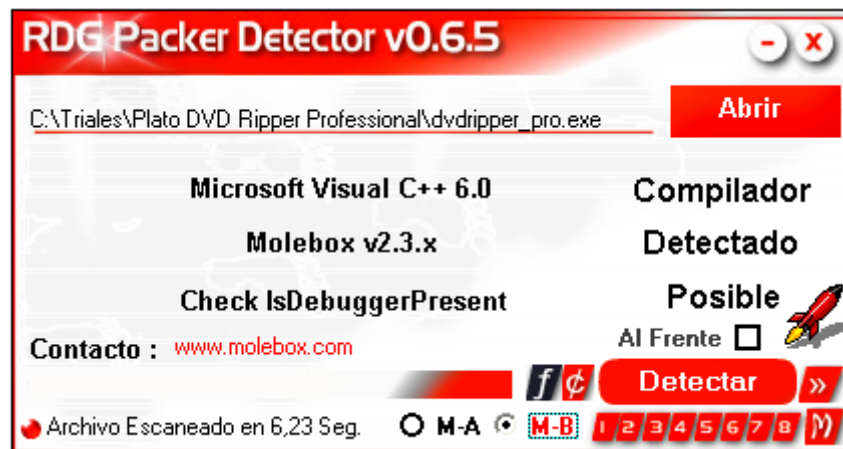




Programa	Plato DVD Ripper Professional v 7.88.18
Download	http://www.dvdtompegx.com
Descripción	Programa para ripear DVD a varios formatos
Herramientas	OllyDbg 1.10, RDG
Dificultad	Newbie
Compilador	Microsoft Visual C ++ v 7.0
Protección	Serial y solo ripea 15 minutos.
Objetivos	Parchar y dejarlo full
Cracker(?)...Newbie	BioHaZarD Fecha: 02/08/09
Tutorial nº	3

Hola a toda la lista! Este es el tercer tuto de la serie Parchando a lo Loco y creo que con este ya está. Aunque soy medio chifladito y por ahí escriba algún otro de esta serie. Además las “vacaciones” por la Gripe A ya terminaron y voy a estar muy ocupado con la facultad, pero bueno en algún momento algún otro tuto voy a escribir, todo sea por devolver a la lista algo de todo lo que me dio con sus tutos.

Bueno basta de tanta palabrería y vamos a trabajar(¿) un poco. Instalamos la víctima y luego pasándola por RDG Packer Detector:




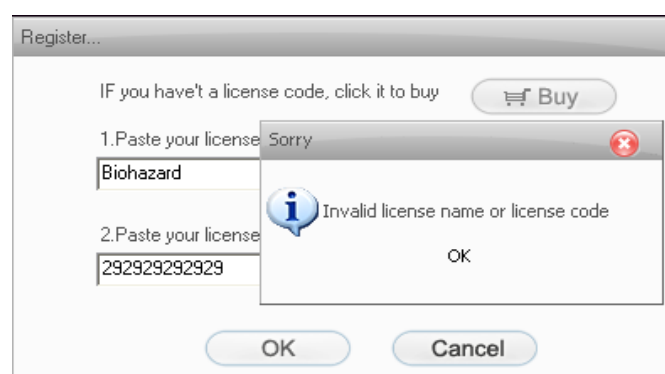
Ops...Molebox...Ya dije que recién doy mis primeros pasos en el unpacking...y no se bien como funciona Molebox pero lo cierto es que si escribo este tuto es porque no necesite desempacarlo; Peid y Exeinfo PE no me detectaban ningún packer...

Vemos que tiene una protección antidebugging: "Check IsDebuggerPresent", si miramos el ejecutable cargado en Olly:

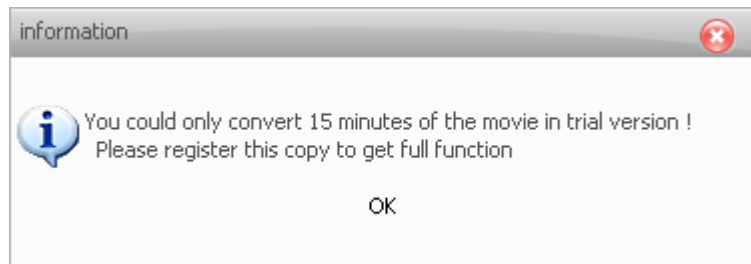
0048C66C	.rdata	Import	USER32.IsChild
0048C19C	.rdata	Import	USER32.IsDebuggerPresent
0048C4AC	.rdata	Import	USER32.IsDialogMessageA

Hay varios plugins que solucionan el problema, entre ellos uno con el mismo nombre "IsDebuggerPresent".

