Tutorial: Crackeando MP3 Joiner by Hendrix

Bueno, este es mi primer tutorial explicativo sobre crackeo de programas, en este tutorial explicare como crackear el MP3 Joiner, un prgorama que me encontre por Softonic, por las fotos, me parecio que era un programa que no era gran cosa, lo descargue y efectivamente no era gran cosa, no estaba empaquetado ni llevaba nada anti-debugger, asi que lo tuve facil...

En este tutorial voy a explicar como sacar el Serial (Nombre y Pass) valido, y ya que estamos, retocaremos el ejecutable para que nos quede a nuestro gusto (mejoras graficas).

Vamos alla...

No se si es una mania mia o no, pero yo al crackear pongo musica, con este programa e usado el nuevo CD de Los Muertos de Cristo, el RapsodiaLibertaria II.

Bien, ya tenemos la musica, ahora, nos descargamos el programa:

http://www.009soft.com/products/MP3Joiner.exe

Ahora lo ejecutamos normalmente y nos sale esto:

Please register M	P3 Joiner	
The product has 30 more than 3 files. Ple product, you will reco after you ordered the	days to try. The trial ve ease press "Buy Now" I sive a registration numb product.	rsion only joins not outton to order the per via an e-mail shortly
User Name:		
Registration Code :		
Buy now	Register	Try

Bueno, empezamos bien...xDDD vamos a ver que pasa si le ponemos de nombre Hendrix y de pass esto: 4242



Bueno, aquí nos dice que tenemos el Codigo incorrecto, si probamos a dejarlo todo vacio nos sale que tenemos el usuario incorrecto.

Es la hora de coger el toro por los cuernos, vamos a ver en que esta echo y si esta empaquetado. Lo pasamos por el PeiD y nos da esto:

腸 PEiD v0).94			
File: C:\Ar	chivos de programa\Mi	P3JOINER\MP3Joiner.exe		
Entrypoint:	00010ED8	EP Section:	.text	
File Offset:	00010ED8	First Bytes:	6A,60,68,A0	>
Linker Info:	7.10	Subsystem:	Win32 GUI	>
Microsoft Visual C++ 7.0 Multi Scan Task Viewer Qptions About ✓ Stay on top				

Muy bien, no esta empaquetado y esta prograamdo con el VC++ 7.0, así que pasamos al ataque.

Lo metemos en el olly, lo ejecutamos para ver si nos para y directamente nos echa....negativo, nos deja ejecutar el ejecutable normalmente, asi que de protecciones, 0. Podemos pasar a analizar el codigo y sacar el nombre y el pass.

Lo tenemos ejecutabo, bien, le metemos los mismos datos que antes y nos sale el cartelito de que tenemos el codigo incorrecto, nos vamos al olly sin cerrar ninguna ventana, clickamos click derecho >> Search for >> All referenced text strings.

Una vez dentro, buscamos la palabra Please, ya que el mensaje de error empieza por Please.

Buscamos, tras unos cuantos Please que no nos interesan nos encontramos con esto:

004053B7 PUSH MP3Joine.0042C15C	ASCII "Please input correct User Name!"
004053DA PUSH MP3Joine.0042C17C	ASCII "Please input correct Registration Code!"
CONCEPTION NOT DITE DID CONFERD OF C	

Nos vamos sobre la primera, click derecho y seleccionamos Copy to clipboard >> Address, que ahce esto, pues mira, vete al CPU (Alt+C), presiona Ctrl+G, ahora Ctrl+V pulsa en ok y nos lleva aquí:

00405390	. 55	PUSH EBP	5 m	10
00405391	. SBEC	MOV EBP, ESP		11
00405393	. 83EC 20	SUB ESP,20		
00405396	. 894D E0	MOV DWORD PTR SS:[EBP-20],ECX		
00405399	. 6H 01	MOULECY DWODD DID CO. LEDD 201		
00405398	- 8840 E0	COLL MP2 Joing 004156PP		
00405303	. 884D FØ	MOU FCX, DWORD PTR SS: [FBP-20]		
004053A6	. 83C1 70	ADD ECX.70		
004053A9	. E8 F2F4FFFF	CALL MP3Joine.004048A0		
004053AE	. 83F8 02	CMP EAX,2		
004053B1	.~7D 13	JGE SHORT MP3Joine.004053C6		
004053B3	. 68 00	PUSH Ø		
00405385	. 6H 00 49 ECC14200	PUSH 0 DUCH MP2 Later 004201EC	OCCLT "Plance input connect	
004053D7	E9 04EE0100	COLL MP2 Joine 00425105	Houri Prease imput correct	
00405301	.VE9 89820000	IMP_MP3.Joine.0040566E		
00405306	> 8B4D E0	MOV ECX. DWORD PTR SS: [EBP-20]		
00405309	. 8301 74	ADD ECX,74		
004053CC	. E8 CFF4FFFF	CALL MP3Joine.004048A0		
004053D1	. 83F8_08	CMP EAX,8		
00405304	.~/0 13	JGE SHUKI MPSJoine.004053E9		
00405306	. 6H 00			
00405300	68 70014200	PUSH MP3 Joine, 00420170	ASCII "Please input correct	
004053DF	. E8 E1FD0100	CALL MP3Joine,004251C5	HOOTI / REDE IMPAG COTTEGO	
004053E4	.~E9 86020000	JMP MP3Joine.0040566F	1785 T.C. 892253392553	
004053E9	> 6A 00	PUSH Ø	F Arg1 = 00000000	
004053EB	. 8B4D E0	MOV ECX, DWORD PTR SS: [EBP-20]		
004053EE	. 8301 70	HDD ECX,70	MDO IN THE ROMODERO	
004053F1	. LO SHEBFFFF	MOU PUTE PTP SS. [EPP_11] OL	-nrsJoine.00403F50	
004053F9	. 60 01	PUSH 1	$-9x_{-1} = 0000001$	122
004053FB	8840 FØ	MOU FOX DWORD PTR SS. FERP-201	Hx 9x = 00000001	

Empieza con un push ebp.

Ahora ponemos un BP en ese push ebp (00405390), reiniciamos el programa (Ctrl+F2) y lo volvemos a arrancar (F9), vemos que no para, introducimos el nombre y el codigo, presionamos en Register y para en nuestro BP, ahora nos toca analizar el codigo.

Fijaros, si dejamos todo en blanco, en el salto condicional de 004053B1 no va a saltar, ya que EAX valdra 0, si introducimos una letra como nombre, EAX valdra 1 y tampoco va a saltar, si introducimos 2 letras, EAX valdra 2 i SI nos va a saltar, lo que hace el call de 004053A9 es mirar la longitud del nombre, si vale 2 o mas, nos libramos del mensage de error de usuario incorrecto, si vale menos de 2 nos da el error. Lo mismo pasa en 004053CC, nos mira la longitud del serial, si vale 8 nos deja pasar, si vale menos nos da el error, eso lo e explicado rapio por no perder tiempo, ya que no tiene misterio.

Seguimos con F8 sin entrar en ningun call y llegamos aquí:

004055B1	. 83F8 35	CMP EAX.35	
004055B4	.~0F85 A7000000	JNZ MP3Joine.00405661	
004055BA	. ØFB64D FD	MOVZX ECX, BYTE PTR SS:[EBP-3]	
004055BE	. 83F9 35	CMP ECX,35	
004055C1	.~0F85 9A000000	UNZ MPSJoine.00405661	
004055C7	. 0FB655 F6	MOVZX EDX, BYTE PTR SS:[EBP-A]	
004055CB	. 83FA 38	CMP EDX, 38	
004055CE	.~0F85 8D000000	JNZ MP3Joine.00405661	
004055D4	. 0FB645 F5	MOVZX EAX, BYTE PTR SS:[EBP-B]	
004055D8	. 83F8 35	CMP EAX,35	
004055DB	.~0F85 80000000	JNZ MP3Joine.00405661	
004055E1	. 0FB64D F9	MOVZX ECX, BYTE PTR SS:[EBP-7]	
004055E5	. 83F9 36	CMP ECX,36	
004055E8	.~75 77	UNZ SHORT MP3Joine.00405661	
004055EA	. 0FB655_F7	MOVZX EDX, BYTE PTR SS: [EBP-9]	
004055EE	. 83FA_37	CMP EDX,37	
004055F1	.~75 6E	JNZ SHORT MP3Joine.00405661	
004055F3	. 0FB645 FE	MOVZX EAX, BYTE PTR SS: [EBP-2]	
004055F7	. 83F8_36	CMP EAX,36	
004055FA	.~75_65	JNZ SHORT MP3Joine.00405661	
004055FC	. ØFB64D_FB	MOVZX ECX, BYTE PTR SS:[EBP-5]	
00405600	. 83F9_35	CMP ECX,35	
00405603	.~75 5C	JNZ SHORT MP3Joine.00405661	
00405605	> 6H 00	PUSH 0	
00405607	. 64 00	PUSH 0	
00405609	. 68 H4C14200	PUSH MP3Joine.0042C1A4	ASCII "Registration has succeeded!"

Abajo del todo, vemos el texto de Registration has succeded, o en español: Registracion completada, exactamente nonde queremos llegar.

Si nos fijamos, hay una serie de comparaciones, compara un numero con el valor de EAX.

Ahora tenemos que echar mano de la tabla ascii, nos vamos a http://www.asciitable.com/

Ahora miramos que vale el 35 de la primera comprobacion, miramos en la tabla y nos da 5, vale, esto podria ser un numero del serial, asi que nos vamos al Bloc de notas y apuntamos el 5. Seguimos con las comparaciones y sacamos esto:

asi que el supuesto serial es 55856765, ejecutamos normalmente el programa, metemos el nombre que queramos ya que de momento no nos hemos encontrado con ninguna comprobacion de nombre. Le metemos el Serial y nos salta esto:



Pues ala, ya tenemos el programa crackeado y funcionando al 100%, como nosotros somos unos "pofesionales" vamos a retocar el programa, ya que el programador parece que se quedo a medias, ya que el programa tiene una interfaz horrible. Empecemos a meterle mano.

Lo vamos a traducir al español con el Resource Hacker y ya que estamos, le daremos el estilo del XP.

Con el Resource hacker lo traducimos. En Dialog podemos editar los forms y traducirlos, y en String table podemos traducir los mensages que nos de (de error, de informacion..) y demás cosas.

Luego, con el XN Resource Editor le damos el estilo del XP. Abrimos el XN Resource Editor >> File >> Open. Seleccionamos el archivo que ya emos traducido, luego nos vamos a Resource >> Add Resource y seleccionamos de la lista el XP Theme Manifest. Guardamos y ya lo tenemos finalizado. Les dejo unas imagenes para que vean como ha quedado.

Este programa esta	crackeado, así que no expira
	Transfer
Nombre de usuario:	Hendrix
	55856765

🐏 MP3 Joiner - Traducido por Hendrix 👘	
MP3 File Name	Agregar MP3
	Arriba
	Abajo
	Borrar
	Limpiar
Archivo resultante	
c:\joiner.mp3	Buscar
Mezclar Previsualizar	Ayuda
Registrar Pagina de Inicio	Salir

En donde dice: *Este programa esta crackeado, asi que no expira* se le podria poner una foto, aunque para eso se tiene que jugar mas con el ResHacker. Hay un tutorial en internet de Karmany sobre la edición de recursos excelente.

Bueno, dedico este tutorial a todo aquel que se haya leido todo este tutorial, espero que les haya gustado y sobretodo, que hayan aprendido, aunque este archivo a crackear no sea gran cosa.

Un Saludo

Hendrix