

REGSHOT

Cuando leemos páginas como ésta donde aparecen técnicas para ocultar todo tipo de troyanos ante los antivirus más sofisticados, surge la desconfianza lógica de algunos usuarios. "¿Y cómo puedo saber yo que el cliente de un troyano, por ejemplo, no está infectado con el servidor?". Ya vemos que los antivirus nos sirven más bien para poco. Bien, pues aquí pretendo mostrarles cómo pueden estar seguros de que el programa que han ejecutado en su ordenador no tiene otro archivo oculto que está actuando silenciosamente. Prepárense para convertirse en auténticos detectives de su ordenador.

Vamos a realizar un análisis de nuestro registro y nuestros archivos cada vez que ejecutemos en nuestro ordenador un archivo que nos pueda resultar de procedencia dudosa. En realidad todos los troyanos, binders, cracks, compresores, etc, son herramientas útiles para el hacking y no debemos confiarnos mucho de ellas. En esta web siempre intentamos probar los programas antes de exponerlos a los lectores. Incluso solemos utilizar enlaces a las páginas web de sus propios programadores para evitar que alguien infecte deliberadamente los archivos. Aún recuerdo un troyano llamado **Infector** (en su primera versión) que tenía el cliente infectado con el servidor.

En verdad en www.troyanos.tk siempre hacemos un análisis exhaustivo del ordenador cuando todos los días probamos un nuevo programa, pero siempre es mejor que Ustedes lo sepan hacer también para evitar suspicacias.

¿Empezamos a analizar nuestro ordenador?. Vamos allá.

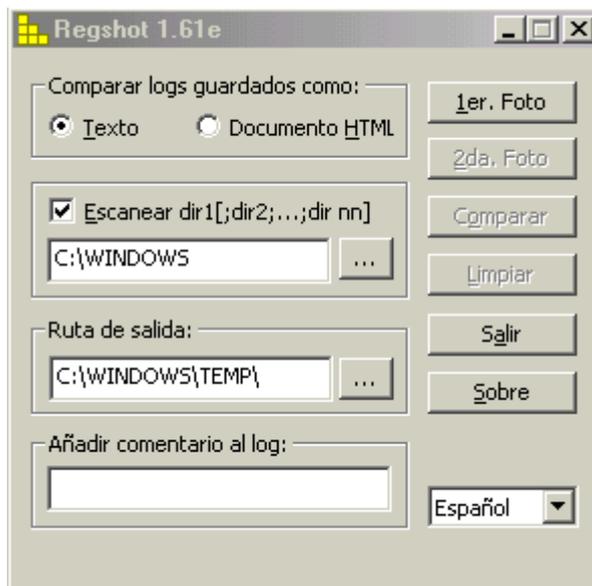
Cuando el servidor de un troyano se instala en nuestro ordenador, es lógico que deje alguna entrada en el **registro** para que la próxima vez que reiniciemos el ordenador, el troyano vuelva a activarse automáticamente. A veces modifica archivos como **System.ini**, **Win.ini**, **Autoexec.bat**, etc. E incluso puede crear nuevos archivos para su funcionamiento como una réplica del servidor, algunas librerías **DLL**, etc.

Todo esto produce cambios en nuestro ordenador, pero el problema al que nos enfrentamos es que hay cientos de carpetas y miles de archivos, además de varias miles de entradas en el registro. ¿Cómo vamos a descubrir los cambios en todo este entramado?.

Nuestra respuesta está en este programa que vamos a presentarles ahora. Se llama **Regshot** y lo vamos a descargar gratuitamente desde: [aquí\(v1.6\)](#) ó [aquí\(v1.7\)](#)

Con **Regshot** podemos realizar una comparación del registro y los archivos de nuestro ordenador un momento antes de ejecutar el archivo sospechoso y un momento después de su ejecución. ¿Lo probamos?

