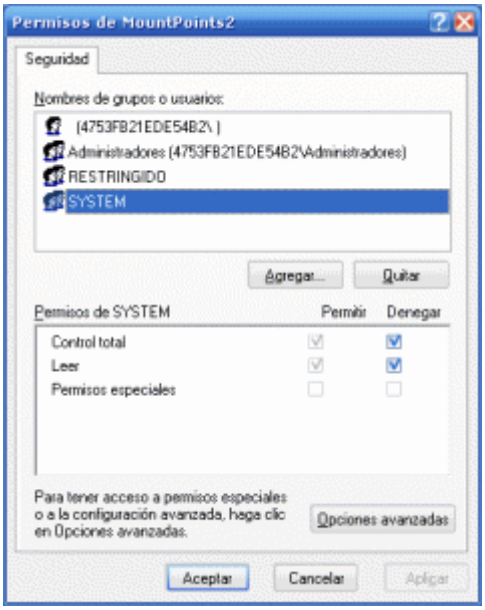
Windows XP:
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2

Windows 2000:
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints



3. Con el botón secundario del ratón, editar los PERMISOS de dicha clave.
4. Denegar el "control total" para todos los usuarios, incluyendo SYSTEM, nombre de PC, etc.

http://mundopc.net/articulos/funcionamiento-de-los-virus/



Aun cuando alguien tenga virus en un dispositivo como una memoria USB, de los virus que funcionan como autorun, este virus no será ejecutado. Dando tiempo al antivirus de escanear el dispositivo externo hasta su desinfección.