Serial Fishing

Programa : MP3 Cutter v1.1.0
Descarga : http://www.mp3cutter.org/down/mp3cutter.exe
Objetivo : Obtener serial válido
Nivel : Fácil
Reverser : Elix

MP3 Cutter es una herramienta que permite cortar audios mp3's, y en este momento me urgía algo así para cortar un audio en partecitas y hacer una especie de dedicatoria personalizada (mentira solo buscando seguir el tutorial de Ivinson http://ricardonarvaja.info/WEB/CURSO%20NUEVO/TEORIAS%20NUMERADAS/1301-1400/1328-AudioCutter-%20Mi%20primer%20tuto%20para%20CLS-By%20Ivinson.pdf) por error baje un binario distinto y esto fue lo que surgió.

1. Instalación y Recojo de Información

La aplicación lo podemos bajar libremente desde la página oficial, lo cual bajamos e instalamos al abrir el programa (MP3 Cutter) en cuestión no muestra NAG (Carteles al inicio de aplicación) ni impedimento alguno para su uso.

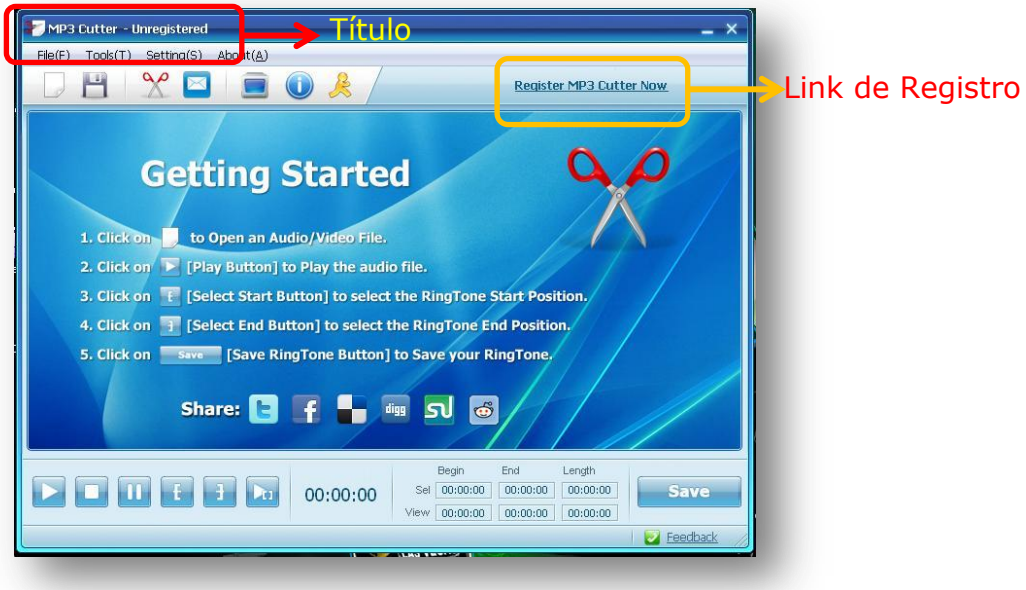

Imagen 01. Ventana principal de MP3 Cutter

Por el título podemos notar que la aplicación necesita registrarse "*MP3 Cutter – Unregistered*" y el link que nos lleva a la ventanita del registro es "*Register Mp3 Cutter Now*" sin mayores perjuicios hagamos clic y veamos a lo que nos enfrentaremos

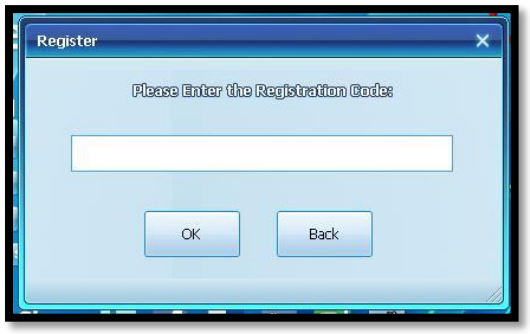

Imagen 02. *Ventana de Registro*

Junto a la ventana del registro se abre el navegador con una página con un contenido web donde podemos distinguir la opción de compra del programa con descuento y todo a…

Imagen 03. *Costo del programa*

Bueno ya sabemos que había en ese contenido web ahora lo cerramos y comencemos por recoger información de nuestro objetivo, ingresemos un serial falso para ver las strings del chico malo otro dato importante es también el título de la ventana *Register* hasta ahí más que suficiente para laburar

