VIRUS INFORMATICOS

Un virus informático es un programa de computadora que tiene la capacidad de causar daño y su característica más relevante es que puede replicarse a sí mismo y propagarse a otras computadoras. Infecta “entidades ejecutables”: cualquier archivo o sector de las unidades de almacenamiento que contenga códigos de instrucción que el procesador valla a ejecutar. Se programa en lenguaje ensamblador y por lo tanto, requiere algunos conocimientos del funcionamiento interno de la computadora.

Un virus tiene tres características primarias:

- Es dañino. Un virus informático siempre causa daños en el sistema que infecta, pero vale aclarar que el hacer daño no significa que valla a romper algo. El daño puede ser implícito cuando lo que se busca es destruir o alterar información o pueden ser situaciones con efectos negativos para la computadora, como consumo de memoria principal, tiempo de procesador, disminución de la performance.
- Es autorreproductor. A nuestro parecer la característica más importante de este tipo de programas es la de crear copias de sí mismo, cosa que ningún otro programa convencional hace. Imagínense que si todos tuvieran esta capacidad podríamos instalar un procesador de textos y un par de días más tarde tendríamos tres de ellos o más. Consideramos ésta como una característica propia de virus porque los programas convencionales pueden causar daño, aunque sea accidental, sobrescribiendo algunas librerías y pueden estar ocultos a la vista del usuario, por ejemplo: un programita que se encargue de legitimar las copias de software que se instalan.

- Es subrepticio. Esto significa que utilizará varias técnicas para evitar que el usuario se de cuenta de su presencia. La primera medida es tener un tamaño reducido para poder disimularse a primera vista. Puede llegar a manipular el resultado de una petición al sistema operativo de mostrar el tamaño del archivo e incluso todos sus atributos.

La verdadera peligrosidad de un virus no está dada por su arsenal de instrucciones maléficas, sino por lo crítico del sistema que está infectando. Tomemos como ejemplo un virus del tipo conejo. Si este infectara una computadora hogareña la máquina se colgaría, pudiendo luego reiniciarla con un disquete de arranque limpio y con un antivirus para eliminar el virus. Si afectara a un servidor de una PyME, posiblemente el sistema informático de la empresa dejaría de funcionar por algún tiempo significando una pérdida de horas máquina y de dinero. Pero si este virus infectara una máquina industrial como una grúa robótica o algún aparato utilizado en medicina como una máquina de rayos láser para operar, los costos serían muy altos y posiblemente se perderían vidas humanas. ¿Qué pasaría si se alteraran los registros médicos de una persona de forma que se mostrara un tipo de sangre o factor RH diferente? El paciente podría morir. ¿Qué pasaría si el dígito 4 millonésimo en los cálculos para el aterrizaje de una misión espacial se alterara en un factor del 0.001 por 100? Los astronautas morirían.

Los virus informáticos no pueden causar un daño directo sobre el hardware. No existen instrucciones que derritan la unidad de disco rígido o que hagan estallar el cañon de un monitor. En su defecto, un virus puede hacer ejecutar operaciones que reduzcan la vida útil de los dispositivos. Por ejemplo: hacer que la placa de sonido envíe señales de frecuencias variadas con un volumen muy alto para averiar los parlantes, hacer que la impresora desplace el cabezal de un lado a otro o que lo golpee contra uno de los lados, hacer que las unidades de almacenamiento muevan a gran

velocidad las cabezas de L / E para que se desgasten. Todo este tipo de cosas son posibles aunque muy poco probables y por lo general los virus prefieren atacar los archivos y no meterse con la parte física.

- ¿Quién los hace?

En primer lugar debemos decir que los virus informáticos están hechos por personas con conocimientos de programación pero que no son necesariamente genios de las computadoras. Tienen conocimientos de lenguaje ensamblador y de cómo funciona internamente la computadora. De hecho resulta bastante más difícil hacer un programa "en regla" como sería un sistema de facturación en donde hay que tener muchísimas más cosas en cuenta que en un simple virus que aunque esté mal programado sería suficiente para molestar al usuario.

