



**Fernando de la Cuadra**  
**Editor Técnico Internacional**  
**Panda Software** ([www.pandasoftware.es](http://www.pandasoftware.es))  
**E-mail:** [Fdelacuadra@pandasoftware.es](mailto:Fdelacuadra@pandasoftware.es)



## Más allá de los antivirus

Cada vez que aparece una nueva amenaza vírica existe un tiempo en el que los usuarios se encuentran expuestos a la infección, exactamente el intervalo entre que el virus está reproduciéndose y los laboratorios de las firmas antivirus ponen a disposición de los usuarios la actualización para neutralizar ese nuevo código. Ese tiempo no suele ser demasiado, apenas unas horas en los casos más complejos, pero hoy en día los autores de los nuevos virus y gusanos, conscientes de la existencia de ese lapso de tiempo de desprotección, han conseguido que sus creaciones se propaguen más rápidamente.

Si nos fijamos en las amenazas más rápidas que han aparecido hasta ahora -como Sasser, Blaster o SQLSlammer- todas ellas han intentado (y conseguido) causar daños en pocos minutos, sin duda un tiempo menor que la capacidad de reacción de cualquier laboratorio de virus.

Para paliar este problema, algunas empresas antivirus intentaron implementar sistemas de detección automática de virus nuevos, de manera que el usuario podía enviar un fichero sospechoso y, de manera automática, se generaba el sistema de desinfección del supuesto virus. Este sistema tiene un gran inconveniente, ya que siempre es necesario que el usuario del ordenador sea consciente de que hay un fichero que puede resultar sospechoso para enviarlo, lo que es muy difícil en usuarios con pocos conocimientos informáticos.

Con el objetivo de poder detectar amenazas desconocidas se han hecho aproximaciones desde el punto de vista del análisis heurístico, en el que se analiza el código interno de un programa para detectar posibles instrucciones maliciosas. Este sistema es válido cuando el código va a llevar a cabo una acción directamente perjudicial en el sistema, como podría ser una sobrescritura de sectores de arranque de un disco duro. Desgraciadamente, las amenazas existentes hoy en día no utilizan una instrucción tan obvia como "format c:". Los creadores de virus saben perfectamente que los motores heurísticos, incluso los más básicos, van a detectar ese intento de daño rápidamente. Por ello intentan utilizar sistemas que hagan pasar desapercibidas a sus creaciones ante los métodos clásicos de detección. Por ejemplo, SQLSlammer o Sasser penetraban en el ordenador a través de una instrucción dada en TCP/IP directamente.

Aprovechando una vulnerabilidad (en SQL Server y en Windows), tanto SQLSlammer como Sasser entraban en los ordenadores sin levantar sospechas. Al no ser ningún fichero que llegara por correo o en un disquete, ni utilizar ninguna instrucción potencialmente peligrosa, los antivirus clásicos no los detectaban. ¿Qué solución puede aportarse a este problema?

En principio, una vez que tenemos un código malicioso en el sistema, tiene que llevar a cabo alguna acción para poder reproducirse, como la explotación de una vulnerabilidad que haga caer la seguridad del sistema. Si mediante algún proceso específico se controlan los elementos básicos del sistema se puede, sin duda, detectar una anomalía. Así, por ejemplo, un sistema que controlara la cantidad de correos electrónicos salientes de un sistema descubriría un incremento de actividad ante un gusano que estuviera reenviándose masivamente. Ante un cambio brusco de la actividad del correo no cabe duda de que algo extraño está pasando, así que bastaría con buscar el proceso que está generando esos envíos masivos para encontrar un más que probable gusano de correo electrónico.

Del mismo modo, si se controlan determinadas acciones dentro de elementos vitales del sistema podremos evitar problemas típicos de los virus. Volviendo al ejemplo de SQLSlammer, la única manera de poder detenerlo es una inspección profunda de todos los paquetes TCP/IP de una comunicación, tanto los de entrada como los de salida. Pero, en este caso, hay que ir mucho más allá: si un virus de este tipo va a atacar en escasos minutos, no debe buscarse un

simple patrón que coincida con una firma vírica, debe analizarse la razón de la transmisión de ese paquete y su contenido para poder detectar como tal una acción peligrosa.

El análisis debe efectuarse en TCP, UDP e ICMP, para así poder detectar ataques a niveles superiores al de red.

Con un sistema de detección de amenazas potenciales como el planteado podrán evitarse ataques de denegación de servicio, escaneos de puertos, ataques directos de hackers, IP-Spoofing, MAC-Spoofing, etc. Sin embargo, una tecnología que lleve a cabo este proceso de detección no podrá ofrecer a un usuario o a un administrador de red el nivel de protección contra virus e intrusos por sí mismo. La protección antivirus clásica no puede dejarse de lado, ya que su protección es ahora mismo muy efectiva contra las amenazas conocidas, pero complementada con sistemas de detección que vayan más allá del simple análisis, incluso con análisis de procesos en ejecución.

La llegada de este tipo de tecnologías es inminente, lo que sin duda redundará en el nivel de protección que todos los usuarios de Internet en 2004 necesitan contra las nuevas amenazas desconocidas.

**Fernando de la Cuadra**

**Editor Técnico Internacional**

**Panda Software** (<http://www.pandasoftware.es/>)

**E-mail:** Fdelacuadra@pandasoftware.es