Virus Informaticos

FERNANDO DE LA CUADRA Y DE COLMENARES
International Manager Tecnical
Panda Software International

1.- QUÉ ES UN VIRUS

La palabra "virus" proviene de la lengua latina, en la cual significaba "veneno".

Un virus informático esta formado por una secuencia o conjunto de secuencias de código máquina (el lenguaje más elemental que el ordenador es capaz de entender) o de un lenguaje de programación que copia su código en otros programas cuando se activa, provocando una infección. Cuando el programa infectado se ejecuta, el código entra en funcionamiento y el virus sigue extendiéndose.

Se definen los virus como "programas informático capaces de autorreplicarse mediante la infección de otros programas mayores, que intentan permanecer oculto en el sistema hasta darse a conocer, momento en el cual producen o provocan daños, problemas o molestias al sistema informático y, por ende, al usuario".

Los virus informáticos, al contrario que sus homólogos biológicos, no son 'descubiertos', sino escritos por especialistas, algunos de ellos, españoles. En una mayoría de los casos sus creadores son estudiantes de informática deseosos de probar su destreza. Su objetivo: destrozar discos duros, alterar el buen funcionamiento de las redes, provocar pérdidas, molestar. Demostrar su valía como programadores. Cuanto mayores sean sus daños, mayor el reconocimiento entre los miembros de la escena.

No obstante, y al objeto de distinguir primero entre lo que es y lo que no es un virus informático, analicemos las cuatro características definidas mencionadas anteriormente.

Son programas: conviene dejar bien asentado este punto. El virus informático es un programa informático, y en ese sentido no se diferencia lo más mínimo de cualquiera de los programas de un ordenador: un procesador de texto, un navegador de Internet o una hoja de cálculo. Al igual que estos programas, el virus ha sido programado utilizando una secuencia de código y cumple una función para la cual ha sido diseñado. Desgraciadamente, toda similitud con los programas

convencionales empieza y acaba en esa definición. Es un programa, sí, pero su forma, sus fines y su modo de funcionamiento difieren por completo de los programas que los usuarios de informática utilizamos habitualmente.

Son autorreplicantes: es decir, que una de sus cualidades es la de poder clonarse, crear copias, ya sean idénticas o evolucionadas, de sí mismos y reproducirse dentro del sistema o sistemas informáticos en los cuales operan. Antes de que nacieran los virus informáticos existían los llamados *worms* o gusanos, auténticos antepasados de los virus actuales, y cuya única función era, precisamente, esta, la de reproducirse y extenderse a lo largo y ancho de los sistemas informáticos de una red para, eventualmente, ralentizarla al concurrir la acción de replicación con la ejecución de otras tareas del sistema. En este caso, el fin nocivo (ralentizar el sistema) era consecuencia de su propia capacidad de autorreplicación. Por otro lado, los gusanos no son algo del pasado, ya que su técnica aún se utiliza hoy día (y con notable éxito, por cierto, gracias a Internet).

Permanece oculto en el sistema hasta el momento de su "explosión": esta característica también es importante. Los virus suelen ser programas de muy pequeño tamaño y que intentan pasar "desapercibidos" en el sistema hasta que llevan a cabo la acción para la cual han sido programados. Y aún en este caso intentan ocultar el daño causado hasta el último momento.

Provoca daños: esta tal vez sea la característica general más discutida. En efecto, hay virus que no provocan daño alguno al sistema y que han sido creados con un mero ánimo experimental y en absoluto destructivo. Sin embargo, lo cierto es que, dañinos o no, son programas que se introducen en nuestro sistema contra nuestra voluntad, alteran de una forma u otra el sistema aunque tan sólo sea modificando mínimamente el tamaño de un archivo, y por esa razón ya pueden ser calificados de molestos. Los daños que pueden provocar los virus informáticos varían enormemente. Desde el daño inexistente que hemos comentado y que no pasa de mera molestia, hasta el borrado de la Flash-BIOS y de los datos del disco duro hay toda una escala de daños más o menos importantes. Por ejemplo, los clásicos virus que se limitan a anunciar periódicamente un pequeño mensaje en pantalla; los que afectan al funcionamiento de los programas de nuestro disco (ya sea inutilizándolos o borrándolos, ya haciéndolos más lentos); o los que causan pérdidas aleatorias de datos de nuestro disco duro. De una forma u otra, todos los virus que podamos calificar como tales causan un daño o al menos una molestia al sistema y al usuario.

2.- TIPOS DE VIRUS

Como vamos a ver, existen muchos tipos de virus de acuerdo con los tipo de archivos que infectan. Además, podremos observar como el mismo tipo de virus ha evolucionado conforme lo han hecho los sistemas operativos, adaptándose siempre a las últimas tecnologías y buscando nuevas formas de atacar nuestros ordenadores. En esta clasificación de los virus no están todos los tipos de virus, sino solamente aquellos más "tradicionales" (por llamarlos de alguna forma), fren-

te a las más recientes amenazas surgidas al amparo de Internet, que trataremos detalladamente más adelante..

2.1 VIRUS DE SECTOR DE ARRANQUE

Como su nombre indica, los virus de esta clase utilizan los sectores de arranque y la tabla de particiones para ejecutarse y tomar el control cada vez que el ordenador arranque desde un disco contaminado. Lo cierto es que se podría discutir si realmente se trata de un virus informático, ya que de acuerdo con la definición tradicional el virus debería infectar un archivo que de alguna forma sea ejecutable, mientras que este tipo de archivos infecta la parte que es en cierto modo ejecutable de un disco. Aunque podría cuestionarse que se trate de un virus se suele aceptar que así sea, ya que su funcionamiento es idéntico al de los virus, aunque su medio de expansión no sea el "oficial".

Vamos a aprovechar la oportunidad para destruir un mito: El hardware de una disquetera impide que se pueda escribir en un disquete protegido contra escritura. La única manera de poder escribir en un disquete protegido es desmontar la disquetera y armado de cable y soldador "trucarla" para que lo permita. En general, es imposible escribir en un disquete protegido contra escritura, lo que incluye la infección de virus.

