Javier Rubio Villacé. Asesor Técnico Docente. Área de Programas Educativos. Tlf.: 983412630 - Fax: 983412679. Dirección Provincial de Educación.Delegación Territorial de Valladolid. Junta de Castilla y León

DETECCIÓN DE PROGRAMAS "PARÁSITOS" QUE ACTÚAN DESDE EL INTERIOR DE LA RED

En las últimas semanas se ha producido un aumento del número de centros que han recibido una notificación de su proveedor de servicios de Internet avisando de que son emisores de SPAN y amenazando con tomar medidas si no lo solucionan. Estas medidas consisten generalmente en cerrar el puerto 25 para bloquear el envío de correo desde la red. Solamente podríamos utilizar Webmail, pero no clientes como Outlook. El siguiente paso, si no tomamos medidas, sería la desconexión de la ADSL.

Para solucionar el problema tendremos que localizar el 'programita' que nos han dejado de regalo en algún equipo de la red. Estas joyas suelen descargarse gratuitamente junto con música o películas. Y no siempre son detectadas por los antivirus.

……

Partimos del supuesto de una red de grupo de trabajo o de dominio, sin servidor de correo y sin servidor de seguridad. Ésta es la situación más común en los centros de enseñanza.

Aquí vamos a ver dos posibilidades, aunque hay más; todo depende de la infraestructura de nuestra red y de nuestros conocimientos informáticos. En cualquier caso el segundo procedimiento de este informe es comparable a cualquier otro más sofisticado.

1º Procedimiento para detectar un relé emisor de spam dentro de la red.

La solución más sencilla, aunque también la más lenta, requiere ir equipo a equipo con un programa de detección de puertos abiertos. **TCPview** (Windows) es una herramienta Freeware, (http://www.microsoft.com/technet/sysinternals/Networking/TcpView.mspx) muy útil para este menester. No requiere instalación alguna, lo que nos da la posibilidad de grabarla en un Pendrive y pasar por todos los PCs activando el ejecutable del programa.

Permite ver los puertos abiertos en el equipo junto con el programa que los abre. Nuestro objetivo SERÁ localizar un ordenador con el puerto 25 abierto. Si hacemos Clic con el botón secundario del ratón sobre la línea sospechosa obtendremos información sobre el proceso que está detrás.

Una vez detectado el malware:

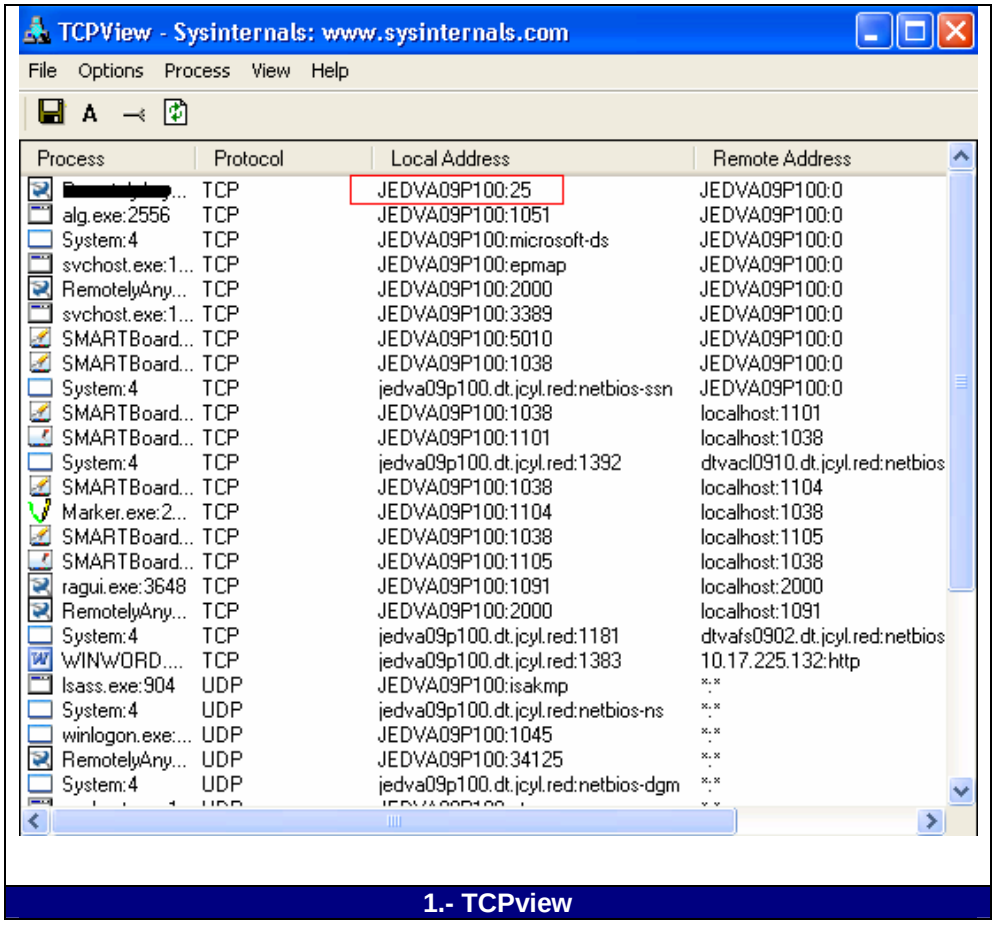
- Localizamos el equipo con la IP detectada y…

