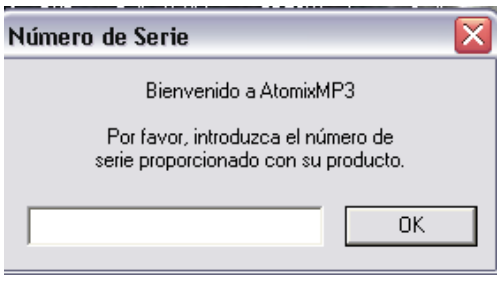
Programa	**Atomix Mp3 2.0**
Download	www.atomixmp3.com
Descripción	Programa para mezclar música
Herramientas	OllyDbg 1.10
Dificultad	Newbie
Compilador	Microsoft Visual C ++ v 7.0
Protección	Serial
Objetivos	Parchar y dejarlo full
Cracker(?)…Newbie	**BioHaZarD** Fecha: 26/07/09 12:24 a.m.
Tutorial nº	2

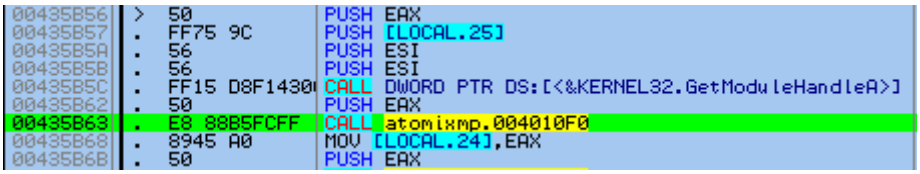
La verdad que la buena onda que me tiraron en la lista me puso las pilas para volver escribir: gracias Ricardo, Solid, NCR y a todos, perdón si no me acuerdo de todos. Voy a hacer algunos tutes más de esta serie "Parchando a lo loco" ya que vi que uno de los pibes dijo que tutes como estos les servía para practicar. Como siempre digo…PERDON! Jeje a los grosos que escriben esos tutes grandiosos que tanto nos ayudan.

EMPECEMOS:

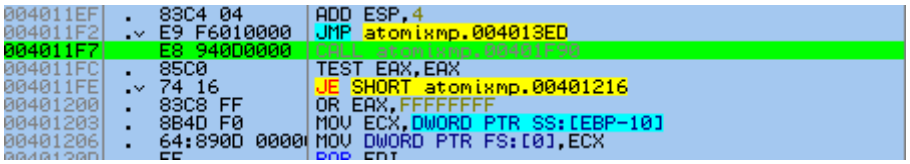
Esto va a ser muy cortito…el enemigo en cuestión es ATOMIX MP3 2.0, que es full por 30 días luego de lo cual nos pide un número de serie:



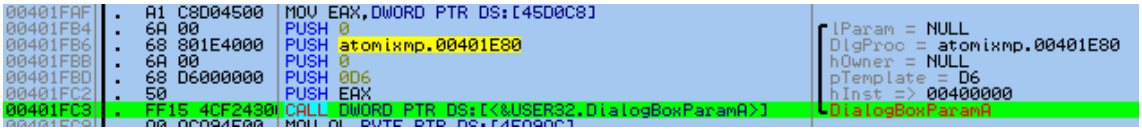
Esa ventana de numero de serie es como una pared detrás de la cual esta nuestro tesoro, si la pasamos detrás de ella estará el programita full full para nosotros(en realidad el programa no me interesa,solo me importa saltarme la protección que tiene). Bueno derribemos la pared. Yo particularmente cuando tengo una nag como esta voy haciendo “Animate over (Ctrl+F8)” cuando salta la nag miro el Olly y veo en que CALL está parado y le pongo un Breakpoint, doy RUN y parara en mi BP, lo quito y entro a la CALL con F7, otra vez hago un Animate Over. Esto es para buscar la CALL correcta que hay que nopear;no se si será coincidencia pero por lo general a mí siempre me pasa que la CALL correcta es la anterior a una CALL intermodular (en este caso es una llamada a USER32,ya lo van a ver).Eso si ANOTEN cada BP que vayan poniendo en el orden que los ponen.
Empecemos con Animate Over (AO) y cuando la nag salta Olly para acá:



Con F2 le ponemos un BP a esa CALL, reiniciamos Olly (Ctrl+F2),damos RUN y cuando pare en el BP que pusimos lo quitamos con F2 y entramos a la CALL con F7;nuevamente AO y ahora la nag aparece y Olly parará aquí:



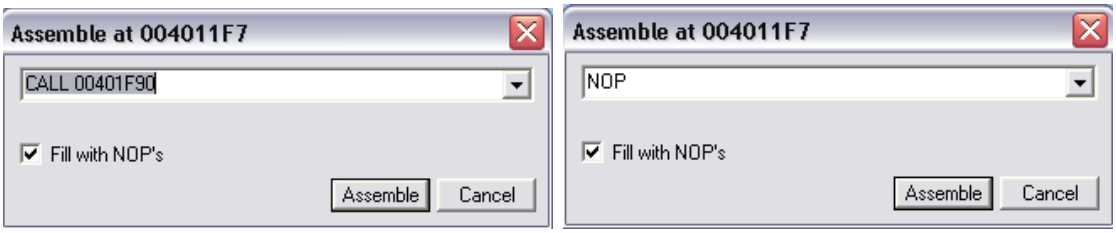
Ponemos BP, reiniciamos Olly y Run, entramos a la CALL y AO y ahora la nag a parece cuando para acá:



Ahí veo la CALL a USER32 y como dije a mi me pasa que la CALL correcta que debo parchar es la anterior a la que es intermodular. Entonces laq que voy a nopear va a ser la anterior a esta.En mis anotaciones tengo que la anterior es:

004011F7 > \E8 940D0000 CALL atomixmp.00401F90

La busco en Olly y la nopeo. O sea situado sobre ella apretó la tecla “espacio” y hago los cambios:



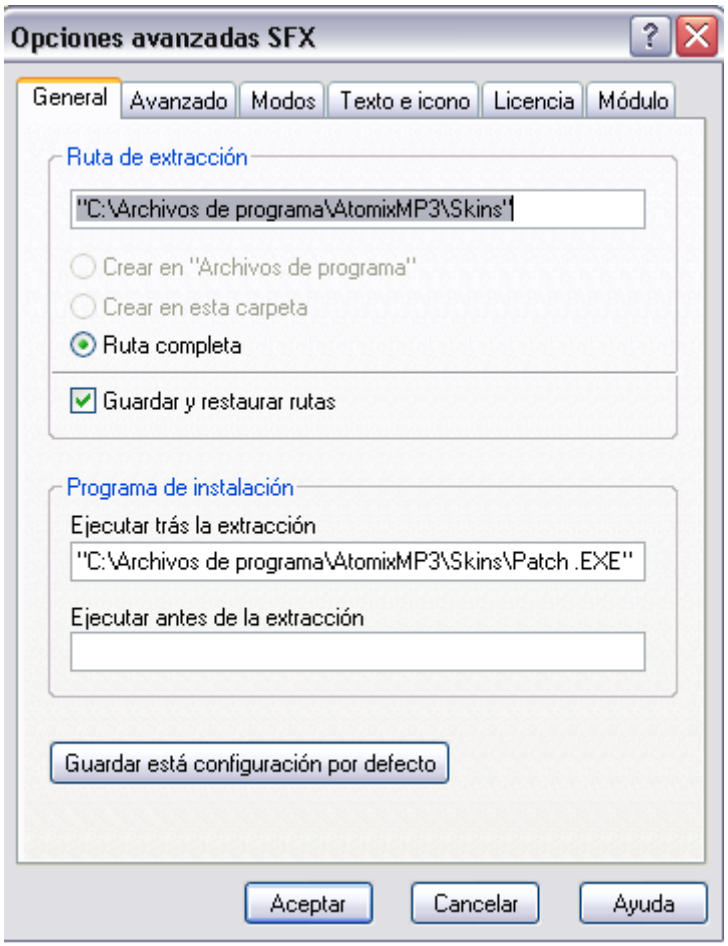
Guardamos los cambios a el ejecutable: click con el botón derecho, COPY TO EXECUTABLE/ALL MODIFICATIONS y en el cuadrito que sale elijo “Copy all”; en la nueva ventana que se abre nuevamente click con el derecho y “Save File”.Lo guardo, lo ejecuto y….no anda…naaa mentira,era chiste SI anda: PARED DERRIBADA.

EXTRA: **Dejando nuestra firma.**

Si quisiéramos dejar nuestra firma como la de la imagen , ”Cracked by BhZd” en este caso, tendríamos que editar “default.bmp”que está en C:\Archivos de programa\AtomixMP3\Skins. Yo hice un Patch distribuible con “Patch FX Generator 1.20” y con la ayuda de WinRar se puede hacer un SFX para que cuando se ejecute nuestro patch también reemplace default.bmp original por el que tiene nuestra firma. Es fácil:

1- Creamos el Patch con Patch FX Generator 1.20(esta en la web de Ricardo en HERRAMIENTAS).Es fácil de usar .
2- Editamos default.bmp a nuestro gusto
3- Copiamos ambos archivos a una misma carpeta, los seleccionamos y click con el botón derecho, elegimos “Añadir al archivo…”(WinRar).

4- En la ventana que se abre tildamos “Crear archivo SFX”
5- Pinchamos en la solapa “AVANZADO” y luego “Opciones SFX”.
6- La ruta de extracción tiene que ser la que aparece en la imagen:



En “Ejecutar tras la extracción” ponemos la misma ruta que en “Ruta de Extracción” agregándole “patch.exe” en mi caso.

Aceptar y listo!

Al extraer en Skins se reemplaza el .bmp original por nuestro .bmp editado,una vez hecho esto se ejecuta el patch para el programa.Lo iba a hacer metiendo un .bat dentro del SFX pero me dio Fiaca.

Saludos a todo el grupo,fue un tute cortito pero espero que sea de utilidad.

BIOHAZARD