Muchos virus de boot gestionan contadores en los que registran el número de disquete que han infectado, de tal manera que cuando este contador alcanza un cierto valor el virus se considerará suficientemente extendido como para poder comenzar su tercer acto: el ataque. Una vez que el virus de boot se ha instalado, y reproducido tantas veces como oportunidades se le hayan presentado, lanzará eventualmente la forma de ataque para la que fue diseñado. El objetivo primario del virus es el ataque y todos los pasos dados hasta este punto han ido encaminados a alcanzar esta etapa.

Los virus de arranque fueron durante mucho tiempo la gran amenaza de la informática. Hasta la popularización de las redes locales no fueron superados en repercusión por los virus de archivo. Aún hoy, un 10% de las infecciones se producen a causa de virus de arranque, y conocidos virus de este tipo como Empire, AntiEXE, AntiCMOS, Form o Parity Boot siguen haciendo de las suyas, aunque en menor medida que hace unos años.

2.2 VIRUS DE FICHERO

Los virus de esta clase utilizan los ficheros ejecutables como medio de transmitirse y tomar el control. Al igual que ocurría con los sectores de arranque infectados, un fichero ejecutable infectado es completamente inofensivo mientras no lo pongamos en marcha.

Lógicamente los programas están para ser ejecutados, por lo que tarde o temprano entrará en funcionamiento ese programa, provenga de donde provenga. En mala hora, ya que si ese programa está contaminado por un virus, nuestro sistema será infectado por ese virus sin que de momento podamos hacer nada al respecto.

Vamos a ver cómo acostumbran los virus de ficheros a acomodarse en nuestros ordenadores: cuando se pone en marcha un programa infectado, las primeras instrucciones que se ejecutan pertenecen al código del virus, y por ello quien toma el control del ordenador es el virus y no el programa.

Una vez que el virus toma el control (es decir, se ejecutan sus instrucciones) pueden pasar numerosas cosas dependiendo de las características de cada virus. En general podemos decir que existen dos vías de comportamiento dependiendo de si se trata de un virus residente o un virus de acción directa.

2.3 VIRUS DE FICHERO RESIDENTE

Un virus residente es aquel que tras ejecutarse es capaz de dejar una copia de sí mismo almacenada en la memoria RAM del ordenador y proseguir con la infección. La copia permanece residente hasta el momento en que reiniciamos el ordenador.

Es en este momento cuando empieza la segunda parte, la reproducción o infección de otros ficheros, y en muchos casos el comienzo de una serie de comportamientos extraños de nuestro ordenador. La gran mayoría de los virus residentes infectan a otros programas en el momento en el que son ejecutados o copiados.

2.4 VIRUS DE FICHERO DE ACCIÓN DIRECTA

Como su nombre indica, estos virus no permanecen en memoria después de ser ejecutados, y por lo tanto tampoco interceptan los servicios del sistema. Debido a esta circunstancia los virus de acción directa se ven obligados a replicarse en el mismo momento de ser ejecutados; precisamente de ahí les viene el nombre.

2.5 VIRUS DE SOBREESCRITURA

La característica principal de este tipo de virus, que pueden ser residentes o no, es que no respetan la información contenida en los ficheros que son infectados. Es decir, el fichero que infectan queda inservible. Otra de sus características es que al infectar un fichero, éste nunca aumentará su tamaño a no ser que el código del virus ocupe más bytes que el de la víctima.

2.6 LOS VIRUS DE MACRO

Este tipo de virus surgió a finales de 1994 y empezó a popularizarse a partir de 1995. Hoy día los virus de macro son los más peligrosos y extendidos, y gracias a Internet han cobrado mayor relevancia si cabe. Hoy día, un 64 % de los desastres informáticos están causados por virus de macro, lo que les convierte en la mayor amenaza contra la seguridad informática del mundo. Por lo tanto, debemos conocer y saber combatir este tipo de virus para estar a salvo de los peligros que implica.

2.6.1 ¿Qué es una macro

Los macros son secuencias automatizadas de comandos. Las antiguas aplicaciones en MS-DOS contenían gran cantidad de comandos que se llevaban a cabo mediante la pulsación de sucesivas teclas, menús, etc. Para llevar a cabo sencillas tareas como imprimir un documento había que llevar a cabo varias acciones, algo que podía llegar a resultar tedioso. Para evitar esto se idearon las macros, que en principio no eran más que sencillas secuencias de los propios comandos del programa que quedaban almacenadas en un simple archivo. Para ejecutarlas se asignaba una combinación de teclas a la macro, lo cual facilitaba enormemente la ejecución de acciones complicadas.

Sin embargo, con el tiempo los programas fueron ganando en complejidad, y también lo hicieron las macros, que empezaron a ser pequeños archivos ejecutables capaces de llevar a cabo acciones complejas. Con la aparición de la suite ofimática Office 4.2 de Microsoft se añadieron nuevas posibilidades a las macros, que ya podían ser programadas en un sencillo lenguaje de programación llamado Word Basic. Esto provocó la aparición, a finales de 1994, del primer virus de macro, un virus experimental que ni siquiera vio la luz. Fue en 1995 cuando apareció el primer virus "salvaje", llamado Concept.

2.6.2 ¿Qué puede hacer un virus de macro?

Los virus de macro son extremadamente simples de generar. La mayoría de los lenguajes de macros son un subconjunto del lenguaje BASIC (el preferido de los autores de virus) mucho más fácil de programar que el lenguaje ensamblador, el preferido por los creadores de virus. Puesto que cualquier persona puede crear virus de macro, no es difícil de comprender que día a día aumente el número y la sofisticación de estos virus.

La capacidad de los lenguajes de macro para llamar a rutinas externas, por ejemplo funciones de una DLL de Windows, permite a los virus de macro realizar prácticamente cualquier operación.

