4. Malware

3. Virus y Gusanos

3.1 Introducción

En la Real Academia nos encontramos con la siguiente definición del termino virus: “Programa introducido subrepticiamente en la memoria de un ordenador que, al activarse, destruye total o parcialmente la información almacenada”.

De una forma más coloquial y quizás más correcta podríamos decir que un virus informático es programa que se copia automáticamente (sin conocimiento ni permiso del usuario), ya sea por medios de almacenamiento o por Internet, y que tiene por objeto alterar el normal funcionamiento del ordenador, que puede ir desde una simple broma; acceso a tus datos confidenciales; uso de tu ordenador como una maquina zombie; borrado de los datos; etc.

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 grandes compañías. 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 virus puede ser o no, muy peligroso, pero independientemente de dicho grado, si el sistema a comprometer es crítico, un virus de bajo grado de peligrosidad podrá causar graves daños. Si por el contrario dicho virus es muy peligroso y afecta a una computadora familiar sus daños serán mínimos. Por ello desde el punto de vista de una empresa o gran corporación, un virus sea cual sea, debe ser considerado siempre como peligroso.

3.2 Características Comunes

- Dañino: Todo virus causa daño, ya sea de forma implícita, borrando archivos o modificando información, o bien disminuyendo el rendimiento del sistema. A pesar de esto, existen virus cuyo fin es simplemente algún tipo de broma.
- Autoreproductor: La característica que más diferencia a los virus es ésta, ya que ningún otro programa tiene la capacidad de autoreplicarse en el sistema.
- Subrepticio: Característica que le permite ocultarse al usuario mediante diferentes técnicas, como puede ser mostrarse como una imagen, incrustarse en librerías o en programas, …

3.3 Un Poco de Historia

Tras contrastar diferentes fuentes de información esta sería una breve cronología de la historia de los virus:

- 1939, el científico matemático John Louis Von Neumann, escribió "Teoría y organización de autómatas complejos", donde se mostraba que era posible desarrollar programas que tomasen el control de otros.
- 1949 – 1950s en los laboratorios de la Bell Computer, subsidiaria de la AT&T, 3 jóvenes programadores: Robert Thomas Morris, Douglas McIlory y Victor Vysottsky, desarrollaron inspirados en la teoría de John Louis Von Neumann un “juego” llamado CoreWar. Los contenedores del CoreWar ejecutaban programas que iban poco a poco disminuyendo la memoria del computador. Ganaría este “juego” el que consiguiera eliminarlos totalmente. El conocimiento de la existencia de CoreWar era muy restringido.
- 1972, aparece Creeper desarrollado por Robert Thomas Morris que atacaba a las conocidas IBM 360. Simplemente mostraba de forma periódica el siguiente mensaje: "I'm a creeper... catch me if you can!" (soy una enredadera, cójanme si pueden). Fue aquí donde podríamos decir que apareció el primer antivirus conocido como Reaper (segadora) el cual eliminaba a Creeper.
- 1975, John Brunner concibe la idea de un “gusano” informático que crece por las redes.
- 1984, Fred Cohen en su tesis acuña el término “virus informático”. Fue en este año donde se empezó a conocer el verdadero peligro de los virus, ya que los usuarios del BIX BBS, un foro de debates de la ahora revista BYTE, avisaron de la presencia y propagación de una serie de programas que habían infectado sus computadoras.
- 1986, aparece lo que se conoce como el primer virus informático, Brain, atribuido a los hermanos pakistaníes.
- 1987, el gusano Christmas tree satura la red de IBM a nivel mundial.
- 1988, Robert Tappan Morris, hijo de uno de los precursores de los virus, difunde un virus a través de ArpaNet, (precursora de Internet) infectando a unos 6,000 servidores.
- 1989, el virus Dark Avenger también conocido como "vengador de la oscuridad", se propaga por Europa y Estados Unidos. Sobre dicho virus se han escrito multitud de artículos e incluso un libro ya que se diferenciaba de los demás en su ingeniosa programación y su rápida infección.
- 1990, Mark Washburn crea “1260”, el primer virus polimórfico, que muta en cada infección.
- 1992, aparece el conocido virus Michelangelo sobre el cual se crea una gran alarma sobre sus daños y amplia propagación, aunque finalmente fueron pocos los ordenadores infectados
- 1994, Good Times, el primer virus broma.
- 1995, aparece Concept con el cual comienzan los virus de macro. Y es en este mismo año cuando aparece el primer virus escrito específicamente para Windows 95.
- 1997, comienza la difusión a través de internet del virus macro que infecta hojas de cálculo, denominado Laroux.
- 1998, aparecen un nuevo tipo de virus macro que ataca a las bases de datos en MS-Access.
- Llega CIH o Chernobyl que será el primer virus que realmente afecta al hardware del ordenador.

