

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

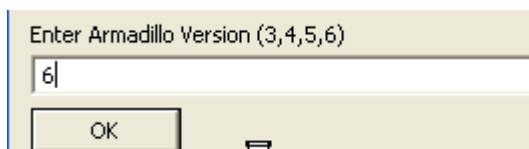
!-Add new version

4BC11100=7.05Alpha6b 11-04-2010

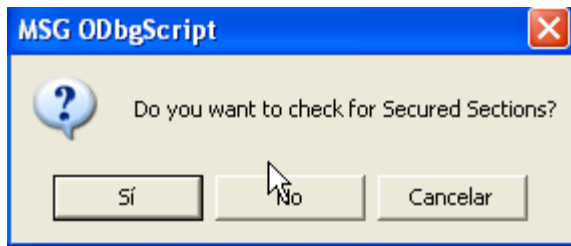
<- Elapsed Time 00h 00m 09s 875ms ->

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

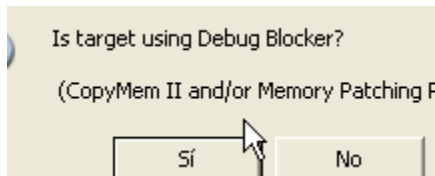
->version 6



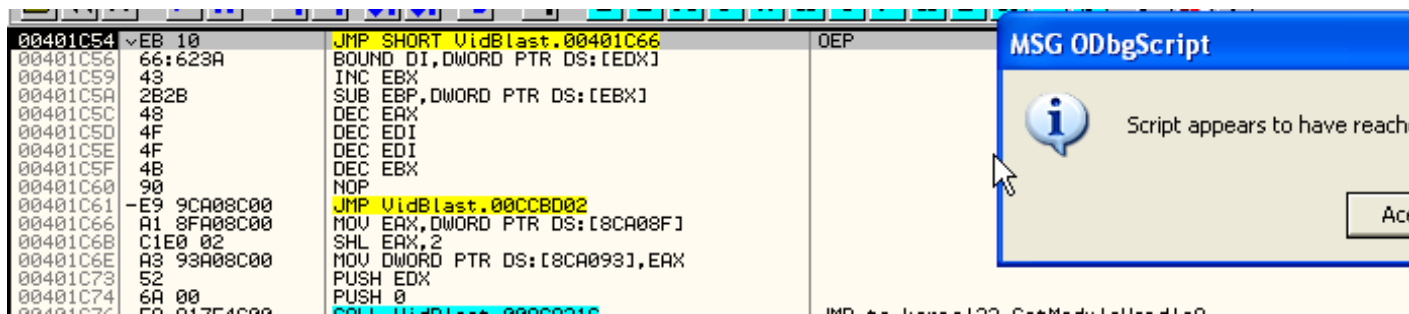
NO->(not check secured)



Yes/si (is using debug blocker)



Now are in OEP/y llegamos al oep



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

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

00401D88	FF35 8FA08C00	PUSH DWORD PTR DS:[8CA08F]
00401D8E	E9 455E4A00	CALL VidBlast.008A78D8
00401D93	C3	RETN
00401D94	A1 8FA08C00	MOV EAX,DWORD PTR DS:[8CA08F]
00401D99	E9 62E25F02	JMP 02A00000
00401D9E	87FA	XCHG EDX,EDI
00401DA0	87FA	XCHG EDX,EDI
00401DA2	C3	RETN
00401DA3	90	NOP
00401DA4	E9 69E25F02	JMP 02A00012
00401DA9	E8 A254100	CALL VidBlast.00814358
00401DAE	C3	RETN
00401DAF	90	NOP
00401DB0	B8 B0A08C00	MOV EAX,VidBlast.008CA0B0
00401DB5	E8 AE254100	CALL VidBlast.00814368
00401DBA	A1 C0A08C00	MOV EAX,DWORD PTR DS:[8CA0C0]
00401DBF	3B05 B4A08C00	CMP EAX,DWORD PTR DS:[8CA0B4]
00401DC5	74 0A	JE SHORT VidBlast.00401DD1
00401DC7	85C0	TEST EAX,EAX
00401DC9	74 06	JE SHORT VidBlast.00401DD1
00401DCB	50	PUSH EAX
00401DCC	E8 85734C00	CALL VidBlast.008C9156
00401DD1	C3	RETN
00401DD2	90	NOP