Una de las características más novedosas que tienen los virus de macro con respecto a los virus convencionales es su independencia del sistema operativo.

Un virus de macro puede funcionar sin cambios en cualquier plataforma soportada por la aplicación que la interpreta. Por ejemplo, un virus de macro de Microsoft Word puede funcionar en cualquier sistema operativo para la que haya una versión de Microsoft Word (Windows 3.1x, Windows 95, Windows 98, Windows NT, Mac OS, OS/2, etc.).

Hay numerosos riesgos para el usuario que inadvertidamente utiliza un documento infectado por un virus de macro. Estos están limitados únicamente por la imaginación del autor de virus. Un ejemplo de algunas acciones maliciosas que son relativamente fáciles de implementar son:

- Infección del ordenador por un virus convencional.
- Borrado de archivos/documentos del disco duro.
- Renombrado de archivos
- Copia de archivos personales a lugares públicos.
- Envío de archivos desde el disco duro a una dirección de correo Internet.
- Formateo del disco duro.

La popularización del uso de Internet ha facilitado enormemente la difusión masiva de documentos infectados a lo largo y ancho del planeta. Debido a que el intercambio de documentación es una tarea cotidiana en cualquier empresa, tanto a nivel de LAN como WAN, un virus de macro puede infectar todos los ordenadores de una empresa en pocas horas. El colapso microinformático de la empresa, además de generar muchas horas de trabajo y dolores de cabeza al departamento de informático, será en general muy costoso.

2.6.3 Virus macro en Excel

Excel es el programa de hoja de cálculo más utilizado del mundo. Naturalmente, tarde o temprano tenía que ser objeto de atención por parte de los creadores de virus, y ya con las anteriores versiones de Excel aparecieron los primeros ejemplares. Naturalmente, con las nuevas versiones el número de estos virus ha aumentado.

El método de propagación es bastante parecido al utilizado en Word, aunque hay una diferencia: los comandos de copiado de macro difieren, ya que en Excel no existe una plantilla como Normal.dot. Para copiarse utilizan el directorio "InicioXL" y las hojas allí almacenadas para su propósito.

Los virus de versiones anteriores también pueden ser ejecutados en las versiones más modernas ya que se ha mantenido la compatibilidad entre los diferentes lenguajes utilizados. Excel utiliza, al igual que Word, el lenguaje Visual Basic for applications.

2.6.4 Macros para Access

La base de datos más utilizada tampoco podía dejar de ser blanco de los creadores de virus. Dado que Access 97 es parte de Office 97, los virus utilizan el mismo lenguaje de programación. Sin embargo, al contrario que Word y Excel, Access no tiene automacros, sino que los macros se activan con distintas acciones. Cabe destacar que el Access se llama "macros" a los scripts y "módulos" a los macros.

2.6.5 Virus para power point

Con la reciente aparición de virus para PowerPoint se completan 4 de los 5 grandes programas de la suite Office de Microsoft para los que existen virus de macro. Los virus de PowerPoint tienen dos formas de extenderse: o bien activándose y buscando archivos *.ppt o copiándose a las plantillas de PowerPoint (incluida la plantilla de presentación en blanco). Existen muy pocos virus de este tipo.

2.6.6 Virus en Ami Pro

Aunque algo desfasado, el procesador de textos AmiPro gozó en su momento de una enorme popularidad. Dado que este programa también permitía la creación de virus de macro también lo analizaremos, aunque lo cierto es que el número de ejemplares que infectan AmiPro es enormemente reducido.

2.6.7 Virus de macro en Corel Draw

La última aplicación para la cual se han descubierto virus de macro ha sido Corel Draw, un famoso programa de creación de gráficos para el cual ha surgido el virus Galadriel.

Galadriel es el primer virus que afecta a los "scripts" de Corel Draw. El nombre se puso en honor a la reina de los elfos que aparecía en "El Señor de los Anillos", el libro más conocido de J.R.R. Tolkien. El virus se activa el 6 de junio de cualquier año y su efecto consiste en mostrar un texto de la mencionada obra.

2.6.8 Virus de macro multiprograma (también llamados multi-macro-partite)

Entre las últimas tendencias en la búsqueda de una mayor complejidad de los virus, los creadores han intentado que los virus de macro sean capaces de infectar diversas aplicaciones a la vez.

Uno de los virus más llamativos en este sentido es el Triplicate, capaz de infectar hasta tres aplicaciones de la suite Office 97: Word, Excel y PowerPoint. El virus se activa desde un documento de Word infectado o por medio de presentaciones de PowerPoint o hojas de cálculo de Excel.

2.7 VIRUS DE COMPAÑÍA

2.7.1 Virus de compañía en MS-DOS

Este tipo de virus, que pueden ser residentes o de acción directa, aprovechan una característica del intérprete de mandatos del DOS (por lo general el COMMAND.COM), por la cual si en un mismo directorio coexisten un fichero COM y otro EXE con el mismo nombre, siempre será ejecutado en primer lugar el que tenga la extensión COM.

El resultado es que cuando el usuario vaya a ejecutar su programa EXE, en realidad lo que habrá ejecutado es un programa con el mismo nombre pero con la extensión COM., es decir, habrá ejecutado una copia del virus.

2.7.2 Virus de compañía en Windows 95/98

En este caso, el método que utilizan los virus es parecido al de los virus en MS-DOS, pero varía ligeramente. Estos virus cambian la extensión EXE de los archivos de programa en su correspondiente directorio (hacen esto con cualquier archivo, sea de DOS, de Windows, o de Windows95/98) por la extensión COM. El virus se copia a sí mismo con el nombre del archivo infectado.