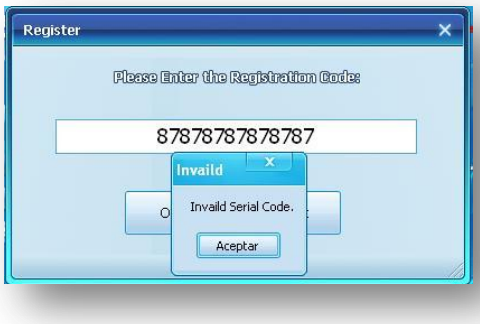

Imagen 04. *Serial falso y chico malo*

Ahora sabemos que la validación lo va hacer en alguna parte de sus entrañas (bien por nosotros). Sigamos con el recojo de información, sometamos a nuestro objetivo al valor de la verdad ;) y hagámosle confesar en que lenguaje le escribieron…. Jejeje no es necesario para esto utilizaremos *RDG Packer Detector* que dicho sea de paso nos dirá también si está empacado o no.

Imagen 05. Información de RDG Packer Detector

Nuestra aplicación está escrita en Visual Basic 6.0 Código Nativo y no cuenta con protección alguna eso nos dice la herramienta.

2. Pescando el Serial

Ahora se viene lo bueno XD, abrimos el OllyDbg y ponemos nuestro programita para verle las entrañas y con algo de suerte pescamos el serial, lo cual es objetivo de este tutorial.
En la imagen a continuación nos muestra justo después de cargar el MP3Cutter en Olly cuyo título nos indica de posible código comprimido pero en pregunta, y dos opciones si queremos que olly continue con el análisis sí o no… nosotros le daremos que no

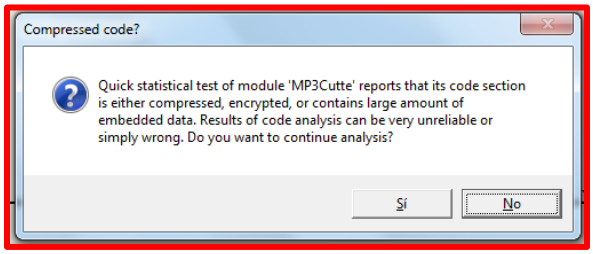

Imagen 05. Posible código compreso

En la ventana del disasembler del OllyDbg vemos el Entry Point (EP) siendo este la primera instrucción a ejecutarse

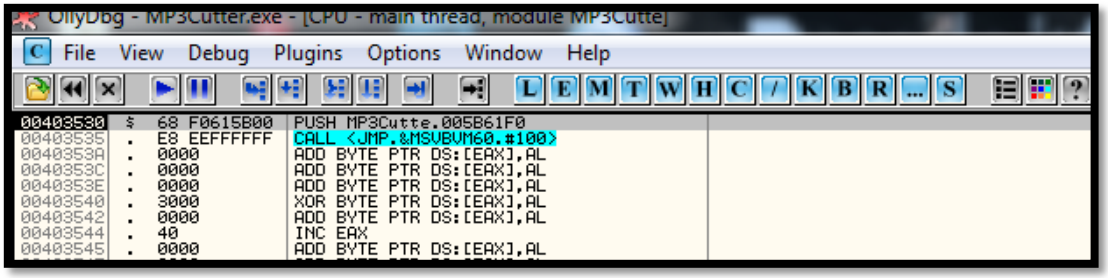

Imagen 06. Entry Point de MP3 Cutter

Para el laburo en esta oportunidad tengo las excepciones del Olly seteado (*Debugging Options > Exceptions*) de este modo

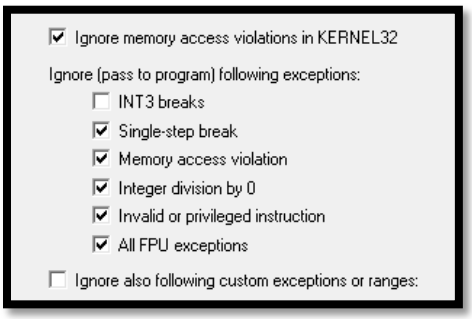

Imagen 07. *Configuración de la ventana de Excepciones*

Con eso marcharía de perlas :P para clarificar más el panorama vayamos a ver las API que importa (utiliza) el programa clic derecho *search for > Name (label) in current module* o [CTRL]+N, como dato primordial sabemos que el objetivo no posee protección alguna lo sabemos por el RDG Packer Detector (ver Imagen 4)