JMP to kernel32.FreeLibrary

Usamos un poco Codedoctor ->Example with codedoctor

CodeDoctor		
Deobfuscate		
Deobfuscate - Single Step		
Run Script		
02A00000	0FCE	BSWAP ESI
02A00002	0FCE	BSWAP ESI
02A00004	64:67:8B16 2C00	MOV EDX,DWORD PTR FS:[2C]
02A0000A	8B0482	MOV EAX,DWORD PTR DS:[EDX+EAX*4]
02A0000D	E9 8C1DA0FD	JMP VidBlast.00401D9E

You see this/vemos esto:

02A00000	90	NOP
02A00001	90	NOP
02A00002	90	NOP
02A00003	90	NOP
02A00004	64:67:8B16 2C00	MOV EDX,DWORD PTR FS:[2C]
02A0000A	8B0482	MOV EAX,DWORD PTR DS:[EDX+EAX*4]
02A0000D	E9 8C1DA0FD	JMP VidBlast.00401D9E

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

00401D99	E9 62E25F02	JMP 02A00000
00401D9E	90	NOP
00401D9F	90	NOP
00401DA0	90	NOP
00401DA1	90	NOP
00401DA2	C3	RETN
00401DA3	90	NOP
00401DA4	E9 69E25F02	JMP 02A00012

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

00401D93	C3	RETN
00401D94	A1 8FA08C00	MOV EAX,DWORD PTR DS:[8CA08F]
00401D99	64:8B15 2C000000	MOV EDX,DWORD PTR FS:[2C]
00401DA0	8B0482	MOV EAX,DWORD PTR DS:[EDX+EAX*4]
00401DA3	C3	RETN
00401DA4	E9 69E25F02	JMP 02A00012
00401DA9	E8 A254100	CALL VidBlast.00814358
00401DAF	C3	RETN

Pero veamos ahora con la misma tool en la misma seccion

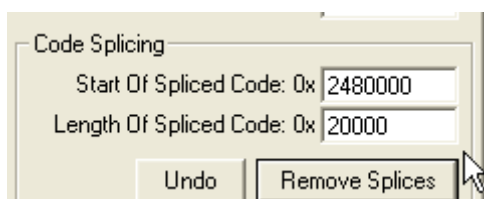
But now see with tool this same section

Now remove with tool

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

01E51000	001B0000	d3dx9_42	.text	SFX,code,lm	Imag	R	RWE	
02001000	00026000	d3dx9_42	.data	data	Imag	R	RWE	
02027000	00001000	d3dx9_42	.rsrc	resources	Imag	R	RWE	
02028000	00000000	d3dx9_42	.reloc		Imag	R	RWE	
020E0000	00020000				Priv	R E	RWE	
10000000	00001000	CHROMAKE		PE header	Imag	R	RWE	
10001000	00036000	CHROMAKE	.text	SFX,code	Imag	R	RWE	
10037000	0000C000	CHROMAKE	.rdata	data,import	Imag	R	RWE	

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

00401093	C3	RETN	
00401094	A1 8FA08C00	MOV EAX,DWORD PTR DS:[8CA08F]	
00401099	64:67:8B16 2C00	MOV EDX,DWORD PTR FS:[2C]	
0040109F	8B0482	MOV EAX,DWORD PTR DS:[EDX+EAX*4]	
00401DA2	C3	RETN	
00401DA3	90	NOP	

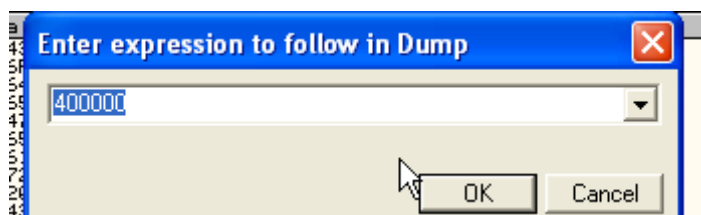
El mensaje dice que hizo 2146 reparados //msg: 2146 splices repaired