2.8 LOS VIRUS DE FICHEROS BAT

Los archivos BAT son archivos utilizados para llevar a cabo una automatización de comandos del sistema. En MS-DOS se utilizaba (y aún se utiliza en los sistemas Windows 95/98) un archivo llamado AUTOEXEC.BAT para la automatización de algunos comandos de inicio, y estos archivos se usaban habitualmente para llevar a cabo la instalación de programas de MS-DOS. Son archivos muy sencillos, basta con un editor de código ASCII (cualquier editor de textos) para escribir una cadena de comandos escrita en un leguaje muy sencillo. Naturalmente, los comandos que ejecuta este archivo hacen uso de las instrucciones del COMMAND.COM o de instrucciones propias del sistema operativo DOS.

Cuando apareció el sistema operativo Windows 95 se desvaneció la amenaza de los virus de script propios de Windows 95 (como los.BAT, que aunque se podían ejecutar en el nuevo sistema fueron cayendo en desuso). Sin embargo, con la aparición de Internet Explorer 4 y Windows 98 ha surgido una nueva posibilidad. Estos programas instalan por defecto el llamado Windows Scripting Host (que ya estaba disponible en Windows 95, pero no en la instalación por defecto), mediante el cual se pueden programar y ejecutar archivos de comandos para Windows 95/98 y Windows NT. Esto da la posibilidad de crear ficheros de ejecución automatizada de tareas, y también de crear virus que hagan uso de esa automatización para extenderse. Los virus se programan en Visual Basic Script y se encuen-

tran en archivos con extensión .VBS. Algunos de estos virus también son capaces de infectar archivos Javascript (.JS)

Aunque los ejemplares existentes de este tipo de virus son escasos e inofensivos, lo cierto es que suponen una nueva amenaza que puede ir en aumento en el futuro, y también han contribuido a la aparición de los virus de HTML.

2.8 VIRUS DE ENLACE O DIRECTORIO

Los virus de este tipo emplean una técnica para infectar extraordinariamente sofisticada, de ahí los pocos ejemplares existentes. Para poder explicar el método que emplean hay que conocer cómo a partir de un nombre de fichero el sistema operativo es capaz de obtener la posición en disco de todas las porciones en las que está dividido el fichero.

Cuando un virus de esta clase desea infectar un fichero, lo que hace es cambiar, en la entrada del directorio de ese fichero. El campo o dato donde se indica cual es el número del primer cluster del fichero, por el número del primer cluster del virus, almacenando en un área sin usar de la misma entrada de directorio el número original.

Una vez hecho ese cambio, cuando el DOS va a ejecutar el fichero en cuestión necesita saber dónde se ubica físicamente en el disco, así que mirará en la entrada del directorio cual es el primer cluster de ese fichero, y encontrará el correspondiente al del virus, por lo que una vez más será este el que tome primero el control al ejecutar el programa.

2.9 VIRUS MULTIPARTITE

Los virus multipartite son virus enormemente avanzados, ya que son capaces de utilizar varias de las técnicas de infección que ya hemos estudiado. Por ejemplo, un virus multipartite es capaz de infectar archivos EXE y COM y a la vez sectores de arranque de disquetes o discos duros, facilitando de esta forma enormemente su difusión. Un virus multipartite también es capaz de infectar virus de macro a la vez que archivos ejecutables. Estos virus también han seguido una evolución lógica. En la época en que tanto los virus ejecutables como los virus de arranque tenían éxito, crear un virus que aunase ambas técnicas era garantía de éxito por su facilidad de expansión. Hoy día lo interesante es crear virus de macro (que también son multiplataforma) que a la vez puedan infectar archivos ejecutables de Windows 95, siendo capaces de afectar a muchos ordenadores.

2.10 Virus multiplataforma

Los virus multiplataforma son aquellos que pueden desarrollarse en diversas plataformas o sistemas operativos distintos. Por ejemplo, PC con respecto a Macintosh.

Como ya hemos visto, los virus de macro pueden ser multiplataforma en la medida en que realmente no están sujetos a una plataforma concreta, sino más bien a la existencia de un programa determinado, sea este en su versión Windows o en su versión Macintosh (si existieran versiones de MS-Office para Linux los virus de macro también serían capaces de infectarlos, ya que no se trata de la plataforma sino del programa.. Estos han sido por tanto los primeros virus capaces de infectar varias plataformas, aunque haya sido de forma accidental.

Realmente, el intento por desarrollar virus multiplataforma de ficheros ejecutables se presentaba posible pero poco interesante. Las dificultades técnicas eran enormes y resultaba menos costoso desarrollar dos virus separados que uno que fuera capaz de infectar todas las plataformas. Lo que si era posible era que los virus convencionales de DOS se extendieran en emuladores de DOS para Macintosh, o que los virus de Windows 95 funcionen en emuladores de Windows 95 para Macintosh. Sin embargo, sólo lo harán cuando esté en funcionamiento el emulador y nunca infectarán el Mac OS (sistema operativo de los Macintosh), por lo que el obstáculo seguía en pie.

2.11 GUSANOS

Los gusanos son los antepasados de los virus, aunque sus técnicas aún se utilizan hoy día con bastante éxito. El gusano se diferencia de un virus en que su forma de autorreplicación no consiste en modificar otros programas para insertar en ellos una copia de sí mismo. El gusano, por lo tanto, es un programa en sí cuya labor consiste en crear copias de sí mismo e infectar con ellas otros ordenadores, ya sea por medio de una red interna o por medio de Internet u otro tipo de red de ordenadores.

Podemos distinguir dos tipos de gusanos de acuerdo con su forma de actuación:

- Gusanos de ordenador: este tipo de gusanos utiliza una copia completa de su programa en cada ordenador que infectan. Es decir, en estos ordenadores el programa está contenido en su integridad. Para expandirse utilizan las conexiones de red, y por medio de ellas se copian íntegramente en otros ordenadores. De esta forma consiguen expandirse y lograr su fin dañino al colapsar la red.
- Gusanos de red: la diferencia de estos gusanos con los anteriores es que estos programas están formados por distintas partes (llamadas "segmentos), cada una de las cuales se ejecuta en distintos ordenadores (y ejecuta distintas

acciones) y utiliza la conexión a la red para comunicar esas partes entre sí. La propagación de los distintos segmentos es tan sólo uno de los propósitos del gusano. Ciertos gusanos tienen un segmento principal que coordina al resto de gusanos; a este tipo de gusanos también se les llama "pulpos".

