# Unpacking Vid Blaster

## Desempacando Vid Blaster

01/11/2010

Apuromafo

Introduction:

Greetings, i was to show a mini write text how was unpacked a vidblaster, maybe not are whe 100% with time, but maybe can help

Voy a mostrar un pequeño texto para desempacar vidblaster, puede ser que no sea con el 100% de tiempo, pero puede ayudar

Unpacking  VidBlaster.exe

Desempacando VidBlaster.exe

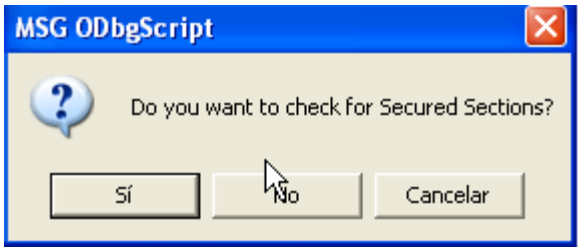
Information with arma fp 2.0 :

Informacion con armadillo find protect v2

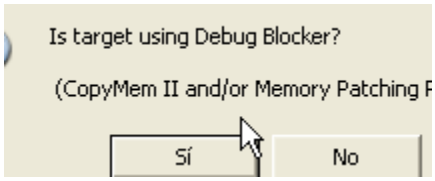
C:\archivos de programa\CombiTech\VidBlaster_tute\VidBlaster.exe
Protected Armadillo
<-Find Protect
Protection system (Professional)
<Protection Options>
Debug-Blocker
Strategic Code Splicing
Nanomites Processing
<Backup Key Options>
Fixed Backup Keys
<Compression Options>
Better/Slower Compression
<Other Options>
Allow Only One Copy
<-Find Version
!-Add new version
4BC11100=7.05Alpha6b 11-04-2010
<- Elapsed Time 00h 00m 09s 875ms ->

Is version 7, now to use the script of fungus /como es version 7, uso el script de fungus para automatizar
->version 6

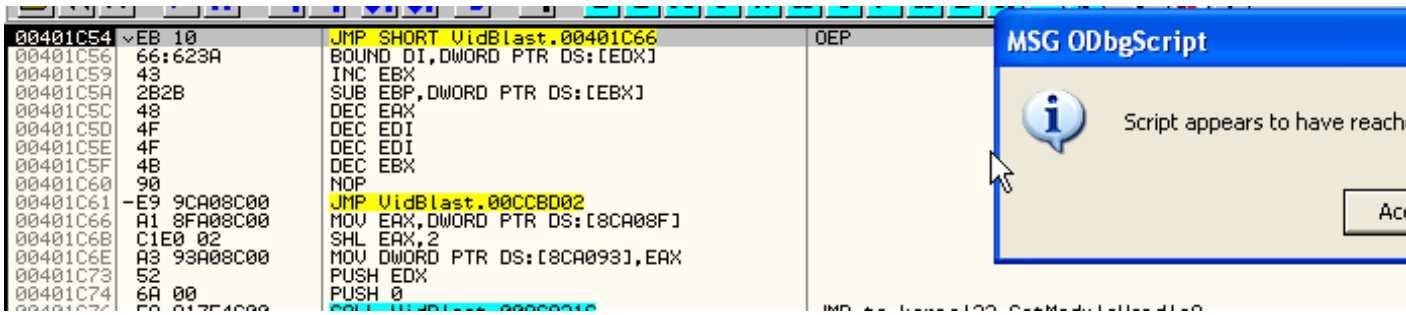

NO->(not check secured)




Yes/si (is using debug blocker)

