Introducción a los virus y antivirus.

Por Nacho Cabanes, Nov. 2002

(Extraído de mi curso de Informática Básica;

última versión disponible en

www.pobox.com/users/ncabanes)

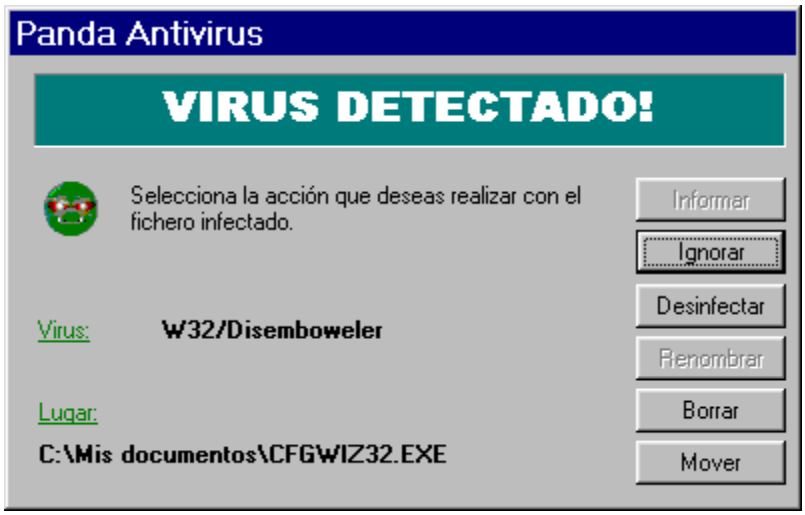
Un virus es un programa de ordenador con intenciones malignas, y que además es capaz de propagarse de un ordenador a otro.

Veremos las nociones básicas sobre cómo trabaja un virus, que tipo de daños puede causar, y cómo se puede propagar. También hablaremos sobre los antivirus, qué tipos de antivirus hay, cómo trabajan y hasta qué puntos son fiables.

- Que hacen y cómo se propagan los virus.
- Los antivirus,
- Recomendaciones.
- Ejemplo de cómo "intuir" un virus sin antivirus.

Virus: qué hacen y cómo se propagan.

Hemos comentado que un virus es un programa de ordenador con **intenciones malignas**. Pero... ¿cómo de malignas? Ha habido un poco de todo: desde virus que se limitaban a mostrar una pelota que rebotaba por la pantalla (molesto pero no realmente dañino) hasta virus que destruyen toda la información contenida en el disco duro (lo que puede suponer unas pérdidas enormes para una empresa, pasando por virus que se limitan a enviar un correo electrónico a todas las personas que aparezcan en la "agenda" de nuestro ordenador (puede saturar las líneas de comunicación pero no tener otras consecuencias más drásticas).



¿Por qué **crea** la gente los virus? Hay muchos posibles motivos: ha habido casos de boicot a ordenadores "enemigos" durante una guerra (declarada o encubierta), chantajes económicos a los poseedores de los ordenadores infectados, pero también en muchos casos se han creado virus simplemente por "el reto"

En cuanto a los detalles concretos en su **forma de actuar**, hay quien distingue entre virus, gusanos, caballos de troya, etc., pero nosotros no entraremos en tanto detalle. Simplemente diremos que hay algunos que actúan una determinada fecha, otros que lo hacen tras propagarse un cierto número de veces, otros actúan en momentos elegidos al azar, y otros provocan los daños nada más llegar a nuestro ordenador.

Lo que sí comentaremos con algo más de detalle son las ideas básicas sobre **cómo se propagan**. La idea básica es que para su propagación hace falta que se den 3 etapas:

1. Que un programa "infectado" llegue a nuestro ordenador.
2. Una vez en nuestro ordenador, que utilicemos ese programa infectado, de modo que el virus pasa a la memoria de nuestro ordenador, queda "oculto" y entonces se podrá propagar a cualquier otro programa que utilicemos a partir de ese momento.
3. Posteriormente, si llega hasta otro ordenador ese programa infectado que había llegado a nuestro ordenador, o cualquier otro que se hubiera podido infectar desde entonces (ya en nuestro ordenador), la propagación del virus continúa.

¿Y cómo **llega** a nuestro ordenador? Hay varias formas posibles:

- Introduciendo en nuestro ordenador un diskette que contiene un fichero infectado.
- Recibiendo un mensaje por correo electrónico, que contenga "adjunto" un fichero infectado.
- Descargando nosotros mismos alguna utilidad "dudosa" a través de Internet.
- En algún CdRom que contenga programas piratas (una práctica tristemente frecuente): los programas originales no pueden estar infectados.