Existe una variación sobre los gusanos que consiste en la eliminación de la copia anterior del gusano. Es decir, que el gusano se copia en otro ordenador pero elimina la copia anterior. En cierto modo, "salta" de un ordenador a otro sin causar daño alguno. A estos programas se les ha llamado "conejos"

El objetivo de estos programas consiste en provocar el colapso de la red (o de un ordenador) bloqueando sus ordenadores y su capacidad de proceso. Los ordenadores en los que los gusanos tradicionales se desarrollaron eran sistemas UNIX capaces de llevar a cabo diferentes procesos al mismo tiempo. Lo que el gusano conseguía era ejecutarse en el ordenador infectado y ocupar con su tarea la capacidad del ordenador infectado hasta bloquearlo y que fuera imposible ejecutar otros programas.

2.12 BOMBAS LÓGICAS

Una "bomba lógica" no es un programa separado, sino un segmento camuflado dentro de otro programa. Tiene por objetivo destruir los datos de una computadora o causar daños en ella cuando se cumplen ciertas condiciones. La condición puede ser de diversa naturaleza: puede darse cuando se teclee una combinación concreta de teclas, cuando se cumpla una determinada fecha o cuando ocurra cualquier otro hecho previsto por el programa. Mientras este hecho no ocurre nadie se percata de la presencia del programa ya que pasa completamente inadvertido.

Las primeras "bombas lógicas" fueron creadas por los propios programadores e introducidas en algún programa realizado por ellos mismos, con objetivos tan variados como destruir el programa o el sistema entero si el cliente no pagaba el trabajo, o como sabotaje por deseos de venganza. También fueron utilizadas para abrir determinadas puertas que permitían al propio programador acceder al sistema más tarde, aún sin el permiso necesario.

Hay que dejar dos características bien claras en torno a esta forma de malware:
No son virus: no intentan replicarse en otros ordenadores, así que no pueden identificarse como virus informáticos. En cierto modo, se podría decir que son virus "a medida", ya que se mantienen bajo control y solamente se introducen de forma voluntaria en los ordenadores por su propio creador. También se activan por el creador.

Son imposibles de detectar por medio de un antivirus: dado que se trata de programas no replicantes y en muchas ocasiones hechos a medida de un solo

ordenador, un antivirus estándar no puede detectarlas. Habitualmente el código dañino está incluido dentro de un programa indefenso, así que resulta imposible sospechar la amenaza.

2.13 CABALLOS DE TROYA (O TROYANOS)

Miles de años después del caballo de Troya original, aquel caballo ha servido para nombrar a una de las más peligrosas amenazas informáticas después de los virus, los Caballos de Troya. Un programa inofensivo –puede ser incluso un programa "regalo", como veremos- llega al ordenador de un usuario desprevenido. El programa se ejecuta y funciona con normalidad... aparente. En realidad, y sin que el usuario se dé cuenta, un programa dañino se instala al mismo tiempo que el programa inofensivo. El programa dañino puede activarse de diferentes formas: puede permanecer activo desde la instalación dejando vulnerable el sistema o abriendo alguna puerta trasera (backdoor) que permita la entrada de intrusos. O bien puede albergar dentro de sí una bomba lógica que en un determinado momento se active y provoque daños al sistema: borrado de archivos, formateo del disco duro, encriptación del disco u otros efectos dañinos.

El programa no es replicante, por lo cual no puede considerarse como un virus. Sin embargo, muchos de estos troyanos sí son detectados por los modernos antivirus, dado que se trata de programas estándar preparados para instalarse en cualquier ordenador personal que tenga instalado un sistema operativo concreto.

3.- PROBLEMAS CAUSADOS POR LOS VIRUS.

Las razones de preocupación son importantes y aumentan en número e intensidad. Si en 1993 el número de virus no era más que una cantidad simbólica, hoy en día el número supera los 40.000 ejemplares, y crece aproximadamente a una media de trescientos virus mensuales. Además, la peligrosidad de los virus no ha cesado de acentuarse en los últimos años, y el número de amenazas, así como de vías de entrada, también se ha incrementado como consecuencia de la popularización de Internet.

Si hace unos años bastaba con tomar ciertas precauciones para evitar una potencial infección, hoy en día resulta cada vez más inconcebible no utilizar un buen programa antivirus capaz de vigilar todas las posibles vías de infección y actualizarse diariamente, ya que los virus se propagan, por medio del correo electrónico, a una velocidad inusitada, lo que puede provocar fácilmente una infección si no se toman las debidas precauciones y no se tiene un poderoso antivirus. También se hace absolutamente necesario que las empresas antivirus ofrezcan un servicio técnico permanente a sus clientes, ya que en ocasiones la infección se extiende a tal velocidad que resulta imposible elaborar una vacuna antes de que muchas empresas ya hayan sido infectadas.

Los virus se extienden con mayor rapidez y son cada vez más destructivos. El ejemplo del virus CIH/Chernobyl capaz de sobreescribir la Flash-BIOS y borrar el contenido del disco duro ya ha sido seguido por otros virus, y muy probablemente en el futuro la capacidad dañina de los virus se incremente aún más.

Los informes de consultoras y expertos no dejan lugar a las dudas. Según Computer Economics, sólo en el primer semestre del año 1999, los virus han causado a las empresas unas pérdidas por valor de 7.600 millones de dólares (alrededor de 1,2 billones de pesetas) en todo el mundo. Según esta consultora norteamericana, los principales enemigos de este año tienen nombres de gusano, I-Worm.ExploreZip y Melissa, ya que han sido éstos quienes han protagonizado los mayores índices de ataques y de pérdidas para las empresas.

Estos 7.600 millones de dólares representan los gastos por pérdidas en productividad y costos de reparación declarados por las 185 compañías que han sido objeto del estudio de Computer Economics y que representan cerca de 900.000 usuarios internacionales.