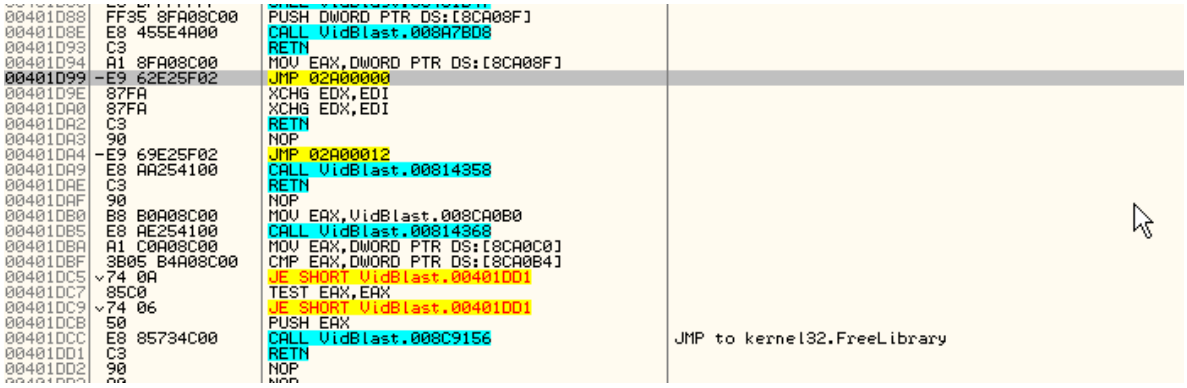



Now are in OEP/y llegamos al oep

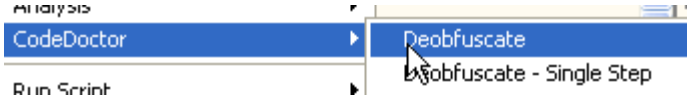


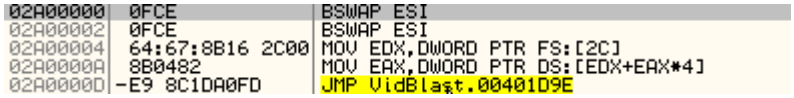
Scroll a little, yoy see the jump to other area, this are Codesplicit

Bajando un poco vemos saltos a otra area, esto es Codesplicit

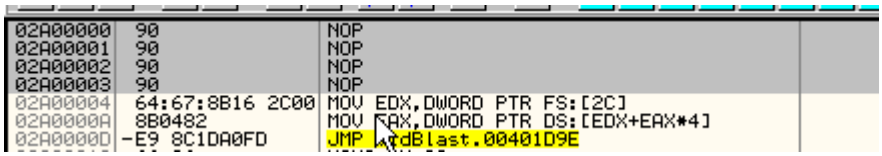



Usamos un poco Codedoctor ->Example with codedoctor

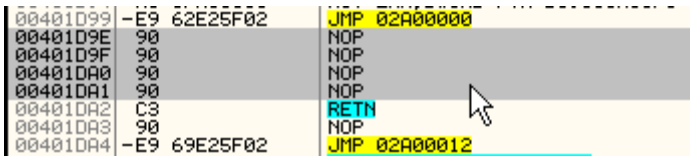


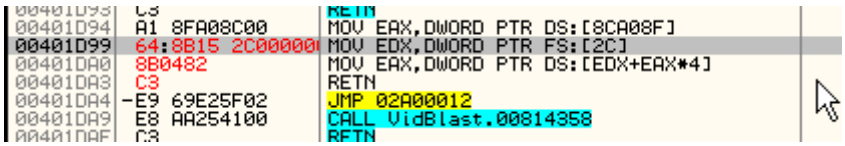

You see this/vemos esto:




And this in desofuscation/desofuscado, es como que no hace nada esas instrucciones:




And retrieve //y colocamos los valores de 2a00004 y lo coloco ahi

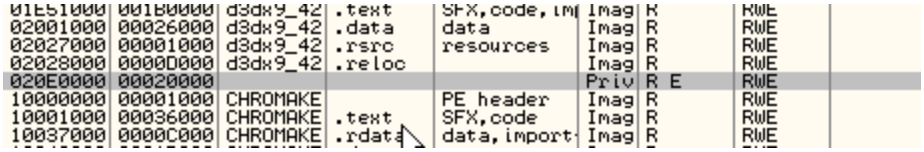


Pero veamos ahora con la misma tool en la misma seccion

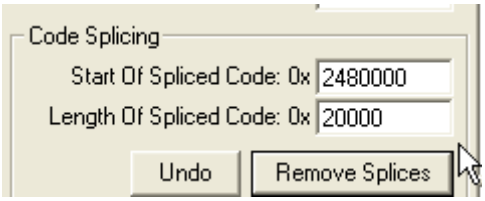
But now see with tool this same section

Now remove with tool

Verificamos la memoria. Check the memory (alt+m)

