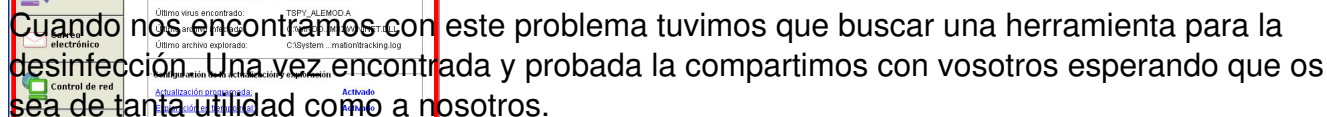


Escrit per Javier Martínez Avedillo
dijous, 18 d'agost de 2005 11:55

La herramienta para librarse de este incómodo parásito que se presenta como :SmithFraud, Win32/Alemod.A, Win32/Oleloa.A

Hace poco tuvimos que desinfectar un ordenador infectado con el virus SmitFraud (SmithFraud según donde se mire).

En la siguiente imagen el antivirus pc-cill in de Trend Micro detecta el virus.



y almacenar todas la webs que visitamos para después hacerle llegar el listado a algún servidor remoto. Por si fuera poco, el virus descarga e instala sin consentimiento del usuario distintos programas presuntamente "anti-spyware". Estos programas se ejecutan consumiendo recursos y bloquean la imagen del escritorio de windows mostrando en él un supuesto mensaje de

Escrit per Javier Martínez Avedillo
dijous, 18 d'agost de 2005 11:55

advertencia del sistema que nos solicita o bien que paguemos la licencia del software instalado o bien que compremos una determinada aplicación etc...

Tras ☐ pelearnos ☐ con el asunto de todas las formas que se nos pasaron con la cabeza dimos con una herramienta en Internet precisamente destinada a la limpieza de esta infección. La herramienta se llama **Generic SmithFraud remover 0.6** y ha sido diseñada por un tal **Marc** para

<http://www.hijackthis.de>

(al César lo que es del César). Puedes descargarte dicha aplicación desde el siguiente link

<http://forum.hijackthis.de/showthread.php?t=6392>

.

El propio autor de esta útil herramienta nos advierte de la posibilidad de que en algunos casos, tras el proceso de ☐ limpieza ☐ , algunos equipos no arranquen correctamente. Esto es debido a que la librería **wininet.dll** es renombrada. Por lo tanto el creador del programa recomienda instalar el siguiente parche de Microsoft

<http://www.microsoft.com/technet/se...n/MS05-025.mspx>

una vez ejecutado su software.

El proceso debería ser el siguiente:

- Descargate el ☐ cleaner ☐ .

- Descargate el parche.

- Ejecuta el cleaner.

- Instala el parche.

- Reinicia la máquina

Esto debería ser suficiente para acabar con este problema. Aún así es conveniente la combinación de este proceso con la ejecución de algún programa anti-spyware como *Spybot*, *BHODemon* y recientemente *Microsoft Antispyware Beta* ([visitar artículo](#)).