- 1999, cuando comienzan a propagarse por Internet los virus anexados a mensajes de correo como puede ser Melissa, BubbleBoy, etc. Este último (BubbleBoy) infectaba el ordenador con simplemente mostrar el mensaje (en HTML).
- 2000, se conoce la existencia de VBS/Stages.SHS, primer virus oculto dentro del Shell de la extensión .SHS. Aparece el primer virus para Palm.
- 2001, el virus Nimda atacó a millones de computadoras, a pocos días del ataque a las Torres Gemelas de la isla de Manhattan.
- Actualmente, existen multitud de técnicas mucho más sofisticadas y conocidas, lo que permite que se hagan mayor cantidad de virus (13 diarios según Panda Software) y sean más complejos. De esta forma aparecen virus como MyDoom o Netsky. A pesar de esto no solo la sofisticación de los virus ha aumentado la infección de equipos sino también la "Ingeniería Social" y la, a veces increíble, ingenuidad de usuarios y administradores que facilitan bastante la labor de los virus. Aun con todos los avances que se están haciendo en la actualidad para mejorar la seguridad de los sistemas, no podemos decir que éstos nos reporten la seguridad necesaria. Por ejemplo el último Sistema Operativo de Microsoft, MS Windows Windows 8.1 también es vulnerable a los virus informáticos y exploits.

3.4 Funcionamiento

Se podría decir que la mayor parte de los virus estaban y quizás estén programados en Ensamblador, lenguaje de bajo nivel que permite trabajar directamente sobre el hardware, sin tener que interactuar con el Sistema Operativo. Actualmente no todos los virus se desarrollan en Ensamblador, sino que se utilizan todo tipo de lenguajes de alto nivel, que no permiten realizar todas las acciones que permite el ensamblador, pero sí facilitan mucho su codificación.

Lo que tratan los virus es de ser ejecutados para con ello poder actuar y replicarse, ya que ningún usuario ejecutaría un virus de forma intencionada. Los virus deben ocultarse, ya sea tras otros programas "benignos" o bien utilizando otras técnicas. Por norma general, un virus intentará cargarse en la memoria para poder ejecutarse, y controlar las demás operaciones del sistema.

Como formas más comunes de infección de los virus podríamos tener las siguientes:

En el caso de que un virus tratara de cargarse en el arranque, intentaría dos cosas.

- Primero si existe la posibilidad de cargarse en la CMOS, lo cual sería posible si la memoria no es ROM, sino que es Flash-ROM.
- Si esto no es posible, intentará cargarse en el sector de arranque. El sistema cargará el MBR en memoria RAM que le indicará las particiones, el tamaño, cual es la activa (en la que se encuentra el S.O.) para empezar a ejecutar las instrucciones. Es aquí donde el virus deberá cargar el MBR en un sector alternativo y tomar su posición de tal forma que cada vez que se arranque el sistema el virus se cargará. Así, ya que el antivirus se carga tras el S.O. la carga del virus en memoria no será detectada.