And scroll

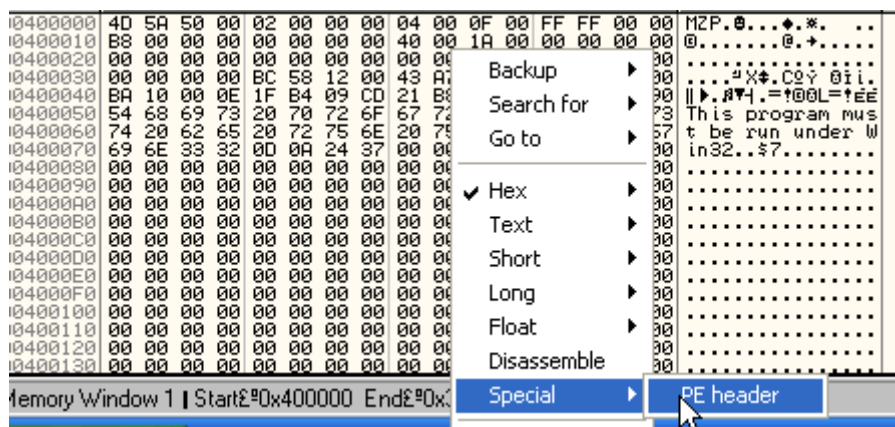
```
----- Code Splicing -----
Process memory buffered successfully.
2146 splices repaired.
Splice repairing complete. Patching process...
Patch succesful
```

Pe header voy a 40000 el comienzo y coloco PE Header

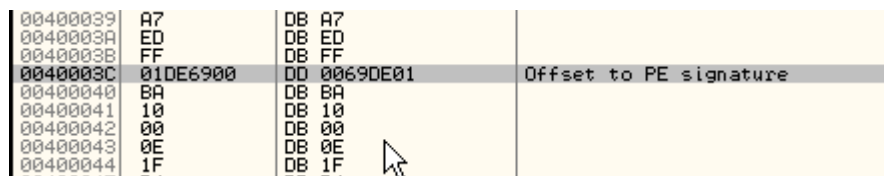
PE header:



Now//ahora

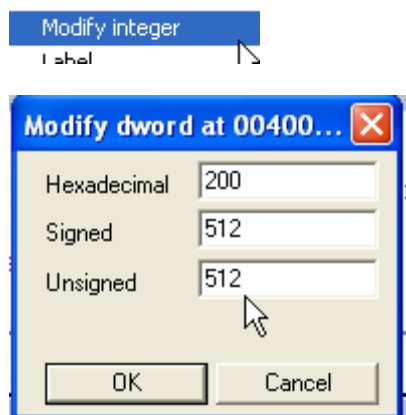


Vemos el puntero a el PE signature con un valor erroneo:



el valor que tenia esta

aplicacion es 200 ., original value in armadillo without unpack is 200



Veamos la seccion TLS

Tls table is

[TLS Table]

TLS Information:

DataBlockStartVA:	00917000
DataBlockEndVA:	009170EC
IndexVariableVA:	008CA0A8
CallBackTableVA:	00918010
SizeOfZeroFill:	00000000
Characteristics:	00000000

OK
Save

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:

Import Elimination

Base Of Existing IAT: 0x	91987C
Length Of Existing IAT: 0x	4D4
New Base VA Of IAT: 0x	918000

Rebase IAT

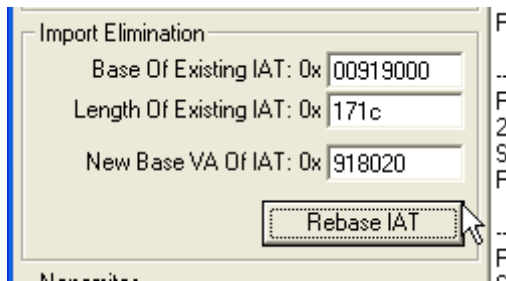
Not use 91800 use from 918014 or other place if use tje 14 that pointer must be 0

