

# ClamTk

## - escáner antivirus

Jean-Pierre Féval

Lo primero que se nos ocurre después de haber oído las palabras “escáner antivirus para Linux” es “¿Qué? Pero si prácticamente no hay virus para Linux...”. Correcto, pero Linux suele emplearse con frecuencia como servidor de ficheros o de correo para los clientes que utilizan el sistema Windows. Puede también compartir un mismo ordenador con el sistema de Redmond. Y en ambos casos los programas antivirus ya pueden resultar mucho más útiles. El programa *Clam AV* ha sido diseñado para escanear el correo que llegue por el servidor de correo en busca de los virus y los gusanos de Internet, pero también puede emplearse para escanear los ficheros individuales, o directorios enteros del disco duro (incluido el contenido de archivos). Sus mayores ventajas abarcan el código abierto, el ser gratuito, así como el tiempo relativamente corto de reacción a la aparición de los virus nuevos (gracias a la contribución de muchos usuarios). Debido a que el uso de la línea de comandos no es muy cómodo para todos, se han elaborado un par de frontends gráficos, de los que *ClamTk* forma parte. Es un frontend excelente tanto para actualizar la base de los virus (y más precisamente sus firmas), como para escanear el disco duro.

Si se trata de *Aurox*, o de distribuciones parecidas, la instalación del programa no produce ninguna dificultad, aunque hay que cumplir con un par de dependencias. Además del paquete *RPM*, creado por el autor, está disponible la versión colocada en el repositorio *DAG* (<http://dag.wieers.com/packages/clamtk/>). Por supuesto, también es necesario instalar el propio programa *ClamAV* (los paquetes *clamav* y *clamav-db*). Podemos descargarlos también del repositorio *DAG*, igual que otros paquetes imprescindibles: *perl-File-Find-Rule*, *perl-Number-Compare*, *perl-Text-Glob* y *perl-Gtk2*. Aunque este último se suministra junto con *Aurox*, es aconsejable instalar su versión más

reciente. El mismo repositorio nos permite descargar los paquetes *Rar* o *Unrar*, lo que permitirá al escáner analizar el contenido de los archivos *RAR*.

Podemos iniciar el frontend *ClamTk* seleccionando el elemento apropiado en el menú, o dando el comando `clamtk`. Si aparece un error, cuyo contenido será “`locale_h` is not exported by the POSIX module”, la solución más sencilla consiste en editar el fichero `/usr/bin/clamtk` y localizar en éste la línea número once, que tiene la siguiente forma: `use POSIX qw/strftime locale_h/`. Basta cambiar las palabras `strftime` y `locale_h` una por otra para que el programa se arranque como es debido. El aspecto final de esta línea será así: `use POSIX qw/locale_h strftime/`. Lo mejor que podemos hacer al principio es actualizar la base de firmas. Para lograrlo, hay que iniciar *ClamTk* con los permisos de administrador. La opción *Signature Date* del menú *Help* permite verificar de qué día es la base de firmas instalada. Puede actualizarse mediante la opción *Update Signatures*.

Para que el programa marche regularmente son suficientes los permisos de un usuario normal. Sólo es importante que éste tenga derechos para escanear los ficheros. Para empezar, conviene comprobar qué actividad va a emprender el programa después de dar con un fichero infectado. Por defecto, no hace nada salvo visualizar la información en la ventana principal del programa. Ahora bien, esto puede cambiarse en el menú *Take This Action*. Escogemos entre someter el fichero a cuarentena (*Quarantine*) o eliminarlo (*Delete*). La última opción debe practicarse con un cuidado especial, puesto que, a pesar de lo bueno que es el programa, siempre puede producirse una falsa alarma.

Existe la posibilidad de grabar la información sobre los escaneados ya concluidos. Desafortunadamente, sólo se graba la fecha del escaneado, la cantidad de las firmas y los ficheros escaneados, así como la información de los virus detectados. En cambio, falta la información de qué directorios han

