Victima:	Everest Ultimate v5,01,1700
Descarga:	Http://www.lavalys.com/
Dificultad:	Facil
Herramientas:	Upx, Ollydbg
Packer:	Upx
Cracker:	ZiKaTRiZ
Fecha:	02 – 04 - 2009

Hola, hay muchas maneras de convertir esta aplicación en full versión, en este manual escogeré la más larga, vallamos a ello:

Primero veremos que nos muestra la victima, tenemos tres problemas claramente visibles, que son:

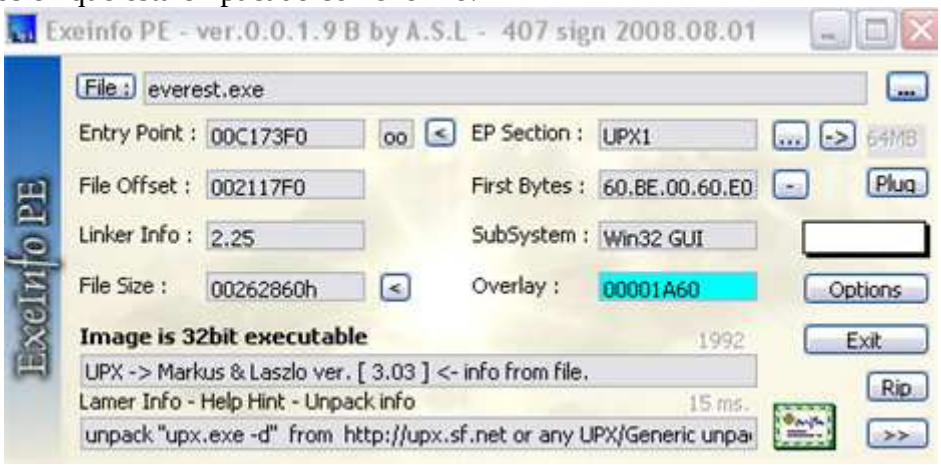
La frase [TRIAL VERSION] en todos los datos importantes, con lo cual esta aplicación no sirve para mucho.
En el inicio.

La advertencia que nos recuerda los 30 días.

El about que es trial.

Empecemos:

Averiguaremos en que está empacado con exeinfo:

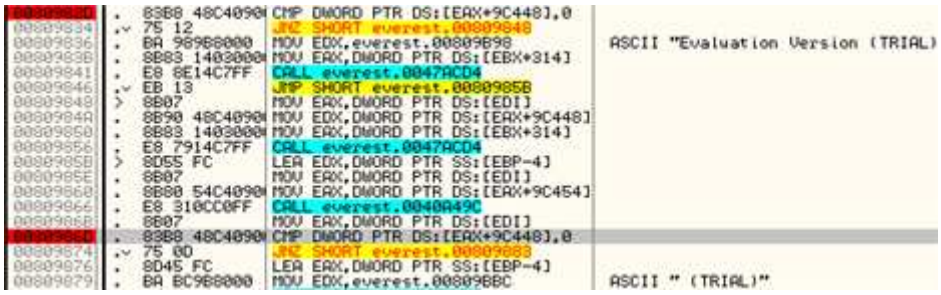


En este caso utilizaremos la misma herramienta que ellos, pero para unpackarlo. Una vez lo tengamos unpackado, lo que haremos será cargarlo en olly, pulsando con el botón derecho del ratón veremos las string references.

En las string references las frases que nos interesan son:

> [TRIAL VERSION] , TRIAL , No expiry.

Por suesto no voy a poner todas las imagenes de esta puñetera aplicación, ya que entre los tres trerminos anteriores salen en 93 lugares diferentes, así que solo pondré una de las imagenes y el resto de las entradas que se den por aludidas.



Lo que haremos sera cambiar la sentencia:

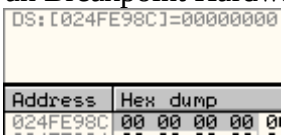
CMP DWORD PTR DS:[EAX+9C448],0

por

CMP DWORD PTR DS:[EAX+9C448],1

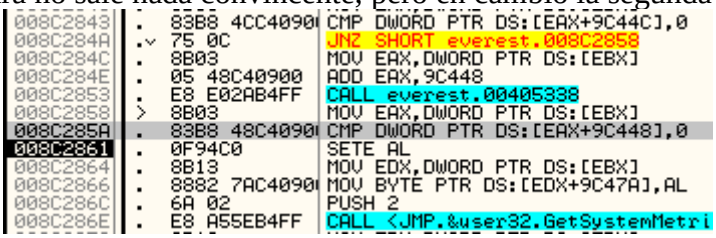
En todos los lugares que aparece, incluido el de la Advertencia.

Pero antes de hacer los cambios debemos de averiguar la dirección de DS. Así que pulsaremos F9 para poder encontrar esa dirección y poder encontrar la Advertencia, la primera vez que para haremos lo siguiente:
botón derecho del ratón: Follow in Dump, Memory address, en el Dump seleccionando la dirección, botón derecho del ratón y colocaremos un Breakpoint Hardware, on access Dword.



Reiniciamos a la victima y seguidamente F9 o Run.

La primera vez que para no sale nada convincente, pero en cambio la segunda vez muestra esto:



Esta comparación que está en la línea 008C285A es la responsable de que salga o no la Advertencia Así que cambiaremos ese 0 por un 1, y problema resuelto.

Hay 5 entradas con el “trial”, “trial version” y “No expiry”, que la comparación es: como se muestra en la imagen anterior de la linea 008C2843. Esas líneas no es necesario tocarlas.

Una vez echos todos los cambios: Copy to executable, All modifications, Save file.

ZiKaTRiZ