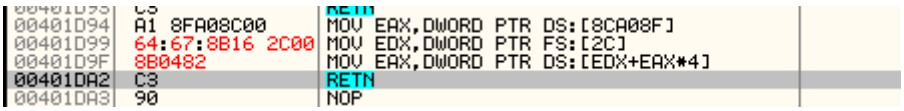



En este caso es de tamaño s 20000/size is 20000



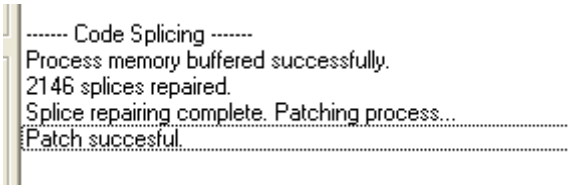

Terminado hace esto: vemos como hay 1 byte menos

Is similar but with 1 byte minus




El mensaje dice que hizo 2146 reparados //msg: 2146 splicies repaired

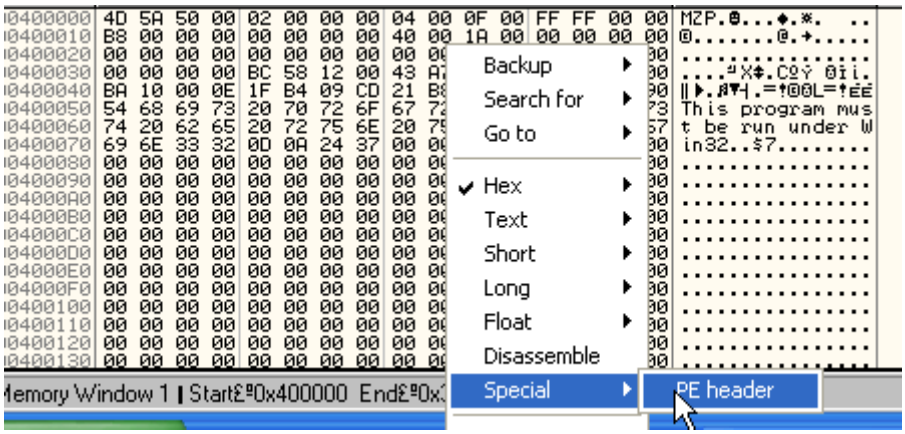
And scroll



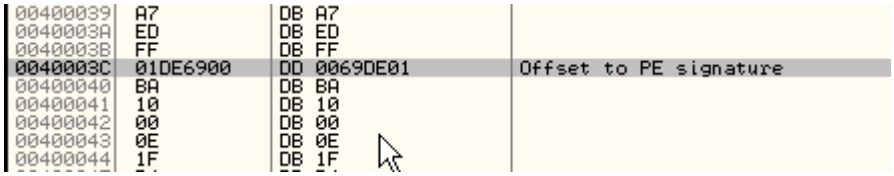
*Pe header voy a 40000 el comienzo y coloco PE HEader*

*PE header:*

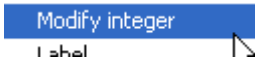

Now//ahora

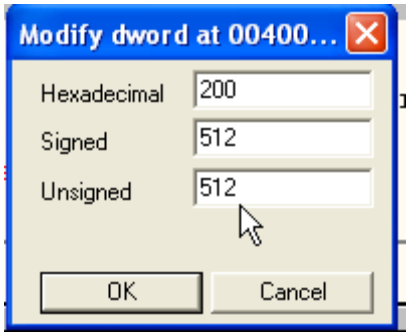



Vemos el puntero a el PE signature con un valor erroneo:



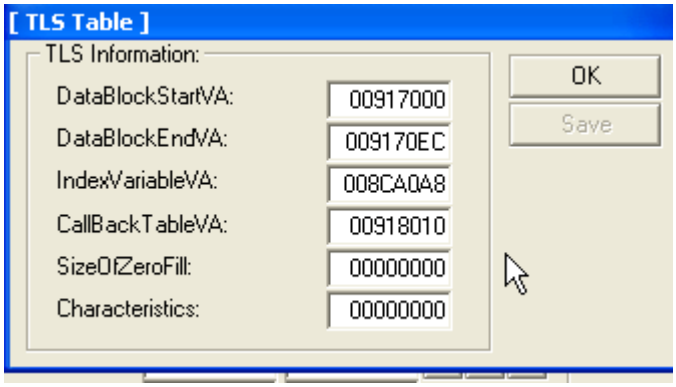

el valor que tenia esta aplicacion es 200 ., original value in armadillo withouth unpack is 200

