

Bracket Trader Software ,armadillo 3.x

CRACKSLATINOS.

28/10/2010

Apuromafo

ESTE ES UN DOCUMENTO DE ACCESO PUBLICO.
PROHIBIDA SU VENTA O REPRODUCCION CON FINES DE LUCRO.

Programa :© 2010 Bracket Trader Software

Proteccion:Arnadillo 3.x

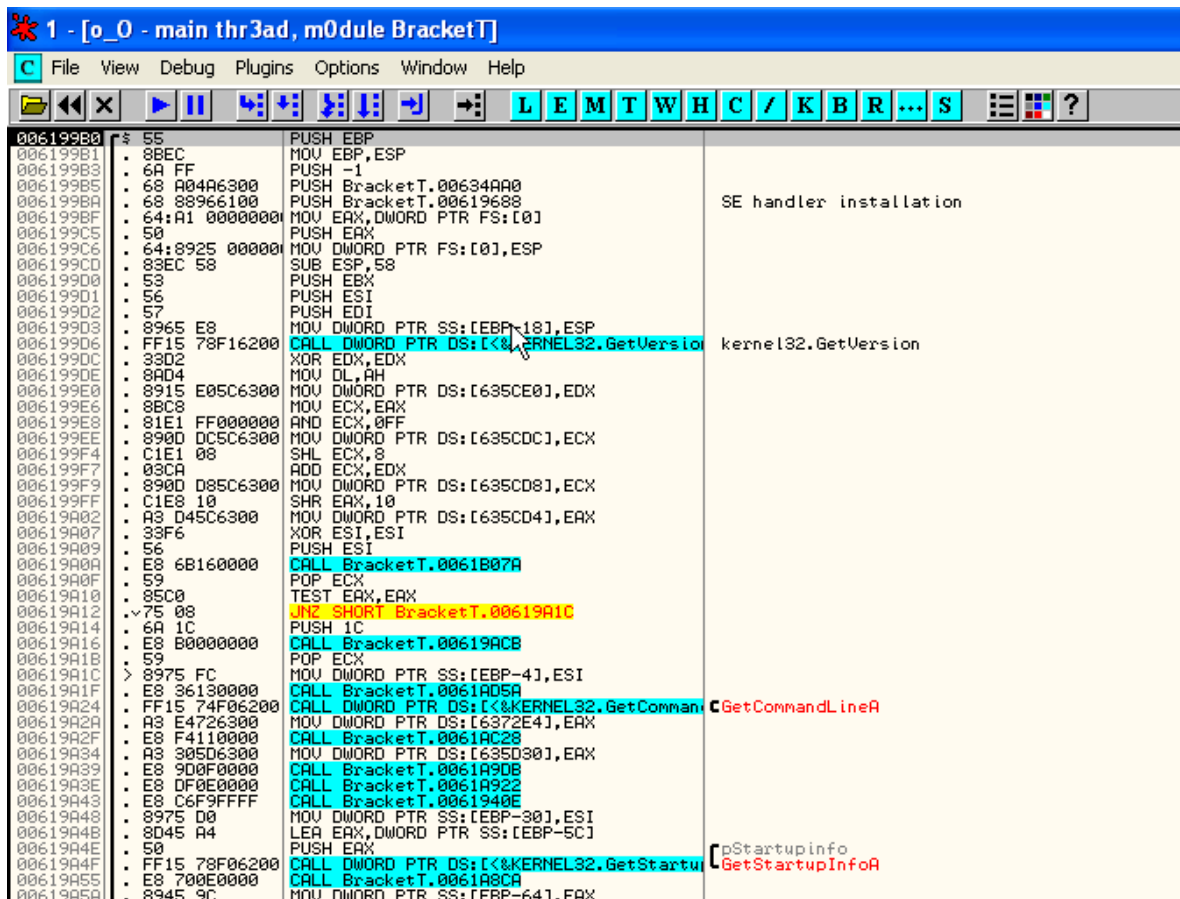
Herramientas:

Armageddon,Armaridder, IDA, Ollydbg, API HELP (Armadillo v8 public version),VB decompiler
SnD 7.6

Objetivo Reconocer el Packer, y si es posible, registrarnos y verlo funcional

Hace poco terminamos con el 8, como no vamos a poder con otro mas.