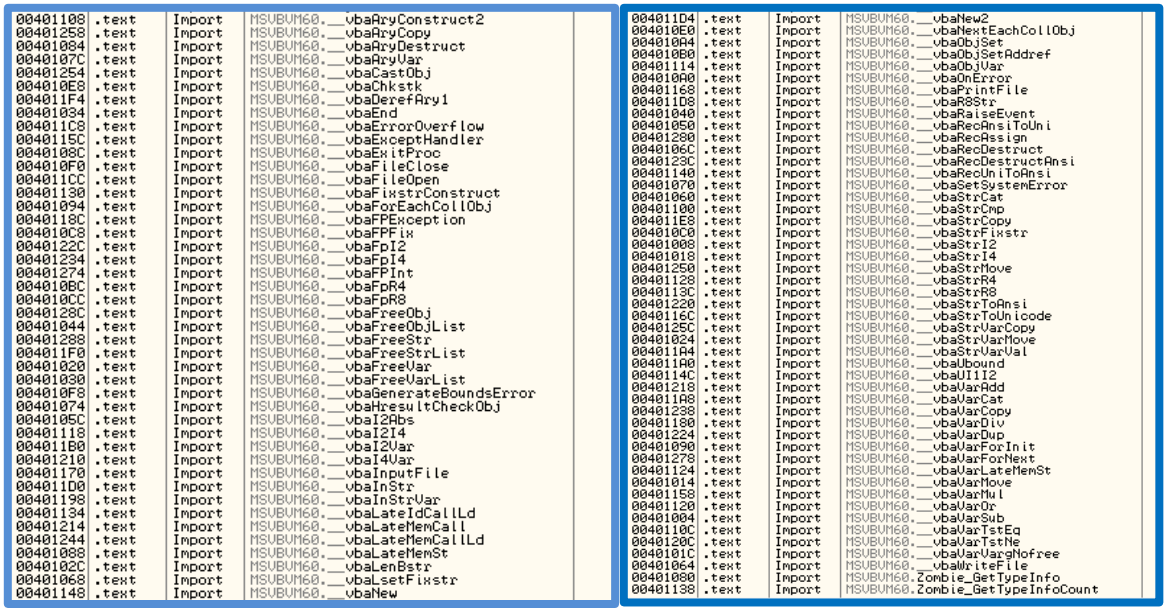

Imagen 08. *Listado principal de las API importadas*

En la imagen de arriba vemos el listado de las API y varias candidatas a BreakPoint (BPX) para no hacerle muy larga y aburrida al tutorial pongamos un BPX en __vbaStrCmp pidiéndole de ese modo a Olly que se detenga (por el BPX) cuando trate de comparar String recordar que nuestro serial falso (ver Imagen 02) también es una String y tal vez la comparación se detenga cuando trate de comparar nuestro serial (falso) con otro string si fuese así nos ahorraríamos labores más tediosas… veamos

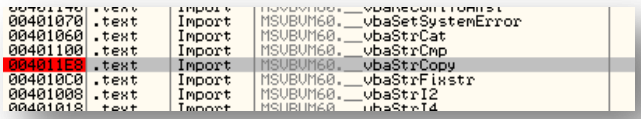

Imagen 09. Breakpoint en API __vbaStrCmp

BPX en __vbaStrCmp hecho esto ponemos al programa en ejecución desde el Olly con [F9]… después de varios [F9] se abrió el MP3 Cutter, ahora vayamos al link de registro y después volvamos a colocar nuestro serial falso

Imagen 10. Link a la Ventana del registro

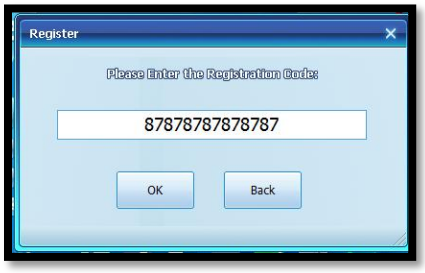

Imagen 11. Registro y serial falso

En la ventana (imagen anterior) damos al botón OK y… caemos acá

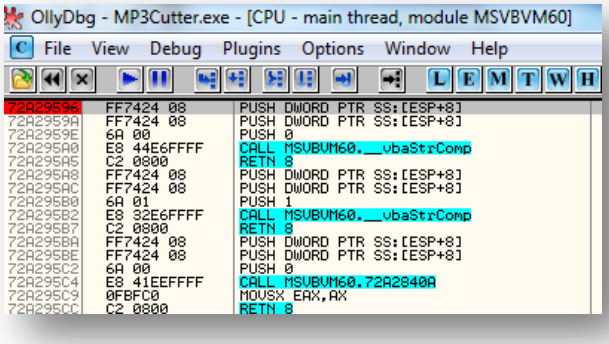

Imagen 12. Metiendo las Strings a la pila para comparación

La cosa se puso buena… vemos tres PUSH seguidas seguramente es cuando se forman los argumentos de la API __vbaStrCmp veamos lo que está tratando de poner en la pila con ese primer PUSH