Antes de seguir ejecutemos el programa y veamos que se trae...Si pinchamos el botón a la izquierda minimizar  nos da una opción para registrarnos, si la elegimos nos aparece una ventana y si ingresamos un nombre y un serial nos dice:



Si cargamos algún DVD e intentamos ripear a algún formato ni bien le damos a START nos avisa:

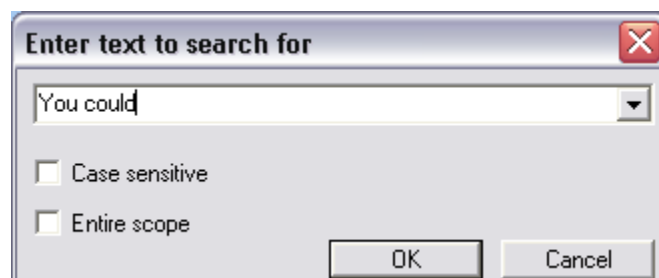


Jeje solo 15 minutos! Dejáme por lo menos convertir una peli completa por lo menos! Rata... Carguemos el programa en Olly (con el plugin para evitar IsDebuggerPresent).Acá empieza:



Pero como vamos a proceder? Podríamos buscar e invertir el salto que decide si vamos a la zona de chico malo o chico bueno para que registre con cualquier user/name y fue!...pero soy fiaca y ni siquiera quiero poner un serial luego de crackearlo, además es muy probable que si cambiamos ese salto tengamos que registrarlo cada vez que lo volvamos a usar (Tarea para ustedes...busquen el salto clave buscando la string *Invalid license name or license code* e inviértánlo, guarden los cambios,regístrenlo, ciérrenlo y vuelvan abrirlo y vean que pasa...es fácil. háganlo no sean fiacas...je je justo yo lo digo).

A ver...busquemos en la lista de strings (Botón derecho y luego SEARCH FOR/ALL REFERENCED TEXT STRINGS) alguna palabra de ese mensaje que nos decía que solo podíamos ripear 15 minutos. Por ejemplo busquemos "you could" (Botón derecho y luego SEARCH FOR/ALL REFERENCED TEXT STRINGS):



Y encontramos el tonto mensaje:

004772F7	PUSH 00497D24	ASCII "information"
004772FC	PUSH 00497D30	ASCII "You could only convert 15 minutes of the movie in trial version ! Please register this copy to get full function"
00477363	PUSH 00497B8C	ASCII "ffencoder"

Hagamos Follow (apretando ENTER) para verlo:

004772E7	. 75 32	JNZ SHORT 0047731B	Arg3 = 00000000 Arg2 = 00497D24 ASCII "information" Arg1 = 00497D30 ASCII "You could only convert 15 minutes dvdrippe.00475640
004772E9	. 813D 70964B01	CMP DWORD PTR DS:[4B9670],384	
004772F3	. 7C 26	JL SHORT 0047731B	
004772F5	. 6A 00	PUSH 0	
004772F7	. 68 247D4900	PUSH 00497D24	
004772FC	. 68 307D4900	PUSH 00497D30	
00477301	. 8B4D EC	MOV ECX,DWORD PTR SS:[EBP-14]	
00477304	. E8 37E3FFFF	CALL 00475640	
00477309	. 8B0D 40A74B01	MOV ECX,DWORD PTR DS:[4BA740]	
0047730F	. 81C1 84030001	ADD ECX,384	

Hay vemos un JNZ y un JL ambos si se producen nos llevan a la misma posición evitando el tonto mensaje. Pongamos un BP en JNZ, Run o F9 , carguemos algún DVD y vemos que para:

004772E0	. 833D 74964B01	CMP DWORD PTR DS:[4B9674],0	Arg3 = 00000000 Arg2 = 00497D24 ASCII "information" Arg1 = 00497D30 ASCII "You could only dvdrippe.00475640
004772E7	. 75 32	JNZ SHORT 0047731B	
004772E9	. 813D 70964B01	CMP DWORD PTR DS:[4B9670],384	
004772F3	. 7C 26	JL SHORT 0047731B	
004772F5	. 6A 00	PUSH 0	
004772F7	. 68 247D4900	PUSH 00497D24	
004772FC	. 68 307D4900	PUSH 00497D30	
00477301	. 8B4D EC	MOV ECX,DWORD PTR SS:[EBP-14]	
00477304	. E8 37E3FFFF	CALL 00475640	
00477309	. 8B0D 40A74B01	MOV ECX,DWORD PTR DS:[4BA740]	

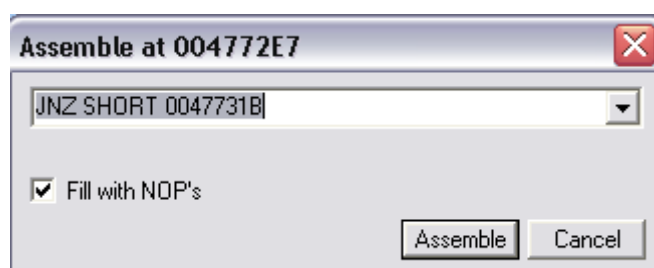
Cambiamos el estado del flag Z para que salte a ver qué pasa. Nos situamos en dicho flag y con un doble click cambiamos el estado del este a 0 para que el JNZ se produzca:

C	0
P	1
A	0
N	0
Z	1
S	0
T	0
O	0
D	0
O	0

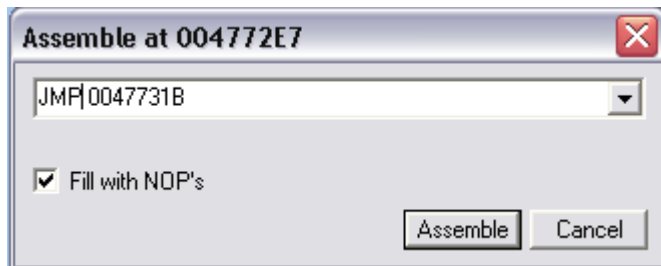
Run o F9 y vemos que el mensaje no aparece y comienza a ripear; yo lo deje y termino con todo el DVD que había cargado. Funcionó.

Volvamos al JNZ en el que pusimos el BP y cambiémoslo por un JMP (Click con el botón derecho y ASSEMBLE):

ANTES:

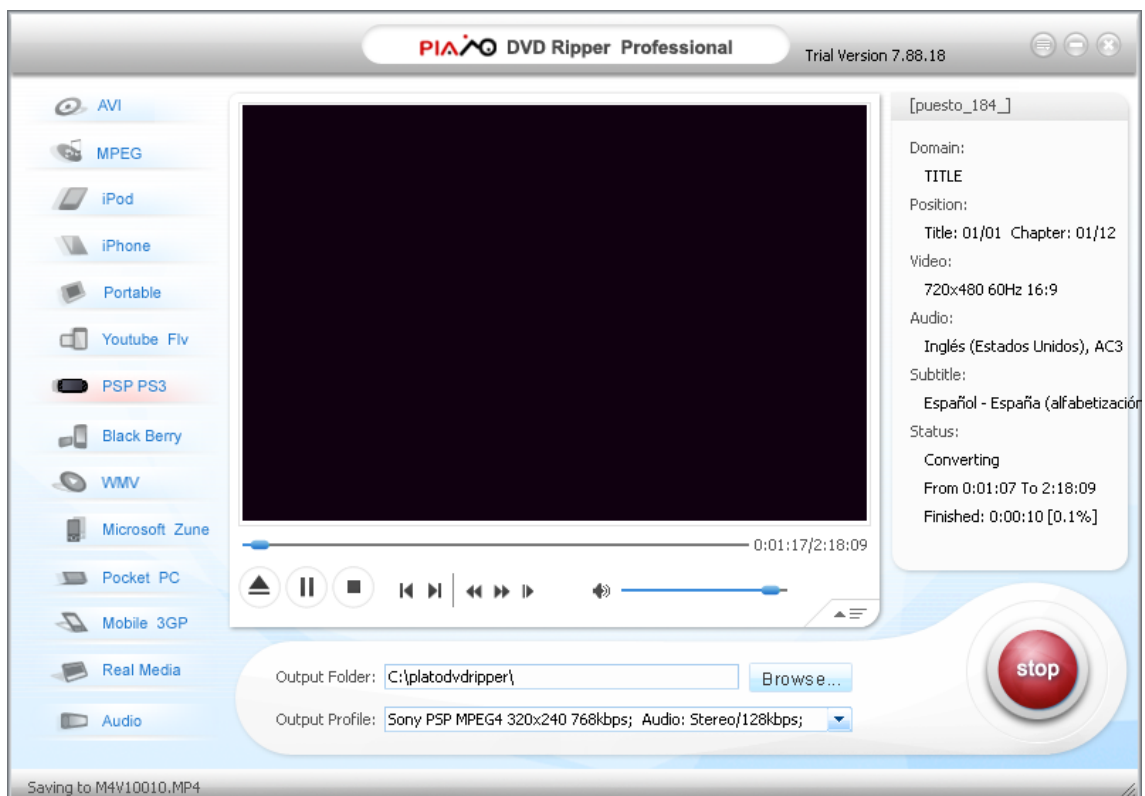


DESPUÉS:

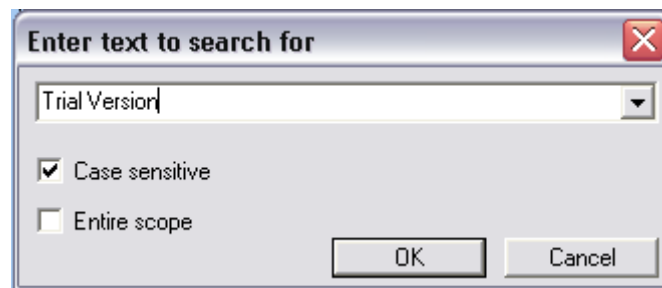


Guardemos los cambios en el ejecutable. Click con el botón derecho COPY TO EXECUTABLE/ALL MODIFICATIONS luego COPY ALL y en la nueva ventana que se abre Click con el botón derecho de nuevo y SAVE FILE. Ojo! A diferencia de los programas de “Parchando a lo Loco Gif Movie Gear y Atomix Mp3” este, si bien pueden guardarlo con otro nombre (dvdripper_pro2.exe por ejemplo), deben hacerlo en el directorio de instalación si no no arranca. Se pone a buscar .dll y no las encuentra....

Bueno guardemos, ejecutemos, carguemos un DVD y veamos si anda:



Si anda...justo saque la impresión de pantalla en una parte de la película en la que no había imagen...jeje,pero anda y eso es lo importante; pero no me gusta algo, ese “Trial Versión” arriba a la derecha. Carguemos el ejecutable modificado que guardamos hoy y busquemoslo en la lista de strings pero marcando Case Sensitive (supongo que en varios lado aparecerá trial o versión por eso me aseguro) y escribámoslo tal cual aparece.



Olly para acá:

0047558F	PUSH 00498408	ASCII "Version %s"
004755C8	PUSH 00498414	ASCII "Trial Version %s"
00475702	PUSH 004983AC	ASCII "question"

Como ven puse un BP.

Con Ctrl + L buscamos el siguiente que en realidad es la última vez que para:

0047AD0C	PUSH 004972DC	ASCII "Version %s"
0047AD3D	PUSH 004972E8	ASCII "Trial Version %s"
0047AD6E	PUSH 004972FC	ASCII "Free Version %s"

También le puse un BP.

Run o F9 y veamos donde para primero:

0047ACF4	833D 849A4B01	CMP DWORD PTR DS:[4B9A84],0	
0047ACFB	75 6A	JNZ SHORT 0047AD67	
0047ACFD	833D 74964B01	CMP DWORD PTR DS:[4B9674],1	
0047AD04	75 30	JNZ SHORT 0047AD36	
0047AD06	A1 9CAD4B00	MOV EAX,DWORD PTR DS:[4BAD9C]	
0047AD08	50	PUSH EAX	
0047AD0C	68 DC724900	PUSH 004972DC	
0047AD11	8D4D F0	LEA ECX,DWORD PTR SS:[EBP-10]	
0047AD14	51	PUSH ECX	
0047AD15	E8 C668F8FF	CALL 004015E0	
0047AD1A	83C4 0C	ADD ESP,0C	
0047AD1D	8D4D F0	LEA ECX,DWORD PTR SS:[EBP-10]	
0047AD20	E8 DB72F8FF	CALL 00402000	
0047AD25	50	PUSH EAX	
0047AD26	8B4D EC	MOV ECX,DWORD PTR SS:[EBP-14]	
0047AD29	81C1 98C10101	ADD ECX,1C198	
0047AD2F	E8 90B9F9FF	CALL 004166C4	
0047AD34	EB 2F	JMP SHORT 0047AD65	
0047AD36	8B15 9CAD4B01	MOV EDX,DWORD PTR DS:[4BAD9C]	
0047AD3C	52	PUSH EDX	
0047AD3D	68 E8724900	PUSH 004972E8	
0047AD42	8D45 F0	LEA EAX,DWORD PTR SS:[EBP-10]	
0047AD45	50	PUSH EAX	
0047AD46	E8 9568F8FF	CALL 004015E0	
0047AD48	83C4 0C	ADD ESP,0C	
0047AD4E	8D4D F0	LEA ECX,DWORD PTR SS:[EBP-10]	
0047AD51	E8 AA72F8FF	CALL 00402000	
0047AD56	50	PUSH EAX	
0047AD57	8B4D EC	MOV ECX,DWORD PTR SS:[EBP-14]	
0047AD5A	81C1 98C10101	ADD ECX,1C198	
0047AD60	E8 5FB9F9FF	CALL 004166C4	
0047AD65	EB 2F	JMP SHORT 0047AD96	
0047AD67	8B0D 9CAD4B01	MOV ECX,DWORD PTR DS:[4BAD9C]	
0047AD6D	51	PUSH ECX	
0047AD6E	68 FC724900	PUSH 004972FC	
0047AD73	8D55 F0	LEA EDX,DWORD PTR SS:[EBP-10]	
0047AD76	52	PUSH EDX	
0047AD77	E8 6468F8FF	CALL 004015E0	
0047AD7C	83C4 0C	ADD ESP,0C	

Arg3 => 00FC67B8 ASCII "7.88.18"

Arg2 = 004972DC ASCII "Version %s"

Arg1

dvdripped.004015E0

Arg3 => 00FC67B8 ASCII "7.88.18"

Arg2 = 004972E8 ASCII "Trial Version %s"

Arg1

dvdripped.004015E0

Arg3 => 00FC67B8 ASCII "7.88.18"

Arg2 = 004972FC ASCII "Free Version %s"

Arg1

dvdripped.004015E0

Ahí vemos las tres posibilidades que nos podría mostrar en la esquina superior derecha:

"Version", " Trial Version" y "Free Versión". Sé que la Trial no es la que quiero pero de las otras dos con cual me quedo ? Si alguno hizo la tareita que deje más arriba(la de parchar para

registrar con cualquier nombre y serial) verán que cuando registran con cualquier nombre arriba se pone “Version 7.88.18” haci que supongo que será la primera opción la que debe mostrar al registrar correctamente. Quienes deciden el texto a mostrar son los 2 JNZ en la parte superior de la imagen: el primero nos manda a “Free Version”, el segundo a “Trial Version” y si no se producen ninguna de las 2 me muestra “Version”. Seleccionemos desde el primer JNZ hasta el último haci:

```

0047ACF4 | . 833D 849A4B00 CMP DWORD PTR DS:[4B9A84],0
0047ACFB | 75 6A JNZ SHORT 0047AD04
0047ACFD | 833D 74964B00 CMP DWORD PTR DS:[4B96741],1
0047AD04 | 75 30 JNZ SHORT 0047AD06
0047AD06 | . A1 9CAD4B00 MOV EAX,DWORD PTR DS:[4BAD9C]

```

Y nopemos: Click con el botón derecho BINARY/FILL WITH NOPs. Guardamos los cambios en ejecutable (ya saben cómo hacerlo) y lo probamos:



Bueno...anda y ahora si me gusta como quedó.

Saludos a toda la lista...espero que los 3 tutes hayan sido de utilidad, en especial a quienes recién comienzan, como yo; quizás cuando avance un poco más vuelva a utilizar los mismos 3 programas de estos tutes para hallar su serial y no parcharlo, pero bueno ya veo que hago.

BiObAzArD