2017

Revisando un pequeño Asprotect

Apuromafo

CLS

4-7-2017

Índice

Contenido

Introducción

Programa	Model Maker v11
Descarga	http://www.modelmakertools.com/modelmaker/download.html
Dificultad	Inicial (Tiempo y ganas)
Packer	Asprotect SKE
Herramientas usadas	X64dbg +Resource hacker+ Ollydbg plugin codedoctor,PID
Fecha	04/07/2017
Cracker	Jhon y Apuromafo

Toda idea nueva pasa inevitablemente por tres fases: primero es ridícula, después es peligrosa, y después... ¡todos la sabían!. Henry George (1839-1897); economista estadounidense .

Herramientas usadas:

Herramienta	***Descarga***	***Utilidad***
Procesador de texto	***(está incluido con el suite de office)***	***Para redactar el tutorial***
Sharex	***https://getsharex.com/***	***Para capturar las imágenes***
Everything	***http://www.voidtools.com/***	***Para buscar los archivos en el pc***
X64dbg	***http://x64dbg.com/***	***Depurador***
PID	***https://web.archive.org/web/20170620171730/http://pid.gcwstorage.xyz/dl.php?f=ProtectionId.685.December.2016.rar***	***Analizador de Ejecutables***
IDR	https://web.archive.org/web/20170501145746/http://kpnc.org/idr32/en/ https://github.com/crypto2011/IDR	***Analizador de Delphi (interactive delphi …)***
IDA	***https://www.hex-rays.com/products/ida/***	Herramienta de analisis estático
InnoSetup	***http://www.jrsoftware.org/isinfo.php***	Herramienta para generar Setup.exe
InnoUnpack	https://sourceforge.net/projects/innounp/?source=typ_redirect	Unpacker para innosetup
Inno Gui (unpack)	https://www.holylinux.net/code/innoextractor	Gui para unpacker de innosetup
De4dot	https://ci.appveyor.com/project/0xd4d/de4dot/build/artifacts	Unpacker/desofuscador para archivos .net
Codedoctor	https://tuts4you.com/download.php?view.2834	Plugin Codedoctor para ollydbg permite hacer unpack a asprotect
ollydbg v1.1	http://ollydbg.de/	Depurador

Explorando el Programa

Bienvenidos a esta pequeña lectura e historia explorando un programa propuesto por un buen amigo, este es una aplicación para delphi, este permite extender una funcionalidad en Delphi, existen algunos gratuitos pero este es trial (free para usar).

Desde el sitio oficial se puede apreciar que es free and fully functional (es gratuito y funcional por completo), refiere que expira despues de 45 días despues de la primera activacion (ejecución).

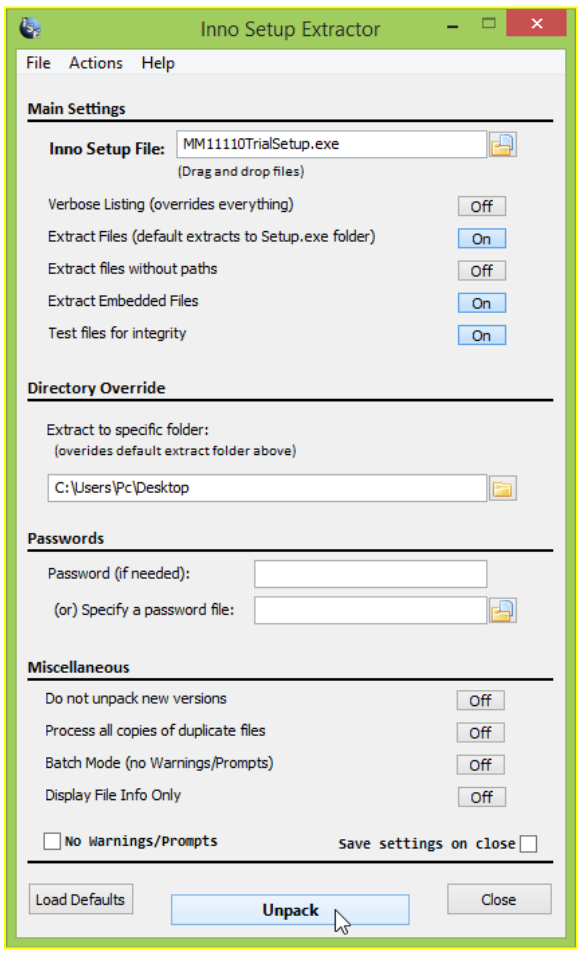
<img1: Info del programa>

PID sobre el setup:

Comenzamos la hazaña, Iuego de descargar el instalador, Analizo con PID y obtengo un setup hecho con inno :

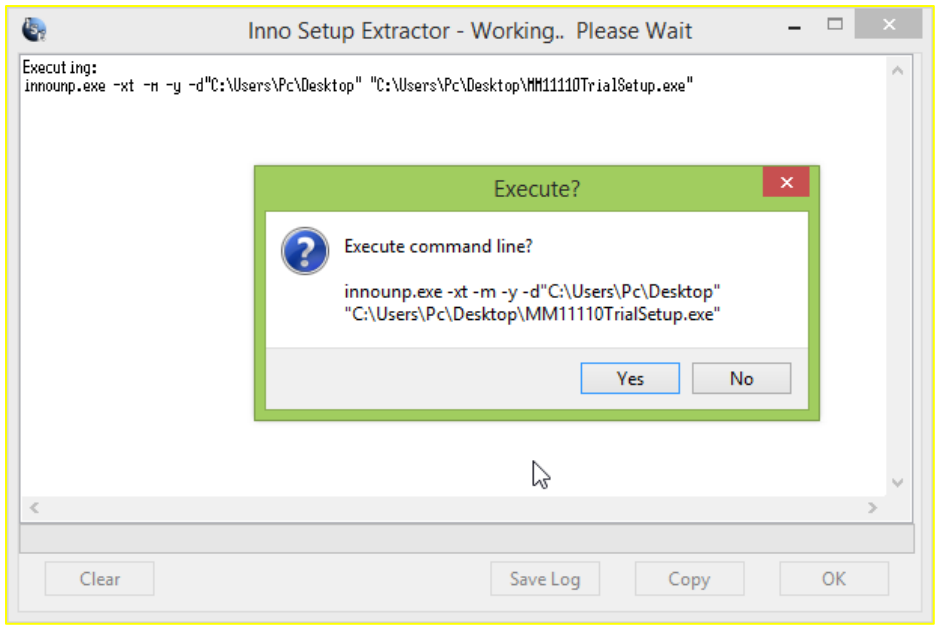
```
-=[ ProtectionID v0.6.8.5 DECEMBER]=-
(c) 2003-2017 CDKiLLER & TippeX
Build 24/12/16-13:09:21
Ready...
Scanning -> C:\Users\Pc\Desktop\MM11110TrialSetup.exe
File Type : 32-Bit Exe (Subsystem : Win GUI / 2), Size : 12380892 (0BCEADCh) Byte(s) | Machine: 0x14C (I386)
Compilation TimeStamp : 0x2A425E19 -> Fri 19th Jun 1992 22:22:17 (GMT)
[TimeStamp] 0x2A425E19 -> Fri 19th Jun 1992 22:22:17 (GMT) | PE Header | - | Offset: 0x00000108 | VA: 0x00400108 | -
-> File has 12323036 (0BC08DCh) bytes of appended data starting at offset 0E200h
[File Heuristics] -> Flag #1 : 00000000000001001101000000100100 (0x0004D024)
[Entrypoint Section Entropy] : 6.65 (section #0) "CODE    " | Size : 0xA1D0 (41424) byte(s)
[DllCharacteristics] -> Flag : (0x8140) -> ASLR | DEP | TSA
[SectionCount] 8 (0x8) | ImageSize 0x15000 (86016) byte(s)
[VersionInfo] Company Name : ModelMaker Tools BV
[VersionInfo] Product Name : ModelMaker Pascal Edition 11.11.0 Trial
[VersionInfo] Product Version : 11.11.0d
[VersionInfo] File Description : ModelMaker Pascal Edition 11.11.0 Trial Setup
[VersionInfo] Version Comments : This installation was built with Inno Setup.
[VersionInfo] Legal Copyrights : Copyright © 1994 - 2017 ModelMaker Tools BV
[ModuleReport] [IAT] Modules -> kernel32.dll | user32.dll | oleaut32.dll | advapi32.dll | kernel32.dll | user32.dll | comctl32.dll | advapi32.dll
[-= Installer =-] Inno Setup v5.5.7 Module
[CompilerDetect] -> Borland Delphi (unknown version) - 40% probability
- Scan Took : 0.109 Second(s) [00000006Dh (109) tick(s)] [39 of 580 scan(s) done]
```

Dado que es un programa creado con inno setup, procedo a descargar un descompilador para ese instalador dado que tengo esa herramienta a mano (busco con Everything), Primero bajo la gui para el programa, luego actualizo el decompilador, con esto esta listo para descompilar el setup.



<img2:gui de inno unpack>

Que en palabras simples ejecuta y Con esto ya tenemos los archivos en cuestión.



<img3:comandos de inno unpack>

PID orientando el camino a recorrer:

Analizamos los más relevantes con PID: Encontramos un archivo para temporales: esta en delphi, no hay mucho que decir

```
Scanning -> C:\Users\Pc\Desktop\{tmp}\MMISUtils.dll
File Type : 32-Bit Dll (Subsystem : Win GUI / 2), Size : 45568 (0B200h) Byte(s) | Machine: 0x14C (I386)
Compilation TimeStamp : 0x2A425E19 -> Fri 19th Jun 1992 22:22:17 (GMT)
[TimeStamp] 0x2A425E19 -> Fri 19th Jun 1992 22:22:17 (GMT) | PE Header | - | Offset: 0x00000108 | VA: 0x00400108 | -
[File Heuristics] -> Flag #1 : 00000000000001001100000100100000 (0x0004C120)
[Entrypoint Section Entropy] : 6.46 (section #0) "CODE    " | Size : 0x814C (33100) byte(s)
[DllCharacteristics] -> Flag : (0x0001) -> PInit
[SectionCount] 7 (0x7) | ImageSize 0x10000 (65536) byte(s)
[Export] 100% of function(s) (1 of 1) are in file | 0 are forwarded | 1 code | 0 data | 0 uninit data | 0 unknown |
[ModuleReport] [IAT] Modules -> kernel32.dll | user32.dll | advapi32.dll | oleaut32.dll | kernel32.dll | kernel32.dll | user32.dll
[CompilerDetect] -> Borland Delphi
[!] File appears to have no protection or is using an unknown protection
- Scan Took : 0.172 Second(s) [0000000ACh (172) tick(s)] [246 of 580 scan(s) done]
```