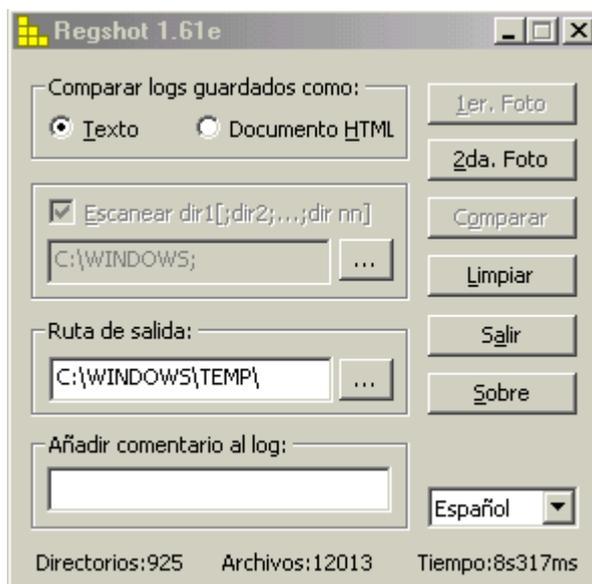
Vamos a volcar todo el contenido de **Regshot161e.zip** en una carpeta y vamos a hacer doble clic sobre **Regshot.exe**. Esto es lo que veremos:



En la parte inferior derecha desplegamos el botón y buscamos el lenguaje **Español** para hacerlo todo más sencillo. Arriba leemos **Comparar logs guardados como**. Debajo podemos señalar **Texto** o **Documento HTML**. Si seleccionamos **Texto**, los datos resultantes se verán en el **Bloc de notas**. Si seleccionamos **Documento HTML**, los datos se verán como en una web.

Si también queremos que analice los archivos en la comparativa (recomendable) deben seleccionar la pestaña **Escanear dir 1**.

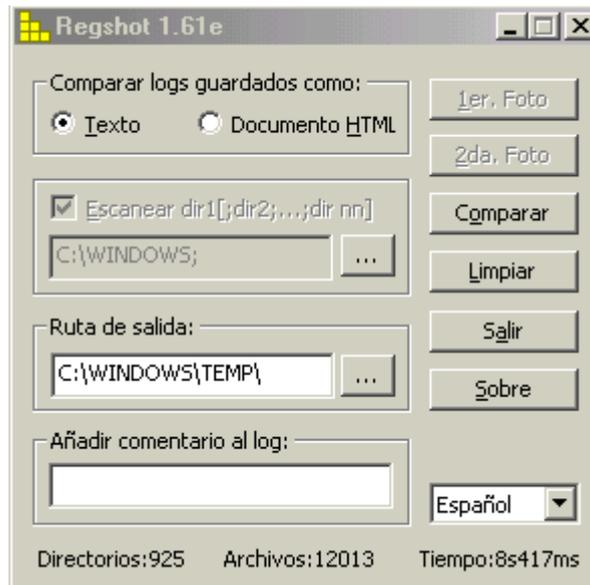
Ahora vamos a hacerle *una foto* al registro y los archivos del ordenador. Para ello pulsamos sobre el botón **1er. Foto**. Ahora pulsamos sobre **Foto**. Esperamos unos segundos hasta que memorice todas las entradas del registro y todos los archivos. Al final veremos esto:



Ahora no debemos hacer ninguna operación más o **Regshot** la registrará y nos puede confundir. Simplemente hagamos doble clic sobre el archivo sospechoso que deseamos probar. En mi caso (y como ejemplo para este tutorial) voy a hacer doble clic sobre el cliente del troyano **Net-Devil v1.5** para comprobar si está *limpio* o contiene algo más.

**NOTA: No cierren en ningún momento la ventana de Regshot. Ésta debe permanecer abierta hasta que finalice el análisis.*

Una vez que he abierto el cliente, vuelvo otra vez a la ventana de **Regshot**. Pulsamos el botón **2da. Foto** y luego el botón **Foto**. Ahora **Regshot** está realizando un segundo análisis al registro y a los archivos. Cuando finalice este segundo análisis, veremos esto:



Ahora el botón que aparece señalado en la parte derecha de la imagen es **Comparar**. Pues eso es lo que vamos a hacer ahora: comparar ambos análisis y así saber qué es lo que el cliente de **Net-Devil** ha variado en nuestro ordenador. Pulsemos el botón **Comparar** y veamos los resultados:

REGSHOT LOG 1.61e

Comentarios:

Fecha y hora:2002/11/5 19:45:36 , 2002/11/5 19:46:04

Computador:My Computer , My Computer

Usuario: ,

Valores modificados:2

HKEY_USERS\DEFAULT\Software\Microsoft\Windows\CurrentVersion\Explorer\User Assist\{Identificación}\Count\HRZR_EHACNGU: 95 00 00 00 8C 0D 00 00 60 C8 E9 DC 03 85 C2 01
HKEY_USERS\DEFAULT\Software\Microsoft\Windows\CurrentVersion\Explorer\User Assist\{Identificación}\Count\HRZR_EHACNGU: 95 00 00 00 8D 0D 00 00 00 76 3A EE 03 85 C2 01
HKEY_USERS\DEFAULT\Software\Microsoft\Windows\CurrentVersion\Explorer\User Assist\{Identificación}\Count\HRZR_EHACNGU:P:\JVAQ
BJF\Rfpevgbevb\Grfg lvehf\Arg Qrivy 5\Arg-Qrivy.rkr: 92 00 00 00 07 00 00 00 00 E3 00 B2 9A 83 C2 01
HKEY_USERS\DEFAULT\Software\Microsoft\Windows\CurrentVersion\Explorer\User Assist\{Identificación}\Count\HRZR_EHACNGU:P:\JVAQ
BJF\Rfpevgbevb\Grfg lvehf\Arg Qrivy 5\Arg-Qrivy.rkr: 95 00 00 00 07 00 00 00 00 76 3A EE 03 85 C2 01

Atributos de archivo modificados:2

C:\WINDOWS\USER.DAT
C:\WINDOWS\WIN386.SWP

Total de cambios:4

Como vemos ha habido una serie de cambios en los valores del registro y algunos atributos de archivo modificados. Pero si miramos bien el registro, no ha dejado ninguna entrada nueva. Están los valores en **User Assist \{Identificación}\Count**, y esos valores son normales.

**NOTA: En {Identificación} realmente tenemos que leer el número de registro de nuestro sistema operativo, que nosotros por ética hemos omitido por la palabra Identificación.*

Vemos también que no se ha creado ningún archivo nuevo y esto nos da mucha más confianza. Lo único que leemos es que el cliente de **Net-Devil v1.5** ha variado los atributos de dos archivos: **USER.DAT** y **WIN386.SWP**. Pero es muy normal también que cualquier archivo que abramos modifique esos dos archivos. De hecho esos archivos contienen una especie de historial de todo lo que abrimos en nuestro ordenador.

La conclusión lógica después de este análisis es que el cliente de **Net-Devil v1.5** está totalmente *limpio*. Ante un archivo así podemos fiarnos.

¿Pero cuándo debemos desconfiar de un archivo?. Pues, por ejemplo, si nos deja entradas como éstas:

**HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\MS Windows 32:
"C:\WINDOWS\SYSTEM\win32.exe"**

**HKEY_USERS\DEFAULT\Software\Microsoft\Windows\CurrentVersion\Run\MS Windows 32:
"C:\WINDOWS\SYSTEM\win32.exe"**

Esto lo podemos interpretar como que el archivo que hemos ejecutado nos ha dejado otro archivo en esta ruta: **C:\WINDOWS\SYSTEM\win32.exe**. Este archivo **win32.exe** es altamente sospechoso en la ruta del registro **...CurrentVersion\Run\MS Windows 32...** Esto quiere decir que la próxima vez que reiniciemos nuestro ordenador, el archivo **win32.exe** será ejecutado sin nuestro consentimiento. ¿No les parece extraño?.

Como ven **Regshot** no nos pone en bandeja la solución, pero sí que activa nuestra lógica. Con un poco de sentido común podemos estar seguros de que lo que hemos ejecutado está haciendo lo que realmente tiene que hacer y no otra cosa.

Les recomiendo que la primera vez que ejecuten un troyano o cualquier otro programa sospechoso, acudan a **Regshot** para evitar las suspicacias lógicas.

Autor: Coolvibes

Página: Indetectables.com.ar