ISEC Lab #3

Creación de un CD de rescate antivirus con PE-Builder

Vicente Aguilera Díaz
vaguilera<arroba>isecauditors.com

1 Introducción

Siguiendo la temática del anterior ISecLab, y que parece que no va a dejar de tener importancia, en este nuevo número vamos a tratar de ayudar a aquellos administradores y empresas en general, con unos recursos limitados, como son las pequeñas empresas que cuando sufren ataques de virus en alguno de sus ordenadores se las ven y se las desean para poder conseguir que esa máquina quede limpia de esos molestos virus y gusanos.

Teóricamente, mantener los antivirus actualizados nos debe salvar de cualquier tipo de intento de contaminación llevado a cabo por un virus, troyano o similar, pero existen diversas situaciones en las que esto no es cierto. Primero, que el virus llegue a nuestro ordenador antes de disponer de la actualización, segundo que el usuario elimine de alguna manera la protección, tercero, que el virus se encuentre previamente en la máquina y burle la seguridad del antivirus y cuarto que el antivirus no identifique ese virus (de aquí las habituales recomendaciones de instalar varios antivirus en una red).

Una solución de coste 0 es emplear una herramienta muy difundida pero poco conocida, no exenta de polémica por cuestiones legales referentes a la copia del software legal: su nombre es PE-Builder (Bart's Preinstalled Environment bootable live windows CD/DVD). Nuestra intención es plantear el uso de esta herramienta siguiendo siempre las más estrictas normas de legalidad de protección intelectual y copia legítima del software.

PE-Builder es un completísimo programa que, a partir de un CD del sistema Operativo Windows XP o 2003, es capaz de construir una imagen de un CD con unas funcionalidades realmente interesantes como herramienta de recuperación de un sistema. En este artículo la orientación será la de disponer de una herramienta de limpieza de virus de sistemas Windows con cualquier tipo de partición soportada por los operativos de Microsoft (FAT, FAT32 o NTFS). De hecho, animaremos a todo aquel que le resulte interesante este artículo a que vea la cantidad increíble de plug-ins existentes con tantas funcionalidades como se pueda imaginar.

2 Requerimientos de PE-Builder

Los requerimientos para disponer de un CD para poder escanear y limpiar nuestras máquinas es bien simple:

Un CD con Windows XP Home o Profesional (y el archivo del SP1 o SP2 del idioma correspondiente) o Windows 2003, el archivo de McAfee (podría ser otro antivirus pero de este hay un plugin para PE-Builder y un front-end gráfico muy cómodo) con las últimas firmas de virus, la última versión de PE-Builder.

A lo largo de este IsecLab veremos de dónde descargar cada uno de ellos, excepto el SO, del que debemos tener un CD original, con la licencia correspondiente, y que no debe estar instalado en ningún otro equipo, para evitar problemas legales: el uso de software Freeware o Open-Source nada tiene que ver con el software ilegal.

Para descargar la última versión de PE-Builder debemos dirigirnos a la web del proyecto: http://www.nu2.nu/pebuilder/ y simplemente descargar la última versión disponible. A continuación tendremos que descomprimir el zip (con la estructura de directorios) a la carpeta donde haremos todo el trabajo (de ahora en adelante C:\PEBuilder).

3 Creación del SO actualizado

Para disponer de los ficheros del SO (trabajaremos con Windows SP Profesional SP2) debemos disponer del CD de Windows original y copiar su contenido a, por ejemplo, C:\WinXP\. La copia debe ser el contenido integro del CD.

A continuación deberemos bajarnos el fichero del Service Pack 2 de la web de Microsoft, cosa cada vez más complicada, gracias a Windows Upodate. Podemos hacer una búsqueda en los downloads de la web y localizaremos un gran fichero de 260 MB llamado (para la versión castellana del operativo) **WindowsXP-KB835935-SP2-ESN.exe**.

Ejecutando este programa se iniciará la descompresión y posterior instalación del SP, pero nosotros deberemos, sin instalar, copiar los ficheros descomprimidos a la carpeta donde hemos copiado el SO, sobrescribiendo los ficheros originales (sin Service Pack) con los del Service Pack 2.