En un principio estos programas eran diseñados casi exclusivamente por los hackers y crackers que tenían su auge en los Estados Unidos y que hacían temblar a las compañías con solo pensar en sus actividades. Tal vez esas personas lo hacían con la necesidad de demostrar su creatividad y su dominio de las computadoras, por diversión o como una forma de manifestar su repudio a la sociedad que los oprimía. Hoy en día, resultan un buen medio para el sabotaje corporativo, espionaje industrial y daños a material de una empresa en particular.

- Un poco de historia

Los virus tienen la misma edad que las computadoras. Ya en 1949 John Von Neumann, describió programas que se reproducen a sí mismos en su libro "Teoría y Organización de Autómatas Complicados". Es hasta mucho después que se les comienza a llamar como virus. La característica de auto-reproducción y mutación de estos programas, que las hace parecidas a las de los virus biológicos, parece ser el origen del nombre con que hoy los conocemos.

Antes de la explosión de la micro computación se decía muy poco de ellos. Por un lado, la computación era secreto de unos pocos. Por otro lado, las entidades gubernamentales, científicas o militares, que vieron sus equipos atacados por virus, se quedaron muy calladas, para no demostrar la debilidad de sus sistemas de seguridad, que costaron millones, al bolsillo de los contribuyentes. Las empresa privadas como Bancos, o grandes corporaciones, tampoco podían decir nada, para no perder la confianza de sus clientes o accionistas. Lo que se sabe de los virus desde 1949 hasta 1989, es muy poco.

Se reconoce como antecedente de los virus actuales, un juego creado por programadores de la empresa AT&T, que desarrollaron la primera versión del sistema operativo Unix en los años 60. Para entretenerse, y como parte de sus investigaciones, desarrollaron un juego llamado "Core Wars", que tenía la capacidad de reproducirse cada vez que se ejecutaba. Este programa tenía instrucciones destinadas a destruir la memoria del rival o impedir su correcto funcionamiento. Al mismo tiempo, desarrollaron un programa llamado "Reeper", que destruía las copias hechas por Core Wars. Un antivirus o antibiótico, como hoy se los conoce. Conscientes de lo peligroso del juego, decidieron mantenerlo en secreto, y no hablar más del tema. No se sabe si esta decisión fue por iniciativa propia, o por órdenes superiores.

En el año 1983, el Dr. Ken Thomson, uno de los programadores de AT&T, que trabajó en la creación de "Core Wars", rompe el silencio acordado, y da a conocer la existencia del programa, con detalles de su estructura.

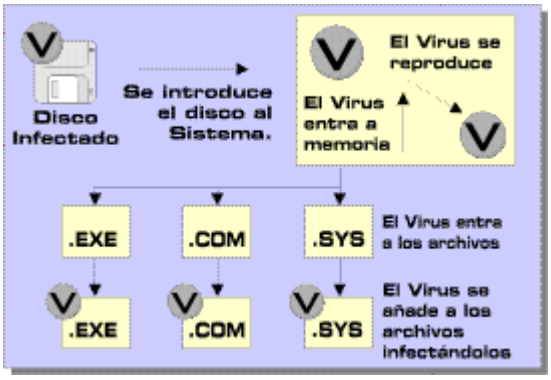
La Revista Scientific American a comienzos de 1984, publica la información completa sobre esos programas, con guías para la creación de virus. Es el punto de partida de la vida pública de estos programas, y naturalmente de su difusión sin control, en las computadoras personales.

Por esa misma fecha, 1984, el Dr. Fred Cohen hace una demostración en la Universidad de California, presentando un virus informático residente en una PC. Al Dr. Cohen se le conoce hoy día, como "el padre de los virus". Paralelamente aparece en muchas PCs un virus, con un nombre similar a Core Wars, escrito en Small-C por un tal Kevin Bjorke, que luego lo cede a dominio público. ¡La cosa comienza a ponerse caliente!

El primer virus destructor y dañino plenamente identificado que infecta muchas PC's aparece en 1986. Fue creado en la ciudad de Lahore, Paquistán, y se le conoce con el nombre de BRAIN. Sus autores vendían copias pirateadas de programas comerciales como Lotus, Supercalc o Wordstar, por suma bajísimas. Los turistas que visitaban Paquistán, compraban esas copias y las llevaban de vuelta a los EE.UU. Las copias pirateadas llevaban un virus. Fue así, como infectaron mas de 20,000 computadoras. Los códigos del virus Brain fueron alterados en los EE.UU., por otros programadores, dando origen a muchas versiones de ese virus, cada una de ellas peor que la precedente. Hasta la fecha nadie estaba tomando en serio el fenómeno, que comenzaba a ser bastante molesto y peligroso.