Por otro lado, si virus infecta un archivo ejecutable .EXE, intentará rastrear en el código los puntos de entrada y salida del programa. Teniendo conocimiento de estos dos puntos, el virus se incrustará antes de cada uno de ellos, asegurándose así de que cada vez que dicho programa se ejecute, el virus será ejecutado. Una vez esté en ejecución decidirá cuál es la siguiente acción a llevar a cabo, ya sea replicarse introduciéndose en otros programas que estén en memoria en ese momento, ocultarse si detecta antivirus, etc.

Tanto virus como gusanos, troyanos,…, tienen unos objetivos comunes. Ocultarse al usuario; reproducirse ya sea en otros ficheros o en el caso de los gusanos autoenviarse; y finalmente llevar a cabo la acción para la cual ha sido programado, destrucción de datos, obtención de datos personales, control remoto de la máquina.

Para conseguir dichos objetivos podríamos decir que su estructura se divide en tres módulos principales:

- Módulo de reproducción: Es la parte encargada de gestionar las rutinas gracias a las cuales el virus garantiza su replicación a través de ficheros ejecutables. Dichos ficheros ejecutables cuando sean trasladados a otras computadoras provocarán también la dispersión del virus.
- Módulo de ataque: Módulo que contiene las rutinas de daño adicional o implícito. Este podrá ser disparado por distintos eventos del sistema: una fecha, hora, el encontrar un archivo específico (COMMAND.COM), …
- Módulo de defensa: Módulo encargado de proteger el código del virus. Sus rutinas se ocuparán de disminuir los síntomas que puedan provocar su detección por parte de los antivirus. Utiliza para ello técnicas que pueden ir desde una simple encriptación, a técnicas muy sofisticadas.

3.5 Tipos de Virus

Existen diversas clasificaciones de los virus. Cada una de ellas clasifica según una característica, ya sea dependiendo de la técnica usada, su origen, lugar donde se esconde, ficheros a los que ataca, daños que produce, etc. No se puede considerar que ninguna de estas clasificaciones sea errónea, ya que muchas de ellas tienen muchos puntos en común. A pesar de que todos se pueden considerar virus, los hemos separado en distintas "categorías":

- Virus residentes: Este tipo de virus se oculta en la memoria principal del sistema (RAM) de tal manera que pueden controlar todas las operaciones realizadas en el Sistema Operativo, pudiendo así infectar todos los archivos que deseen. Normalmente sus creadores le indican una serie de condiciones (fecha, hora,…) bajo las cuales llevará a cabo la acción para la cual fue programado. Ejemplos de este tipo de virus son: Randex, CMJ, Meve.
- Virus de acción directa: Estos virus no se ocultan en la memoria. Su funcionamiento consiste en que una vez cumplida una determinada condición, actuarán buscando los ficheros a infectar dentro de su mismo directorio o en aquellos directorios que se encuentren especificados en la línea PATH del fichero AUTOEXEC.BAT. Este tipo de virus se puede desinfectar totalmente y recuperar los archivos infectados.
- Virus de sobreescritura: Se escriben dentro del contenido del fichero infectado, haciendo que pueda quedar inservible. Se ocultan por encima del fichero de tal forma que la única manera de desinfectarlo es borrar dicho archivo, perdiendo así su contenido. Algún ejemplo: Trj.Reboot, Trivial.88.D.
- Virus de boot o arranque: Son aquellos virus que no infectan a ficheros directamente, sino que actúan sobre los discos que los contienen, más concretamente al sector de arranque de dichos discos, de tal manera que si un ordenador se arranca con un disquete infectado, el sector de arranque del disco duro se infectará. A partir de este momento, se infectarán todas las unidades de disco del sistema. Algún ejemplo de virus de boot: Polyboot.B.
- Retrovirus: Un Retrovirus es un tipo de virus cuyo objetivo principal es atacar a los antivirus, ya sea de una forma genérica o un ataque a un antivirus específico. En sí mismo no produce ningún daño al sistema sino que simplemente permiten la entrada de otros virus destructivos que lo acompañan en el código.
- Virus multipartites: Tipo de virus muy complejo que ataca mediante el uso de diferentes técnicas, infectando tanto programas, macros, discos, etc. Sus efectos suelen ser bastante dañinos. Por ejemplo el virus Ywinz.
- Virus de macro: Se caracterizan por infectar los ficheros que sean creados con aplicaciones que usen macros (Word, Excel, PowerPoint, Corel Draw, …). Las macros son pequeños programas asociados a los ficheros cuya función es automatizar conjuntos de operaciones complejas. Esto permite que en un documento de texto al existir un pequeño programa en su interior, dicho programa y en consecuencia dicho documento pueda ser infectado. Al abrirse, guardarse, realizar algún tipo de operación, puede que alguna de las macros se ejecute, en cuyo caso si contiene virus, se ejecutará. La mayoría de las aplicaciones que utilizan macros están protegidas, pero aun así existen virus que esquivan dichas protecciones. Estos son algunos ejemplos: Relax, Melissa.A, Bablas.
- Virus de enlace o directorio: La característica principal de este tipo de virus reside en modificar la dirección que indica donde se almacena un fichero. Así, cuando queramos ejecutar un fichero, si a dicho fichero se le ha modificado la dirección se ejecutará el virus produciéndose la infección. Los ficheros se ubican en determinadas direcciones