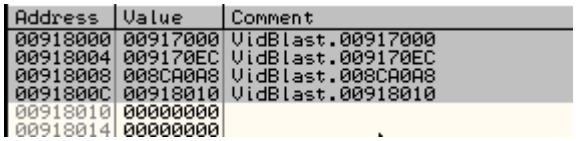


Veamos la seccion TLS

Tls table is

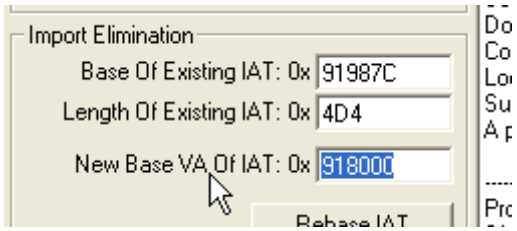


| Address | Value | Comment |
|---|---|---|
| 00918000 | 00917000 | VidBlast.00917000 |
| 00918004 | 009170EC | VidBlast.009170EC |
| 00918008 | 008CA0A8 | VidBlast.008CA0A8 |
| 0091800C | 00918010 | VidBlast.00918010 |
| 00918010 | 00000000 | |
| 00918014 | 00000000 | |

Default iat elimination point to 918000, if use that place, will lost the tls values

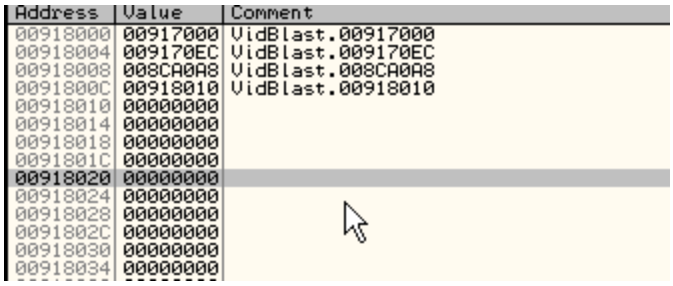
Por defecto aprovecha la seccion de 918000 , pero ahi estan los valores de TLS, asi que no debemos usar esa direccion, sino un poquito mas adelante:




Not use 91800 use from 918014 or other place if use tje 14 that pointer must be 0

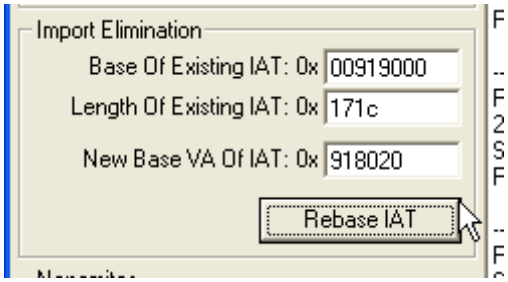
Maybe 18 or 1c better use the 0020

I will select 918020 (in import rect 518020)//selecciono el nº 918020 (en import rect 518020)



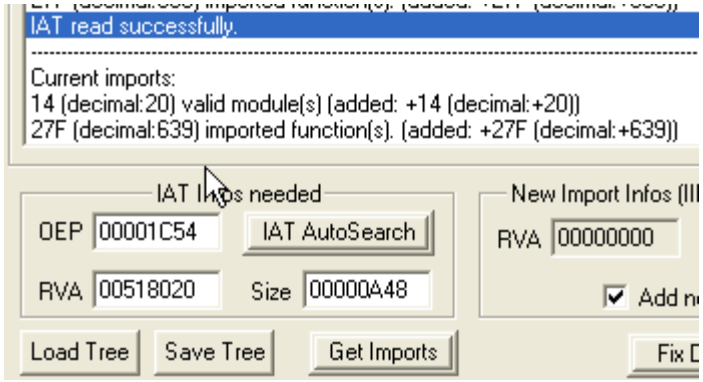
| Address | Value | Comment |
|---|---|---|
| 00918000 | 00917000 | VidBlast.00917000 |
| 00918004 | 009170EC | VidBlast.009170EC |
| 00918008 | 008CA0A8 | VidBlast.008CA0A8 |
| 0091800C | 00918010 | VidBlast.00918010 |
| 00918010 | 00000000 | |
| 00918014 | 00000000 | |
| 00918018 | 00000000 | |
| 0091801C | 00000000 | |
| 00918020 | 00000000 | |
| 00918024 | 00000000 | |
| 00918028 | 00000000 | |
| 0091802C | 00000000 | |
| 00918030 | 00000000 | |
| 00918034 | 00000000 | |