¿Y cómo llega de nuestro ordenador a otros? También hay varias formas posibles:

- Si nosotros grabamos un diskette o un Cd, y entre la información que guardamos hay algún fichero infectado.
- Si enviamos un correo electrónico, en el que "adjuntamos" un fichero que esté infectado.
- Si el propio virus es capaz de enviar correos electrónicos sin que nosotros nos demos cuenta (lo que es bastante posible), de adjuntar a esos correos un fichero "propagador del virus", y de enviarlos mientras estamos conectados a Internet haciendo cualquier otra cosa.

¿Y cómo podemos **detectarlos y eliminarlos**? Empleando antivirus, que veremos en el siguiente apartado.

Los antivirus.

La forma de detectar y eliminar virus es empleando las utilidades conocidas como "Antivirus".

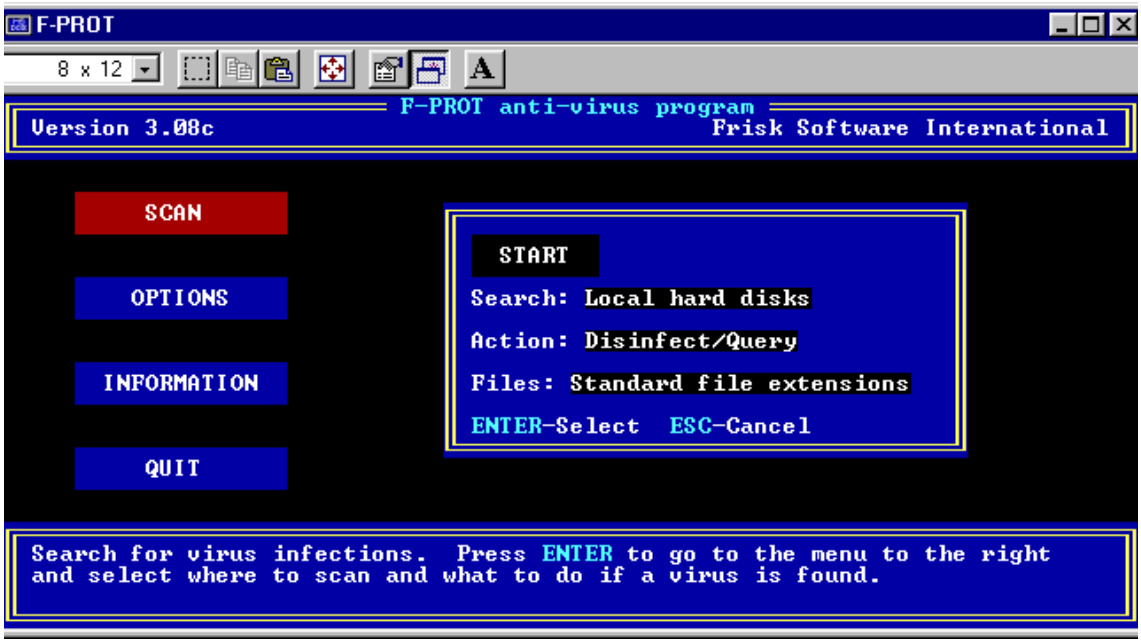
Básicamente hay **dos formas** en que pueden actuar los antivirus:

- Permaneciendo atento a cualquier información que se introduzca en nuestro ordenador, para analizarla "al vuelo", buscando posibles virus.
- Revisando todo nuestro ordenador (normalmente sólo cuando nosotros se lo pidamos) en busca de ficheros infectados que ya se encuentren dentro del ordenador (lo que no necesariamente quiere decir que el virus ya se haya activado).