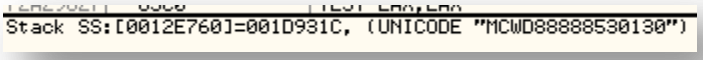

Imagen 13. Posible serial en la ventana de ayuda de Olly

Ahora veamos el segundo PUSH

Imagen 14. Segundo PUSH

Y en la ventana de ayuda…

Imagen 15. Nuestro serial falso a la vista

Vemos nuestro serial falso, lleguemos hasta el push 0 y veamos cómo quedó el stack

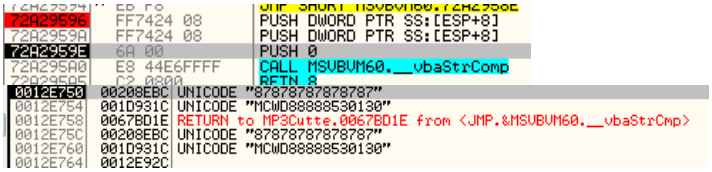

Imagen 16. Como queda el stack hasta el PUSH 0

En la ventanita de ayuda de Olly podemos ver una string medio sospechosa y si vemos la ventana del stack justo arribita de está string vemos nuestro serial falso

[IMAGEN QUITADO A PROPOSITO]

Imagen 17. *String a compararse*

¿Será la string sospechosa nuestro serial verdadero? La emoción nos llevaría a sacar conclusiones precipitadas y decir que sí, pero vayamos con calma y tracemos hasta pasar al call de la API

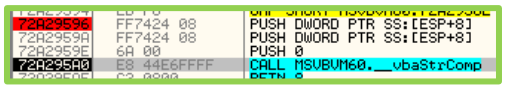

Imagen 18. *Llamada a la API*

Veamos ahora como quedó el stack

Imagen 19. *Parámetros de __vbaStrCmp en el stack*

Ohhh mai.. cambió las string en ASCII por Arg1, Arg2 y Arg3 que son los argumentos de la API __vbaStrCmp donde los argumentos Arg2 y Arg3 son las que contienen las String que serán sometidas a comparación.

Si llegamos al RETN 4 que es la siguiente línea de código después del CALL de la API y regresamos vemos mucho código que por ahora da fiaca reversearlo

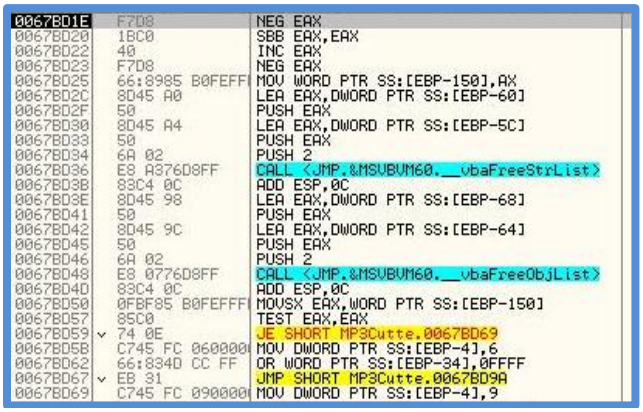

Imagen 20. *Mucho más código*

Solo tocaría probar si lo ingresado es correcto o no demos F9 para correr la aplicación… y para nuevamente en la misma línea de código de comprobación de String (ver Imagen 12). Pero ahora tenemos otra string en la ayuda de Olly será esto los ¿seriales verdaderos?... Y así va parando unas cuantas veces yo fui apuntando todos las string por si fueran los seriales correctos ☺ (MP3Cutter-serial.txt) después que termina de

comprobar nuestro serial falso con algunas string sospechosas nos muestra el siguiente cartelito

Imagen 21. Una vez más chico malo

Pero si reiniciamos la aplicación y probamos una string de la lista por ejemplo esto MCWD88888530130 que es la primera que apareció y ponemos nuevamente un BPX en __vbaStrCmp volvemos a parar unas cuantas veces hasta llegar nuevamente a la parte que queremos si vemos el STACK ambos son iguales

[IMAGEN QUITADO A PROPOSITO]

Imagen 21. Serial pescado en comparación

Si damos F9 nuevamente vamos viendo las mismas string comparándose sabemos qué hace esto por la API y…

Imagen 22. Eureka

Eureka!! Eureka!! Esos eran los seriales veamos ahora la ventana del MP3 Cutter

Imagen 23. Ventana de MP3 Cutter registrado

Ahora ya no está el Unregistered en el título en cambio tenemos la versión de programa.

3. Despedida

Hasta acá hicimos una pesca de seriales exitosa, quizás obvie algunas cosillas pero igual la pesca fue un éxito, está vez tuvimos suerte al toparnos con una aplicación sencillita nos ahorramos 19.95 USD. Quiero saludar a todos los que llegaron hasta acá y a la lista completa de CracksLatinoS.

Elix

Happy Cracking!!