File	Type	Size	Status
clspack.exe	MS Windows PE 32-bit Intel 80386 GUI executable	49,42 KB	Clean
javacpy.dll	MS Windows PE 32-bit Intel 80386 GUI DLL	187,15 KB	Clean
javapxy.dll	MS Windows PE 32-bit Intel 80386 GUI DLL	63,25 KB	Clean
javart.dll	MS Windows PE 32-bit Intel 80386 GUI DLL	404,75 KB	Clean
xvid.dll	MS-DOS executable (EXE), OS/2 or MS Windows	684,03 KB	Clean
jdbmgr.exe	MS Windows PE 32-bit Intel 80386 GUI executable	15,12 KB	Clean
jview.exe	MS Windows PE 32-bit Intel 80386 console executable	172,30 KB	Clean
olecvt32.dll	MS-DOS executable (EXE), OS/2 or MS Windows	34,30 KB	Clean
olevr32.dll	MS-DOS executable (EXE), OS/2 or MS Windows	22,02 KB	Clean
olethk32.dll	MS-DOS executable (EXE), OS/2 or MS Windows	69,12 KB	Clean
xvid.ax	MS-DOS executable (EXE), OS/2 or MS Windows	372,74 KB	Clean
msawt.dll	MS Windows PE 32-bit Intel 80386 GUI DLL	154,38 KB	Clean
msjava.dll	MS Windows PE 32-bit Intel 80386 GUI DLL	947,47 KB	Clean
msjdc10.dll	MS Windows PE 32-bit Intel 80386 GUI DLL	21,26 KB	Clean
vmhelper.dll	MS Windows PE 32-bit Intel 80386 GUI DLL	286,99 KB	Clean
wjview.exe	MS Windows PE 32-bit Intel 80386 GUI executable	171,79 KB	Clean
wurweb.dll	MS-DOS executable (EXE), OS/2 or MS Windows	120,29 KB	Clean
zonedoff.reg	ASCII text, with CRLF line terminators	< 1 KB	Clean
zonedon.reg	ASCII text, with CRLF line terminators	< 1 KB	Clean
dx3.dll	MS Windows PE 32-bit Intel 80386 GUI DLL	313,86 KB	Clean
javaee.dll	MS Windows PE 32-bit Intel 80386 GUI DLL	139,54 KB	Clean
javasup.vxd	MS-DOS executable (EXE), OS/2 or MS Windows	7,32 KB	Clean
ntprint.dll	MS-DOS executable (EXE), OS/2 or MS Windows	92,16 KB	Clean

Files Scanned: 42 Viruses Found: Elapsed time: 00:45

Figura 1. El escaneado de un gran número de ficheros puede tardar un poco

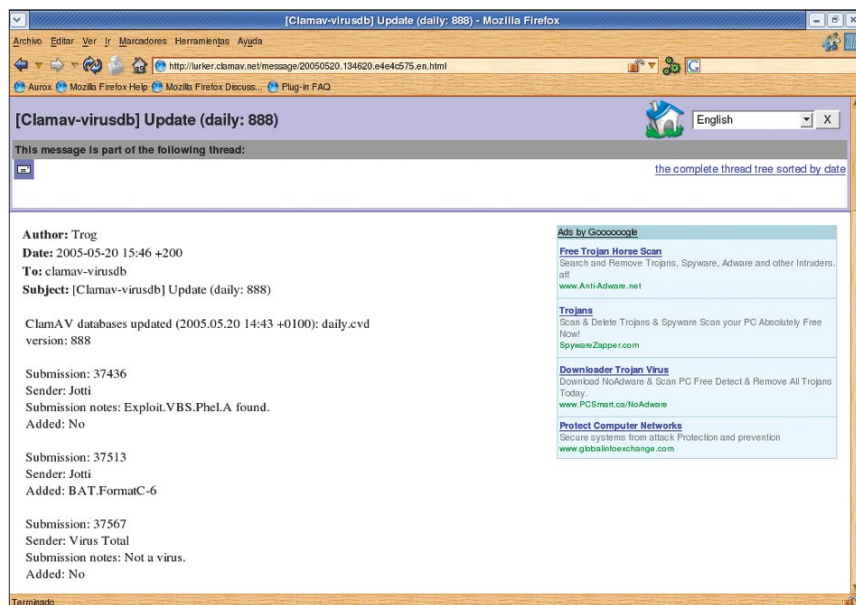


Figura 2. Se aconseja actualizar las firmas de virus, porque cada día aparecen muchos nuevos

sidio escaneados. Para iniciar la autorización basta pulsar la tecla [F1] o seleccionar la opción adecuada en el menú *Scan Options*. Los ficheros del registro se almacenan en el directorio `~/clamtk/history/`, provistos de nombres correspondientes a las fechas del escaneo. Es posible verlos después, aprovechando la opción *View->View Histories*. Cuando ya dejan de ser útiles, se pueden borrar a través de *View->Delete Histories*.

Además de la autorización, disponemos de dos opciones de escaneado más. Es el escaneado de los ficheros ocultos (cuyos nombres empiezan con un punto) que se inicia con la tecla [F2], y la visualización en la pantalla principal de los nombres de todos los ficheros escaneados, y no sólo los infectados (se inicia con la tecla [F3]).