El programa protegido 1 : esta en delphi, protegido con asprotect

```
Scanning -> C:\Users\Pc\Desktop\{app}\bin\mm11.exe
File Type : 32-Bit Exe (Subsystem : Win GUI / 2), Size : 3066368 (02ECA00h) Byte(s) | Machine: 0x14C (I386)
Compilation TimeStamp : 0x58E4D5EA -> Wed 05th Apr 2017 11:32:58 (GMT)
[TimeStamp] 0x58E4D5EA -> Wed 05th Apr 2017 11:32:58 (GMT) | PE Header | - | Offset: 0x00000108 | VA: 0x00400108 | -
[File Heuristics] -> Flag #1 : 00000000000001001100000000100010 (0x0004C022)
[Entrypoint Section Entropy] : 8.00 (section #0) "        " | Size : 0x21E000 (2220032) byte(s)
[DllCharacteristics] -> Flag : (0x0000) -> NONE
[SectionCount] 12 (0xC) | ImageSize 0xA4C000 (10797056) byte(s)
[VersionInfo] Company Name : ModelMaker Tools BV
[VersionInfo] Product Name : ModelMaker
[VersionInfo] Product Version : 11
[VersionInfo] File Description : ModelMaker 11 - Pascal Edition
[VersionInfo] File Version : 11.11.0.5488
[VersionInfo] Original FileName : MM11.exe
[VersionInfo] Internal Name : MM11
[VersionInfo] Version Comments : MMToolsApi v12
[VersionInfo] Legal Copyrights : © 1994-2017 ModelMaker Tools BV
[ModuleReport] [IAT] Modules -> kernel32.dll | oleaut32.dll | advapi32.dll | user32.dll | user32.dll | msimg32.dll | gdi32.dll | version.dll |
advapi32.dll | oleaut32.dll | ole32.dll | ole32.dll | oleaut32.dll | shell32.dll | shfolder.dll | comctl32.dll | imm32.dll | shell32.dll | comdlg32.dll
| winspool.drv | winspool.drv | libcairo-2.dll | librsvg-2-2.dll | libglib-2.0-0.dll | libgobject-2.0-0.dll | libpango-1.0-0.dll | libpangocairo-1.0-
0.dll | winmm.dll | gdi32.dll | mm8converter.dll | oleacc.dll | gdi32.dll | oleaut32.dll | kernel32.dll
[!] ASProtect SKE v2.72 or higher detected !
[CompilerDetect] -> Borland Delphi (unknown version) - 40% probability
- Scan Took : 0.281 Second(s) [000000119h (281) tick(s)] [441 of 580 scan(s) done]
```

El archivo ofuscado 2: esta en .net , al parecer solo es ofuscación.

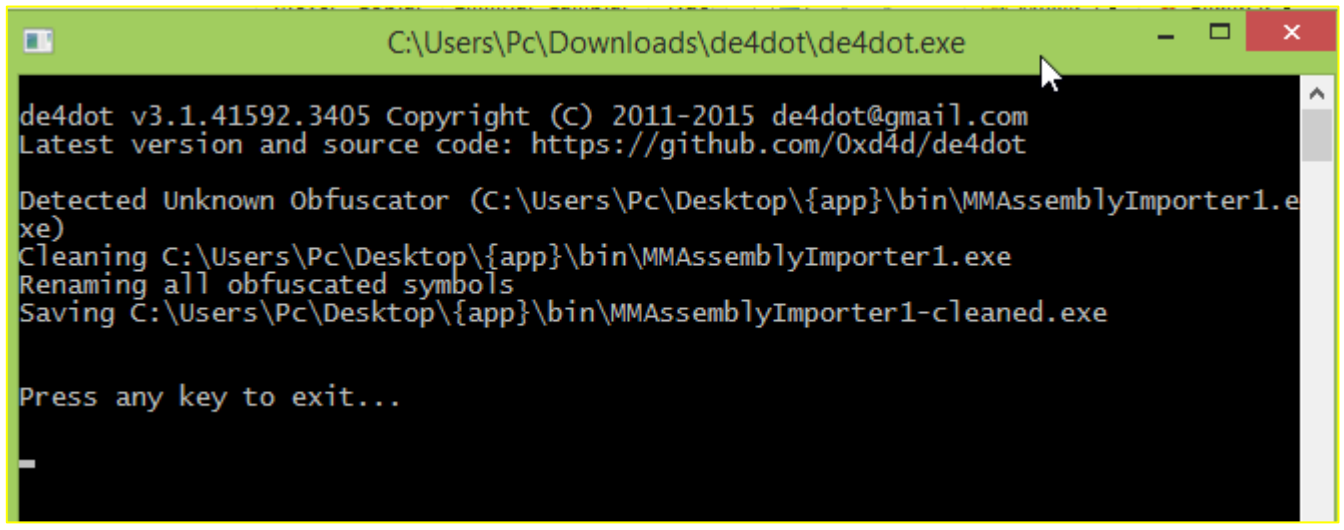
```
Scanning -> C:\Users\Pc\Desktop\{app}\bin\MMAssemblyImporter1.exe
File Type : 32-Bit Exe (Subsystem : Win CUI / 3), Size : 40960 (0A000h) Byte(s) | Machine: 0x14C (I386)
Compilation TimeStamp : 0x454B1880 -> Fri 03rd Nov 2006 10:22:56 (GMT)
[TimeStamp] 0x454B1880 -> Fri 03rd Nov 2006 10:22:56 (GMT) | PE Header | - | Offset: 0x00000088 | VA: 0x00400088 | -
[File Heuristics] -> Flag #1 : 00000000000001001100000000110000 (0x0004C030)
[Entrypoint Section Entropy] : 5.25 (section #0) ".text   " | Size : 0x6334 (25396) byte(s)
[DllCharacteristics] -> Flag : (0x0400) -> NOSEH
[SectionCount] 3 (0x3) | ImageSize 0xE000 (57344) byte(s)
[VersionInfo] Company Name : ModelMaker Tools BV
[VersionInfo] Product Name : ModelMaker
[VersionInfo] Product Version : 1.0.2498.20488
[VersionInfo] File Version : 1.0.2498.20488
[VersionInfo] Original FileName : MMAssemblyImporter1.exe
[VersionInfo] Internal Name : MMAssemblyImporter1.exe
[VersionInfo] Version Comments : ModelMaker C# Reflector
[VersionInfo] Legal Copyrights : Copyright (c) 1995-2005 ModelMaker Tools BV
[ModuleReport] [IAT] Modules -> mscoree.dll
[.] .net @ FileOffset 0x3CFC | MetaData->Version 1.1 (struct version) -> v1.1.4322 (net version required)
[.] Flags : 0x0 | Streams : 0x5 (5)  -> #~ | #Strings | #US | #GUID | #Blob
[!] [.net scan core] dotNetReactor detected!
[COR20] MajorRuntimeVersion 0x2 (2) | MinorRuntimeVersion 0x2 (2) -> 0x2.2 (2.2)
[COR20] Flags 0x1
[COR20 Flags] [x] IL_ONLY [ ] 32BITREQUIRED [ ] IL_LIBRARY
[COR20 Flags] [ ] STRONGNAME [ ] NATIVE_EP [ ] TRACKDEBUGDATA
[COR20 Flags] [ ] 32BITPREFERRED | 0x0 UNKNOWN
[COR20 Flags] Assembly is NOT strong name signed
- Scan Took : 0.109 Second(s) [00000006Dh (109) tick(s)] [506 of 580 scan(s) done]
```

Y el ofuscado 3 : en .net , al parecer solo es ofuscación.

```
Scanning -> C:\Users\Pc\Desktop\{app}\bin\MMAssemblyImporter2.exe
File Type : 32-Bit Exe (Subsystem : Win CUI / 3), Size : 40960 (0A000h) Byte(s) | Machine: 0x14C (I386)
Compilation TimeStamp : 0x454B183A -> Fri 03rd Nov 2006 10:21:46 (GMT)
[TimeStamp] 0x454B183A -> Fri 03rd Nov 2006 10:21:46 (GMT) | PE Header | - | Offset: 0x00000088 | VA: 0x11000088 | -
[File Heuristics] -> Flag #1 : 00000000000001001100000000110000 (0x0004C030)
[Entrypoint Section Entropy] : 5.34 (section #0) ".text   " | Size : 0x61E4 (25060) byte(s)
[DllCharacteristics] -> Flag : (0x0400) -> NOSEH
[SectionCount] 3 (0x3) | ImageSize 0xE000 (57344) byte(s)
[VersionInfo] Company Name : ModelMaker Tools BV
[VersionInfo] Product Name : ModelMaker
[VersionInfo] Product Version : 1.0.2498.20453
[VersionInfo] File Version : 1.0.2498.20453
[VersionInfo] Original FileName : MMAssemblyImporter2.exe
[VersionInfo] Internal Name : MMAssemblyImporter2.exe
[VersionInfo] Version Comments : ModelMaker C# Reflector
[VersionInfo] Legal Copyrights : Copyright (c) 1995-2005 ModelMaker Tools BV
[ModuleReport] [IAT] Modules -> mscoree.dll
[.] .net @ FileOffset 0x3A58 | MetaData->Version 1.1 (struct version) -> v2.0.50727 (net version required)
[.] Flags : 0x0 | Streams : 0x5 (5)  -> #~ | #Strings | #US | #GUID | #Blob
[!] [.net scan core] dotNetReactor detected!
[COR20] MajorRuntimeVersion 0x2 (2) | MinorRuntimeVersion 0x2 (2) -> 0x2.2 (2.2)
[COR20] Flags 0x1
[COR20 Flags] [x] IL_ONLY [ ] 32BITREQUIRED [ ] IL_LIBRARY
[COR20 Flags] [ ] STRONGNAME [ ] NATIVE_EP [ ] TRACKDEBUGDATA
[COR20 Flags] [ ] 32BITPREFERRED | 0x0 UNKNOWN
[COR20 Flags] Assembly is NOT strong name signed
- Scan Took : 0.94 Second(s) [00000005Eh (94) tick(s)] [506 of 580 scan(s) done]
```