Maybe 18 or 1c better use the 0020

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

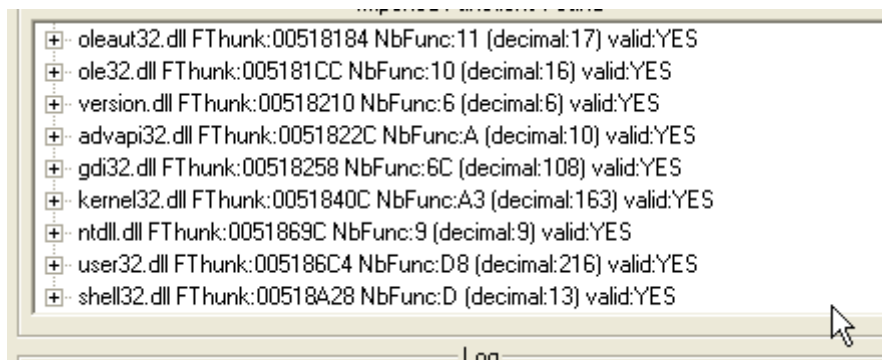
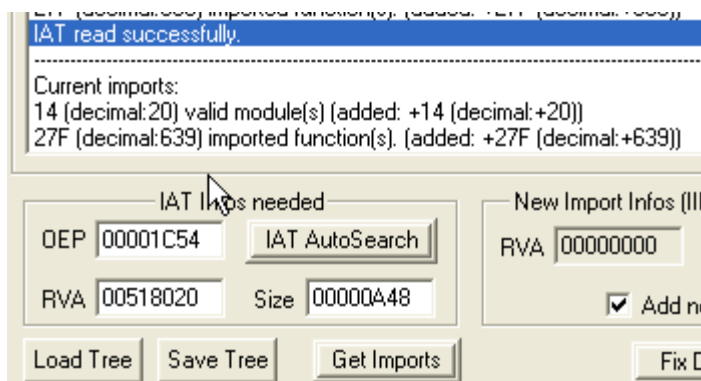
Address	Value	Comment
00918000	00917000	VidBlast.00917000
00918004	009170EC	VidBlast.009170EC
00918008	008CA0A8	VidBlast.008CA0A8
0091800C	00918010	VidBlast.00918010
00918010	00000000	
00918014	00000000	
00918018	00000000	
0091801C	00000000	
00918020	00000000	
00918024	00000000	
00918028	00000000	
0091802C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



```
----- Rebasng 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:

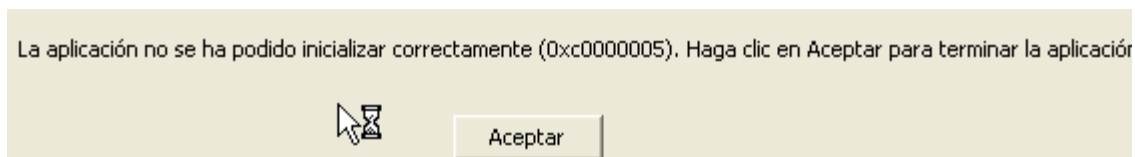


008C98B4	-FF25 38849100	JMP DWORD PTR DS:[<&shell32.Shell_NotifyIconW	shell32.Shell_NotifyIconW
008C98B8	CC	INT3	
008C98BB	CC	INT3	
008C98BC	-FF25 48819100	JMP DWORD PTR DS:[<&shfolder.SHGetFolderP	shfolder.SHGetFolderPathA
