Índice

Los virus

Los virus informáticos se llaman virus por compartir ciertas analogías entre los virus biológicos: mientras los biológicos son agentes externos que invaden células para alterar su información genética y reproducirse, los segundos son programas de infectar archivos de ordenadores, 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.

Los virus informáticos son programas de ordenador que se reproducen a sí mismos e interfieren con el *hardware* de un ordenador o con su SO, estos programas están diseñados para reproducirse y evitar su detección y como cualquier otro programa informático, un virus debe ser ejecutado para que funcione: es decir, el ordenador debe cargar el virus desde la memoria del ordenador y seguir sus instrucciones. Estas instrucciones se conocen como carga activa del virus. La carga activa puede trastornar o modificar archivos de datos, presentar un determinado mensaje o provocar fallos en el SO.

Existen algunos programas que, sin llegar a ser virus, ocasionan problemas al usuario. Estos no−virus carecen de por lo menos una de las tres características identificatorias de un virus (dañino, auto reproductor y subrepticio). Estos programas se dividen en tres categorías: caballos de Troya, bombas lógicas y gusanos. Un caballo de Troya aparenta ser algo interesante e inocuo, por ejemplo un juego, pero cuando se ejecuta puede tener efectos dañinos. Una bomba lógica libera su carga activa cuando se cumple una condición determinada, como cuando se alcanza una fecha u hora determinada o cuando se teclea una combinación de letras. Un gusano se limita a reproducirse, pero puede ocupar memoria del ordenador y hacer que sus procesos vayan más lentos.

Lo virus tienen el fin ineludible de causar daño en cualquiera de sus formas:

- Módulo de Reproducción
- Módulo de Ataque
- Módulo de Defensa

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 un ordenador a otro a través de algunos de estos archivos.

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 del ordenador indica 6 de Marzo. En estas condiciones la rutina actúa sobre la información del disco duro volviéndola inutilizable.

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.

Historia

En 1949, el matemático estadounidense de origen húngaro John von Neumann, en el Instituto de Estudios Avanzados de Princeton (Nueva Jersey), planteó la posibilidad teórica de que un programa informático se reprodujera. Esta teoría se comprobó experimentalmente en la década de 1950 en los Laboratorios Bell, donde se desarrolló un juego llamado **Core Wars** en el que los jugadores creaban minúsculos programas informáticos que atacaban y borraban el sistema del oponente e intentaban propagarse a través de él. 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.

En 1983, el ingeniero eléctrico estadounidense Fred Cohen, que entonces era estudiante universitario, acuñó el término de "virus" para describir un programa informático que se reproduce a sí mismo. En 1985 aparecieron los primeros caballos de Troya, disfrazados como un programa de mejora de gráficos llamado EGABTR y un juego llamado NUKE−LA. Pronto les siguió un sinnúmero de virus cada vez más complejos. El virus llamado Brain apareció en 1986, y en 1987 se había extendido por todo el mundo. En 1988 aparecieron dos nuevos virus: Stone, el primer virus de sector de arranque inicial, y el gusano de Internet, que cruzó Estados Unidos de un día para otro a través de una red informática. El virus Dark Avenger, el primer infector rápido, apareció en 1989, seguido por el primer virus polimórfico en 1990. En 1995 se creó el primer virus de lenguaje de macros, WinWord Concept.

Uno de los primeros registros que se tienen de una infección data del año 1987, cuando en la Universidad de De laware 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 boot de un disquete contenía un código ejecutable, y que dicho código se ejecutaba cada vez que la máquina se iniciaba 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 en ese equipo.

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 Pakistán, 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 muchísima gente alrededor del planeta, algunos de ellos dicen hacerlo por divertimento, otros quizás para probar sus habilidades.

Clasificación y funcionamiento

Existen ocho categorías de virus:

- Parásitos.
- Del sector de arranque inicial.

- Multipartitos.
- Acompañantes.
- De vínculo.
- Virus de macro.
- Virus e−mail.

Además de estos tipos también existen otros programas informáticos nocivos similares a los virus, pero que no cumplen ambos requisitos de reproducirse y eludir su detección. Estos programas se dividen en tres categorías:

- Caballos de Troya.
- Bombas lógicas.
- Gusanos.
- **Los virus parásitos.**

Infectan ficheros ejecutables o programas del ordenador. No modifican el contenido del programa huésped, pero se adhieren al huésped de tal forma que el código del virus se ejecuta en primer lugar. Estos virus pueden ser:

  - De acción directa.
  - Residentes.