Funcionamiento de los virus

Los virus informáticos están hechos en Assembler, un lenguaje de programación de bajo nivel. Las instrucciones compiladas por Assembler trabajan directamente sobre el hardware, esto significa que no es necesario ningún software intermedio –según el esquema de capas entre usuario y hardware- para correr un programa en Assembler (opuesto a la necesidad de Visual Basic de que Windows 9x lo secunde). No solo vamos a poder realizar las cosas típicas de un lenguaje de alto nivel, sino que también vamos a tener control de cómo se hacen. Para dar una idea de lo poderoso que puede ser este lenguaje, el sistema operativo Unix está programado en C y las rutinas que necesitan tener mayor profundidad para el control del hardware están hechas en Assembler. Por ejemplo: los drivers que se encargan de manejar los dispositivos y algunas rutinas referidas al control de procesos en memoria.



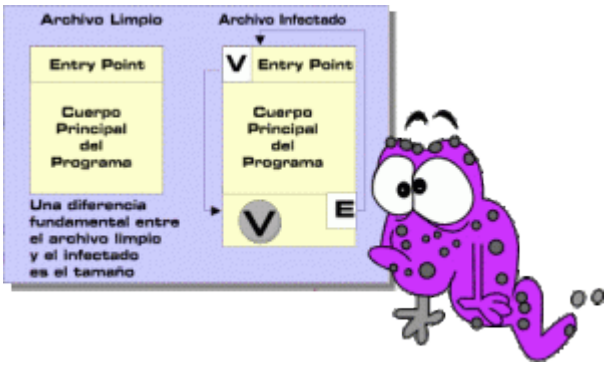
Sabiendo esto, el virus puede tener control total de la máquina -al igual que lo hace el SO- si logra cargarse antes que nadie. La necesidad de tener que "asociarse" a una entidad ejecutable viene de que, como cualquier otro programa de computadora, necesita ser ejecutado y teniendo en cuenta que ningún usuario en su sano juicio lo hará, se vale de otros métodos furtivos. Ahora que marcamos la importancia para un virus el ser ejecutado, podemos decir que un virus puede encontrarse en una computadora sin haber infectado realmente algo. Es el caso de personas que pueden coleccionar virus en archivos comprimidos o encriptados.

Normalmente este tipo de programas se pega a alguna entidad ejecutable que le facilitará la subida a memoria principal y la posterior ejecución (métodos de infección). Como entidades ejecutables podemos reconocer a los sectores de arranque de los discos de almacenamiento magnéticos, ópticos o magneto-ópticos (MBR, BR), los archivos ejecutables de DOSs (.exe, .com, entre otros), las

librerías o módulos de programas (.dll, .lib, .ovl, .bin, .ovr). Los sectores de arranque son fundamentales para garantizar que el virus será cargado cada vez que se encienda la computadora.

Según la secuencia de booteo de las PCs, el microprocesador tiene seteada de fábrica la dirección de donde puede obtener la primer instrucción a ejecutar. Esta dirección apunta a una celda de la memoria ROM donde se encuentra la subrutina POST (Power On Self Test), encargada de varias verificaciones y de comparar el registro de la memoria CMOS con el hardware instalado (función checksum). En este punto sería imposible que el virus logre cargarse ya que la memoria ROM viene grabada de fábrica y no puede modificarse (hoy en día las memorias Flash-ROM podrían contradecir esto último).

Luego, el POST pasa el control a otra subrutina de la ROM BIOS llamada "bootstrap ROM" que copia el MBR (Master Boot Record) en memoria RAM. El MBR contiene la información de la tabla de particiones, para conocer las delimitaciones de cada partición, su tamaño y cuál es la partición activa desde donde se cargará el SO. Vemos que en este punto el procesador empieza a ejecutar de la memoria RAM, dando la posibilidad a que un virus tome partida. Hasta acá el SO todavía no fue cargado y en consecuencia tampoco el antivirus. El accionar típico del virus sería copiar el MBR en un sector alternativo y tomar su posición. Así, cada vez que se inicie el sistema el virus logrará cargarse antes que el SO y luego, respetando su deseo por permanecer oculto hará ejecutar las instrucciones del MBR.