Esta cifra contrasta con la ofrecida el año pasado por la misma consultora y que situaba las pérdidas de todo el año por encima de los 1.500 millones de dólares. En el estudio de 1.998 no sólo se incluyeron las pérdidas por virus, sino también las debidas a intrusiones en los sistemas informáticos por hackers y usuarios maliciosos.

Computer Economics hace hincapié en que las cifras de pérdidas en este primer semestre del año son ya cinco veces superiores a los totales del pasado año, sólo en cuanto a virus se refiere. Incluso se estima que estos números son conservadores e inferiores a los reales, ya que la mayor parte de las compañías lógicamente tienden a minimizar los gastos y las incidencias producidas a fin de no provocar una mala imagen entre sus clientes.

No obstante, no debemos ser catastrofistas ni alarmistas ante estas graves amenazas. Un buen antivirus y unas grandes dosis de prudencia son la herramienta perfecta para evitar una infección.

4.- VÍAS DE ENTRADA DE VIRUS.

Sin lugar a dudas, Internet es, hoy por hoy, la más importante vía de entrada de virus en nuestros ordenadores o redes. El increíble crecimiento del correo electrónico en los últimos años ha propiciado que los creadores de virus se fijen en este formidable instrumento de comunicación. Esto ha convertido nuestros buzones en focos de peligro potencial –pero sólo potencial-. Hay, además de esta, otras vías de entrada que no son menos importantes. A continuación estudiaremos cada una de ellas, las formas que tienen de manifestarse y, sobre todo, las precauciones que debemos tomar para prevenir el ataque.

4.1 EL CORREO ELECTRÓNICO: EL PRINCIPAL PORTAL DE ENTRADA DE LOS VIRUS MODERNOS

Los sistemas de mensajería electrónica son ya hoy en día imprescindibles para muchas empresas y usuarios de ordenadores y cada día se intercambian millones y millones de mensajes de correo en todo el mundo. Esto ha provocado el interés de los creadores de virus, que han conseguido pasar de hacer virus que infectan el ordenador mediante un fichero adjunto colocado en un mensaje de correo (en esa categoría entrarían casi todos los virus actuales), para llegar a programar virus y gusanos que se transmiten "por medio" del correo electrónico tras la ejecución de ese mismo archivo. Es decir, que automáticamente y sin conocimiento del usuario se reenviasen a sí mismos desde el ordenador del usuario a otros ordenadores, expandiéndose de esta forma por toda la red y destrozando o infectando millones de sistemas. Esto ya se ha conseguido, y el ejemplo más notorio es Melissa.

Sin embargo, debe quedar bien claro una vez más que, aunque la regla general es que no es posible infectar el ordenador solamente mediante la apertura de un mensaje de correo. Si bien lo cierto es que actualmente no son casos de excesiva gravedad, no obstante, es una amenaza que no se debe desdeñar.

Las formas de recepción del correo electrónico son diversas: algunas convencionales, como los disquetes que se pueden utilizar para transportar mensajes de un ordenador a otro, pero lo normal es que los mensajes se reciban, bien dentro de una red interna, o bien a través de Internet. En cualquiera de los casos, se deben extremar las precauciones.

Las características más importantes de los virus en el correo electrónico son:

1. Su capacidad de replicación y propagación. Un virus puede extenderse por una empresa en cuestión de minutos y en pocas horas puede infectar cientos de miles de ordenadores.

2. Es el sistema con la conectividad más extensa que se conoce. Permite el intercambio de información y ficheros entre prácticamente cualquier tipo de sistema y en segundos se puede conectar con cualquier ordenador del mundo.

3. Los ficheros normalmente no son guardados directamente en el disco sino en bases de mensajes, lo que convierte en inútil cualquier forma de escaneo antivirus de forma convencional. La única manera de proteger el ordenador es disponiendo de un antivirus específico para cada sistema de correo.

En cuanto a las vías de entrada de virus por medio del correo electrónico, hoy por hoy la única forma grave de infectarse con un virus informático es mediante la ejecución de los ficheros adjuntos. Junto a un mensaje de correo, esto es, el texto del mensaje, se pueden añadir todo tipo de ficheros, programas, archivos comprimidos, etc... Y ahí precisamente es donde está el peligro ya que esos

archivos pueden llevar incluidos todo tipo de virus convencionales: pueden ser Caballos de Troya, que al ser ejecutados instalen un servidor y posibiliten a otros usuarios malintencionados tomar control de nuestro ordenador. Pueden ser virus de macro que dañen nuestro sistema y además se reenvíen a otras direcciones de nuestra libreta de direcciones, posibilitando la extensión de la infección. Pueden ser gusanos que se extiendan desde nuestro equipo a otros ordenadores de la Red, o virus normales y corrientes que dañen nuestro sistema. En definitiva, los archivos adjuntos pueden ser una fuente infinita de daños para nuestro ordenador, y por ello deben ser vigilados con gran atención. Debemos tener en cuenta que la infección por medio de ficheros adjuntos requiere de una acción por parte del receptor, y por lo tanto las precauciones que éste tome serán decisivas a la hora de evitar una infección.

Para protegernos de los ficheros adjuntos en el correo electrónico se debe combinar el uso de un buen antivirus actualizado diariamente con unas dosis de precaución. Para ello bastará con seguir las siguientes pautas:

1. No abrir ningún fichero que resulte sospechoso, extraño, que venga de un destinatario desconocido o que contenga textos extraños, con cadenas de caracteres sin sentido, o sencillamente que no sean esperados y cuyo contenido no se halle correctamente explicado en el cuerpo del mensaje.

2. En lugar de abrir el fichero, archivarlo en un directorio del disco y analizarlo con un antivirus actualizado. Los más modernos antivirus llevan directamente a cabo la revisión de los ficheros adjuntos incluidos dentro del mensaje de correo.