Un virus de acción directa selecciona uno o más programas para infectar cada vez que se ejecuta.

Un virus residente se oculta en la memoria del ordenador e infecta un programa determinado, cuando se ejecuta dicho programa.

- **Los virus del sector de arranque inicial.**

Estos virus residen en la primera parte del disco duro o flexible, conocida como sector de arranque inicial, y sustituyen los programas que almacenan información sobre el contenido del disco o los programas que arrancan el ordenador. Estos virus suelen difundirse mediante el intercambio físico de discos flexibles.

- **Los virus multipartitos.**

Estos virus combinan las capacidades de los virus parásitos y de sector de arranque inicial, y pueden infectar tanto ficheros como sectores de arranque inicial.

- **Los virus acompañantes.**

Los virus acompañantes no modifican los ficheros, sino que crean un nuevo programa con el mismo nombre que un programa legítimo y engañan al SO para que lo ejecute.

- **Los virus de vínculo.**

Estos modifican la forma en que el SO encuentra los programas, y lo engañan para que ejecute primero el virus y luego el programa deseado. Un virus de vínculo puede infectar todo un directorio de un ordenador, y cualquier programa ejecutable al que se acceda en dicho directorio ejecutará el virus.

- **Virus de macro.**

Son un tipo de virus que ha cobrado mucha importancia en el mundo de la informática, lo curioso es que no se

transmiten por ficheros ejecutables, sino mediante los ficheros de extensión .DOC de Microsoft Word, estos virus son capaces de cambiar la configuración de Windows, borrar ficheros de nuestro disco duro, enviar por correo cualquier archivo sin que nos demos cuenta, e incluso infectar nuestro disco duro con un virus de fichero.

Estos virus no son muy complicados de diseñar como los virus convencionales. Están codificados en forma de macros del Word y por tanto puede entrar en acción nada mas cargar un documento. El Word contiene una especie de lenguaje de programación llamado *WordBasic* y es con este lenguaje como se diseñan.

- **Virus e−mail.**

Un concepto sobre este tipo de virus debe quedar claro, no existen tales virus, no puede haber un virus de correo electrónico porque precisamente el correo no es auto ejecutable. Puede ser que recibamos un programa infectado con un virus pero solo pasará a tener efecto cuando lo ejecutemos. Pero debemos ejecutarlo ya desde nuestro ordenador, así que todos esos rumores de que hay correos que con sólo abrirlos nos pueden destruir toda la información de nuestro disco duro, todo eso es mentira.

Uno de los correos de este tipo más famoso era el **Good Times**.

- **Caballos de Troya.**

Un caballo de Troya aparenta ser algo interesante e inocuo, por ejemplo un juego, pero cuando se ejecuta puede tener efectos dañinos.

- **Bombas lógicas.**

Una bomba lógica libera su carga activa cuando se cumple una condición determinada, como cuando se alcanza una fecha u hora determinada o cuando se teclea una combinación de letras.

- **Gusanos.**

Un gusano se limita a reproducirse, pero puede ocupar memoria del ordenador y hacer que sus procesos vayan más lentos.

PUNTOS DE INFECCIÓN

Los puntos de infección son los lugares o programas del sistema en donde los virus insertan su código ejecutable para posteriormente entrar en acción cuando este punto o programa sea ejecutado, hay virus que infectan el sector de arranque, el interprete de comandos, archivos ejecutables, drivers de dispositivos, monitores residentes en memoria, etc.

Cada técnica de infección proporciona ventajas y desventajas a los programadores de virus, algunos métodos son mejores porque es más difícil que un software antivirus los detecte, pero exigen técnicas de programación muy rigurosas y mucho tiempo de desarrollo.
Algunas de las técnicas frecuentemente usadas utilizan los siguientes puntos de infección:

− Contaminación del sector de arranque.

El virus sustituye el sector de booteo original del ordenador cambiando así la secuencia normal de booteo. De esta manera, lo primero que se ejecuta al encender el sistema es el código del virus, el cual queda residente en memoria y luego carga el núcleo del SO.