Clasificación de los virus

La clasificación correcta de los virus siempre resulta variada según a quien se le pregunte. Podemos agruparlos por la entidad que parasitan (sectores de arranque o archivos ejecutables), por su grado de dispersión a nivel mundial, por su comportamiento, por su agresividad, por sus técnicas de ataque o por como se oculta, etc. Nuestra clasificación muestra como actúa cada uno de los diferentes tipos según su comportamiento. En algunos casos un virus puede incluirse en más de un tipo (un multipartito resulta ser sigiloso).

- Caballos de Troya

Los caballos de troya no llegan a ser realmente virus porque no tienen la capacidad de autoreproducirse. Se esconden dentro del código de archivos ejecutables y no ejecutables pasando inadvertidos por los controles de muchos antivirus. Posee subrutinas que permitirán que se ejecute en el momento oportuno. Existen diferentes caballos de troya que se centrarán en distintos puntos de ataque. Su objetivo será el de robar las contraseñas que el usuario tenga en sus archivos o las contraseñas para el acceso a redes, incluyendo a Internet. Después de que el virus obtenga la contraseña que deseaba, la enviará por correo electrónico a la dirección que tenga registrada como la de la persona que lo envió a realizar esa tarea. Hoy en día se usan estos métodos para el robo de contraseñas para el acceso a Internet de usuarios hogareños. Un caballo de troya que infecta la red

de una empresa representa un gran riesgo para la seguridad, ya que está facilitando enormemente el acceso de los intrusos. Muchos caballos de troya utilizados para espionaje industrial están programados para autodestruirse una vez que cumplan el objetivo para el que fueron programados, destruyendo toda la evidencia.

- Camaleones

Son una variedad de similar a los Caballos de Troya, pero actúan como otros programas comerciales, en los que el usuario confía, mientras que en realidad están haciendo algún tipo de daño. Cuando están correctamente programados, los camaleones pueden realizar todas las funciones de los programas legítimos a los que sustituyen (actúan como programas de demostración de productos, los cuales son simulaciones de programas reales). Un software camaleón podría, por ejemplo, emular un programa de acceso a sistemas remotos (rlogin, telnet) realizando todas las acciones que ellos realizan, pero como tarea adicional (y oculta a los usuarios) va almacenando en algún archivo los diferentes logins y passwords para que posteriormente puedan ser recuperados y utilizados ilegalmente por el creador del virus camaleón.

- Virus polimorfos o mutantes

Los virus polimorfos poseen la capacidad de encriptar el cuerpo del virus para que no pueda ser detectado fácilmente por un antivirus. Solo deja disponibles unas cuantas rutinas que se encargaran de desencriptar el virus para poder propagarse. Una vez desencriptado el virus intentará alojarse en algún archivo de la computadora.

En este punto tenemos un virus que presenta otra forma distinta a la primera, su modo desencriptado, en el que puede infectar y hacer de las suyas libremente. Pero para que el virus presente su característica de cambio de formas debe poseer algunas rutinas especiales. Si mantuviera siempre su estructura, esté encriptado o no, cualquier antivirus podría reconocer ese patrón.

Para eso incluye un generador de códigos al que se conoce como engine o motor de mutación. Este engine utiliza un generador numérico aleatorio que, combinado con un algoritmo matemático, modifica la firma del virus. Gracias a este engine de mutación el virus podrá crear una rutina de desencripción que será diferente cada vez que se ejecute.

Los métodos básicos de detección no pueden dar con este tipo de virus. Muchas veces para virus polimorfos particulares existen programas que se dedican especialmente a localizarlos y eliminarlos. Algunos softwares que se pueden baja gratuitamente de Internet se dedican solamente a erradicar los últimos virus que han aparecido y que también son los más peligrosos. No los fabrican empresas comerciales sino grupos de hackers que quieren protegerse de otros grupos opuestos. En este ambiente el presentar este tipo de soluciones es muchas veces una forma de demostrar quien es superior o quien domina mejor las técnicas de programación.

Las últimas versiones de los programas antivirus ya cuentan con detectores de este tipo de virus.