Comenzamos En el Entrypoint de esta aplicacion



```
006199B0 55          PUSH EBP
006199B1 8BEC        MOV EBP,ESP
006199B3 6AFF        PUSH -1
006199B5 68 A04A6300 PUSH BracketT.00634AA0
006199BA 68 88966100 PUSH BracketT.00619688
006199BF 64:A1 00000000 MOV EAX,DWORD PTR FS:[0]
006199C5 50          PUSH EAX
006199C6 64:8925 00000000 MOV DWORD PTR FS:[0],ESP
006199CD 83EC 58     SUB ESP,58
006199D0 53          PUSH EBX
006199D1 56          PUSH ESI
006199D2 57          PUSH EDI
006199D3 8965 E8     MOV DWORD PTR SS:[EBP-18],ESP
006199D6 FF15 78F16200 CALL DWORD PTR DS:[<<kernel32.GetVersion
006199DC 33D2        XOR EDX,EDX
006199DE 8AD4        MOV DL,AH
006199E0 8915 E05C6300 MOV DWORD PTR DS:[635CE0],EDX
006199E6 8BC8        MOV ECX,EAX
006199E8 81E1 FF000000 AND ECX,0FF
006199EE 8900 DC5C6300 MOV DWORD PTR DS:[635CDC],ECX
006199F4 C1E1 08     SHL ECX,8
006199F7 03CA        ADD ECX,EDX
006199F9 8900 D85C6300 MOV DWORD PTR DS:[635CD8],ECX
006199FF C1E8 10     SHR EAX,10
00619A02 8B D45C6300 MOV DWORD PTR DS:[635CD4],EAX
00619A07 33F6        XOR ESI,ESI
00619A09 56          PUSH ESI
00619A0A E8 6B160000 CALL BracketT.0061B07A
00619A0F 59          POP ECX
00619A10 85C0        TEST EAX,EAX
00619A12 75 08       JNZ SHORT BracketT.00619A1C
00619A14 6A 1C       PUSH 1C
00619A16 E8 B0000000 CALL BracketT.00619ACB
00619A18 59          POP ECX
00619A1C 8975 FC     MOV DWORD PTR SS:[EBP-4],ESI
00619A1F E8 36130000 CALL BracketT.0061A05A
00619A24 FF15 74F06200 CALL DWORD PTR DS:[<<kernel32.GetComm
00619A2A 8B E4726300 MOV DWORD PTR DS:[6372E4],EAX
00619A2F E8 F4110000 CALL BracketT.0061AC28
00619A34 8B 305D6300 MOV DWORD PTR DS:[635D30],EAX
00619A39 E8 3D0F0000 CALL BracketT.0061A90B
00619A3E E8 DF0E0000 CALL BracketT.0061A922
00619A43 E8 C6F9FFFF CALL BracketT.0061940E
00619A48 8975 D0     MOV DWORD PTR SS:[EBP-30],ESI
00619A4B 8D45 A4     LEA EAX,DWORD PTR SS:[EBP-5C]
00619A4E 50          PUSH EAX
00619A4F FF15 78F06200 CALL DWORD PTR DS:[<<kernel32.GetStartu
00619A55 E8 700E0000 CALL BracketT.0061A8CA
00619A5A 8945 9C     MOV DWORD PTR SS:[FBP-64],EAX
```