(compuestas básicamente por unidad de disco y directorio), que el sistema operativo conoce para poder localizarlos y trabajar con ellos. Una vez producida la infección, resulta imposible localizar y trabajar con los ficheros originales.

- Virus de FAT: Tipo de virus muy dañino ya que atacan a la FAT (Tabla de Asignación de Ficheros), que es la encargada de enlazar la información del disco. Al atacar dicha tabla, impiden el acceso a ciertos ficheros o directorios críticos del sistema, provocando pérdidas de la información contenida en dichos ficheros o directorios.
- Virus de fichero: Infectan programas o ficheros ejecutables, por lo que al ejecutarse dicho fichero el virus se activará y llevará a cabo las acciones para las cuales ha sido creado. La mayoría de los virus existentes son de este tipo.
- Virus de compañía: Clase de virus de fichero que como su nombre indica acompañan a otros ficheros existentes antes de llegar al sistema. Pueden ser residentes o de acción directa. Su modo de actuar consiste en o bien esperar ocultos en la memoria hasta que se produzca la ejecución de algún programa o bien actuar directamente haciendo copias de sí mismo. Como ejemplos citamos el virus Stator, Terrax.1069.
- De Active Agents y Java Applets: Programas que se ejecutan y se graban en el disco duro cuando el usuario está en una página web que los usa. Hoy en día cada vez que se necesita ejecutar o guardar cualquiera de estos programas se le pide la autorización al usuario, el cual será responsable de los posibles daños que causen.
- De HTML: Son más eficaces que los anteriores ya que simplemente con acceder al contenido de la página web el usuario puede ser infectado, ya que el código dañino se encuentra en el código HTML de dicha web. Este tipo de virus son desarrollados en Visual Basic Script.
- Virus lentos: Como su nombre indica, estos virus infectan de forma lenta. Únicamente infectarán aquellos archivos que el usuario hará ejecutar por el Sistema Operativo. Son virus muy difíciles de eliminar ya que cuando se le muestra un aviso al usuario, éste no presta atención ya que en ese determinado momento estaba realizando alguna acción de la cual ya esperaba algún aviso. A pesar de esto con este tipo de virus sí son eficaces los demonios de protección que vigilarán cualquier creación, borrado,…
- Virus voraces: Son altamente destructivos ya que se dedican a destruir completamente todos los datos a los que pueden acceder.
- Sigilosos o Stealth: Son virus que poseen módulos de defensa muy sofisticados. Se encuentran en el sector de arranque y su modo de funcionamiento consiste en engañar al S.O. a la hora de verificar el tamaño, fecha, nombre,…, de los ficheros.
- Reproductores o conejos: Virus cuya característica principal es reproducirse constantemente hasta terminar ya sea con la capacidad total del disco duro o con la capacidad de la memoria principal. Esto lo consiguen simplemente creando clones de sí mismos que harán lo mismo que ellos, reproducirse.
- Virus encriptados: Más que un tipo de virus, son una técnica que usan diversos virus, los cuales se descifran ellos mismos para poderse ejecutar y acto seguido se vuelven a cifrar. De esta manera lo que intentan es evitar o dificultar ser detectados por los antivirus.
- Virus polimórficos: La diferencia esencial con los virus encriptados reside en que éstos se cifran/descifran de forma distinta en cada una de sus infecciones. Así consiguen impedir que los antivirus los localicen a través de la búsqueda de cadenas o firmas. Por esta característica, este tipo de virus son los más difíciles de detectarse. Como ejemplos: Elkern, Satan Bug, Tuareg.