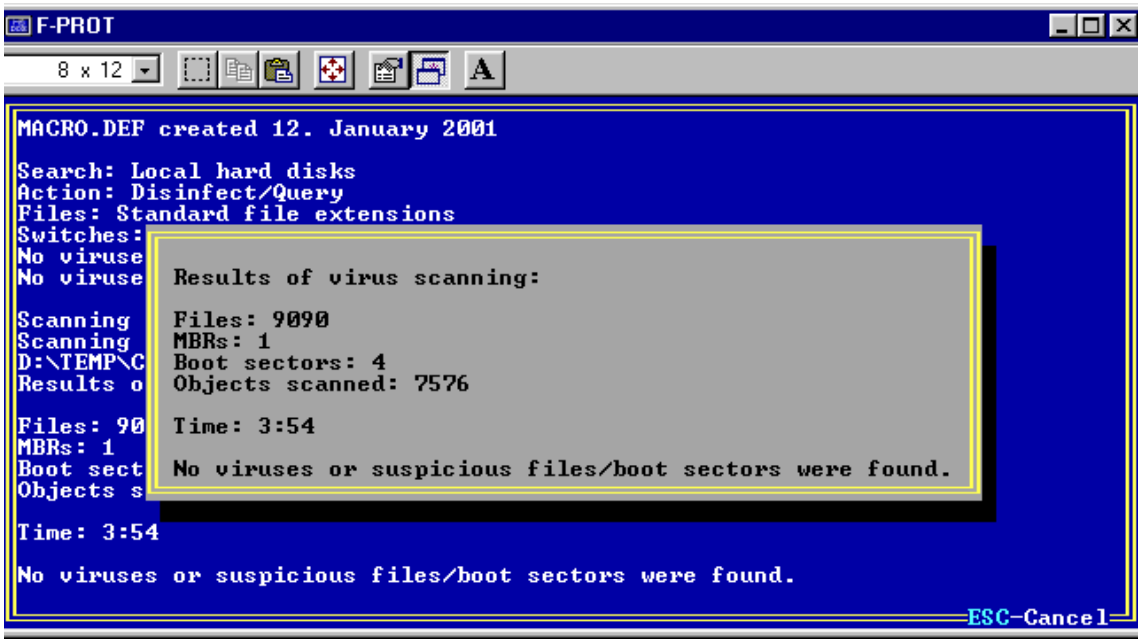
Hay virus que pueden actuar de las dos formas, y los hay especializados en una concreta. **Hoy en día** en que las agresiones pueden venir de tantos sitios distintos, lo habitual es tener trabajando continuamente un antivirus "permanente" (a cambio se suele perder un poco de velocidad de trabajo en nuestro ordenador), mientras que **hace algún tiempo** lo habitual era utilizar el antivirus sólo antes de introducir un diskette en nuestro ordenador, para asegurarnos de que el diskette no contenía nada nocivo, pero no perder rendimiento en el ordenador.

Por **ejemplo**, vamos a ver la forma en la que se usaría un antivirus "antiguo", como F-Prot en su versión para MsDos:

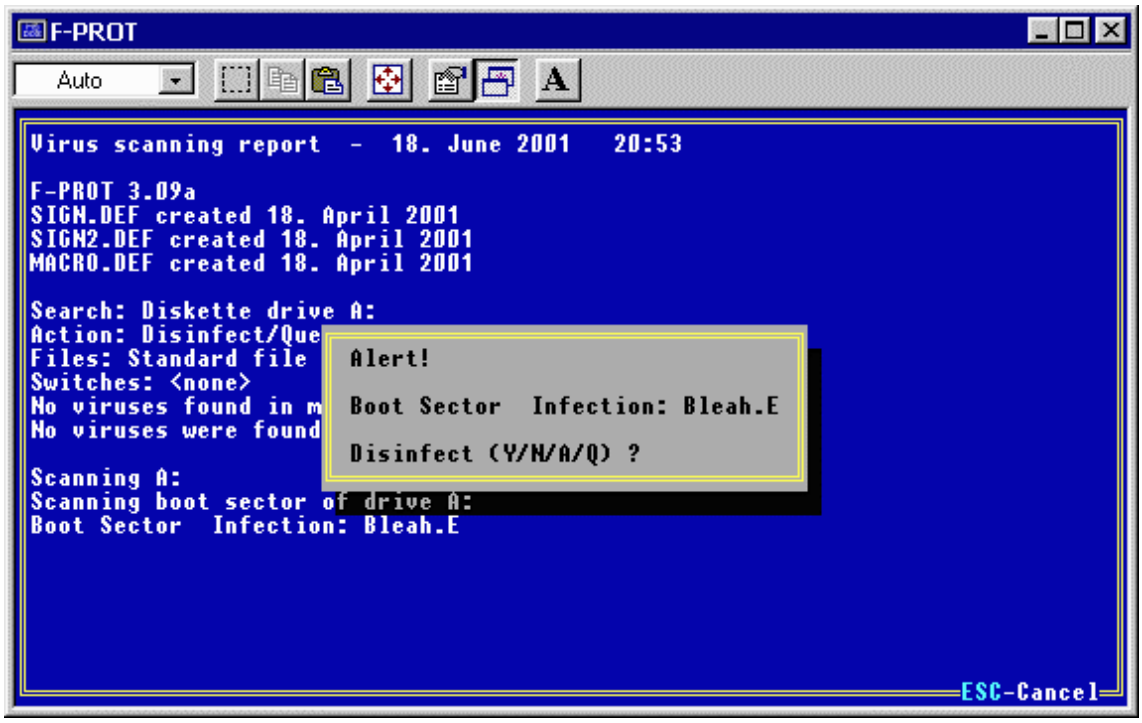
El primer paso sería (por supuesto) entrar al antivirus para revisar el diskette o nuestro disco duro:



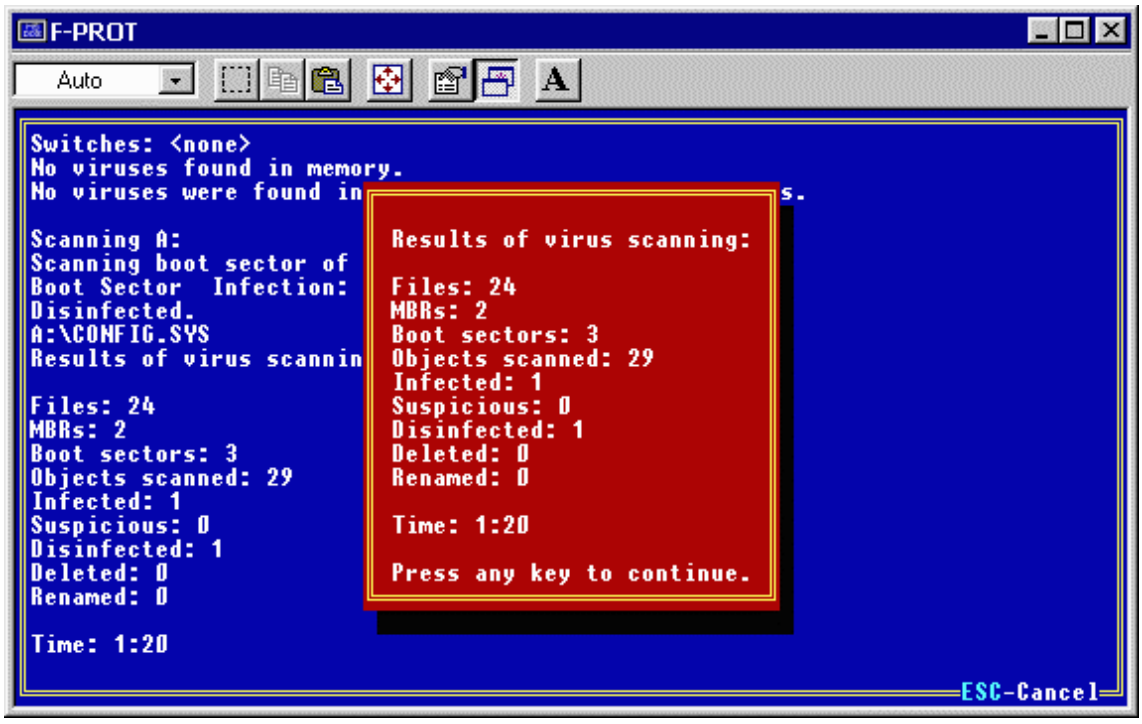
El segundo paso sería decirle las opciones concretas que nos interesan (revisar el diskette o el disco duro, si queremos que nos avise o que desinfecte automáticamente, qué tipo de ficheros queremos revisar, etc) y pedir que comience la búsqueda. Si todo es correcto, al final se nos mostraría una información de resumen:



Pero también puede ocurrir que sí se encuentre algún virus. Según las opciones que hayamos indicado, puede ocurrir que el antivirus lo elimine automáticamente o que nos pida confirmación:

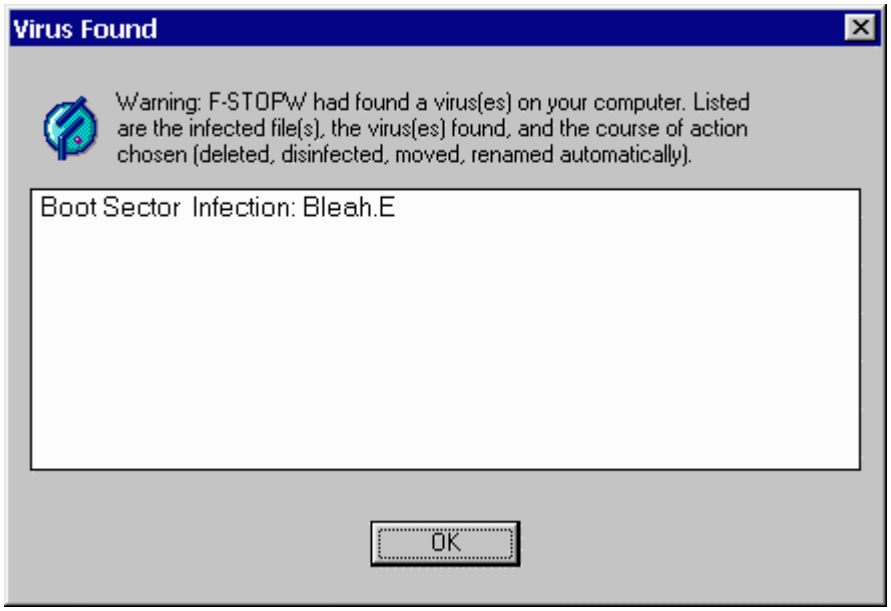


En cualquier caso, al final obtendríamos nuestro resumen, sólo que esta vez sería un poco distinto:

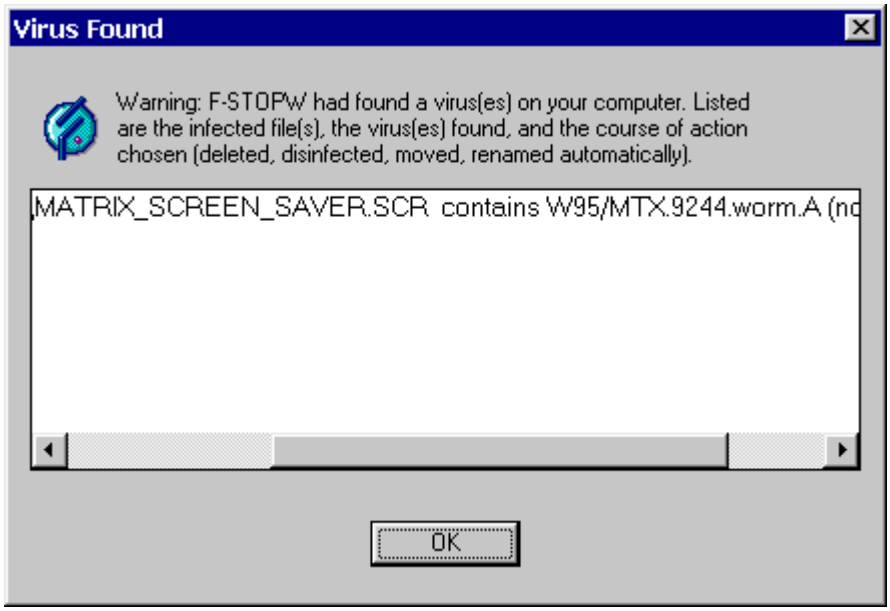


En el otro extremo están los antivirus **permanentes**. Estos se activan apenas acabamos de entrar a nuestro ordenador, e intentar interceptar cualquier cosa que utilicemos a partir de entonces, y rastrearla en busca de virus. Por ejemplo, la siguiente pantalla muestra la información de F-STOPW, la versión para Windows de F-Prot:

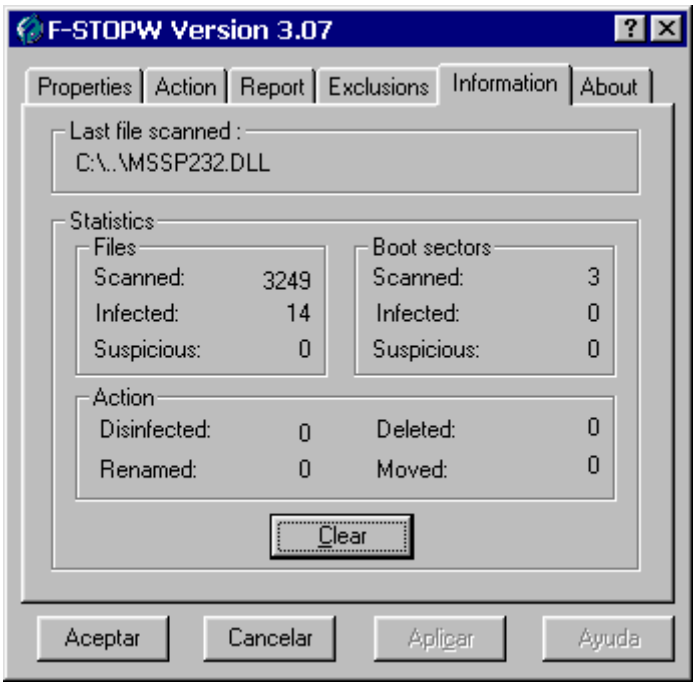
Y si el antivirus descubre algo anormal, nos avisaría y lo eliminaría. Por ejemplo, la siguiente imagen muestra a F-STOPW capturando un virus de los llamados "boot" (los que quedan escondidos en la pista de arranque de un diskette o disco duro):