3. Finalmente, si el archivo no está infectado pero tenemos nuestras reservas sobre su origen conviene no ejecutarlo tampoco. Debemos tener en cuenta que los virus hoy día se expanden a una enorme velocidad, y que existe la posibilidad de que el virus llegue a nuestro buzón de correo antes incluso de que las empresas antivirus tengan conocimiento de su existencia. Esto es una razón de más para contar con un antivirus que se actualice diariamente y que venga acompañado por un servicio técnico que responda rápida y eficazmente.

4.2 LOS GRUPOS DE NOTICIAS

Los grupos de noticias o newsgroups proporcionan la capacidad de difusión, en grupos temáticos, de mensajes como si de un tablón de anuncios se tratara. La cantidad de grupos temáticos es casi ilimitada. En lo que respecta a esta obra, en muchos grupos de noticias podemos encontrar parches de software, nuevos productos, información técnica, consejos de programación y pequeños programas, entre otras cuestiones. Por otra parte, las dudas y problemas que los usuarios plantean son respondidas –por lo general en menos de 24 horas- por otros usua-

rios que o bien tienen mayores conocimientos técnicos, o bien han tenido la misma experiencia y pueden aportar su solución.

USENET, red encargada de gestionar los grupos de noticias, proporciona un sistema para reducir la gran cantidad de recursos que consumen las listas de correo (mail lists). Consiste en una central en la que se van reemplazando diferentes artículos y un programa que consigue acceder a ellos para leer los que resulten de interés para el usuario. Los suscriptores pueden elegir los artículos que quieren ver.

Sin embargo, dentro de las news corremos exactamente los mismos riesgos que en cualquier otro sistema de envío de información a través de Internet. Los archivos que descarguemos del servidor pueden ir acompañados de ficheros adjuntos que contengan virus, exactamente igual que en el correo electrónico. Las medidas a tomar, por lo tanto, son las mismas, pero en este caso se debe extremar la precaución, ya que en la mayoría de los casos los mensajes han sido enviados al servidor por desconocidos.

Los grupos de noticias son, en los últimos tiempos, el medio más utilizado por los programadores de virus para dar a conocer sus creaciones, sobre todo si esos virus o gusanos son de los que se reproducen haciendo uso de los programas de e-mail. Los grupos de noticias son el escaparate perfecto para que miles o millones de personas se infecten con un virus y den así comienzo a una infección que puede extenderse a todo el mundo y causar graves daños en miles de ordenadores. Por lo tanto, los grupos de noticias pueden ser un enorme foco de infección potencial. Además, en ocasiones podemos encontrar mensajes con ficheros adjuntos que contienen virus enviados involuntariamente por internautas que ignoran por completo que sus mensajes están infectados y que están expandiendo la plaga sin ni siquiera darse cuenta.

Por esta razón, se deben seguir las mismas precauciones a la hora de utilizar este medio de información y comunicación que a la hora de vigilar nuestro correo electrónico.

4.3 La descarga de ficheros por FTP

El FTP (File Transfer Protocol) es el protocolo de transferencia de archivos que permite la carga y descarga de programas o ficheros de Internet. Se trata de uno de los servicios más populares, ya que muchos internautas buscan programas shareware o freeware, actualizaciones de programas comerciales, demostraciones, documentos, etc.

El FTP también puede ser una vía de entrada de virus, ya que podemos encontrar ficheros infectados en nuestras descargas, máxime si se trata de sitios FTP sin las debidas garantías. Debemos estar alerta ante todos los ficheros que descar-

guemos de la red, almacenarlos en el disco y analizarlos con el antivirus antes de ejecutarlos.

Además, debemos evitar por completo la descarga de ficheros provenientes de páginas underground. En Internet hay numerosas páginas dedicadas a pirateo de programas, hacking o cracking. Estas páginas no son de por sí seguras, pero además pueden servir archivos piratas por FTP. Desgraciadamente, es muy frecuente que esos archivos, no sólo no funcionen, sino que además incluyan virus de última generación, troyanos u otros tipos de código maligno. La mejor forma de evitar una infección por esta vía es no visitar estas páginas.

4.4 Los peligros de la navegación web

Hasta hace bien poco no resultaba peligroso navegar por páginas web: el lenguaje HTML era de una enorme sencillez y no encontrábamos demasiada complejidad en las páginas ya que determinadas tecnologías no se habían generalizado aún. Con la popularización y la masificación de Internet, cuyo servicio más popular es sin duda la World Wide Web, ya han surgido amenazas que utilizan las últimas tecnologías web para difundir virus o dañar nuestro ordenador aprovechándose de las deficiencias de nuestro navegador. Además de los virus HTML también encontramos virus de Java y Active X, dos lenguajes enormemente extendidos por Internet y que, si bien pueden incrementar la potencia de las páginas, también pueden ser una fuente de problemas para los navegantes. El resto de amenazas las podríamos englobar dentro del concepto general de Malware, y consisten en el aprovechamiento, por parte de desaprensivos, de bugs o fallos de programación de los navegadores con fines dañinos o molestos.

Como podremos comprobar, las amenazas que estos virus representan no son especialmente preocupantes y pueden ser evitadas con algo de precaución y un buen antivirus. No obstante, en un futuro estos virus podrían llegar a ser peligrosos, por lo que conviene conocer y prevenir la amenaza.

4.5.1 Los virus HTML

El HTML (o Hypertext Markup Languaje) es el lenguaje utilizado en el diseño y visualización de páginas web. Se trata de un lenguaje relativamente sencillo y en principio, con un editor de texto y unos mínimos conocimientos se puede empezar rápidamente a elaborar páginas web. Sin embargo, con los años se han añadido nuevas funcionalidades al HTML que han facilitado la creación de potentes páginas multimedia.

Precisamente esas funcionalidades son las que han permitido la creación de virus de HTML, es decir, virus cuya infección puede producirse mediante la mera visualización de una página infectada. De momento, el daño potencial de estos virus no es muy grande, y su amenaza es fácilmente combatible, pero conviene

estar prevenido ya que el aumento de prestaciones del HTML es continuo y en el futuro es muy posible que surjan nuevos peligros.

