

GUÍAS FÁCILES DE LAS TIC

del

COLEGIO OFICIAL DE INGENIEROS DE TELECOMUNICACIÓN

Trabajo Premiado 2006

Virus

Autor:

D. José Manuel Huidobro Moya

17 de Mayo 2006
DIA DE INTERNET



colegio oficial
ingenieros de telecomunicación

Virus informáticos

Los virus informáticos representan uno de los temores más grandes que tienen los usuarios de ordenadores. La infección y propagación de los virus es un problema importante para cualquier ordenador y/o red.

Un *virus informático* es un programa, con efectos más o menos destructivos, que afecta a los archivos y a los discos del ordenador. Actúa intercalándose en otros programas y tomando el control del sistema operativo, haciendo duplicados de sí mismo e insertándolos en otros programas. La creación de un virus es muy fácil y, de hecho, en Internet existen programas para crearlos, algo para lo que no se necesita ser un experto y, muchos lo hacen por pura diversión o para causar daños económicos en venganza de algo, pero hay que tener en cuenta que su creación y propagación está penada y el que lo hace puede acabar en la cárcel.

El virus es realmente un programa informático con características de autorreproducción que contiene una secuencia de instrucciones y rutinas capaces de crear copias de sí mismo, y su objetivo es alterar de alguna forma el funcionamiento de los equipos informáticos. En un elevado porcentaje, los virus destruyen información de los discos y de la memoria de los ordenadores, llegando a destruir por completo todo su contenido. Son programas pequeños que necesitan ir insertados dentro de un archivo, llamado *huésped*, mediante el que se propaga.



Al ir contenido en otro archivo, y tener un tamaño reducido, su detección resulta difícil. Los virus sólo tienen efecto si se ejecutan, porque son simplemente programas que llevan a cabo acciones, de modo que no pueden hacer nada si no se llegan a ejecutar. Al ejecutar el virus, éste se instala para comenzar su propagación, comienza a reproducirse y a infectar los diferentes archivos o memoria, y se pone en funcionamiento, ejecutando las acciones que se hubieran establecido, acciones éstas que nunca son buenas para el ordenador que lo contiene, sino muy perjudiciales.

Existen virus realmente peligrosos que llegan a formatear el disco duro (lo que provoca la pérdida de todos los datos), aunque otros son “amables”, y únicamente muestran algún dibujo o un mensaje de saludo desplazándose por la pantalla. Entre estos extremos existe una interminable lista de posibilidades. Normalmente, los virus no actúan directamente, sino que suelen encontrarse en programas ejecutables (con extensiones .COM y .EXE, por ejemplo), de modo que al ejecutar el programa que contiene al virus, éste pasa a la memoria y se sitúa en condiciones de actuar. Cuando el virus se activa, todos los programas que se utilicen en el ordenador se irán infectando, de manera que se irá propagando por todo él.

En los últimos tiempos, y debido principalmente a la generalización del uso de la informática y del acceso a Internet entre el gran público, además de los virus, gusanos y troyanos (programas con cierto parecido), han aparecido otras amenazas (*malware*) capaces de resultar muy dañinas. La palabra *malware* proviene de la

contracción de las palabras inglesas *malicious software*, es decir, software malicioso. Así, pues, se entiende por *malware* cualquier programa (adware, spyware, etc.) o mensaje (spam) que puede resultar perjudicial para un ordenador, tanto por causar pérdida de datos como por pérdida de productividad.

Tipos de virus

Dependiendo de su concepción y de la forma de actuar, existen varios tipos de virus, que explicamos a continuación:

Virus de programas: son los que infectan archivos ejecutables (nunca de datos). Sólo se pueden encontrar en archivos con extensiones .EXE, .COM, .SYS y .DLL.

Virus del sector de arranque (Boot): son los que infectan el sector de arranque del disco duro (es decir, el sector 0, que contiene los datos relativos a su estructura y el programa de inicialización del mismo). Al cargarse el programa de arranque en la memoria del ordenador (al encender el equipo) también se carga el virus, que toma el control de todas las acciones a ejecutar, interceptando todas las operaciones de lectura y escritura en el disco.

Virus multipartición: se consideran virus mixtos, es decir de programa y de arranque, ya que son capaces de infectar ambos tipos de elementos.

Virus polimórficos: son virus encriptados que modifican su modo de encriptación cada vez que infectan un archivo, de manera que dos archivos infectados por el mismo virus pueden no guardar ninguna relación. Este es el virus más difícil de detectar, porque el sistema tradicional de búsqueda de cadenas no es válido en este caso, al variar entre cada infección.

Virus de macros: las macros (o macroinstrucciones) son lenguajes de programación relativamente sencillos de los que suelen disponer las aplicaciones potentes, tales como procesadores de texto, hojas de cálculo y bases de datos. Cuando un virus se ha generado en forma de macro, entonces se guarda en un *archivo de datos*, lo que hace que por primera vez no sea necesario que el archivo sea ejecutable para infectarse. Además, al estar contenido en archivos de datos, este tipo de virus es independiente de la plataforma informática, lo que resulta un peligro adicional.

Virus invisibles: son los que, debido a su configuración, son difíciles de detectar con los programas antivirus, lo que hace que sea muy difícil su eliminación.

Fases de actuación

Los virus actúan de diferentes maneras según su tipo y la programación que tengan, pero podemos decir que tienen unas fases determinadas desde el momento que se introducen en el ordenador. A continuación vamos a describir las distintas fases de actuación de un virus:

Infección: el virus llega al ordenador, a través de un disco contaminado o de una red (por ejemplo, Internet), contenido en un archivo ejecutable. Al ejecutar ese

programa, el virus se activa instalándose en la memoria.