y la siguiente es el mismo antivirus capturando un virus "convencional", que se encontraba oculto en un salvapantallas:

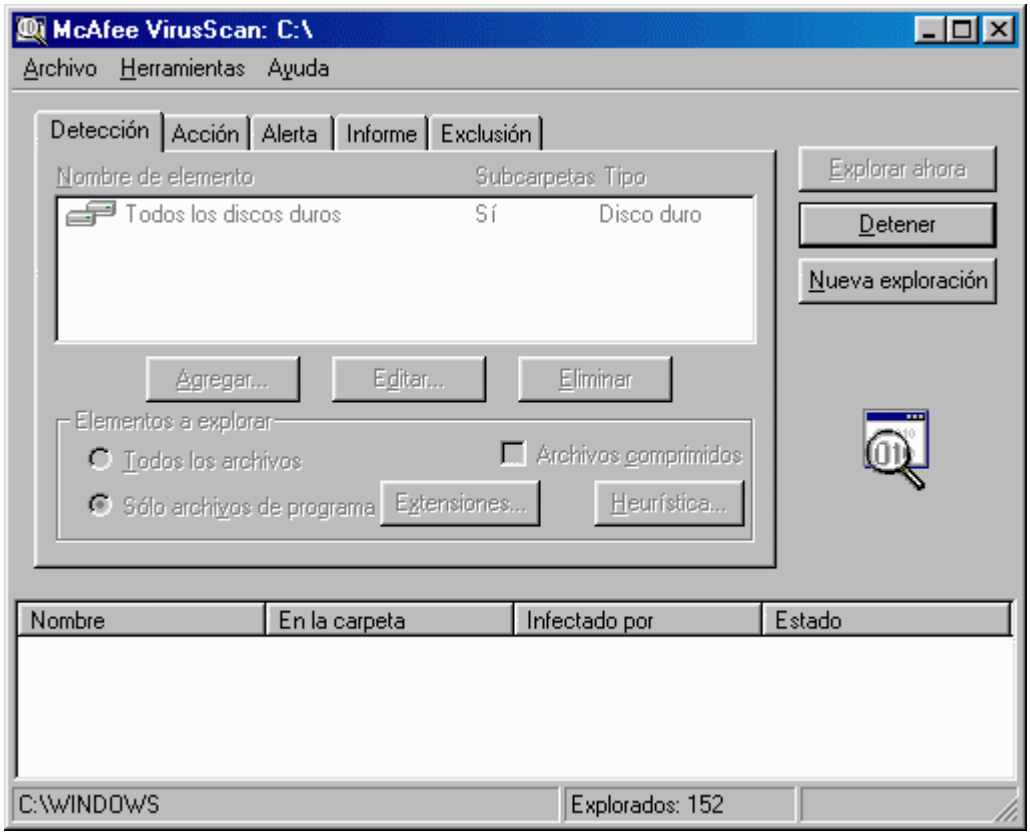


Al igual que en la versión para MsDos, podemos pedir estadísticas sobre el funcionamiento del antivirus:

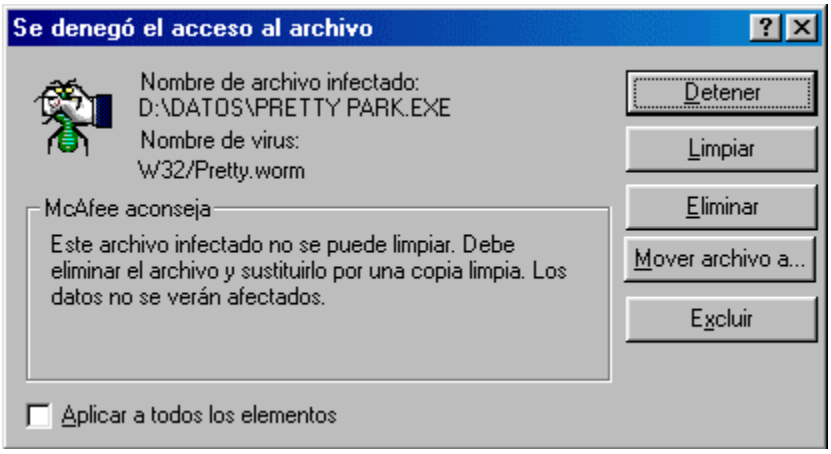


Yo suelo utilizar F-PROT (y su evolución F-STOPW) en mi ordenador particular porque es gratis, pero tiene el inconveniente de que está en inglés y de que es más difícil de instalar.

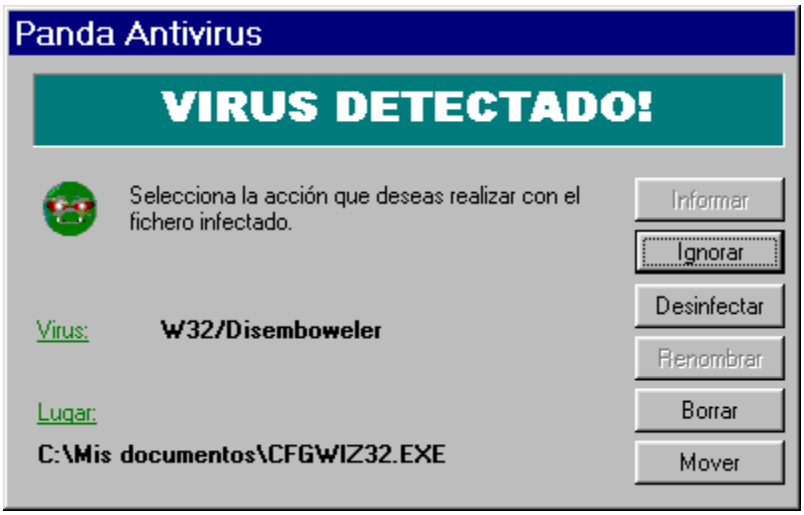
En mi anterior empresa empleaban **VirusScan** de McAfee, que no es gratis pero tampoco resulta caro y es muy bueno y fácil de actualizar. La siguiente imagen muestra este antivirus haciendo una exploración "bajo pedido"



y éste es el mismo antivirus cazando un virus "al vuelo":



Otra opción, por una casa española de software, es **Panda Antivirus**. Las versiones iniciales eran más lentas que los dos anteriores, pero parece muy fiable, lo actualizan a diario, y los usuarios registrados pueden descargar las actualizaciones gatuitamente de su página Web:



Y hay otras muchas más. Lo importante es escoger un antivirus con un cierto nombre (como garantía de que la casa que lo crea no va a cerrar poco después) y que se pueda actualizar con frecuencia:

Insisto: se puede utilizar cualquier antivirus de estos o de los otros muchos que existen en el mercado... pero, sea el que sea, **lo importante es usar uno**. Y tenerlo actualizado.

Recomendaciones sobre virus.

Nunca estaremos seguros al 100%, porque los antivirus SIEMPRE van por detrás de los virus: primero aparece el virus y después se mejoran los antivirus para ser capaces de detectarlo y eliminarlo. Pero al menos hay unas pautas básicas que podemos intentar seguir:

- Tener siempre instalado un antivirus de los que actúan de forma permanente (hoy en día cualquiera lo será).
- Asegurarnos de que está actualizado (un antivirus con más de 3 meses de antigüedad es muy poco fiable, especialmente para alguien que use medios como Internet, por los que los nuevos virus se pueden propagar a una velocidad enorme). La mayoría de las empresas creadoras de antivirus permiten descargar de su página Web las últimas actualizaciones (lo que se suele llamar "firmas de virus").
- Aun así, desconfiar siempre antes de abrir ficheros que recibamos por correo electrónico o por cualquier otro medio "no totalmente fiable", especialmente si proceden de desconocidos, pero también de conocidos, por la forma de propagarse de muchos virus actuales
- Son especialmente críticos los ficheros con extensión EXE (programas ejecutables), COM (algunos programas de MsDos), SCR (salvapantallas), y les siguen de cerca los ficheros DOC (documentos de Word), XLS (hojas de cálculo de Excel), MDB (bases de datos de Access), PPT (presentaciones de Powerpoint) y algún otro.
- No serán peligrosos los ficheros TXT (texto puro), JPG (imágenes fotográficas) y GIF (imágenes con menos colores o imágenes animadas), por poner un ejemplo.