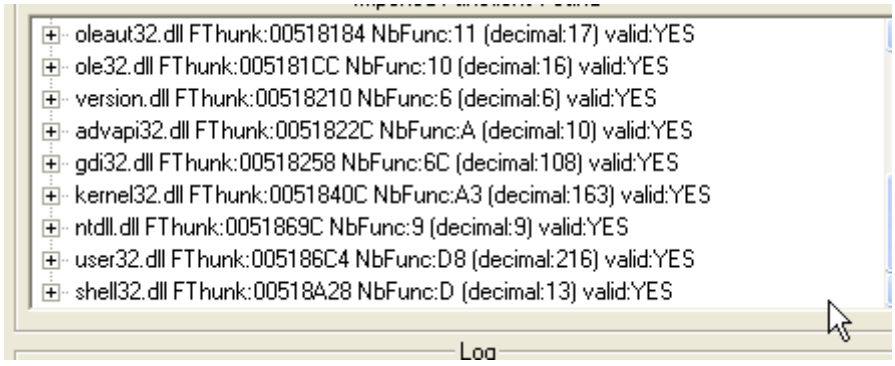
Coloco el comienzo de la seccion con la iat, y el final del ultimo valor, para que redireccione todas las apis/i point all section where are the iat:

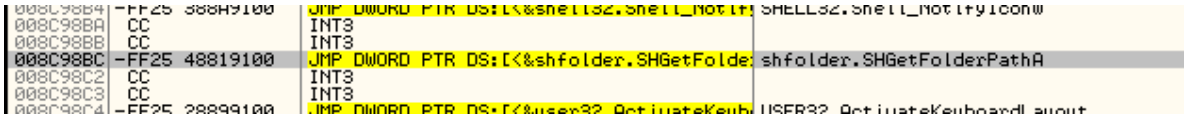



```
------- Rebasing IAT -------
Process memory buffered successfully.
642 DLL calls found total.
Analysing...
639 API functions referenced from 20 DLLs.
Redirecting DLL references:
642 calls redirected total.
Patching process...
Process succesfully patched.
```

All is fine 20 dll:



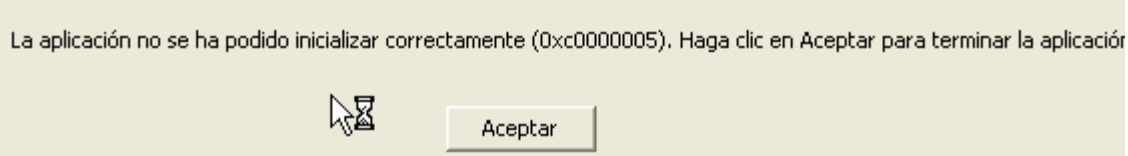



Is ok the iat , tls, peheader

//////

If you not  have good the tls if doble clik us this



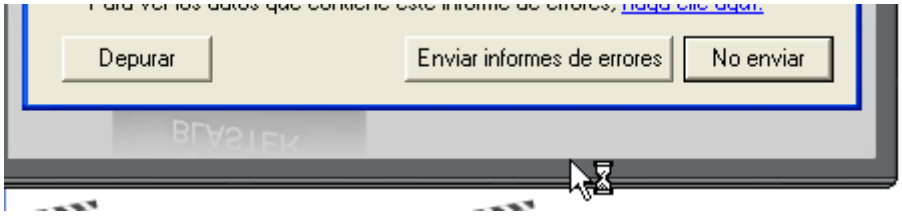

Or if not have some dll can add with lord PE with option

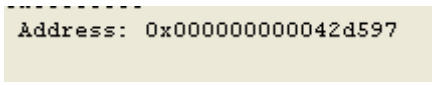
add import trunk with api (nameapi and + ) +dll(namedll.dll)