008C98C2	CC	INT3	
008C98C3	CC	INT3	
008C98C4	-EE25 28999100	JMP DWORD PTR DS:[<&user32.GetActivateKeyb	USER32.GetActivateKeyboardLayout

Is ok the iat , tls, peheader

/////

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



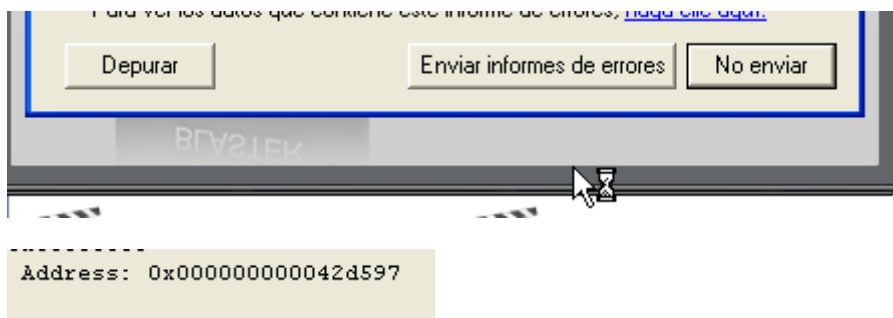
Or if not have some dll can add with lord PE with option

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

////

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

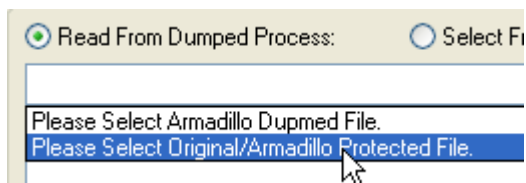
Veo un error por el nanomite: When are good see the error for nanomite



Nanomite: tool for Armadillo Version 1.2

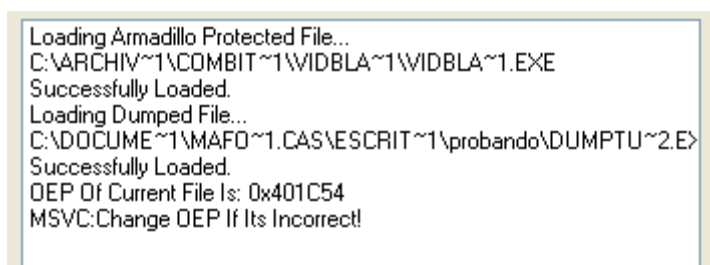
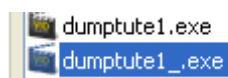


Armadillo Nanomites Fixer v1.2

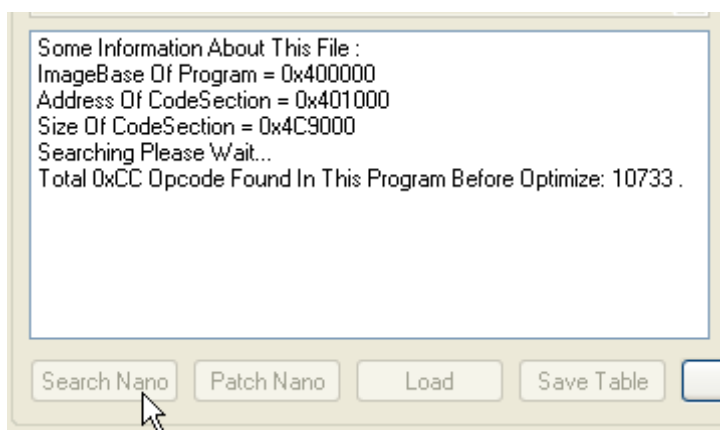


Original  VidBlaster.exe

Dumped:



Pulse search nano



Now wait