- Virus sigiloso o stealth

El virus sigiloso posee un módulo de defensa bastante sofisticado. Este intentará permanecer oculto tapando todas las modificaciones que haga y observando cómo el sistema operativo trabaja con los archivos y con el sector de booteo. Subvirtiendo algunas líneas de código el virus logra apuntar el flujo de ejecución hacia donde se encuentra la zona que infectada.

Es difícil que un antivirus se de cuenta de estas modificaciones por lo que será imperativo que el virus se encuentre ejecutándose en memoria en el momento justo en que el antivirus corre. Los antivirus de hoy en día cuentan con la técnica de verificación de integridad para detectar los cambios realizados en las entidades ejecutables.

El virus Brain de MS-DOS es un ejemplo de este tipo de virus. Se aloja en el sector de arranque de los disquetes e intercepta cualquier operación de entrada / salida que se intente hacer a esa zona. Una vez hecho esto redirigía la operación a otra zona del disquete donde había copiado previamente el verdadero sector de booteo.

Este tipo de virus también tiene la capacidad de engañar al sistema operativo. Un virus se adiciona a un archivo y en consecuencia, el tamaño de este aumenta. Está es una clara señal de que un virus lo infectó. La técnica stealth de ocultamiento de tamaño captura las interrupciones del sistema operativo que solicitan ver los atributos del archivo y, el virus le devuelve la información que poseía el archivo antes de ser infectado y no las reales. Algo similar pasa con la técnica stealth de lectura. Cuando el SO solicita leer una posición del archivo, el virus devuelve los valores que debería tener ahí y no los que tiene actualmente.

Este tipo de virus es muy fácil de vencer. La mayoría de los programas antivirus estándar los detectan y eliminan.

- Virus lentos

Los virus de tipo lento hacen honor a su nombre infectando solamente los archivos que el usuario hace ejecutar por el SO, simplemente siguen la corriente y aprovechan cada una de las cosas que se ejecutan.

Por ejemplo, un virus lento únicamente podrá infectar el sector de arranque de un disquete cuando se use el comando FORMAT o SYS para escribir algo en dicho sector. De los archivos que pretende infectar realiza una copia que infecta, dejando al original intacto.

Su eliminación resulta bastante complicada. Cuando el verificador de integridad encuentra nuevos archivos avisa al usuario, que por lo general no presta demasiada atención y decide agregarlo al registro del verificador. Así, esa técnica resultaría inútil.

La mayoría de las herramientas creadas para luchar contra este tipo de virus son programas residentes en memoria que vigilan constantemente la creación de cualquier archivo y validan cada uno de los pasos que se dan en dicho proceso. Otro método es el que se conoce como Decoy launching. Se crean varios archivos .EXE y .COM cuyo contenido conoce el antivirus. Los ejecuta y revisa para ver si se han modificado sin su conocimiento.

- Retro-virus o Virus antivirus

Un retro-virus intenta como método de defensa atacar directamente al programa antivirus incluido en la computadora.

Para los programadores de virus esta no es una información difícil de obtener ya que pueden conseguir cualquier copia de antivirus que hay en el mercado. Con un poco de tiempo pueden descubrir cuáles son los puntos débiles del programa y buscar una buena forma de aprovecharse de ello.

Generalmente los retro-virus buscan el archivo de definición de virus y lo eliminan, imposibilitando al antivirus la identificación de sus enemigos. Suelen hacer lo mismo con el registro del comprobador de integridad.

Otros retro-virus detectan al programa antivirus en memoria y tratan de ocultarse o inician una rutina destructiva antes de que el antivirus logre encontrarlos. Algunos incluso modifican el entorno de tal manera que termina por afectar el funcionamiento del antivirus.

- Virus multipartitos

Los virus multipartitos atacan a los sectores de arranque y a los ficheros ejecutables. Su nombre está dado porque infectan las computadoras de varias formas. No se limitan a infectar un tipo de archivo ni una zona de la unidad de disco rígido. Cuando se ejecuta una aplicación infectada con uno de estos virus, éste infecta el sector de arranque. La próxima vez que arranque la computadora, el virus atacará a cualquier programa que se ejecute.

- Virus voraces

Estos virus alteran el contenido de los archivos de forma indiscriminada. Generalmente uno de estos virus sustituirá el programa ejecutable por su propio código. Son muy peligrosos porque se dedican a destruir completamente los datos que puedan encontrar.