  1. Como primer paso lo desconectamos de la red.

  2. Averiguamos el programa que actúa desde el puerto 25. (http://www.microsoft.com/technet/sysinternals/Networking/TcpView.mspx)

3. Si el Malware 'no se deja eliminar' tendremos que arrancar el equipo en modo seguro (a prueba de fallos). Es posible que venga acompañado de otro programa que monitoriza continuamente si el malware está operativo; en caso contrario lo reinstala.

4. Si se hace evidente que el punto 3 es cierto, la recomendación es restaurar el equipo a un punto anterior a la aparición del malware o incluso formatearlo.



1.- TCPview

2º Procedimiento para detectar un relé emisor de spam dentro de la red. Análisis del tráfico de entrada y salida a Internet.

La configuración que podéis ver en el esquema de la figura 4 permite analizar todo el tráfico que entra y sale de una red con destino a Internet. Es útil para detectar relés emisores de spam o cualquier otro tipo de troyano instalado en la RED INTERNA. No son necesarios conocimientos de informática superiores al nivel de usuario.

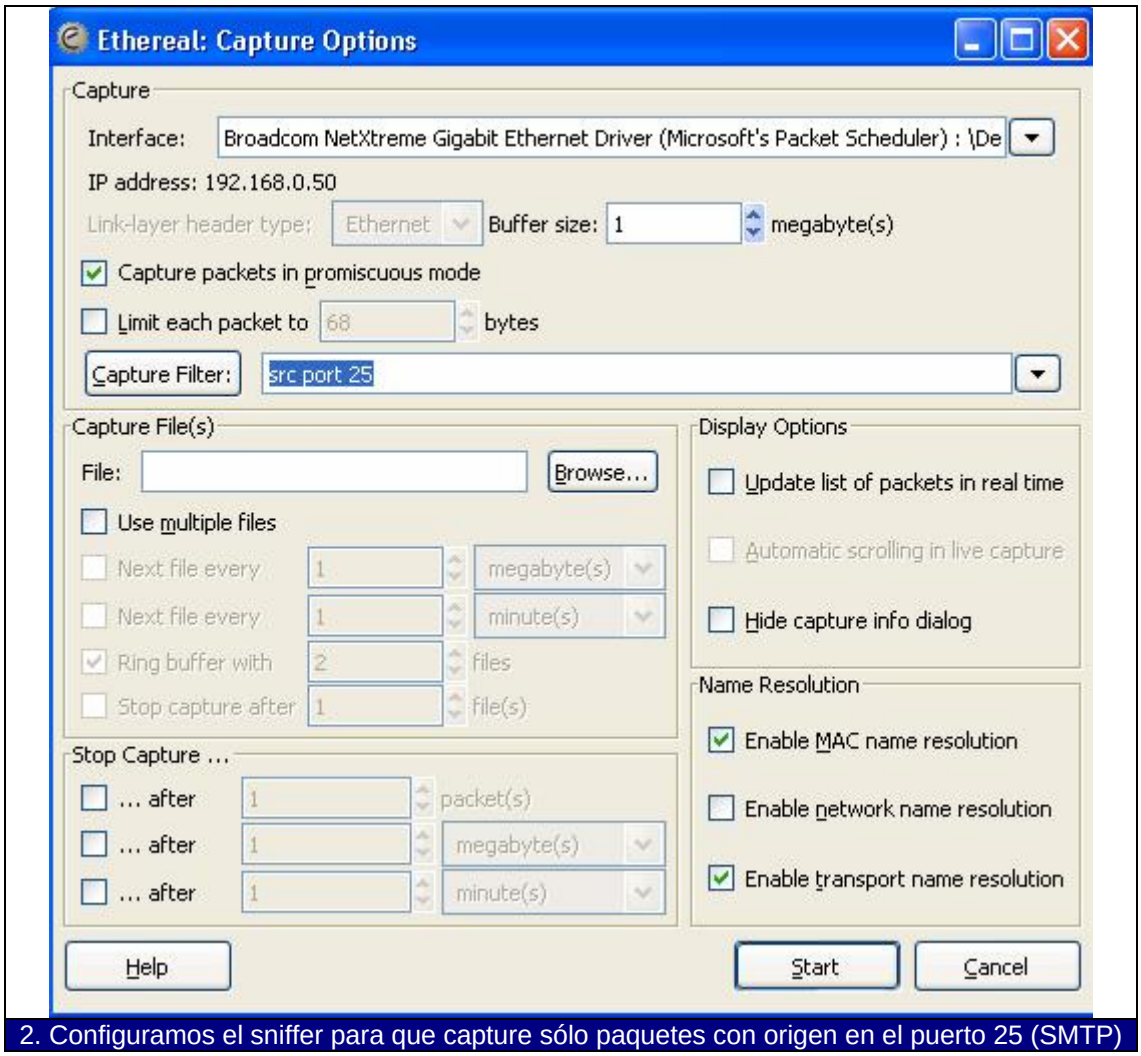
Elementos necesarios:

1. Equipo de sobremesa o portátil.
2. Hub (no Switch)

3. Analizador de protocolos: Wireshark (antiguo Ethereal) http://www.wireshark.org/download.html, disponible bajo licencia GNU. Esta herramienta tiene versiones para Windows y para Linux. En la dirección http://club.telepolis.com/websecure/tutoriales/manual_ethereal.pdf podéis descargar un pequeño manual sobre esta aplicación, aunque hay muchos más en Internet.

Pasos:

- Creamos un filtro para que capture paquetes cuyo puerto de origen sea el 25 (SMTP)



2. Configuramos el sniffer para que capture sólo paquetes con origen en el puerto 25 (SMTP)

- Activamos el sniffer para que escuche mediante la interfaz de red en uso.

- Es posible configurar el programa para que guarde los paquetes capturados en un fichero.

- Analizamos el contenido de la captura fijándonos en los paquetes que utilizan el protocolo SMTP y anotamos si IP. En la figura podemos ver que el equipo que envía desde el puerto 25 (SMTP) tiene la dirección IP 192.168.0.50.

3. Captura de paquetes con origen en el puerto 25

- Localizamos el equipo con la IP detectada y actuamos como ya vimos en el procedimiento 1º

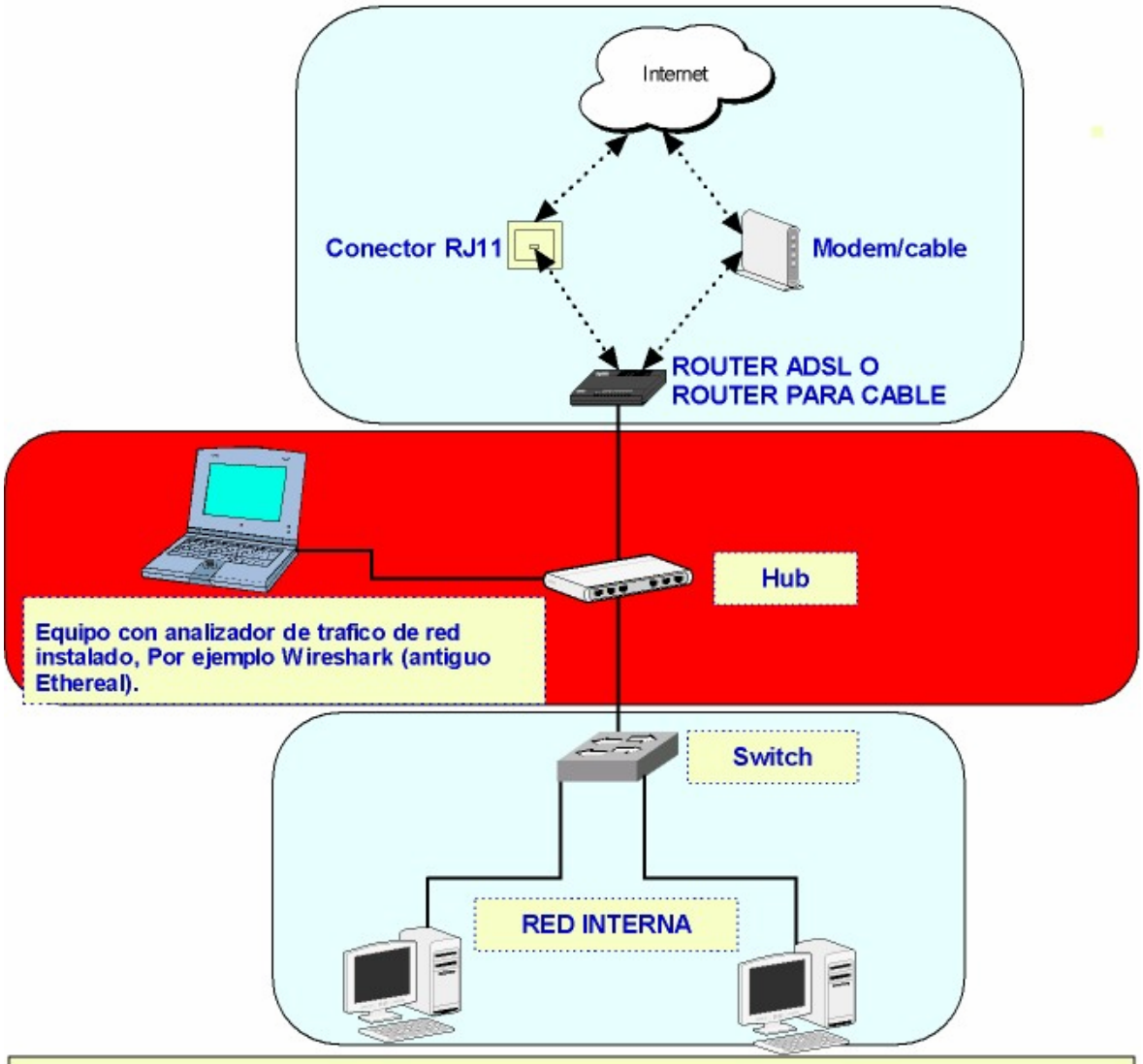
5. Como primer paso lo desconectamos de la red.

6. Averiguamos el programa que actúa desde el puerto 25. En Windows podemos utilizar la herramienta TCPview (http://www.microsoft.com/technet/sysinternals/Networking/TcpView.mspx)