- Virus falsos: Hoy en día han surgido ciertos mensajes de correo electrónico, o programas, que pueden ser confundidos con virus. El principal tipo son los hoaxes, emails engañosos que pretenden alarmar sobre supuestos virus. Tratan de engañar al usuario proponiendo una serie de acciones a realizar para eliminar dicho virus que en realidad no existe. Lo más probable es que dichas acciones sean dañinas.
- Gusanos (Worms): Pueden no ser considerados como virus, ya que para replicarse no necesitan infectar otros ficheros. Los gusanos realizarán una serie de copias de sí mismos (sin tener que infectar ningún otro fichero) a la máxima velocidad posible y enviándose a través de la red. Debido a esa replicación a alta velocidad pueden llegar a saturar la red a través de la que se propagan. Los canales más típicos de infección son el Chat, correo electrónico, … Algún que otro ejemplo de gusano podrían ser los siguientes: PSWBugbear.B, Lovgate.F, Trile.C, Sobig.D, Mapson.

3.6 Métodos de Infección

A la hora de realizar la infección se pueden utilizar diferentes técnicas. Algunas podrían ser las siguientes:

- Añadidura o empalme: Consiste en agregar al final del archivo ejecutable el código del virus, para que así una vez se ejecute el archivo, el control pase primeramente al virus y tras ejecutar la acción que desee, volverá al programa haciendo que funcione de manera normal. El inconveniente de esta técnica es que el tamaño del archivo será mayor que el original haciendo que sea más fácil su detección.
- Inserción: No es una técnica muy usada por los programadores de virus ya que requiere técnicas de programación avanzadas. El motivo es que este método consiste en insertar el código del virus en zonas de código no usadas dentro del programa infectado. Así lo que se consigue es que el tamaño del archivo no varíe, pero el detectar las zonas de código en donde puede ser insertado el virus es complejo.
- Reorientación: Es una variante del método de inserción. Consiste en introducir el código del virus en zonas del disco que estén marcadas como defectuosas o en archivos ocultos del sistema. Al ejecutarse introducen el código en los archivos ejecutables infectados. La ventaja principal es que al no estar insertado en el archivo, su tamaño puede ser mayor con lo que podría tener una mayor funcionalidad. Como inconveniente se encuentra su fácil eliminación ya que bastaría con eliminar archivos ocultos sospechosos o con sobrescribir las zonas del disco marcadas como defectuosas.
- Polimorfismo: Es el método más avanzado de contagio. Consiste en insertar el código del virus en un ejecutable al igual que el método de añadidura o empalme, pero para evitar que el tamaño del mismo aumente lo que realiza es una compactación del propio código del virus y del archivo infectado, haciendo que entre ambos el tamaño del archivo no aumente. Una vez se ejecuta el archivo, el virus actúa descompactando en memoria las partes del código que había compactado anteriormente. Esta técnica se podría mejorar usando métodos de encriptación para disfrazar el código del virus.
- Sustitución: Es el método más primitivo. Consiste en sustituir el código del archivo infectado por el código del virus. Cuando se ejecuta, actúa únicamente el código del virus, infectando o eliminando otros archivos y terminando la ejecución del programa mostrando algún tipo de mensaje de error. La ventaja de esta técnica es que cada vez que se ejecuta se realizan “copias” del virus en otros archivos.
- Tunneling: Técnica compleja usada por programadores de virus y antivirus para evitar las rutinas al servicio de interrupción y conseguir control directo sobre ésta. El demonio de protección de los antivirus cuelga de todas las interrupciones usadas por los virus (INT 21, INT 13, a veces INT 25 Y 26), de tal forma que cuando un virus pretende escribir/abrir un ejecutable el antivirus recibe una alerta donde comprobará si es o no virus y le permite o no su acceso. Si la llamada no tiene peligro el módulo del antivirus llamará a la INT 21 original. De esta forma un virus con tunneling intentará obtener la dirección original de la INT 21 que está en algún lugar del módulo residente del antivirus. Si se consigue obtener esa dirección podrá acceder directamente a INT 21 sin necesidad de pasar por el antivirus. De esta forma le "pasará por debajo", lo "tuneleará".