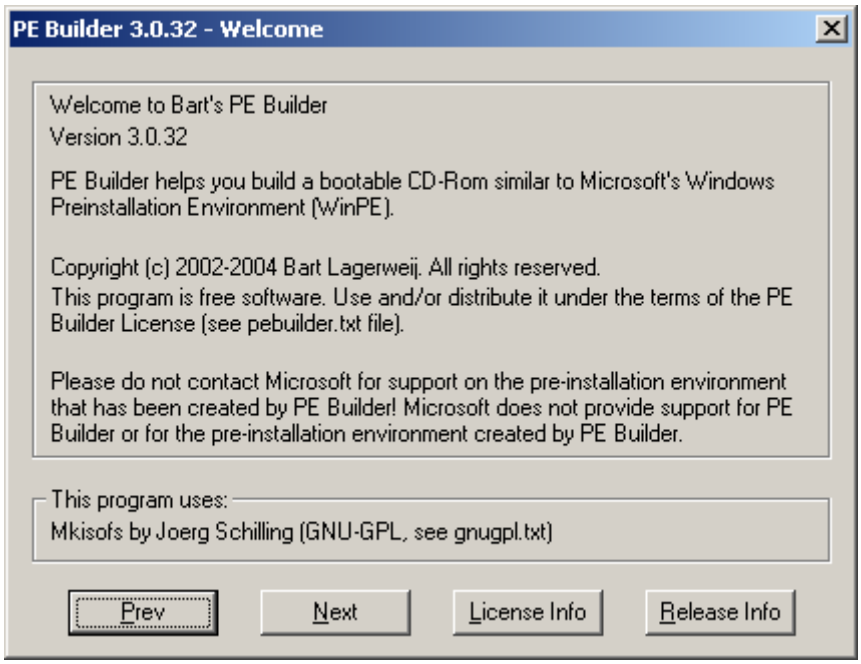
Para hacer esto deberemos dirigirnos a C:\ durante la descompresión del SP y veremos que se ha creado una carpeta donde encontramos los fichero descomprimidos del SP (un nombre de carpeta muy largo con letras y números aparentemente aleatorios). Antes de continuar con la instalación de éste, deberemos copiar la carpeta i386 a la carpeta dónde hayamos copiado el SO original (C:\WinXP\), dónde debe haber otra carpeta con ese nombre. Esto lo podemos hacer directamente con nuestro compresor habitual, descomprimiéndolo directamente, sin ejecutar el fichero ejecutable del SP.

Con esto, lo que habremos conseguido es disponer de un instalable del SO con el Service Pack 2 de Windows XP Professional.

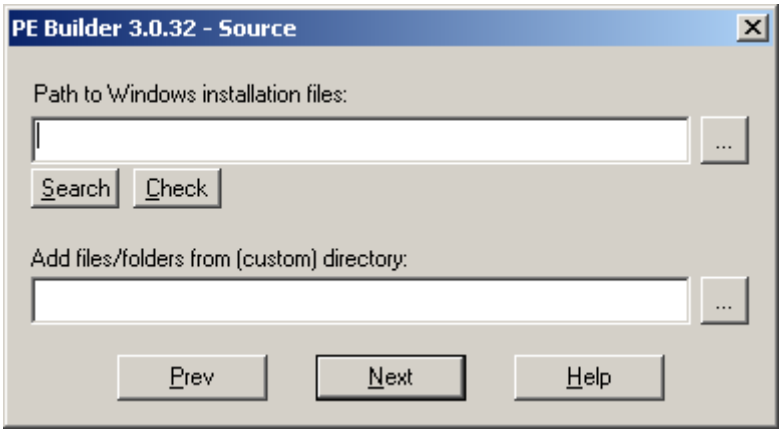
4 Creación de la ISO

Ahora ya tenemos todo lo necesario para poder crear la imagen de nuestro CD de descontaminación.

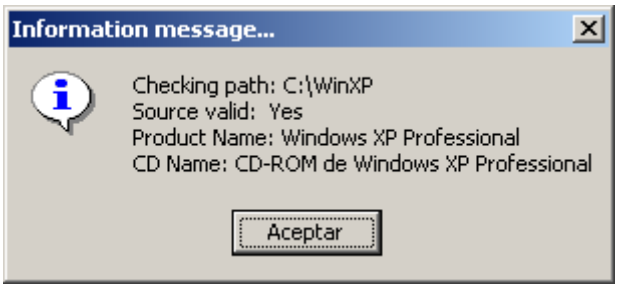
Si ejecutamos PEBuilder, es decir **pebuilder.exe**, (de ahora en adelante la versión que usaremos será la 3.0.32) veremos los siguientes avisos de licencias:



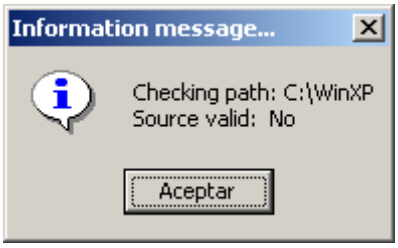
Pulsando "Next" tendremos que elegir, dónde se encuentra el Sistema Operativo y dónde se encuentran los archivos adicionales que queramos incluir (en este caso ninguno, puede quedar vacío).