////

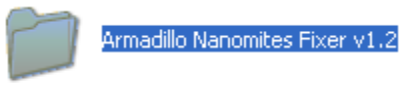
Ahora vemos y ejecuto://now runing the unpacked see this:

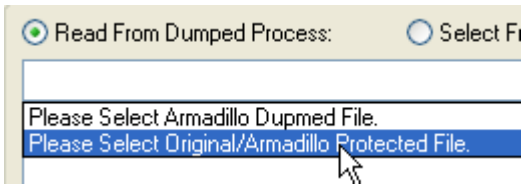
Veo un error por el nanomite: When are good see the error for nanomite

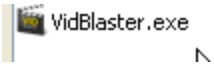


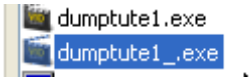
Nanomite: tool for Armadillo Version 1.2

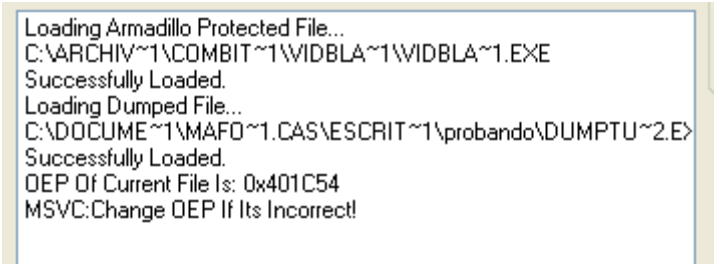


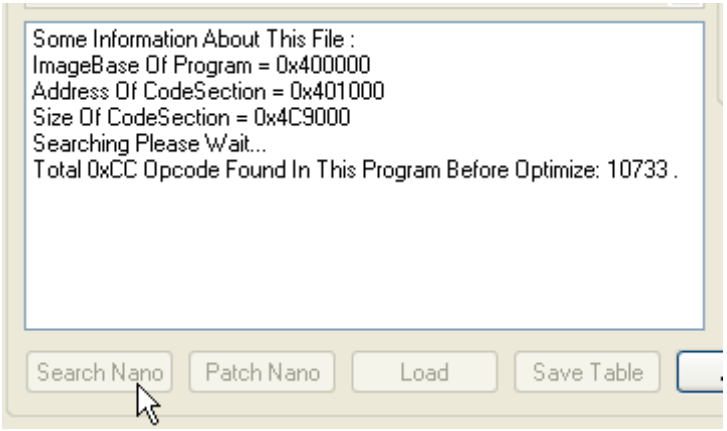

Original 


Dumped:

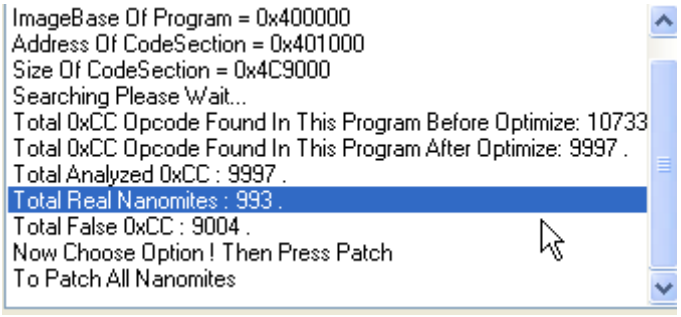


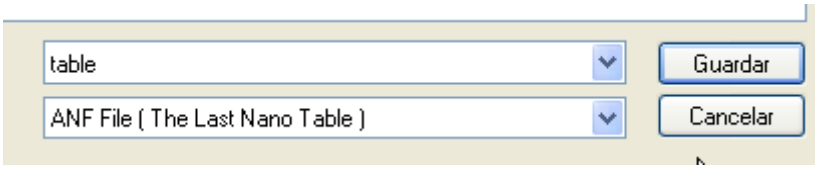

Pulse search nano

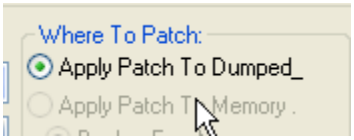


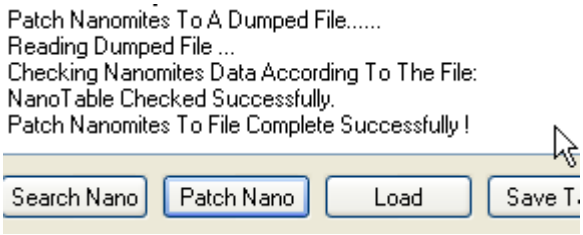

Now wait



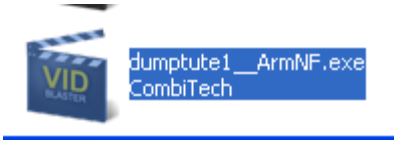

Save table (atached in old tut)



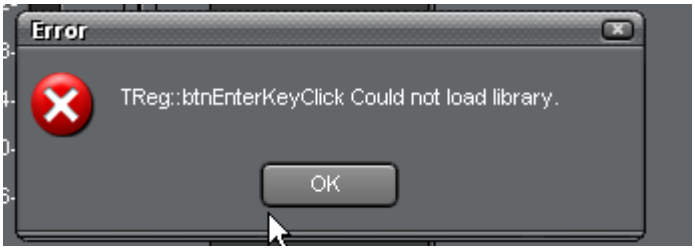




You see now




Is unpacked:

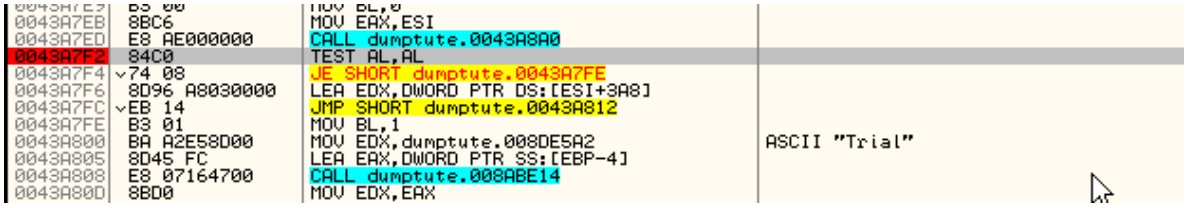

But if use option of registry:

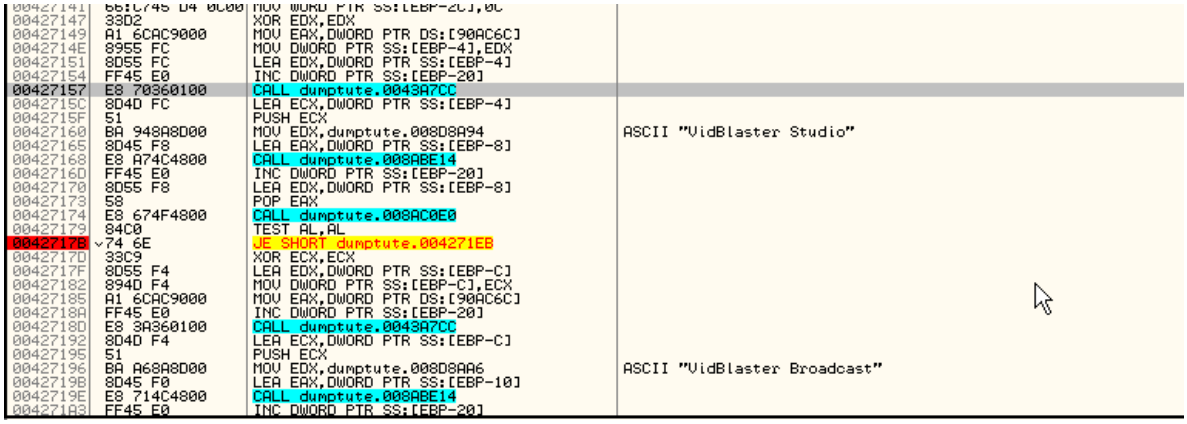


The library that search is  :Armaccess.dl

Exist some versions:

Versiones de la aplicacion:




GetEnvironmentVariableA->variables of armadillo

must use SetEnviroment for username, expired, daylefts and others..but the important is keytipe.

Its's all, unpacked armadillo 7.xx

Esta desempacado, eso es todo

Saludos Apuromafo/Greetings Apuromafo