Propagación: durante esta fase el virus no se manifiesta pero está latente, a la espera de que llegue su momento para actuar. Esta etapa es muy peligrosa, porque el usuario no es consciente de su existencia, pero el virus está contaminando a todos los archivos ejecutables que se vayan utilizando. Si se pasan archivos de este ordenador a otro, éste se contaminará también. Esta fase puede ser muy larga, lo que hace que se pueda contaminar todo el ordenador y otros muchos.

Activación: al producirse ciertas circunstancias, variables según el virus (pero habitualmente tras la ejecución del programa que lo contiene), éste se activa y comienza a manifestar sus efectos, siempre negativos.

Propagación de los virus

Ya sabemos lo que son los virus y las partes de los equipos informáticos que pueden infectarse. Pero, ¿cómo se propagan? Las fuentes más comunes de propagación son los discos removibles o extraíbles (tales como disquetes, CD-ROM, DVD, Zip, magnetoóptico, etc.), así como los puertos de comunicaciones (principalmente a través del correo electrónico, Internet y los archivos recuperados mediante estos sistemas).

Los virus que más rápidamente pueden propagarse son los más efectivos y dañinos. Pero también tienen que ser difíciles de detectar para que tengan tiempo suficiente como para llevar a cabo su labor de instalación, propagación y destrucción. Por ello, los virus suelen estar residentes en memoria, de manera que pueden monitorizar el funcionamiento del sistema operativo y bloquear los procesos que no le convengan, especialmente algunas de las interrupciones, que pueden dar información al usuario sobre su existencia.

Una vez instalados como residentes en la memoria, se suelen dedicar a infiltrarse en todos los archivos ejecutables que se vayan utilizando, de modo que queden *infectados*. En los últimos tiempos hay virus que no necesitan infectar programas y/o que se arrancan directamente con el sistema operativo, lo que les hace ,más difíciles de eliminar.

Protección frente a virus

Para protegerse de los virus hay que tener mucha precaución, y seguir ciertas normas: utilizar siempre programas originales (especialmente en el caso de los juegos), proteger contra escritura todos los discos que deben conservar intacto su contenido (especialmente los programas originales) y disponer de un CD o disquete de arranque, para poder arrancar el ordenador en caso de que un virus haya afectado a nuestro equipo.

Lógicamente, existen programas detectores y eliminadores de virus, y conviene instalarlos en el ordenador. Estos programas son fáciles de conseguir, y se han de ir actualizando cada poco tiempo, ya que continuamente aparecen virus nuevos y *mutaciones* de los anteriores. Las *mutaciones* son modificaciones en el programa

vírico que los hacen pasar desapercibidos ante antivirus que eran capaces de reconocerlos en su forma anterior.

Aunque existen muchos y muy buenos programas en el mercado, los más famosos, conocidos y eficaces son los de Norton, McAfee, y Panda (que, además, es una empresa española con gran reconocimiento internacional). En la figura se muestra la ventana de Norton Antivirus, en la que pueden apreciarse las características y opciones del programa. Observe en la zona superior izquierda la opción LiveUpdate, que es la que permite actualizar el programa y las definiciones de virus nuevos.

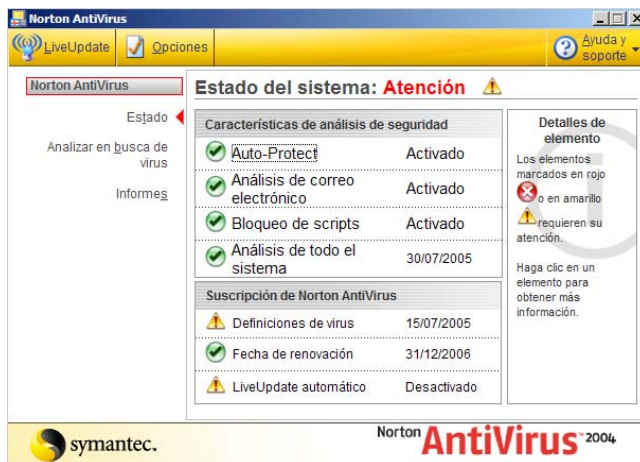


Figura. Ventana del antivirus de Norton.

No existe ningún sistema seguro al cien por cien contra los virus, especialmente debido a que en la actualidad la información (tanto programas como datos y recursos) cada vez se comparte más entre diferentes usuarios. Precisamente, el hecho de compartir información es la forma de exponerse a la infección, ya que si un ordenador no intercambia ningún tipo de información con el exterior no podrá verse afectado por ningún virus. Éste es el sistema más perfecto de antivirus, pero casi siempre resulta imposible trabajar aislado del resto de la información.

Para detectar la presencia de un posible virus en un ordenador hay que observar si su comportamiento cambia de un día para otro, especialmente en cuanto a la velocidad de arranque del ordenador y de ejecución de programas. También hay que comprobar si la capacidad del disco parece haberse reducido, si la fecha y hora del sistema se han visto modificadas, si la pantalla hace extraños o si los atributos de los archivos han cambiado. Además, siempre hay que verificar los discos (de cualquier tipo) que se vayan a cargar en el equipo, buscando si contiene algún virus, y eso hay que hacerlo siempre antes de instalar ningún componente.

Para que en caso de que nos ataque un virus, las pérdidas sean mínimas hay que efectuar copias periódicas de los datos y utilizar un software antivirus y un firewall lo más actualizado posible, algo que podemos hacer periódicamente desde nuestro ordenador con conexión de banda ancha, si estamos suscritos al servicio.