3.7 ¿Cómo Detectar una Infección?

Detectar la posible presencia de un virus dentro de una computadora no es una tarea sencilla. Cada vez existen más, mejores y más conocidas técnicas de programación de virus, que dificultan la labor de detección de los mismos. A pesar de ello podríamos enumerar una serie de acciones o condicionantes que pueden indicar la presencia de virus, que serían las siguientes:

- Aplicaciones que ya en un principio eran lentas, de forma inexplicable, pasan a ser aún más lentas.
- El disco duro o dispositivos de almacenamiento realizan lecturas sin justificación aparente.
- Aumento del tamaño de los ficheros, ya que la mayoría de los virus cuando infectan lo que hacen es colocarse al inicio y al final del código de dichos ficheros ejecutables. Hoy en día puede que este no sea un indicador totalmente válido ya que los propios virus modificarán el tamaño para que el usuario vea el tamaño antiguo y no el real del fichero.
- Modificación de la fecha original de los archivos, aunque puede suceder como en el caso anterior, que el virus remodifique dicha fecha para que el usuario la vea de forma correcta.
- Ralentización a la hora de ejecutar comandos o acciones. Esta característica no es muy "visible" ya que el tiempo de cómputo del código del virus es inapreciable.
- Aparición de programas o procesos en memoria desconocidos para el usuario. Esto tiene fácil detección ya que los Sistemas Operativos poseen distintos comandos para poder ver qué programas y procesos se encuentran en memoria en un determinado momento.
- Modificación sin justificación del nombre de ciertos ficheros.
- Imposibilidad de acceder al disco duro o a alguna partición.
- Aparición en pantalla de objetos (imágenes, mensajes,…) desconocidos.
- Disminución del espacio libre del disco duro sin razón, ya que algunos virus se caracterizan por extenderse hasta ocupar todo el disco duro.
- Apagado o reinicio del sistema.
- Aparición o eliminación de ficheros.
- Dificultad a la hora de arrancar la computadora.
- Aparecen nuevas macros en los documentos (Word, Excel,…).
- Las opciones de ver macros aparecen desactivadas.
- Peticiones de contraseñas no configuradas de antemano por el usuario.

Todos estos no son más que posibles síntomas, lo que quiere decir que aunque se cumpla uno de ellos o incluso todos, no debe de significar que tengamos un virus en el sistema. Como en la mayoría de las cosas lo que se necesita principalmente es experiencia, que será la que nos indique si realmente o no estamos infectados.

En los usuarios domésticos la presencia de un antivirus podrá ser la mejor solución a la hora de detectar y desinfectar el sistema. En el ámbito empresarial en ocasiones es necesario eliminar de forma manual dichos virus, ya que muchos de los parches son publicados de forma tardía y la criticidad de los datos de estos sistemas es máxima.