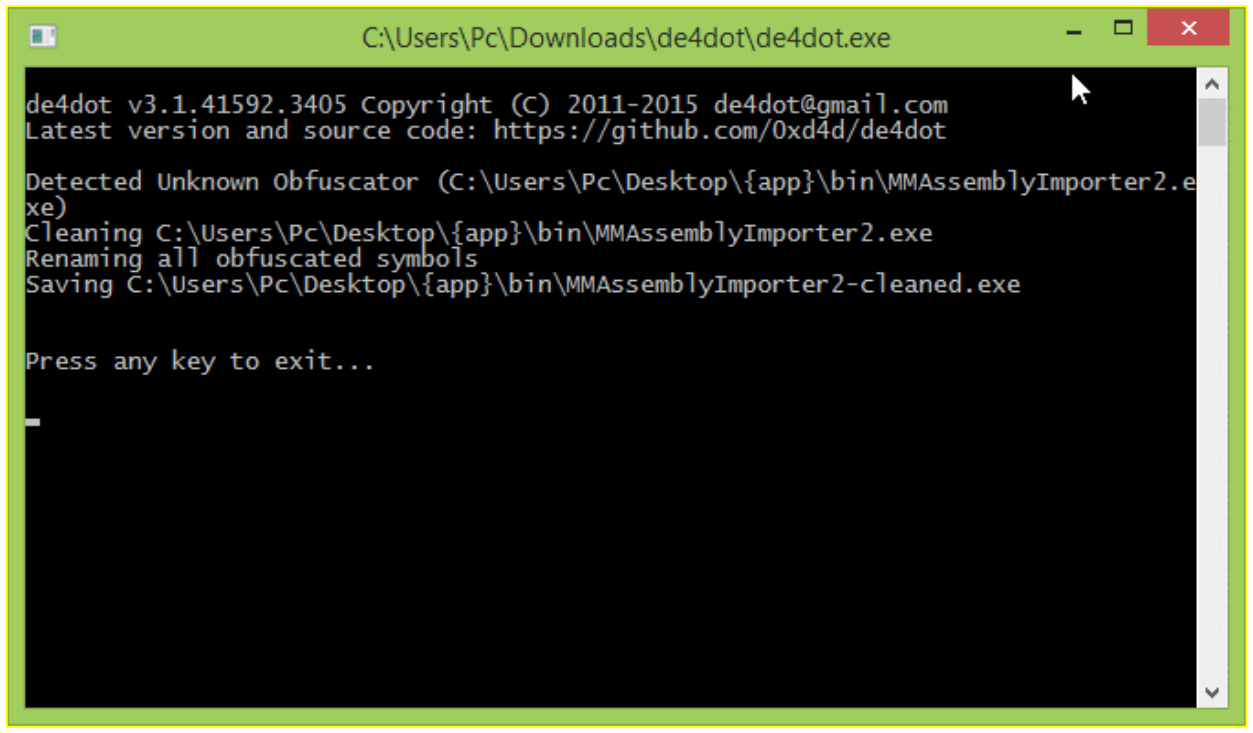
Quitando las proteccion al .net con de4dot:

Comenzamos con los .net usando de4dot: el primer resultado es que ha quedado desofuscado



<img4:De4dot .net unpack>

Para el segundo lo mismo



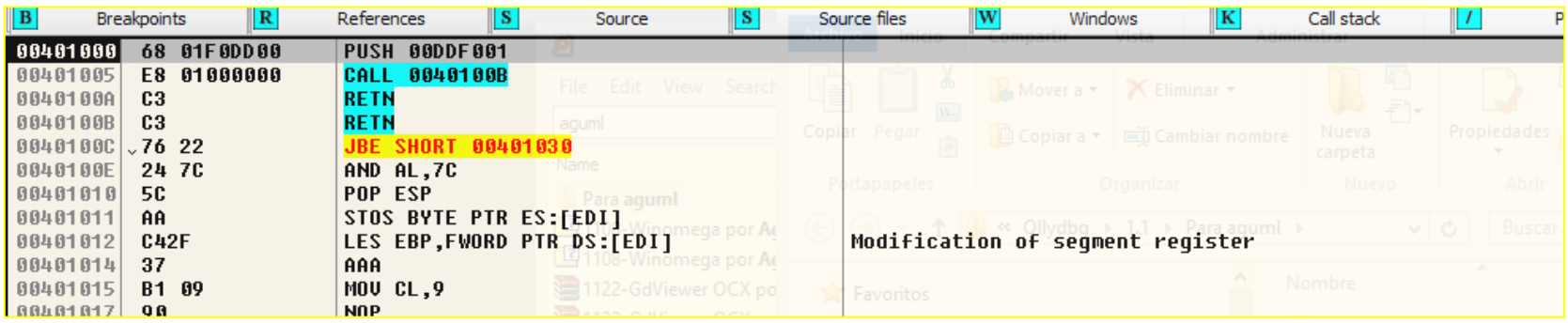
<img5:De4dot .net unpack>

Ambos corren, asi que primera misión lista.

Conociendo la victima de hoy

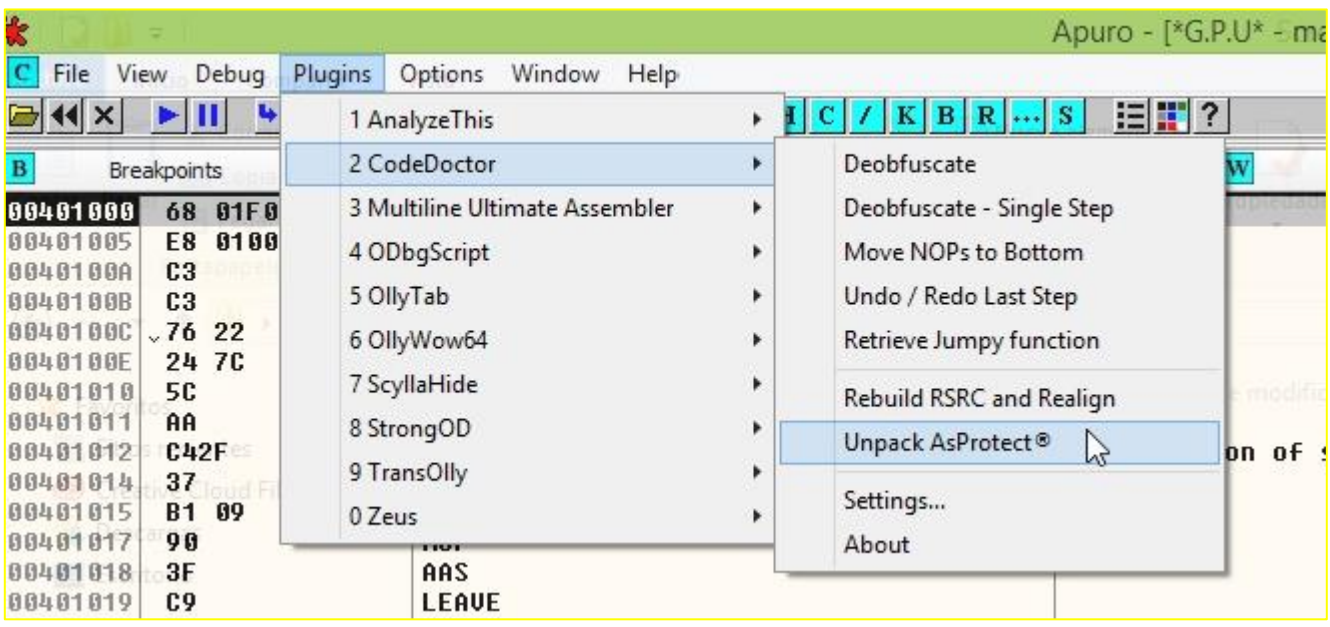
Ahora le toca el turno de asprotect, asprotect es un protector comercial bastante conocido, es bastante dificil de desempacar, pero existen herramientas que nos ayuda, ahora lo cargo en ollydbg 1.1 con el plugin codedoctor, el resultado son en 3 pasos

1) Cargar el programa



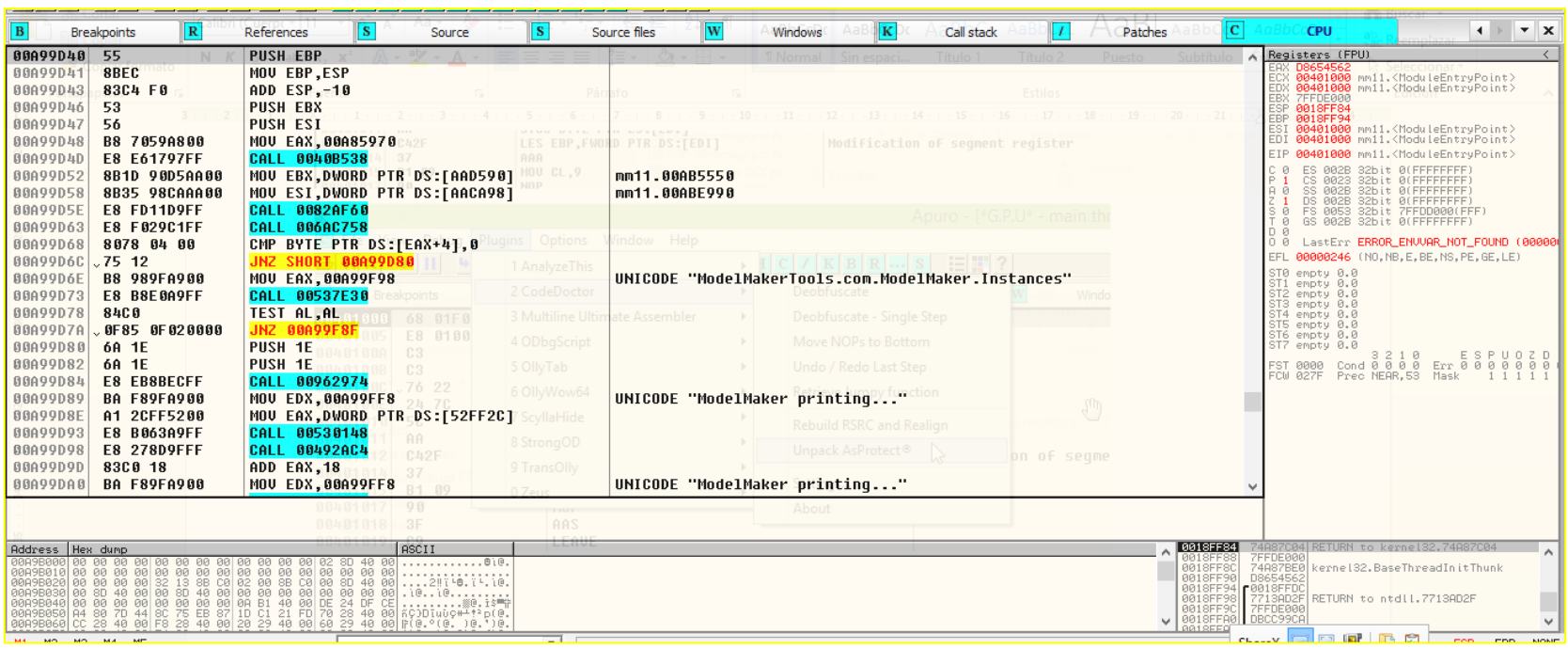
<img6:Ollydbg en el entrypoint>

2) Ejecutar el plugin Codedoctor en la opción Unpack Asprotect, 3) luego al unpacked la opcion rebuild rsrc and realign