Las principales ventajas de este tipo de infección son que, por un lado, es fácil de programar un virus de estas características y, por otro lado, al quedar el virus por debajo del SO tiene virtualmente un control total sobre las acciones del mismo e incluso puede engañar mas fácilmente a muchos antivirus.

Su principal desventaja es que son fácilmente detectables y eliminables ya que basta con reinstalar nuevamente un sector de arranque "bueno" para eliminar el virus.

− Contaminación del interprete de comandos.

Este tipo de infección es muy similar a la anterior, ya que el virus únicamente infecta un solo programa del SO, el interprete de comandos. La principal ventaja de estos virus es que pueden "interceptar" todas las ordenes que el usuario le da al sistema y en algunos casos (dependiendo de la función del virus) solapar las acciones que se deben realizar con otras acciones falsas introducidas por el mismo virus. Por ejemplo: Cuando el usuario quiere ver el contenido de un directorio el virus se lo muestra, pero lo que en realidad hace es borrar totalmente ese directorio. El engaño puede llegar incluso hasta el punto de que durante toda la sesión presente, el virus muestre el contenido del directorio como si aun existiese, aunque en realidad ya esta borrado.

− Contaminación de propósito general.

Este método de infección es uno de los mas usados, ya que los virus de este tipo contagian todos los archivos ejecutables que encuentren en el sistema de archivos. Independientemente de la acción destructiva que realizan, son extremadamente difíciles de erradicar, ya cuando se los detecta posiblemente ya hayan contaminado decenas o cientos de programas del sistema, los cuales en muchos casos no se pueden recuperar e incluso es posible que el virus haya contagiado algún otro sistema al cual se llevo alguno de los programas infectados.

Por lo general este tipo de virus asegura su permanencia contagiando cierta cantidad de archivos antes de iniciar sus acciones destructivas, con lo cual, al momento de detectarlo, el virus puede haber infectado todo el sistema e incluso otros sistemas. Una variante de este tipo de virus son los virus de propósitos específicos diseñados generalmente con fines de competencia entre empresas de software o para castigar la piratería de algún paquete de software en particular. Este tipo de virus solamente ataca determinados programas o paquetes de software de determinadas empresas y por lo general termina destruyéndolo o modificándolo para que en apariencia funcione mal. Algunas variantes de estos virus también contagian otros archivos ejecutables en general persiguiendo dos fines fundamentales:

- Poder actuar en el futuro ante una reinstalación del software que combaten
- Y por otro lado, la infección de otros archivos en general desvía las sospechas sobre las verdaderas intenciones del virus.

− Virus residentes en memoria.

El ultimo tipo de infección son lo virus residentes en memoria, los cuales, a diferencia de los anteriores que solo actuaban mientras se ejecutaba el programa infectado, se instalan en memoria y allí permanecen hasta que se apague el sistema. Estando en memoria el virus puede realizar todas las acciones de contagio y destrucción que desee en cualquier momento.

Como se producen las infecciones

Los virus informáticos se propagan cuando las instrucciones que hacen funcionar los programas pasan de un ordenador a otro. Una vez que un virus está activado, puede reproducirse copiándose en discos flexibles, en el disco duro, en programas informáticos o a través de redes informáticas. Estas infecciones son mucho más frecuentes en PC que en sistemas profesionales de grandes computadoras, porque los programas de los PC se

intercambian fundamentalmente a través de discos flexibles o de redes informáticas no reguladas.

Los virus funcionan, se reproducen y liberan sus cargas activas sólo cuando se ejecutan. Por eso, si un ordenador está simplemente conectado a una red infectada o se limita a cargar un programa infectado, no se infectará probablemente. Un usuario no ejecuta conscientemente un código informático potencialmente nocivo como si nada; sin embargo, los virus engañan frecuentemente al SO del ordenador o al usuario para que lo ejecute.

Los virus también pueden residir en las partes del disco duro o flexible que cargan y ejecutan el SO cuando se arranca el ordenador, por lo que dichos virus se ejecutan automáticamente. En las redes, algunos virus se ocultan en el *software* que permite al usuario conectarse al sistema.

Tácticas

Los usuarios pueden prepararse frente a una infección creando regularmente copias de seguridad del *software* original y de los ficheros de datos, para poder recuperarlo en caso necesario.