Este tipo de virus se programan con rutinas de Visual Basic Script que se ocultan en el código HTML de la página y se ejecutan automáticamente al visualizarse la misma en un navegador cualquiera. Al ejecutarse, el archivo infecta todas las páginas con las extensiones .HTM o .HTML que haya en el mismo directorio. Los daños varían según el virus.

4.5.2 Java y Javascript

Java y Javascript son dos lenguajes de alto nivel implementados en varias plataformas, incluyendo el PC. Además, los más populares navegadores de Internet soportan estos lenguajes, lo que ha permitido que los llamados "applets" Java y los scripts de JavaScript se puedan ejecutar en ellos. Esto ha facilitado enormemente el desarrollo de pequeñas aplicaciones interactivas y dinámicas. Además, una de las características de Java, la de "write once, run everywhere" (escribir una vez, ejecutar en todas partes), permite que estas aplicaciones se ejecuten en todas las plataformas.

Java funciona en los navegadores porque los programas escritos en este lenguaje se ejecutan en una máquina Java virtual, es decir, como una pequeña computadora escrita en software y que puede residir en tan solo 220 Kilobytes de memoria. La máquina virtual Java puede incluirse en un navegador de Internet. Esto significa que cualquier programa se ejecuta de la misma forma dentro de la máquina virtual Java del navegador, sin importar la plataforma en la que éste se haya instalado.

Java convierte, por tanto, al navegador en un sistema de ejecución de software y no en un mero visor de gráficos y texto.

En lo referente a la seguridad, los creadores de Java han intentado evitar que los applets tengan efectos dañinos. Para ello, hacen que estos pequeños programas que se descargan de Internet se ejecuten en un espacio de memoria aparte, llamado "Sandbox" (cajón de arena). El Sandbox dispone de cuatro líneas de defensa: la primera analiza las características del lenguaje/compilador, la segunda verifica el código de bytes, la tercera se fija en el cargador de clases y la cuarta es un gestor de seguridad.

Según señala Gonzalo Álvarez Marañón, del Consejo Superior de Investigaciones Científicas, estas barreras no son sucesivas, sino simultáneas. Es decir, basta con superar una de ellas para romper toda barrera de seguridad existente.

Y eso es, precisamente, lo que hacen gran cantidad de applets dañinos. Aunque aquí vamos a centrarnos en los virus de Java, también vamos a mencionar todas las posibilidades de ataque, ya que existen gran cantidad de applets dañinos.

Java tiene toda una serie de restricciones de seguridad que limitan enormemente las posibilidades de utilización de applets para producir daños. Según Alvarez Marañón, se resumen en dos:

- No se puede trabajar con ficheros en la máquina del usuario a menos que éste lo permita.
- Sólo se puede conectar, a través de una conexión por Internet, con la máquina que envió el applet.

En la práctica, esto supone que los applets sólo pueden acceder a recursos muy limitados dentro del cajón de arena. Para que puedan acceder al disco, se ha establecido un sistema de firmas digitales similar al ya establecido para Active X (aunque con distinta filosofía).

A través de Java se pueden sufrir diversos tipos de ataques, como robo o destrucción de información, robo de recursos y denegación de servicio. Java puede defenderse de muchos de estos ataques, pero no de otros. Más tarde veremos como prevenir esta amenaza.

También han surgido virus Java que toman partido de algunos puntos débiles en el lenguaje para expandirse.

4.5.3 ACTIVE X

Active X es la respuesta de Microsoft a Java. Se trata de una versión reducida de OLE, es decir, que son como los controles de Windows (controles de edición, botones, listas, check box, etc.) pero de una forma más específica y sofisticada, y permiten la descarga de pequeños objetos ejecutables que pueden ser llamados directamente desde la máquina del usuario. Los controles de Active X son comparables en su función con los applets Java, pero existen ciertas diferencias. Los applets Java se ejecutan dentro de la sandbox, lo que proporciona una mayor seguridad pues restringe su acceso al sistema. En cambio, los controles Active X tienen total acceso al sistema operativo Windows. Esto les da sin duda más poder pero también los convierte en más inseguros.

La forma de controlar la seguridad de estos controles consiste en el sistema de verificación digital y de firmas electrónicas. Si la fuente de código autentificado por la firma es fiable se ejecuta el programa.

4.6 IRC

El IRC (o Internet Relay Chat) es el sistema de charla "escrita" (o "chateo" –del inglés chat, charla-, como lo conocen muchos internautas) más popular de Internet. Mediante este servicio el internauta se conecta a un servidor en el cual se organizan diversos canales o "cuartos" (rooms) de charla agrupados por temas.

En estos canales se puede conversar en tiempo real y a través del teclado con otros usuarios, así como intercambiar ficheros. Miles de internautas utilizan este servicio para conocer gente por Internet, para relacionarse a gran distancia o para intercambiar o compartir archivos. Incluso hay programas que han sido desarrollados en conjunto por varios programadores que intercambian códigos y discuten sobre el proyecto a través del chat. Pero este maravilloso potencial del IRC también le confiere algunos peligros.

El mIRC es uno de los programas más utilizados para acceder a los canales IRC. Este programa soporta un lenguaje script que es interpretado por la aplicación y que además puede ser enviado de uno a otro usuario, ya que según el "script" que se utilice se puede tener acceso a la ejecución automatizada de algunos comandos y a la puesta en funcionamiento de otros a partir de algunas palabras predefinidas o combinaciones de teclas que pueden ser pulsadas durante el chat.

Como siempre, la solución consiste no aceptar jamás archivos de personas que no conocemos, y en particular jamás aceptar un archivo script.ini. Si deseamos recibir este archivo, lo mejor es utilizar versiones posteriores a la 5.3. También es recomendable no activar la opción "autoget", ya que eso permite que cualquiera nos envíe un archivo sin nuestro consentimiento.