<img6:Ollydbg +Codedoctor "unpack asprotect">

Luego que pasan unos segundos

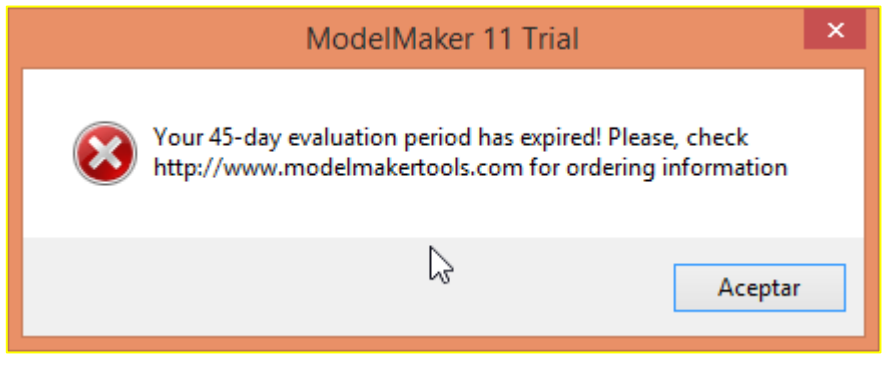


<img6:Ollydbg está en el OEP>

El programa queda desempacado como "nombre_dumped.exe"

Hasta aquí Asprotect Unpacked

Es conocido por todos que hay dificultades, Pensemos el caso si ejecuto luego de 45 dias expira:

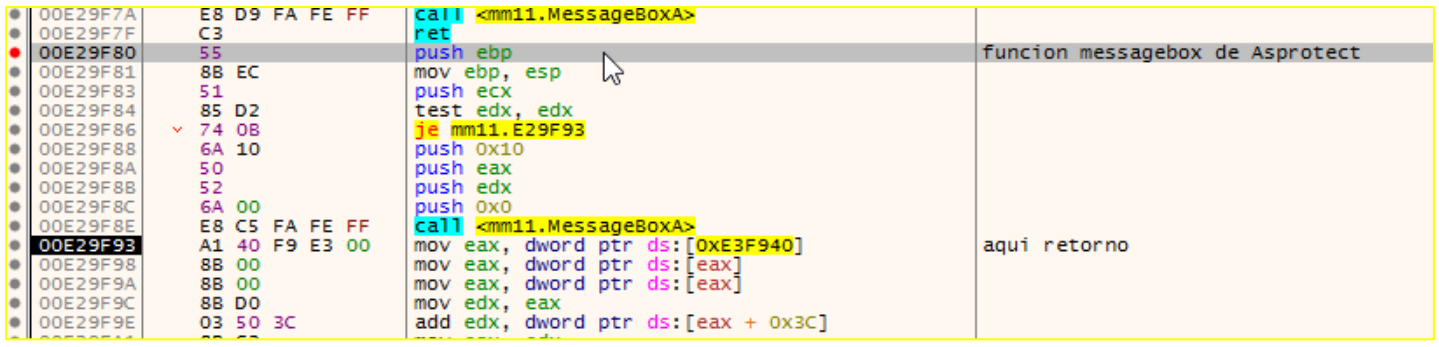


<img7:Messagebox que indica que esta expired desde el programa expirado>

Tengo algunas opciones por hoy:

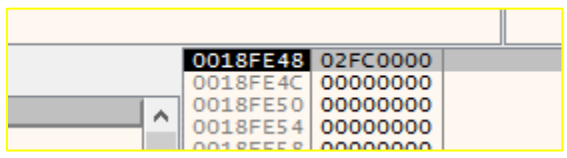
a) Desempacarlo estando expirado (reviviendo un muerto) con x64dbg

Digamos que me aparece expired, porque realmente me expiró. Configuro lo necesario X64dbg con el buscador de archivos, luego en la linea de comandos , usar el comando hidedebugger o hide para que sea invisible a los ojos de asprotect, luego de ejecutado el programa con el depurador tengo este mensaje de expired(imagen 7) ,Podemos guiarnos con tecnicas de pausa, call stack , ver cual es de "user" y luego volver a donde estaba la llamada, Asi veo, depuro el programa y al retornar apunto donde estoy, coloco bp en el comienzo de esta funcion que yo le llamo"messagebox"



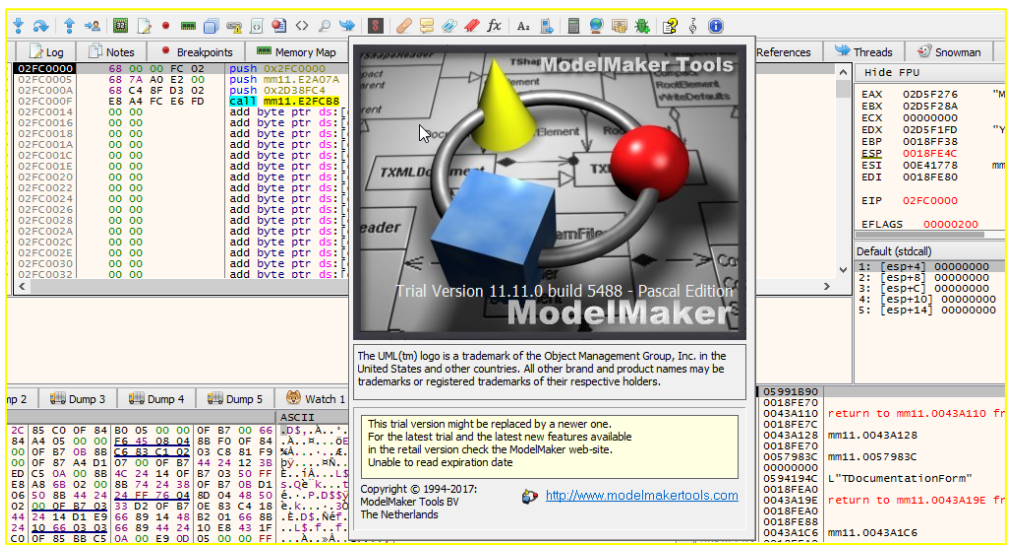
<img08:Messagebox del Asprotect en nuestra vícitma, nos avisa que estamos expirados>

Al observar stack tenemos:



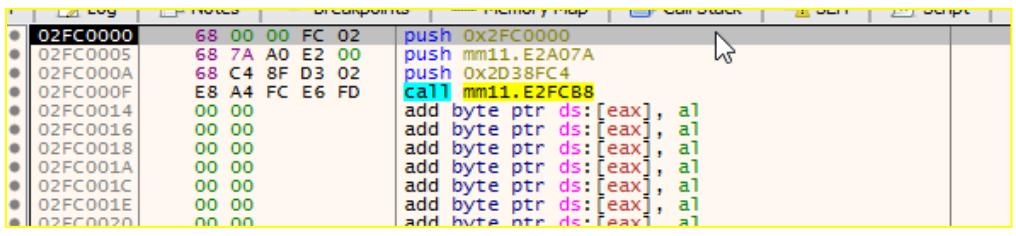
<img09:stack indica una direccion que no es nada mas ni nada menos que el entrypoint de un asprotect stub>

Por lo que si coloco ret (anular la funcion mesagebox) deberia continuar la ejecución en 2fc0000



<img10: luego del ret y ejecutado desde la direccion el programa demuestra que corre>

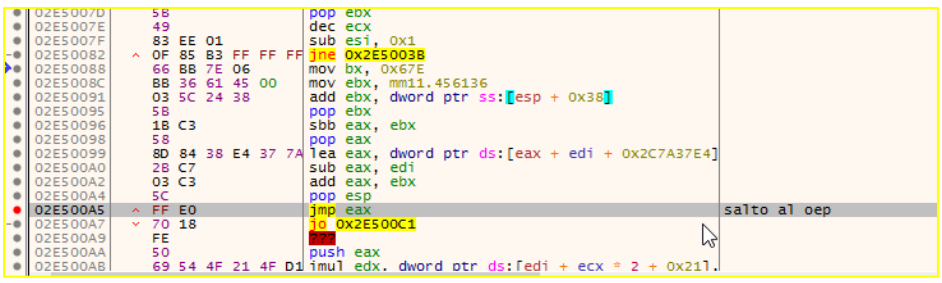
Es correcto, el programa corre, repito la hazaña, bp en ejecucion, ret y ahora veamos con un run que muestra:



<img11: x64dbg-> entrypoint del stub de asprotect>

Podemos ir en busqueda del oep del asprotect, Puedo colocar un bp en access en la seccion y llegaremos por encima del oep, vuelvo a depurar un poquito mas y si Si retornamos a un poco antes inclusive pillamos el salto del oep.

vuelvo a repetir la hazaña y ahora si lo encuentro.

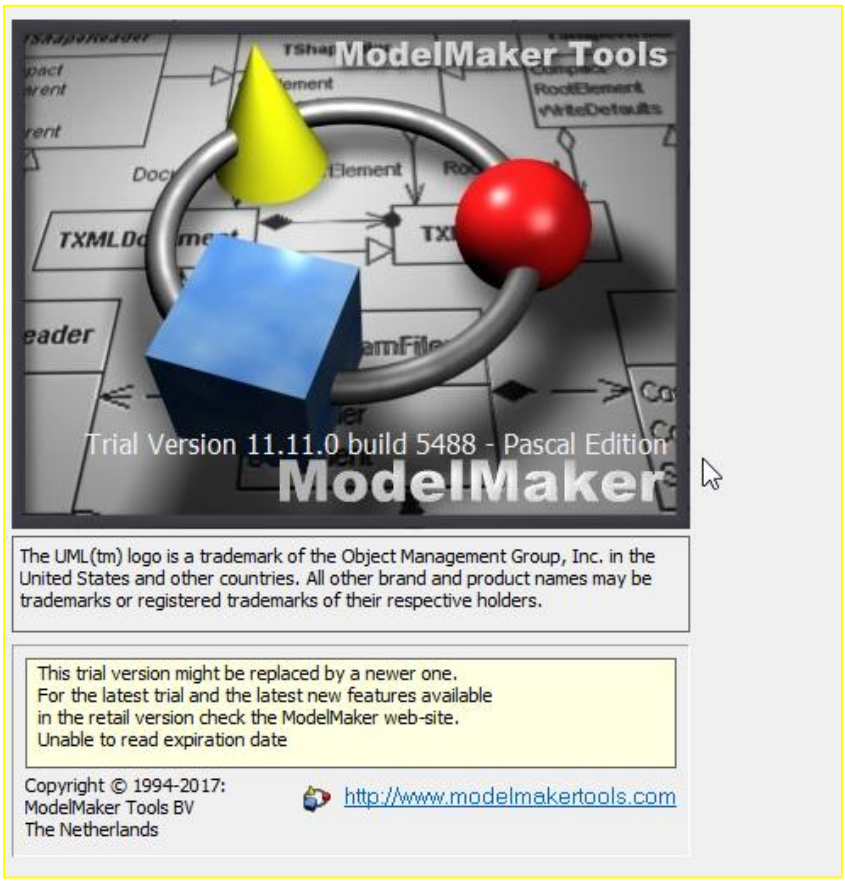


<img12:x64dbg-> salto al oep>

Si doy run: vemos como he logrado ademas bypasear con packer que me bloquea los 45 dias tener la ejecucion…

b) Analizando el unpacked antes o despues de expirar:

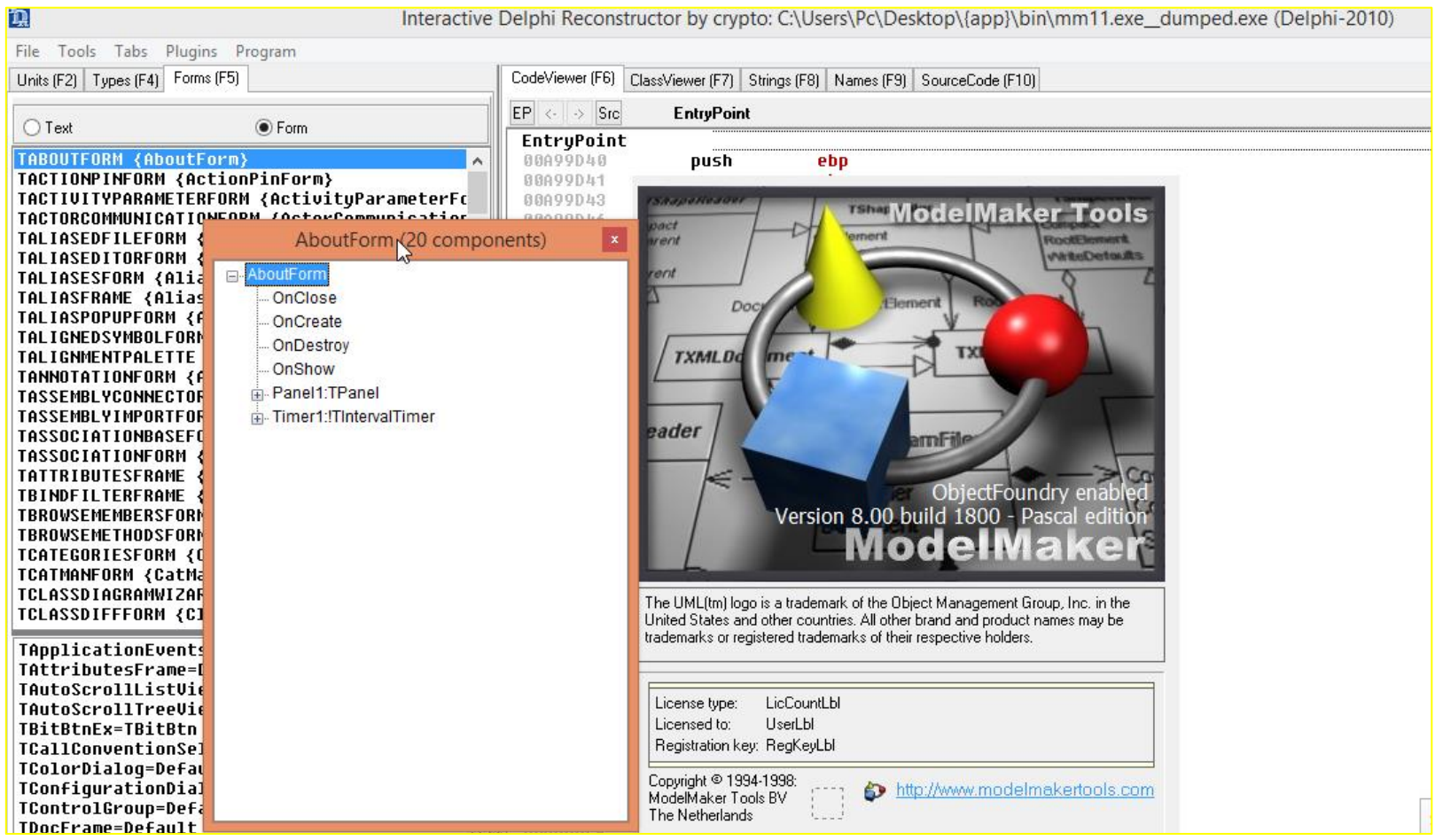
Si vemos o comparamos el unpacked, corre sin problema, ya esta hecho el trabajo mas dificil, ahora falta ver lo estético que queda es el acerca de o llamado “about”



<img13:About Form que indica que es una version Trial, desde x64dbg>

Comienza el ataque en IDR

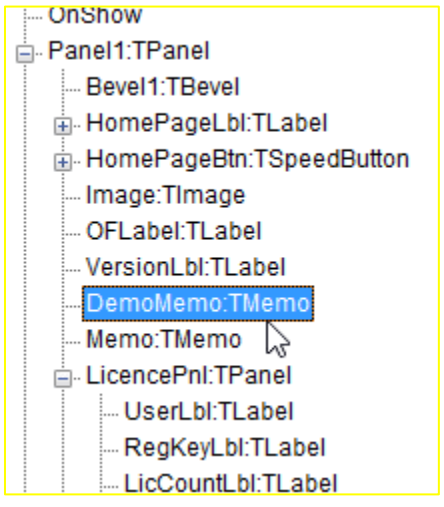
Ahora a investigar de la aplicación, ese about esta bastante especial para ser editado, para esto se hará uso de Interactive Delphi Reconstructor , alias IDR



<img14:About Form desde IDR>

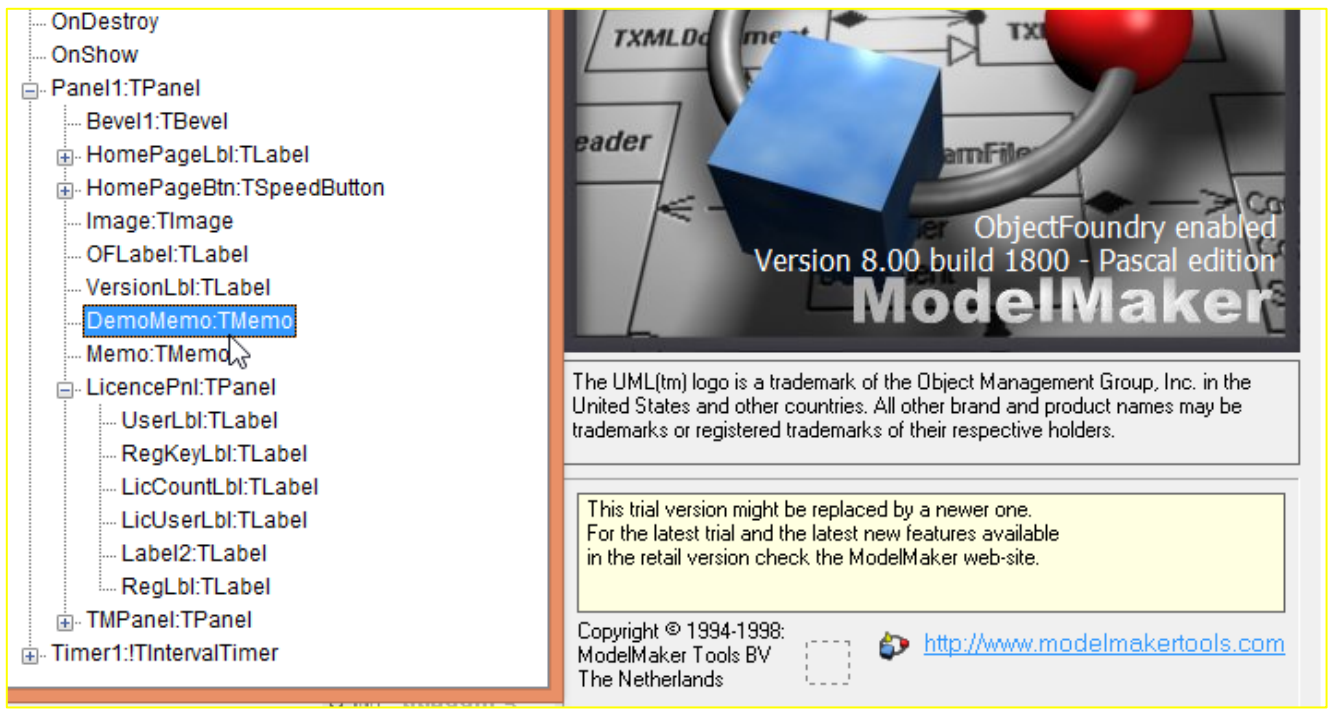
Vemos que trabaja con sdk (notese las palabras User Lbl, entre otros)

En general un packer como asprotect configura todo el entorno demo, deja todo demo y con la licencia sobreescribe ciertos datos para mostrar los registrados para que pueda mostrarse el licenciado, por lo que debemos anular el demomemo y hacer visible lo necesario, debo explorar el programa para ver mas menos como se ve, esto se hace haciendo **doble click** sobre el lugar que se tiene duda.



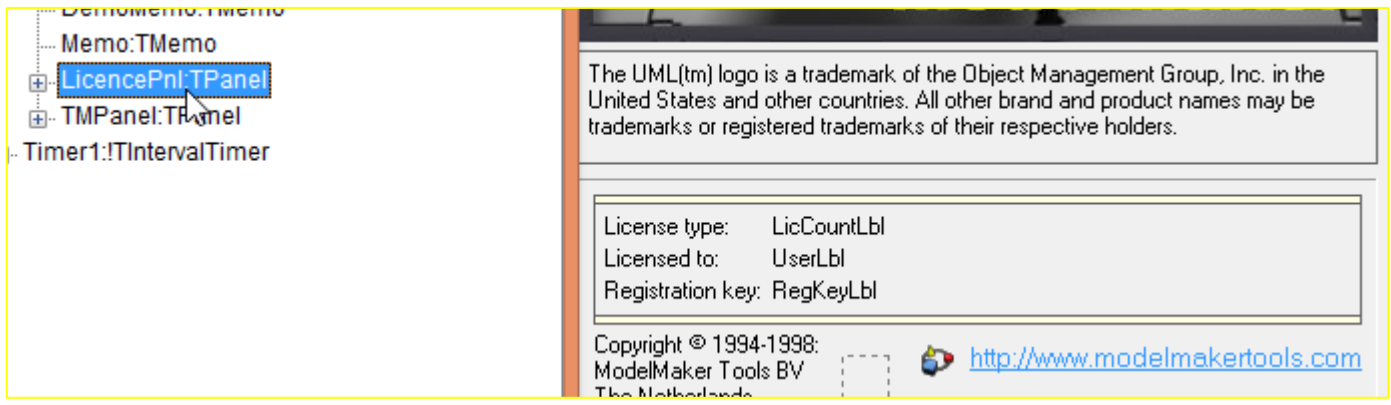
<img15: IDR->DemoMemo en About Form>

Si hago doble clic en demo memo:



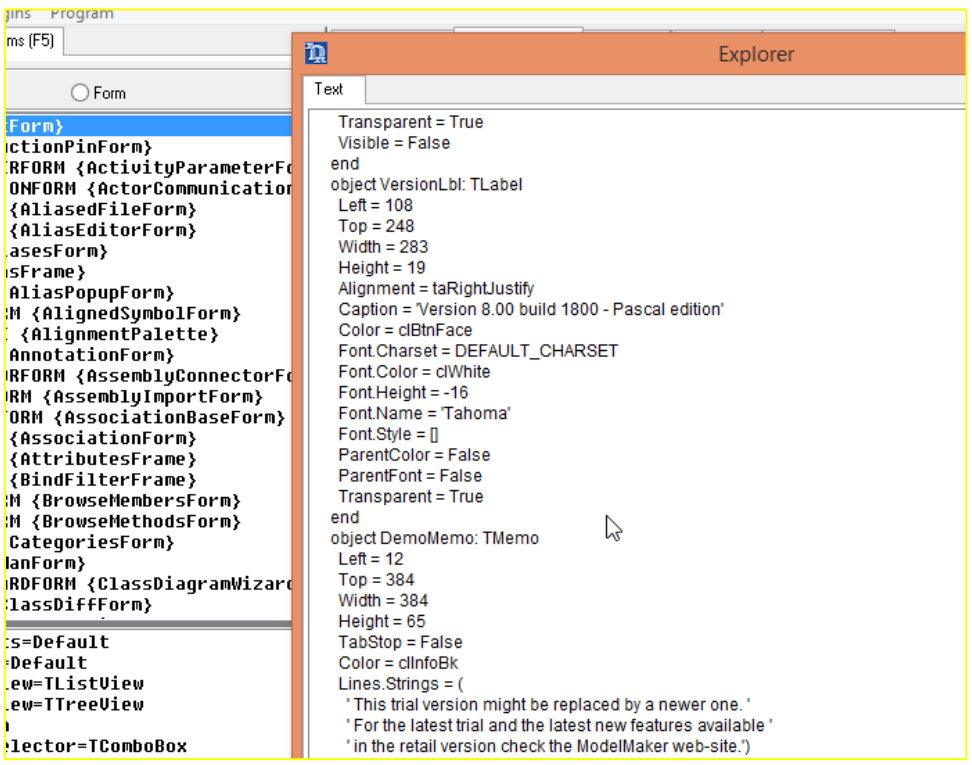
<img16: IDR->DemoMemo en About Form con doble click muestra "this trial version"…>

Si hago doble click licencepnl



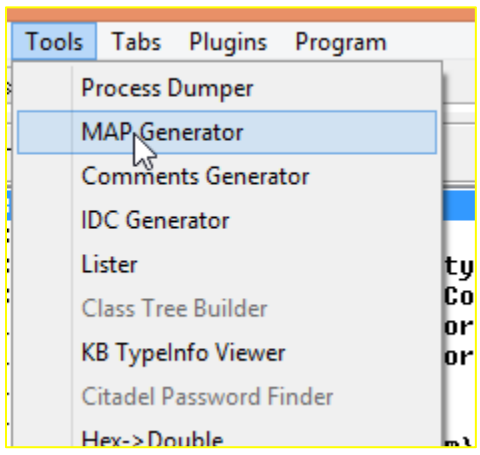
<img17: IDR->LicencePnlen About Form con doble click muestra "License Type.."…>

Como podemos ver sobre escribe encima de la otra. Lo mas rapido sera buscar referencias, pero busco en explorador que me dice



<img18:IDR->LicencePnlen con los labels, y DemoMemoen la exploración, muy similar a Resource hacker."…>

Que estas versiones son caption, por lo cual debe haber algo mas Me dice que en general hay un controles transparentes y/o visibles y/o invisibles voy a generar un map y/o comentarios, no es del todo indispensable, pero cuando se ven direcciones son bastante útiles, es sugerible que ademas se pase por IDA para tener algo mas potente.



<img19:IDR-> exportando algunas referencias /map, comments entre otros>

A mi me interesa la direccion del About Form, al encontrarla la apunto: "**006A2CB6 TaboutForm"**

Comienza el ataque en x64dbg

En esa direccion tenemos pascal edition ; No es el unico asociado al about, pero se que con eso puedo comenzar

```
006A2C9E    68 F6 2C 6A 00    push <mm11.exe__dumped.sub_6A2CF6>
006A2CA3    64 FF 30          push dword ptr fs:[eax]
006A2CA6    64 89 20          mov dword ptr fs:[eax], esp
006A2CA9    FF 05 DC DB AB 00 inc dword ptr ds:[0xABDBDC]
006A2CAF    75 37             jne mm11.exe__dumped.6A2CE8
006A2CB1    E8 8E 99 ED FF    call <mm11.exe__dumped.sub_57C644>
006A2CB6    8B 15 14 17 6A 00 mov edx, dword ptr ds:[<sub_6A1714>]
006A2CBC    E8 97 A0 ED FF    call <mm11.exe__dumped.sub_57CD58>
006A2CC1    A1 44 34 AA 00    mov eax, dword ptr ds:[0xAA3444]
006A2CC6    33 D2             xor edx, edx
006A2CC8    89 15 44 34 AA 00 mov dword ptr ds:[0xAA3444], edx
006A2CCE    E8 09 28 D6 FF    call <mm11.exe__dumped.sub_4054DC>
006A2CD3    B8 48 34 AA 00    mov eax, mm11.exe__dumped.AA3448   AA3448:&L"Pascal Edition"
006A2CD8    B9 02 00 00 00    mov ecx, 0x2
006A2CDD    8B 15 40 12 40 00 mov edx, dword ptr ds:[<sub_401240>]
006A2CE3    E8 5C 59 D6 FF    call <mm11.exe__dumped.sub_408644>
006A2CE8    33 C0             xor eax, eax
006A2CEA    5A                pop edx
006A2CEB    59                pop ecx
006A2CEC    59                pop ecx
006A2CED    64 89 10          mov dword ptr fs:[eax], edx
006A2CF0    68 FD 2C 6A 00    push <mm11.exe__dumped.sub_6A2CFD>
006A2CF5    C3                ret                                sub_6A2CF5
```

<img20:X64dbg >encontrando referencias del About form>

Busco referencias para esa palabra

```
006A27A1  mov eax,dword ptr ds:[AA3448]
006A2CD3  mov eax,mm11.exe__dumped.AA3448
```

<img21:X64dbg >encontrando x referencias del “Pascal Edition” >

```
006A27A1  .  A1 48 34 AA 00     mov eax, dword ptr ds:[0xAA3448]          AA3448:&L"Pascal Edition"
006A27A6  .  89 45 E4           mov dword ptr ss:[ebp - 0x1C], eax
006A27A9  .  C6 45 E8 11        mov byte ptr ss:[ebp - 0x18], 0x11
006A27AD  .  8D 55 D4           lea edx, dword ptr ss:[ebp - 0x2C]
006A27B0  .  B9 02 00 00 00     mov ecx, 0x2
006A27B5  .  B8 A0 28 6A 00     mov eax, mm11.exe__dumped.6A28A0          6A28A0:L"%s %s - %s"
006A27BA  .  E8 45 61 D7 FF     call <mm11.exe__dumped.sub_418904>
006A27BF  .  8B 55 EC           mov edx, dword ptr ss:[ebp - 0x14]
006A27C2  .  8B 45 F8           mov eax, dword ptr ss:[ebp - 0x8]
006A27C5  .  8B 80 C0 03 00 00  mov eax, dword ptr ds:[eax + 0x3C0]
006A27CB  .  E8 2C 81 E5 FF     call mm11.exe__dumped.4FA8FC
006A27D0  .v EB 1D              jmp mm11.exe__dumped.6A27EF
006A27D2  >  8B 45 F8           mov eax, dword ptr ss:[ebp - 0x8]
006A27D5     8B 80 C0 03 00 00  mov eax, dword ptr ds:[eax + 0x3C0]
006A27DB     8B 70 64           mov esi, dword ptr ds:[eax + 0x64]
006A27DE     8B C6              mov eax, esi
006A27E0     E8 BF 7D DB FF     call <mm11.exe__dumped.sub_45A5A4>
006A27E5     8B D0              mov edx, eax
006A27E7     4A                 dec edx
006A27E8     8B C6              mov eax, esi
006A27EA     E8 D1 7D DB FF     call mm11.exe__dumped.45A5C0
006A27EF  >  8B 45 F8           mov eax, dword ptr ss:[ebp - 0x8]
006A27F2     8B 98 C0 03 00 00  mov ebx, dword ptr ds:[eax + 0x3C0]
006A27F8     83 7B 40 0C        cmp dword ptr ds:[ebx + 0x40], 0xC        C:'\f'
006A27FC   v 7D 0D              jge mm11.exe__dumped.6A280B
006A27FE     8B 43 64           mov eax, dword ptr ds:[ebx + 0x64]
006A2801     E8 9E 7D DB FF     call <mm11.exe__dumped.sub_45A5A4>
```

<img22:X64dbg >rutina del About form>

Esta rutina se ve como mas apropiada o mas bien esta es la rutina que busco.

Cuandos se analiza un poco tenemos temas importantes, 1 la palabra trial siempre se carga, se puede remplazar con otra direccion donde su dword apunte a un string nulo o otra palabra.