Hay tres métodos de escaneado disponibles. Se puede escanear un fichero individual (la combinación de teclas [Ctrl]+[F]), un directorio (la combinación [Ctrl]+[D]), así como un directorio de forma recursiva ([Ctrl]+[R]). A la hora de realizar la selección del directorio a escanear hay que tener cuidado de no entrar en él: si contiene cualquier subdirectorio, se escaneará el subdirectorio indicado.

El escaneado recursivo de los directorios más grandes puede durar un poco. No hay que preocuparse si a veces el programa aparece como hibernado: si sólo oscila el control del disco duro, lo más probable es que el programa esté analizando algún archivo. Las actividades realizadas por *ClamTk* en el caso de detectar un fichero con virus dependen de las opciones que acaban

de mencionarse. El programa se limita, de forma estándar, a alertar al usuario mediante un aviso en la ventana principal. Si se ha seleccionado la cuarentena como acción por defecto, además de avisarlo, el programa lleva el fichero infectado al directorio `~/clamtk/viruses/`, y a su nombre se le agrega el sufijo `.VIRUS`. Podemos conocer la cantidad de ficheros afectados por la cuarentena al seleccionar *Quarantine->Status*. Si resulta que en el caso de cualquier fichero se ha dado una falsa alarma, hay que llevarlo de vuelta a su directorio manualmente; por desgracia *ClamTk* carece de la funcionalidad correspondiente. Podemos eliminar los demás ficheros escogiendo la opción *Quarantine->Empty*.

Utilizando el software antivirus conviene recordar que ningún programa es perfecto. La protección es mucho más eficaz si nos ponemos dos escáners antivirus independientes. Esto se refiere en particular a los servidores de correo, pero también es una buena solución en el caso de los ordenadores de sobremesa.

El cambio más importante en la última versión del programa *ClamTk* consiste en añadir el test de la conexión de Internet antes del arranque de la actualización de las firmas. Esto permite evitar la "hibernación" larga del programa, aunque de todas formas, si se produce un problema con la conexión, da como resultado un inevitable minuto de espera. Además, se han introducido un par de correcciones pequeñas.

<http://freshmeat.net/projects/clamtk/>

### Logwatch 6.1

Logwatch es uno de los programas responsables del análisis de las bitácoras del sistema y de la generación de informes. Arrancándose cada periodo fijo de tiempo, proporciona a cada administrador de sistema los informes necesarios. Su última versión cuenta con una serie de correcciones y mejoras. Se ha mejorado la opción `--range`, se han añadido servicios nuevos: *audit*, *sonicwall* y *zz-network*, y se ha agregado la opción `--numeric`, que permite bloquear ciertas consultas DNS.

<http://freshmeat.net/projects/logwatch/>

### Gujin 1.1

*Gujin* puede resultar una alternativa interesante para los programas populares *LILO* o *GRUB*. Este cargador de arranque (*boot loader*) intenta analizar por su cuenta las particiones bootables disponibles (no sólo las de Linux, sino también las de los sistemas de las familias *BSD*, *MS-DOS*, *Windows* y otras) y visualiza un menú gráfico, en el que se puede seleccionar el sistema para iniciar. Su punto fuerte se basa en que detecta por su cuenta las imágenes del núcleo fijados en el directorio `/boot`, así que no es necesario que cambiemos la configuración del *bootloader* después de instalar uno nuevo. La versión más reciente ofrece, sobre todo, las correcciones de los errores que ocurrieron.

<http://freshmeat.net/projects/gujin/>

### TCP/IP Connection Cutter 1.03

Todos los administradores de Red deben agregar a sus conjuntos de herramientas este interesante programa. Permite cerrar las conexiones *TCP/IP* que pasen un cortafuegos basado en *IPtables*. Resulta curioso que la conexión se cierre de una forma que hace pensar a cada parte que ha sido la otra quien la ha cerrado. Por cierto, esta herramienta no debe utilizarse para hacerles la vida más dura a los usuarios, sino sólo en casos justificados. En la nueva versión se ha ampliado el mecanismo de análisis de ficheros en el directorio `/proc/net/`, gracias a que el programa es capaz de cooperar con más versiones del núcleo y más opciones *conntrack*.

<http://freshmeat.net/projects/tcpipcutter/>

### Blueflops 2.0.10

*Blueflops* es una distribución que ocupa dos disquetes y contiene el navegador *Linx* y *Tirc*, un sencillo cliente de *IRC*. El núcleo contiene la mayoría de los controladores de las tarjetas de Red compilados como módulos, así como el soporte de *PPP*. La última versión está provista, además, de una traducción holandesa. La versión del núcleo ha ascendido a 2.6.11.9, y *Syslinux* se ha actualizado a la versión 3.08-pre11.

<http://freshmeat.net/projects/blueflops/>