- Bombas de tiempo

Son virus convencionales y pueden tener una o más de las características de los demás tipos de virus pero la diferencia está dada por el trigger de su módulo de ataque que se disparará en una fecha determinada. No siempre pretenden crear un daño específico. Por lo general muestran mensajes en la pantalla en alguna fecha que representa un evento importante para el programador. El virus Michel Angelo sí causa un daño grande eliminando toda la información de la tabla de particiones el día 6 de marzo.

- Conejo

Cuando los ordenadores de tipo medio estaban extendidos especialmente en ambientes universitarios, funcionaban como multiusuario, múltiples usuarios se conectaban simultáneamente a ellos mediante terminales con un nivel de prioridad. El ordenador ejecutaba los programas de cada usuario dependiendo de su prioridad y tiempo de espera. Si se estaba ejecutando un programa y llegaba otro de prioridad superior, atendía al recién llegado y al acabar continuaba con lo que hacia con anterioridad. Como por regla general, los estudiantes tenían prioridad mínima, a alguno de ellos se le ocurrió la idea de crear este virus. El programa se colocaba en la cola de espera y cuando llegaba su turno se ejecutaba haciendo una copia de sí mismo, agregándola también en la cola de espera. Los procesos a ser ejecutados iban multiplicándose hasta consumir toda la memoria de la computadora central interrumpiendo todos los procesamientos.

Macro-virus

Los macro-virus representan una de las amenazas más importantes para una red. Actualmente son los virus que más se están extendiendo a través de Internet. Representan una amenaza tanto para las redes informáticas como para los ordenadores independientes. Su máximo peligro está en que son completamente independientes del sistema operativo o de la plataforma. Es más, ni siquiera son programas ejecutables.

Los macro-virus son pequeños programas escritos en el lenguaje propio (conocido como lenguaje script o macro-lenguaje) propio de un programa. Así nos podemos encontrar con macro-virus para editores de texto, hojas de cálculo y utilidades especializadas en la manipulación de imágenes.

En Octubre de 1996 había menos de 100 tipos de macro-virus. En Mayo de 1997 el número había aumentado a 700.

Sus autores los escriben para que se extiendan dentro de los documentos que crea el programa infectado. De esta forma se pueden propagar a otros ordenadores siempre que los usuarios intercambien documentos. Este tipo de virus alteran de tal forma la información de los documentos infectados que su recuperación resulta imposible. Tan solo se ejecutan en aquellas plataformas que tengan la aplicación para la que fueron creados y que comprenda el lenguaje con el que fueron programados. Este método hace que este tipo de virus no dependa de ningún sistema operativo.

El lenguaje de programación interno de ciertas aplicaciones se ha convertido en una poderosa herramienta de trabajo. Pueden borrar archivos, modificar sus nombres y (como no) modificar el contenido de los ficheros ya existentes. Los macro-virus escritos en dichos lenguajes pueden efectuar las mismas acciones.

Al día de hoy, la mayoría de virus conocidos se han escrito en WordBasic de Microsoft, o incluso en la última versión de Visual Basic para Aplicaciones (VBA), también de Microsoft. WordBasic es el lenguaje de programación interno de Word para Windows (utilizado a partir de la versión 6.0) y Word 6.0 para Macintosh. Como VBA se ejecuta cada vez que un usuario utiliza cualquier programa de Microsoft Office, los macro-virus escritos en dicho lenguaje de programación representan un riesgo muy serio. En otras palabras, un macro-virus escrito en VBA puede infectar un documento de Excel, de Access o de PowerPoint. Como estas aplicaciones adquieren más y más importancia cada día, la presencia de los macro-virus parece que está asegurada.

Taller:

1) Cuales son las principales características de los virus?

2) Cual es la causa más peligrosa que poseen los virus informáticos?

3) Cuando un virus se reproduce en un computador, cuales son los principales daños que ocasiona, ataca al hardware y al software ? porque y como lo hace

4) Quien es un hacker y un craker y que hacen con los virus?

5) Realiza una breve explicación sobre como funcionan los virus.

6) Describe como se clasifican los virus informáticos y nombra y describe algunos de ellos según la explicación?