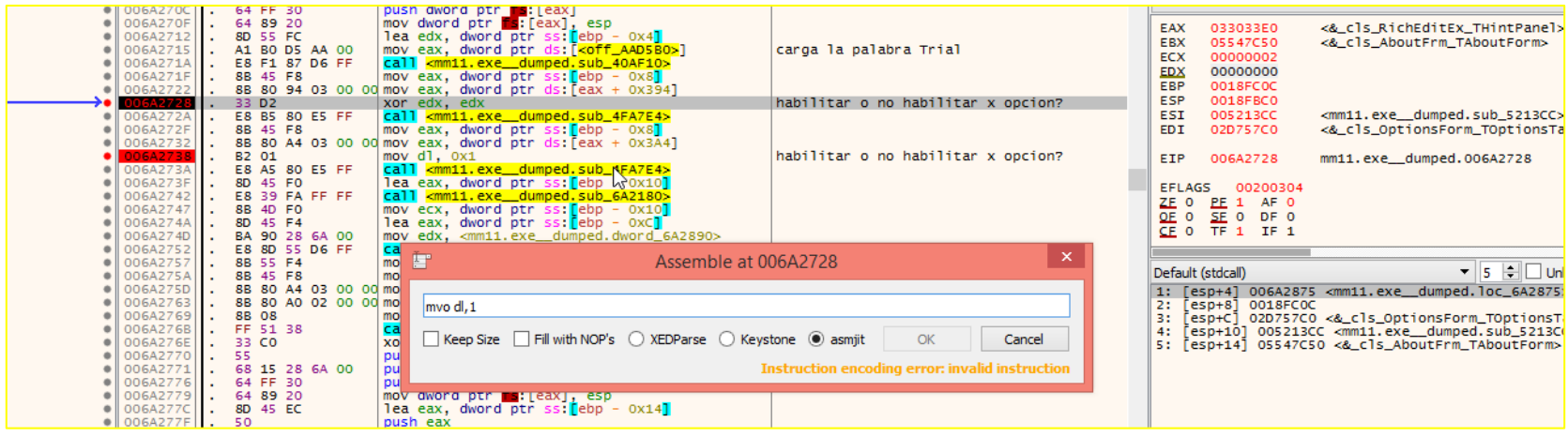
```
006A2701  .  89 45 F8           mov dword ptr ss:[ebp - 0x8], eax
006A2704  .  33 C0              xor eax, eax
006A2706  .  55                 push ebp
006A2707  .  68 75 28 6A 00     push <mm11.exe__dumped.loc_6A2875>
006A270C  .  64 FF 30           push dword ptr fs:[eax]
006A270F  .  64 89 20           mov dword ptr fs:[eax], esp
006A2712  .  8D 55 FC           lea edx, dword ptr ss:[ebp - 0x4]
006A2715  .  A1 B0 D5 AA 00     mov eax, dword ptr ds:[<off_AAD5B0>]      carga la palabra Trial
006A271A  .  E8 F1 87 D6 FF     call <mm11.exe__dumped.sub_40AF10>
006A271F  .  8B 45 F8           mov eax, dword ptr ss:[ebp - 0x8]
006A2722  .  8B 80 94 03 00 00  mov eax, dword ptr ds:[eax + 0x394]
006A2728  .  B2 01              mov dl, 0x1                               habilitar o no habilitar x opcion?
006A272A  .  E8 B5 80 E5 FF     call <mm11.exe__dumped.sub_4FA7E4>
006A272F  .  8B 45 F8           mov eax, dword ptr ss:[ebp - 0x8]
006A2732  .  8B 80 A4 03 00 00  mov eax, dword ptr ds:[eax + 0x3A4]
006A2738  .  B2 00              mov dl, 0x0                               habilitar o no habilitar x opcion?
006A273A  .  E8 A5 80 E5 FF     call <mm11.exe__dumped.sub_4FA7E4>
006A273F  .  8D 45 F0           lea eax, dword ptr ss:[ebp - 0x10]
006A2742  .  E8 39 FA FF FF     call <mm11.exe__dumped.sub_6A2180>
006A2747  .  8B 4D F0           mov ecx, dword ptr ss:[ebp - 0x10]
006A274A  .  8D 45 F4           lea eax, dword ptr ss:[ebp - 0xC]
006A274D  .  BA 90 28 6A 00     mov edx, <mm11.exe__dumped.dword_6A2890>
006A2752  .  E8 8D 55 D6 FF     call <mm11.exe__dumped.sub_407CE4>
006A2757  .  8B 55 F4           mov edx, dword ptr ss:[ebp - 0xC]
006A275A  .  8B 45 F8           mov eax, dword ptr ss:[ebp - 0x8]
```

<img23:X64dbg >se aprecian 3 variables importantes>

El tema de habilitar las opciones es visible/not visible, se mueven con dl,1 visible y dl,0 no visible, siendo el call de 4fa7e4 el encargado de evaluar en edx el valor si lo muestra o no.

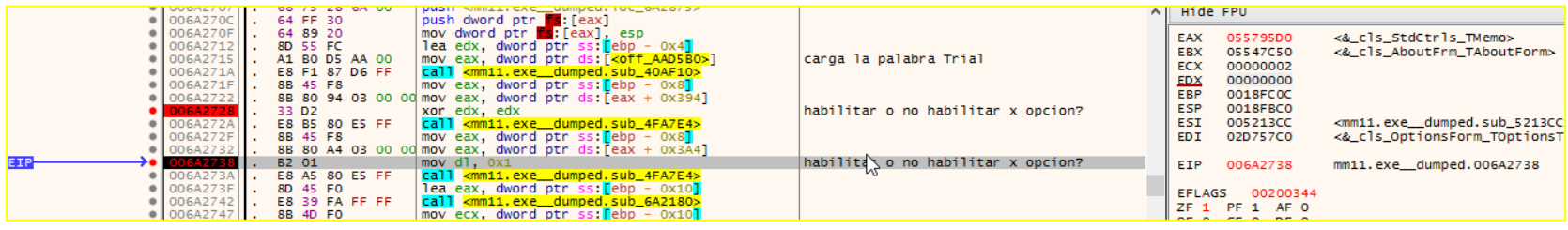
El primero hace alusion al thint panel (el que se asocia a registred),

Nota: si no tenemos un map/comentario cargado solo veremos direcciones sin descripción, para ver estos componentes con su nombre es indispensable que se usen .map desde IDA o bien IDR)



<img24:X64dbg >con mov dl,1 habilitamos la opcion de HintPanel>

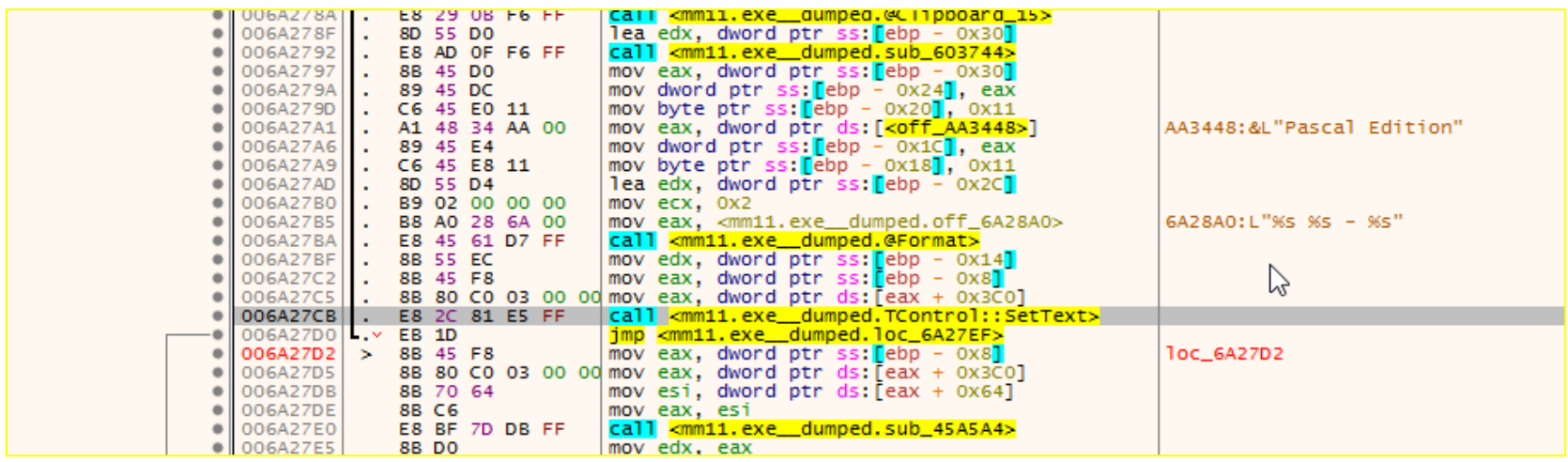
El segundo al memo (el que se asocia al trial)



<img25:X64dbg >con mov dl,0 des-habilitamos la opcion de Memodemo>

Dado que el memo (trial) es el que se necesita desactivar es mov dl,0

Notese el orden, si se carga el registred veremos registred, pero al existir un label demo que se carga encima, se verá el demo tapando el registred, por consiguiente será demo (aunque mostrara registrado a quien quiera, siempre se verá el demo encima porque se creó despues (nótese este detalle). **Una vez que ha pasado por todo concatena trial+version una vez validado la rutina como si de internet se tratara…**