Para comprobar que hemos realizado bien todas las acciones anteriores deberemos seleccionar la ruta C:\WinXP y pulsar el botón "Check". Si hemos creado correctamente el SO actualizado, el resultado será este:



En caso contrario recibiremos el siguiente mensaje:



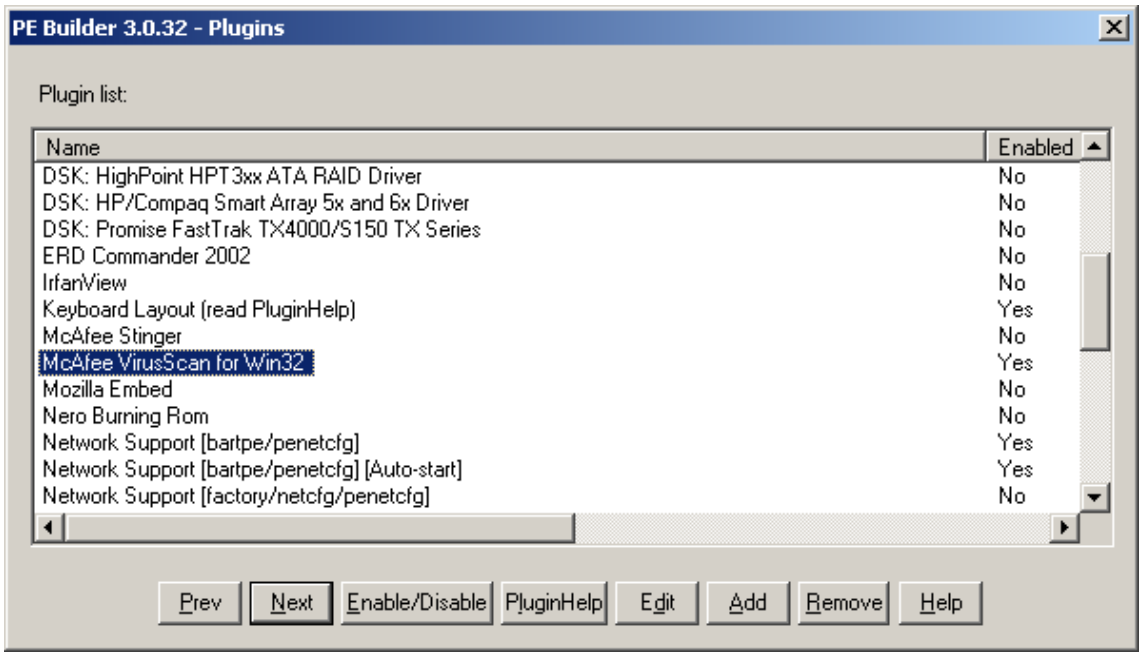
Si este es el caso, volvamos al principio y revisemos qué podemos haber hecho mal.

5 Configuración de los Plugins

Una de las capacidades más impresionantes de PE-Builder es la cantidad de plugins que ha desarrollado su creador, Bart Lagerweij, y otra mucha gente. Tenemos plugins para antivirus, para acceso remoto, disco duros SCSI, tarjetas diversas y todo aquello que se nos pueda ocurrir. Todos consultable e indexados en la página web de PE-Builder.

Nosotros únicamente deberemos llevar a cabo una configuración muy rápida y trivial del plugin del antivirus de McAfee (por defecto desactivado, pero incluido en PE-Builder).

En el siguiente paso del proceso de creación de nuestro CD de desinfección es la de activación/configuración de plugins como se muestra en la siguiente captura:



Donde, mediante el botón "Enable/Disable" podremos activar el plugin de "McAfee VirusScan for Win32". Para que esta activación tenga sentido, simplemente tendremos que obtener el antivirus como tal.