7. Si el Malware 'no se deja eliminar' tendremos que arrancar el equipo en modo seguro (a prueba de fallos). Es posible que venga acompañado de otro programa que monitoriza continuamente si el malware está operativo; en caso contrario lo reinstala.

8. Si se hace evidente que el punto 3 es cierto, la recomendación es restaurar el equipo a un punto anterior a la aparición del malware o incluso formatearlo.

La configuración de la figura permite analizar todo el tráfico que entra y sale de nuestra red con destino a Internet. Es útil para detectar relés emisores de spam o cualquier otro tipo de troyano instalado en la RED INTERNA.



En el esquema de red podemos distinguir tres bloques:

1.- La red interna del centro 'colgando' de un switch normalmente conectado al router

2.- El router ADSL, o neutro si disponemos de conexión ADSL vía modem (Ono).

3.-Un equipo al que le previamente habremos instalado un analizador de protocodlos tipo Ethereal o su versión moderna, Wireshark (En Internet podemos encontrar varios manuales que nos aportarán los conocimientos que necesitamos para su utilización básica, suficiente para nuestras necesidades.

4.- Un hub (es probable que tengamos que acudir al armario de los trastos para encontrar uno, puesto que actualmente es difícil encontrarlos en las tiendas de componentes informáticos).

Los tres primeros bloques mencionados se conectan al Hub mediante un cable de red normal (UTP).

4. Esquema de conexión