```

ImageBase Of Program = 0x400000
Address Of CodeSection = 0x401000
Size Of CodeSection = 0x4C9000
Searching Please Wait...
Total 0xCC Opcode Found In This Program Before Optimize: 10733
Total 0xCC Opcode Found In This Program After Optimize: 9997 .
Total Analyzed 0xCC : 9997 .
Total Real Nanomites : 993 .
Total False 0xCC : 9004 .
Now Choose Option ! Then Press Patch
To Patch All Nanomites

```

Save table (attached in old tut)

table

ANF File (The Last Nano Table)

Guardar

Cancelar

Where To Patch:

☒ Apply Patch To Dumped_

☐ Apply Patch To Memory .

```

Patch Nanomites To A Dumped File.....
Reading Dumped File ...
Checking Nanomites Data According To The File:
NanoTable Checked Successfully.
Patch Nanomites To File Complete Successfully !

```

Search Nano

Patch Nano

Load

Save T.

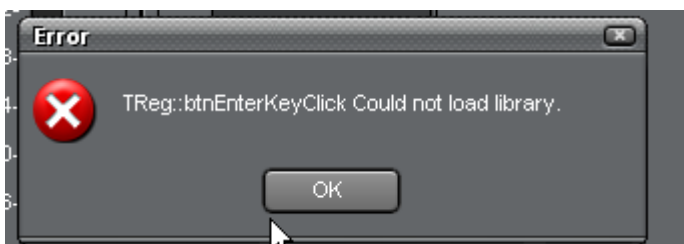
You see now



Is unpacked:



But if use option of registry:



The library that search is :Armaccess.dll

Exist some versions:

Versiones de la aplicacion:

0043A7E2	B3 00	MOV BL,0	
0043A7EB	8BC6	MOV EAX,ESI	
0043A7ED	E8 AE000000	CALL dumptute.0043A8A0	
0043A7F2	84C0	TEST AL,AL	
0043A7F4	74 08	JE SHORT dumptute.0043A7FE	
0043A7F6	8D96 A8030000	LEA EDX,DWORD PTR DS:[ESI+3A8]	
0043A7FC	EB 14	JMP SHORT dumptute.0043A812	
0043A7FE	B3 01	MOV BL,1	
0043A800	BA A2E58D00	MOV EDX,dumptute.008DE5A2	ASCII "Trial"
0043A805	8D45 FC	LEA EAX,DWORD PTR SS:[EBP-4]	
0043A808	E8 07164700	CALL dumptute.008ABE14	
0043A80D	8BD0	MOV EDX,EAX	

00427141	BB0745 04 0000	MOV WORD PTR SS:[EBP-2C],00	
00427147	33D2	XOR EDX,EDX	
00427149	A1 6CAC9000	MOV EAX,DWORD PTR DS:[90AC6C]	
0042714E	8955 FC	MOV DWORD PTR SS:[EBP-4],EDX	
00427151	8D55 FC	LEA EDX,DWORD PTR SS:[EBP-4]	
00427154	FF45 E0	INC DWORD PTR SS:[EBP-20]	
00427157	E8 70360100	CALL dumptute.0043A7C0	
0042715C	8D4D FC	LEA ECX,DWORD PTR SS:[EBP-4]	
0042715F	51	PUSH ECX	
00427160	BA 948A8D00	MOV EDX,dumptute.008D8A94	ASCII "VidBlaster Studio"
00427165	8D45 F8	LEA EAX,DWORD PTR SS:[EBP-8]	
00427168	E8 A74C4800	CALL dumptute.008ABE14	
0042716D	FF45 E0	INC DWORD PTR SS:[EBP-20]	
00427170	8D55 F8	LEA EDX,DWORD PTR SS:[EBP-8]	
00427173	58	POP EAX	
00427174	E8 674F4800	CALL dumptute.008AC0E0	
00427179	84C0	TEST AL,AL	
0042717B	74 6E	JE SHORT dumptute.004271EB	
0042717D	33C9	XOR ECX,ECX	
0042717F	8D55 F4	LEA EDX,DWORD PTR SS:[EBP-C]	
00427182	894D F4	MOV DWORD PTR SS:[EBP-C],ECX	
00427185	A1 6CAC9000	MOV EAX,DWORD PTR DS:[90AC6C]	
0042718A	FF45 E0	INC DWORD PTR SS:[EBP-20]	
0042718D	E8 3A360100	CALL dumptute.0043A7C0	
00427192	8D4D F4	LEA ECX,DWORD PTR SS:[EBP-C]	
00427195	51	PUSH ECX	
00427196	BA A68A8D00	MOV EDX,dumptute.008D8AA6	ASCII "VidBlaster Broadcast"
0042719B	8D45 F0	LEA EAX,DWORD PTR SS:[EBP-10]	
0042719E	E8 714C4800	CALL dumptute.008ABE14	
004271A3	FF45 E0	INC DWORD PTR SS:[EBP-20]	

GetEnvironmentVariableA->[variables of armadillo](#)

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

Its's all, unpacked armadillo 7.xx

Esta desempacado, eso es todo

Saludos Apuromafo/Greetings Apuromafo