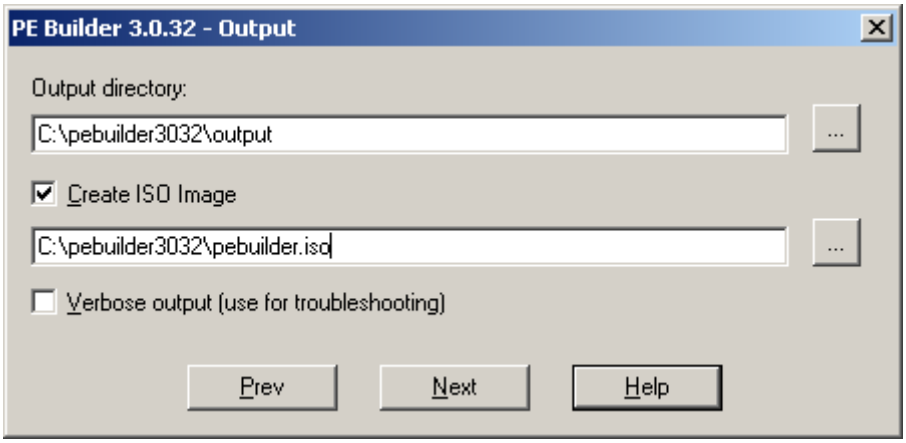
Para descargar el antivirus de McAffee, para DOS, con las últimas firmas, debemos descargar el último fichero superdat (sdatxxxx.exe) de la web de Network Associates ftp site en ftp://ftp.nai.com/CommonUpdater/. Copiar el fichero sdatxxxx.exe en la carpeta C:\PEBuilder\plugin\mcafee\files. Para descomprimirlo, en lugar de ejecutarlo simplemente, deberemos abrir una ventana de comandos y ejecutarlo (en la carpeta donde se encuentre) con el parámetro "/e", es decir ejecutar "sdatxxxx.exe /e" (donde xxxx es el número de versión, por ejemplo sdat4411.exe). No veremos ningún mensaje, pero eso simplemente será porque lo descomprime sin ningún aviso.

De hecho, esta versión, al ser para DOS no dispone de interfaz gráfica y esto es precisamente lo que incorpora el plugin de PE-Builber, una cómoda y sencilla interfaz para poder ejecutar el antivirus de linea de comandos.

6 Creación de la ISO (2ª Parte)

Ahora sí que podemos continuar el proceso de creación de nuestro CD de desinfección vírica.

Siguiendo el proceso, se nos pedirán dos directorios, el primero (output) será aquel donde se almacenarán los archivos temporales de la creación del CD, el segundo, y realmente importante será donde se creará la imagen del CD. Para que este fichero (ISO) se cree es necesario activar la opción "Create ISO Image".



A continuación, el proceso automático de generación de PE-Builder iniciará la creación del archivo ISO.

Sólo quedará, una vez finalizado el proceso, emplear nuestro programa de grabación preferido grabar el CD a partir de la imagen ISO generada mediante PE-Builder.

7 Imprescindible antes de crear la imagen ISO

Tras la creación de la imagen del CD sin ningún problema, se detectó que el archivo ISO no contenía un fichero imprescindible para el arranque del sistema operativo. Este fichero es "ntoskrnl.exe". Tras analizar los ficheros de configuración de PE-Builder se identificó el problema que corregía dicho defecto: en el fichero **pebuilder.inf** hay una línea en la parte inicial que fuerza el renombramiento de dicho archivo a "**ntkrnlmp.exe**", la línea es esta:

```
ntoskrnl.exe=2,ntkrnlmp.exe
```

Sustituyendo dicha línea por simplemente esta:

```
ntoskrnl.exe=2
```

Se evita el cambio de nombre y el funcionamiento del CD será correcto.

Se contactó con Bart Lagerweij para saber la razón de este cambio de nombre y su respuesta inicial fue que esta era correcta, aunque se le indicó que de esa forma la ISO no funcionaba y con el cambio sí, con lo que no se entendía ese cambio en el nombre del fichero.

Durante la escritura de este ISecLab no he vuelto a recibir respuesta por su parte, con lo que simplemente anoto el cambio que se debe llevar a cabo en este archivo de configuración (que incluye el .ZIP de PE-Builder), aunque también animo a todo aquel que quiera ponerse manos a la obra que es probable que este error no se produzca con todos los sistemas operativos + service packs.

8 Enlaces de Interés

- PE-Builder: http://www.nu2.nu/pebuilder/