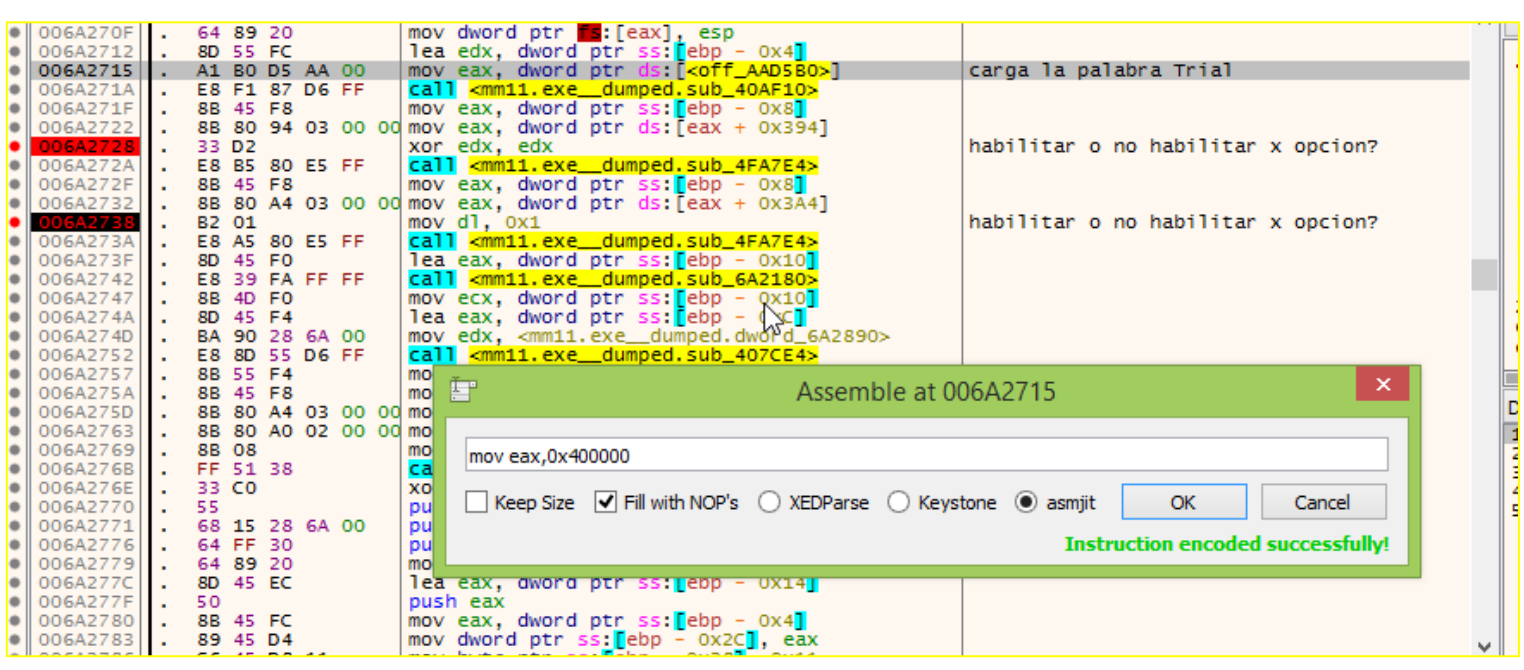


<img26:X64dbg >lugares donde se formatea trial+version+edition>

De aquí tengo 2 opciones nuevas

c) Anulando el trial String v1

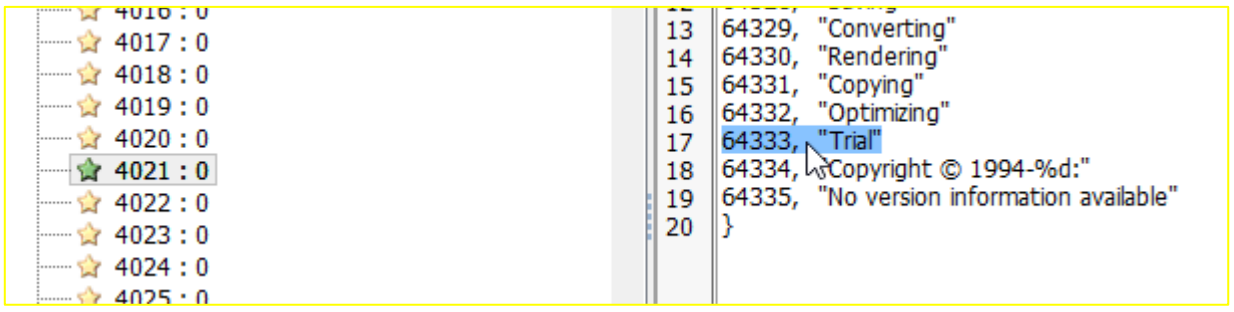
Anular la palabra trial con un arreglo de una direccion que no le de problema ejemplo 0x400000



<img27:X64dbg >opcion 1 para anular la palabra trial>

d) Anulando el trial String v2

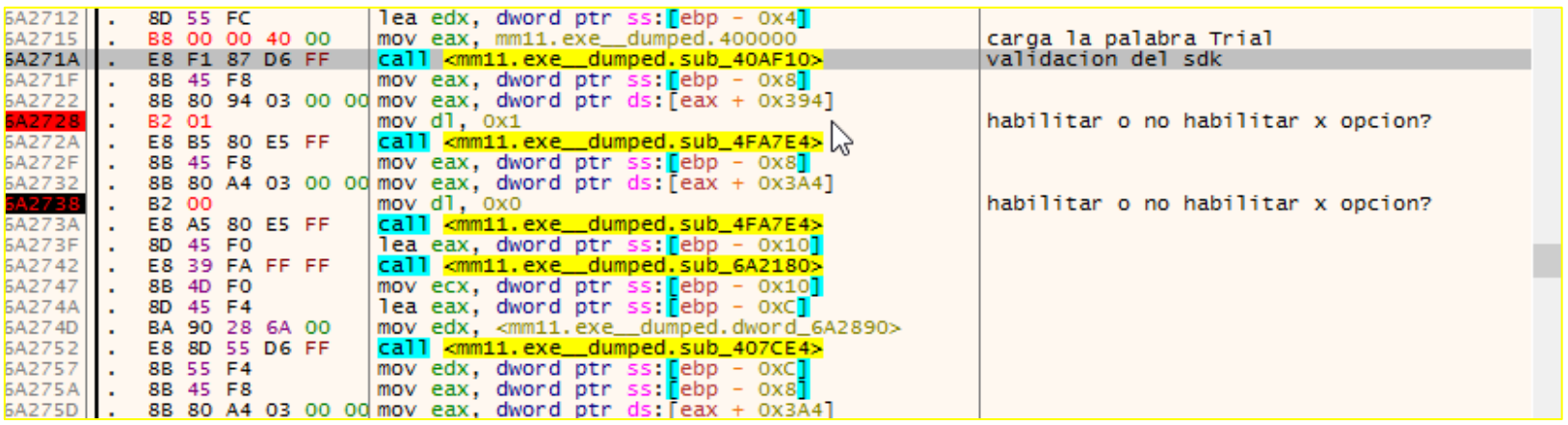
Edito en los recursos la string Trial (string en recurso 4021) : la string dice Trial, se puede cambiar al nombre del team a gusto o simplemente dejandolo en comillas (sin string xD)



<img28:Resource Hacker >opcion 2 Editar la String Trial>

e) Resumen de los Parches:

Todo lo visto se resumen en una imagen donde está casi todo hecho (ignorado el trial text en titulo, habilitado registred, desactivado trial) en el about son solo esos los cambios.



<img29:x64dbg >Resumen de los cambios hechos >

Ahora bien observo lo que tenemos:

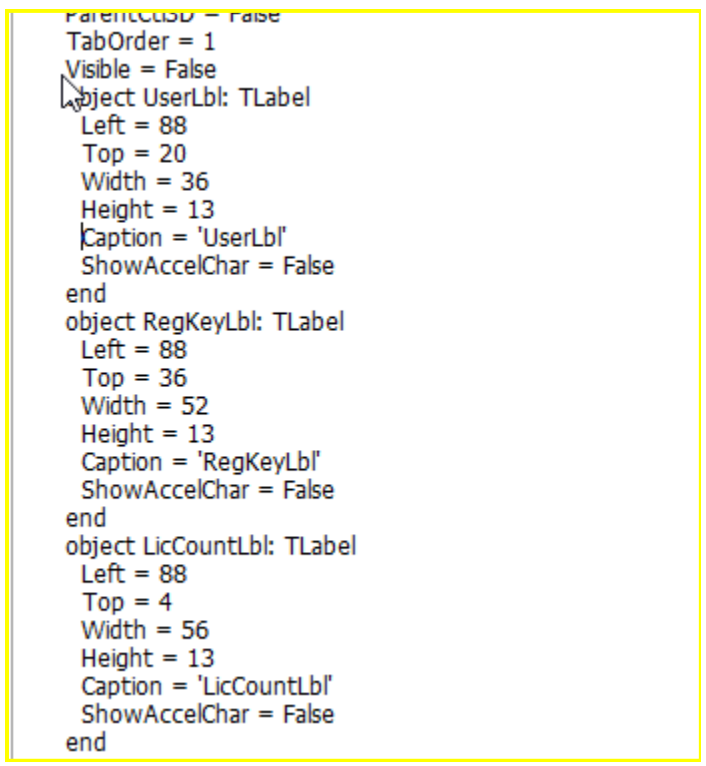
<img30:Programa >Version esteticamente registrada>

Por un About un poco más estético:

Solo nos queda Ahora es editar las strings, Para esto hare uso de Resource Hacker, a mi parecer al ser gratuito y práctico de usar es bastante usado.

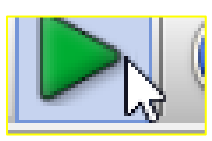
<img31:Programa >About de Resource Hacker>

Voy directamente al dialogo about form y me dedico a observar detenidamente lo que necesito modificar:



```
TabOrder = 1
Visible = False
object UserLbl: TLabel
  Left = 88
  Top = 20
  Width = 36
  Height = 13
  Caption = 'UserLbl'
  ShowAccelChar = False
end
object RegKeyLbl: TLabel
  Left = 88
  Top = 36
  Width = 52
  Height = 13
  Caption = 'RegKeyLbl'
  ShowAccelChar = False
end
object LicCountLbl: TLabel
  Left = 88
  Top = 4
  Width = 56
  Height = 13
  Caption = 'LicCountLbl'
  ShowAccelChar = False
end
```

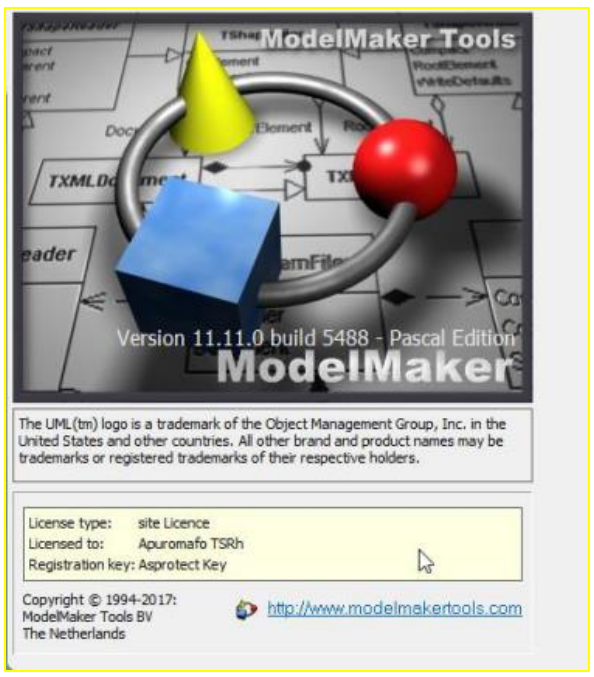
<img32:editando en Resource Hacker>



<img33:Compilar script en Resource Hacker>

Cambio Las caption UserLbl, RegKeyLbl,LcCountLbl ,Luego compilo el script y guardo el ejecutable con un nuevo nombre. Ejemplo "editado.exe"

Con el cual se veria algo así:



<img34:Programa ->Version registrada a Apuromafo TSRh>

Palabras Finales:

Tengo un programa full que dura 45 dias ,al analizar tenemos asprotect, si lo quiero dejar con packer debo parchar la funcion del messagebox pero tambien tendré que tener cuidado del crc, podria usar trial reset y usarlo cada 45 dias mas, por otro lado casi siempre un programa con asprotect tiene funciones cifradas por su licencia,posiblemente el que realmente compra puede usarlo con libertad para tenerlo completo ,pero para el que desempaca, siempre se encontrará con la misma opcion, un programa sin el protector y sin los datos de licencia , el plugin de ollydbg codedoctor recupera las zonas que estan emuladas/cifradas , y el mismo autor refiere que es un programa free y full funcional, por lo que al quitar el packer, o bypasear el tiempo, lo tenemos de forma completa (sin opciones demo) , asi que en general solo debemos preocuparnos cuando son dependientes de licencia (donde si hay codigo que está cifrado) , en lo particular con el unpacked bastaba, no era necesario hacer mas, pero de forma exploratoria hemos querido dejarlo funcional el about (como si fuera un registrado a gusto), la mención a Jhon en tutorial, es porque inicialmente depuramos en su computador, luego me ofrecí a realizar el tutorial de lo hecho,aquí queda plasmada una experiencia con un asprotect pequeño, Saludos A la Lista de Crackslatinos y a TSRh.

Dedicado a los lectores que suelen practicar y/o aprender reversing o simplemente una lectura amena, está mas que decir que si te ha gustado el software y si tienes la posibilidad de comprarlo no dejes de apoyar al soporte del programa.

Saludos Cordiales

Apuromafo TSRh