Todas estas recomendaciones son para gente que trabaja con **Windows** (y en algunos casos, equipos más antiguos como MsDos). **Otros sistemas**, como los Unix (y en concreto Linux) son mucho más inmunes a los virus, porque en estos sistemas cada usuario sólo tiene acceso a SU parte del ordenador, y no podrá borrar ni modificar información que pertenezca a otro usuario (algo que sólo puede hacer ese otro usuario o el Administrador del sistema). Por eso, es casi imposible que un virus pudiera causar tantos destrozos en un sistema Linux como en un sistema "poco fiable" como los Windows 95/98/Me; lo más que podría hacer es destruir información concerniente a un único usuario.

Está claro que cualquier administrador de un sistema Unix sólo debería usar su cuenta de administrador para "administrar", y usar otra cuenta de usuario "normal" para el resto de operaciones (si el virus se le cuela al administrador, que sí tiene permisos para hacer "de todo", se habría perdido esa seguridad extra). Pero se supone que un administrador de un sistema Unix es un experto y que ya sabe este tipo de cosas... esperemos...

Ejemplo de cómo "intuir" un virus sin antivirus.

Vamos a ver un ejemplo de un caso en el que podemos "sospechar" que un virus intenta entrar en nuestro ordenador.

Nos pondremos en el caso de los virus que se propagan a través de correo electrónico, que es el más frecuente en la actualidad. Una buena forma de hacerles un poco más difícil la entrada es **no usar Outlook Express**. Este programa de correo descarga todos los mensajes sin que antes podamos echar un vistazo a sus cabeceras, y, lo que es más grave, nos muestra el mensaje en pantalla si hacemos clic sobre él para eliminarlo, lo que deja las puertas abiertas a muchos virus.

Por eso, yo recomendaría **usar correo web**. Es el correo (normalmente gratuito) que muchos proveedores de Internet nos permiten leer desde una página Web. En este tipo de correo se nos muestra habitualmente la "cabecera" de los mensajes antes de que pasemos a leerlos:

El caso de la imagen anterior es típico (aunque extremo):

- Se trata de **mensajes "grandes"** (un mensaje "normal" debería ocupar entre 1 y 15 K).

- Los nombres de los **remitentes son "extraños"** (además de desconocidos): en ninguno aparece detallado el nombre y los apellidos (aunque ciertos virus sí podrían propagarse realmente desde el ordenador del remitente, y entonces sí aparecería su nombre y apellidos, incluso el de una persona conocida).

- Unos tienen **asuntos extraños** (BorderColor), otros piden que vuelva a enviar un mensaje que yo no he enviado, y otros tienen contenidos supuestamente interesantes (herramientas para eliminar el virus Klez, parche para Internet Explorer 6.0, introducciones a ADSL) pero que yo no he pedido.

- Para colmo, están **en inglés**, y el 99,99% del correo que yo envío/recibo es en castellano (aunque hay algún virus que se propaga en castellano).

- ...

Pues sí, yo en este caso seleccionaría todos ellos con la casilla de la izquierda, y los borraría directamente sin leerlos, porque tienen **todas** las características que nos pueden hacer preocuparnos. Sólo con una de ellas sería suficiente para no leerlo, y, en todo caso, responder antes al remitente preguntándole "¿Me has enviado tú este mensaje?". Si él lo ha enviado, puede que contenga virus, pero si no lo ha enviado él, está claro que sí se trata de un virus.

Pero lo dicho: **es peligroso** abrir mensajes grandes (algo que outlook express hace sin preguntarnos), es peligroso leer mensajes de desconocidos, es peligroso abrir mensajes con asuntos extraños, o que no hayamos solicitado, o que estén en un idioma distinto al nuestro... y es **un suicidio** abrir un mensaje que tenga varias de estas características juntas, como los de la imagen anterior o como estos otros:

☑	✉	1:11 am	sherror	190K	Welcome to my hometown
☐	✉	3:22 am	klopez	134K	Let's be friends
☐	✉	4:47 am	artifactsmx	129K	Hello,sos!
☐	✉	6:35 am	ninos	131K	A very nice game