Para detectar la presencia de un virus pueden emplearse varios tipos de programas antivíricos. Los programas de rastreo pueden reconocer las características del código de un virus y buscar estas características en los ficheros del ordenador. Como los nuevos virus tienen que ser analizados cuando aparecen, los programas de rastreo deben ser actualizados periódicamente para resultar eficaces. Los programas caparazones de integridad establecen capas por las que debe pasar cualquier orden de ejecución de un programa (el residente del Panda Antivirus).

Una vez detectada una infección, ésta puede contenerse aislando los ordenadores de la red, parando el intercambio de ficheros y empleando sólo discos protegidos contra escritura. Para que un sistema informático se recupere de una infección, primero hay que eliminar el virus.

Algunos programas antivirus intentan eliminar los virus detectados, pero a veces fallan. Se obtienen resultados más fiables desconectando el ordenador infectado, arrancándolo de nuevo desde un disco flexible protegido contra escritura, borrando los ficheros infectados y sustituyéndolos por copias de seguridad de ficheros originales y borrando los virus que pueda haber en el sector de arranque inicial.

Ejemplos

HAPPY99.− No es específicamente un virus, sino un programa enviado por mail(correo electrónico) que abre una ventana titulada "Happy New Year 1999!!" con fuegos artificiales. Manipula la conectividad con Internet en Windows 95 y 98.

MELISSA.−El nuevo virus de macro de Word se está expandiendo a una velocidad increíble. Infecta al MS Word y éste a todos los archivos que se abren. Se envía a sí mismo por mail y sólo funciona con Word97 y Word 2000. Existen variantes de este virus (PAPA VIRUS), pero son versiones para Excel 97.

VIRUS CHERNOBYL (W95.CIH). Este virus devastó computadoras alrededor del mundo, tuvo sus menores efectos en Estados Unidos, donde la mayoría de los usuarios habían actualizado sus antivirus a causa del famoso Melissa. Todas las variantes de este virus borran gran parte del disco duro(1 Mb) necesitando reformatearlo. Además intentan rescribir el BIOS de la computadora, dejándola inservible hasta cambiar la placa madre. Puede ser activado el día 26 de Abril, y sus variantes el 26 de Junio y cada 26 de mes. El virus infecta los ficheros ejecutables de 32 bits de WINDOWS 95/98 e infectará todos los ficheros de este tipo que encuentre. Es necesario saber que los daños por virus se extienden a todos los archivos, anteriormente solo podían dañar archivos EXE y COM pero actualmente se incluyen los archivos de texto y ZIP(comprimidos).

MICHELANGELO. Es un virus de boot sector, que lleva ese nombre porque se activa en la fecha de cumpleaños del artista italiano. Se cree que se originó en Suecia u Holanda, o al menos es allí donde fue aislado. Está basado en el virus Stoned pero, a diferencia de este último, que es inofensivo, Michelangelo es altamente destructivo cuando se activa. El virus queda residente en memoria cuando se intenta bootear desde un disquete infectado y, aunque el disco no contenga el sistema operativo, puede copiarse a un disco rígido. Se instala residente dentro de los 640 Kb de memoria del DOS y ocupa 2 Kb. El DOS va a reportar 2 Kb menos de memoria disponible si el virus está activo. El virus se instala en el boot sector de los disquetes, y copia el boot original en uno de los sectores finales del directorio. En los discos rígidos se instala en la tabla de particiones y copia la tabla original en una parte del disco que normalmente no se usa. Cuando el virus está activo en memoria infecta cada disco al que se acceda, tanto para lectura como para escritura. El día 6 de marzo (de cualquier año) se activa su rutina de destrucción. Esta rutina toma un área de memoria y copia su contenido secuencialmente en el disco rígido, con lo cual se pierde toda la información e, incluso, el DOS no será capaz de reconocer el disco ya que se sobrescribe la tabla de particiones.

WHISPER: Descubierto a mediados de 1994, es uno de esos virus que sólo infectan archivos, pero sin borrarlos ni formatear el disco. Infecta sólo archivos .EXE menores a 64 Kb aumentando entonces su tamaño en 438 bytes. Cuando se ejecuta un archivo infectado, el virus se instala residente en memoria e intercepta cada llamada a la interrupción número 21, encargada de las funciones D. O. S. para saber si se trata de ejecutar un programa. De ser así, el archivo que se quiere ejecutar es infectado. También se lo conoce como **TAI PAN**.

VIENNA: Virus alemán, sencillo y antiguo. No es residente, por lo que infecta sólo cuando es ejecutado. Ataca sólo archivos .COM en máquinas con D. O. S. 2.0 o superior.

GALICIA:

Es un virus de origen español que infecta el sector de arranque de disquetes y disco rígido y queda residente en memoria convencional (parte alta).

Utiliza un algoritmo de encriptación y su efecto destructivo consiste en formatear las primeras 255 pistas del disco.

Se activa el 22 de Mayo de cualquier año a partir de las 18hs.

Si se efectúa un acceso a disco en ese momento; se observará la aparición en pantalla de la frase ¡GALICIA CONTRA TELEFÓNICA!.

Es un virus fácil de detectar y eliminar.

MANUEL: Es un virus que queda residente en memoria. Ataca sólo archivos con extensión .COM. Su activación se debe a la ejecución de un archivo infectado 3 meses antes.

Su efecto destructivo consiste en agregar 995 bytes a estos archivos y efectúa una rotación lógica del contenido de los primeros sectores del disco, creando una enorme cantidad de vínculos cruzados y cadenas perdidas e inutilizando por lo tanto casi toda la información contenida en el disco.

Es un virus bastante fácil de detectar por su largo tiempo de incubación.

1946: Es un virus español creado en Abril de 1992. Infecta archivos con extensión .EXE siempre que su tamaño no sea inferior a 5 Kb. No queda residente en memoria y posee una muy buena técnica de encriptado. Su activación se debe a un contador interno que al llegar a 10 borra el contenido de la memoria CMOS (perdiendo así la configuración del sistema), y destruye el sector de arranque del disco y parte del directorio

raíz . Se lo conoce también como **MARIPURI**.

PETER II: Cuando ataca, formula una serie de preguntas al usuario, y si no se responde correctamente, el virus encripta los dos primeros cilindros de las dos primeras cabezas (además de más de 100 sectores) del disco rígido.

WINWORD.CONCEPT: Infecta documentos realizados con el procesados de textos Microsoft Word, por lo cual se convierte en uno de los pocos virus multiplataforma, pudiendo infectar tanto bajo OS/2, Windows 3.11, Windows 95 y Windows NT como ordenadores Macintosh.

Se le identificó por primera vez en Agosto de 1995, gracias a que el virus mismo se delata: la primera vez que infecta el archivo NORMAL.DOT muestra una caja de diálogo con un "1" y espera que se pulse OK. Desde ese momento, cada nuevo documento basado en dicha plantilla contendrá una serie de macros que hacen las veces de los módulos representados en la figura.

También puede aparecer bajo los nombres WW6infector, WBMV, WordBasic Macro Virus y WW6macro.

COLORS: Virus de origen portugués que infecta el NORMAL.DOT y sobrescribe la siguientes macros: AUTOOPEN, AUTOCLOSE, AUTOEXEC, FILENEW, FILEEXIT, FILESAVE Y FILESAVEAS.

Posee un contador en el WIN.INI gracias al cual, cada vez que llega a 300, cambia los colores del texto, el fondo, los botones de herramientas, los bordes, etc.

NUCLEAR: Infecta el NORMAL.DOT y luego, cuando se imprima un archivo, agregará un pequeño texto al final del documento pidiendo por el cese de las pruebas nucleares que se realizan en Francia.

DMV: De origen americano. Infecta el NORMAL.DOT al usarse el comando File/Close (Archivo / cerrar)

Mediante cajas de diálogo va comunicando al usuario los daños que está produciendo.

FORMATC: Troyano que infecta al Word y que, al abrir un archivo infectado, formatea el disco rígido.

WIEDEROFFNEN: Troyano de origen alemán que crea el subdirectorio C:\TROJA y copia en él el archivo AUTOEXEC.BAT, borrándolo del directorio raíz.

Infecta las macros AUTOOPEN y AUTOCLOSE.

LAROUX: Uno de los descubrimientos más recientes es este virus de tipo macro que infecta planillas de cálculo de Microsoft Excel versiones 5 y 7.

Consiste en dos archivos macro llamados "auto_open" y "check_files" y una planilla de cálculo escondida llamada "Laroux".

11