Search all string

Address	Disassembly	Text string
00604280	PUSH BracketT.0062F2EC	ASCII "System"
006044E3	PUSH BracketT.0062F4E8	ASCII "Insufficient memory!"
0060460A	PUSH BracketT.0062F500	ASCII "SetFunctionAddresses"
00604836	PUSH BracketT.0062F51C	ASCII "PDATA000"
006048ED	ADD ECX,10000	UNICODE "=::::\\"
00604926	ADD EDX,10000	UNICODE "=::::\\"
00604992	PUSH BracketT.0062F528	ASCII "ARMSPLASHOFF"
00605375	PUSH BracketT.0062F56C	ASCII "File \"%s\", error %d"
006053F2	PUSH BracketT.0062F554	ASCII "File \"%s\", ordinal %d"
00605442	PUSH BracketT.0062F538	ASCII "File \"%s\", function \"%s\""
006055C8	PUSH BracketT.0062F604	ASCII "%X:DA%08X"
00605638	PUSH BracketT.0062F5FC	ASCII "RN%08X"
006056C4	PUSH BracketT.0062F5F4	ASCII "%08X"
00605706	PUSH BracketT.0062F5E8	ASCII "MainClass"
006057E3	PUSH BracketT.0062F5E0	ASCII "-PAD64"
0060583E	PUSH BracketT.0062F5D8	ASCII "-PAD%d"
00605965	PUSH BracketT.0062F5B8	ASCII "(Location XEB, error code %d)"
006059CA	PUSH BracketT.0062F604	ASCII "%X:DA%08X"
00605A10	PUSH BracketT.0062F5AC	ASCII "Kernel32"
00605A2A	PUSH BracketT.0062F598	ASCII "IsDebuggerPresent"
00605BF1	PUSH BracketT.0062F590	ASCII "%X:DAF"
00605C65	PUSH BracketT.0062F580	ASCII "(Error code %d)"
00605D3A	PUSH BracketT.0062F628	ASCII "KERNEL32.DLL"
00605D4A	PUSH BracketT.0062F610	ASCII "RegisterServiceProcess"
00605DD3	PUSH BracketT.0062F5AC	ASCII "Kernel32"
00605DE7	PUSH BracketT.0062F598	ASCII "IsDebuggerPresent"
00605E00	PUSH BracketT.0062F590	ASCII "%X:DAF"
00605E9F	PUSH BracketT.0062F63C	ASCII "INITIALIZEDLLADDR"
00606028	MOV DWORD PTR SS:[EBP-4],BracketT.0062F604	ASCII "Loading..."
00606336	PUSH BracketT.0062F700	ASCII "SERVER"
006063A2	PUSH BracketT.0062F6F4	ASCII "DOWN"
00606448	PUSH BracketT.0062F6E8	ASCII "REGISTER"
00606480	PUSH BracketT.0062F6D8	ASCII "QUIETREGISTER"
006064B8	PUSH BracketT.0062F6CC	ASCII "TRANSFER"
006064DF	PUSH BracketT.0062F6C0	ASCII "FIXCLOCK"
00606506	PUSH BracketT.0062F6B8	ASCII "INFO"
0060652D	PUSH BracketT.0062F6AC	ASCII "UNREGISTER"
00606551	PUSH BracketT.0062F69C	ASCII "SHOWNETUSERS"
00606575	PUSH BracketT.0062F690	ASCII "HWCHANGELOG"
0060659B	PUSH BracketT.0062F684	ASCII "ARMDEBUG="
00606A18	PUSH BracketT.0062F708	ASCII "DISPLAY"
00606B21	MOV DWORD PTR SS:[EBP-108],BracketT.0062F604	ASCII "ArBase Bitmap Window"
00606B2B	MOV DWORD PTR SS:[EBP-4],BracketT.0062F604	ASCII "ArBase Test Bitmap Window"
00606DE7	PUSH BracketT.0062F5F4	ASCII "%08X"
00606E02	PUSH BracketT.0062F710	ASCII "LOADINGWINDOW"

Esto es un armadillo vease Armdebug y PDATA000,son tipicos en estas cosas

, ejecuto Armadillo Find Protect 2.0 by Vel

<- 19-10-2010 22:34:03 - [2.0] ->

C:\BracketTrader\BracketTrader.exe

Protected Armadillo

<-Find Protect

Protection system (Basic)

<Protection Options>

Standard protection or Minimum protection

<Backup Key Options>

Fixed Backup Keys

<Compression Options>

Better/Slower Compression

<Other Options>

Disable Monitoring Thread

<-Find Version

Version 3.78 22Sep2004

<- Elapsed Time 00h 00m 03s 828ms ->

Como es version 3, intento si resultan mis script:

Ejecuto un script y selecciono version 3

6199B0	IsDebuggerPresent patched		
6199B0	OutputDebugString patched		
D15C6E	Import Redirection patched		
D17378	No Secured Sections Detected.		
418910	OA of OEP = 00418910		
418910	RVA of OEP = 00018910		

0041890E	-FF25 54114000	JMP DWORD PTR DS:[401134]	MSVBUM60.EVENT_SINK_Release
0041890F	-FF25 88114000	JMP DWORD PTR DS:[401188]	MSVBUM60.ThunRTMain
0041890A	-FF25 58124000	JMP DWORD PTR DS:[401258]	
00418910	68 508F4100	PUSH BracketT.00418F50	OEP
00418915	E8 F0FFFFFF	CALL BracketT.0041890A	JMP to MSVBUM60.ThunRTMain
0041891A	0000	ADD BYTE PTR DS:[EAX],AL	
0041891C	0000	ADD BYTE PTR DS:[EAX],AL	
0041891E	0000	ADD BYTE PTR DS:[EAX],AL	

Esto es el visualbasic version 6

O bien usar armaggedon para desempacar, y unpacked.tambien funciona,

Si vamos por la dll interna:

```
Starting the Extraction Procedure!
-> Real PDATA Size: 000A9A7A
-> Appears to be 0x0059 DWORDS
Processing File For DWORDS: C:\BracketTrader\Copia de
BracketTrader.exe*
-> Offset Calculator Initialized
-> DWORD Replacement is NOT used
-> ZLIB DLL Found!
-> Compressed Size: 00023284
-> Decompressed Size: 0003F000
-> Decompressing...
Decompressed! Saving File...
-> Saved!
Getting correct CRC Info...
```

Tambien la tenemos. Podemos parchar y hacer como se pueda porque podemos tener el unpacked y parchar inclusive la dll interna, pero muestra que necesita algo:

http://www.interactivebrokers.com/download/InstallAX_964.exe

busco la referencia, pues no me parece bajar por bajar cosas

0052AE59	6A 01	PUSH 1	
0052AE5B	8B4D D4	MOV ECX, DWORD PTR SS:[EBP-2C]	
0052AE5E	51	PUSH ECX	
0052AE5F	68 4C944400	PUSH BracketT.0044944C	UNICODE "Tws.ocx"
0052AE64	6A 01	PUSH 1	
0052AE66	FF15 1C124000	CALL DWORD PTR DS:[401210]	MSUBUM160.__vbaInStr
0052AE6C	66:8945 D8	MOV WORD PTR SS:[EBP-28], AX	
0052AE6D	8D4D D4	LEA ECX, DWORD PTR SS:[EBP-2C]	
0052AE6E	FF15 F8124000	CALL DWORD PTR DS:[4012F8]	MSUBUM160.__vbaFreeStr
0052AE6F	8D4D B0	LEA ECX, DWORD PTR SS:[EBP-50]	
0052AE70	FF15 FC124000	CALL DWORD PTR DS:[4012F0]	MSUBUM160.__vbaFreeObj
0052AE72	C745 FC 5E000000	MOV DWORD PTR SS:[EBP-4], 5E	
0052AE73	66:8B55 D8	MOV DX, WORD PTR SS:[EBP-28]	
0052AE74	66:8995 FCFFFFFF	MOV WORD PTR SS:[EBP-104], DX	
0052AE75	C745 FC 5F000000	MOV DWORD PTR SS:[EBP-4], 5F	
0052AE76	66:83BD FCFFFFFF	CMP WORD PTR SS:[EBP-104], 0	
0052AE77	0F8E 33010000	JLE BracketT.0052B06C	
0052AE78	C745 FC 61000000	MOV DWORD PTR SS:[EBP-4], 61	
0052AE79	C785 6CFFFFFF 0	MOV DWORD PTR SS:[EBP-34], 80020004	
0052AE7A	C785 64FFFFFF 0	MOV DWORD PTR SS:[EBP-9C], 0A	
0052AE7B	C785 7CFFFFFF 0	MOV DWORD PTR SS:[EBP-84], 80020004	
0052AE7C	C785 74FFFFFF 0	MOV DWORD PTR SS:[EBP-8C], 0A	
0052AE7D	C785 5CFFFFFF B	MOV DWORD PTR SS:[EBP-A4], BracketT.0044	UNICODE "Missing Component"
0052AE7E	C785 54FFFFFF 0	MOV DWORD PTR SS:[EBP-AC], 0	
0052AE7F	8D95 54FFFFFF	LEA EDI, DWORD PTR SS:[EBP-8C]	
0052AE80	8D4D 84	LEA ECX, DWORD PTR SS:[EBP-7C]	
0052AE81	FF15 84124000	CALL DWORD PTR DS:[401284]	MSUBUM160.__vbaVarDup
0052AE82	68 60944400	PUSH BracketT.00449460	UNICODE "The required component 'Tws.ocx' is missing from your system."
0052AE83	68 00AC4300	PUSH BracketT.0043AC00	UNICODE "j"
0052AE84	FF15 84104000	CALL DWORD PTR DS:[401084]	MSUBUM160.__vbaStrCat
0052AE85	8B00	MOV EDI, EAX	
0052AE86	8D4D D4	LEA ECX, DWORD PTR SS:[EBP-2C]	
0052AE87	FF15 B4124000	CALL DWORD PTR DS:[4012B4]	MSUBUM160.__vbaStrMove
0052AE88	50	PUSH EAX	
0052AE89	68 B88C4300	PUSH BracketT.00438CB8	
0052AE8A	FF15 84104000	CALL DWORD PTR DS:[401084]	MSUBUM160.__vbaStrCat
0052AE8B	8B00	MOV EDI, EAX	
0052AE8C	8D4D D0	LEA ECX, DWORD PTR SS:[EBP-30]	
0052AE8D	FF15 B4124000	CALL DWORD PTR DS:[4012B4]	MSUBUM160.__vbaStrMove
0052AE8E	50	PUSH EAX	
0052AE8F	68 00AC4300	PUSH BracketT.0043AC00	UNICODE "j"
0052AE90	FF15 84104000	CALL DWORD PTR DS:[401084]	MSUBUM160.__vbaStrCat
0052AE91	8B00	MOV EDI, EAX	
0052AE92	8D4D CC	LEA ECX, DWORD PTR SS:[EBP-34]	
0052AE93	FF15 B4124000	CALL DWORD PTR DS:[4012B4]	MSUBUM160.__vbaStrMove
0052AE94	50	PUSH EAX	
0052AE95	68 E0944400	PUSH BracketT.004494E0	UNICODE "The file will be downloaded after you click OK. Save and run the file first"
00449460=BracketT.00449460	INITIATE		"The required component 'Tws.ocx' is missing from your system."

Me indica que me falta un componente tws.ocx

O mas abajo el enlace que me indica, y mas abajo otro enlace,

http://individuals.interactivebrokers.com/en/p.php?f=programInterface&ib_entity=llc

Debo usar ademas internet explorer 6

```

jH EDX
UNICODE "You need to install Internet Explorer 6.")

```

Y si no lo tengo debo ir a :

00448464=BracketT.00448464 (UNICODE

"<http://www.microsoft.com/downloads/details.aspx?FamilyID=1e1550cb-5e5d-48f5-b02b-20b602228de6&Displa>")

Buscando Los Export de Armadillo:

Luego busco un poco si hay alguna importacion con Dll Function call , pues hay una documentacion importante en cada api, y en esta aplicacion encuentro 3

0043B721	00	DB 00	
0043B722	00	DB 00	
0043B723	00	DB 00	
0043B724	. 49 6E 73 74 6	ASCII "InstallKey",0	
0043B72F	00	DB 00	
0043B730	. 63 6D 64 42 4	ASCII "cmdBE",0	
0043B736	00	DB 00	
0043B737	00	DB 00	
0043B738	44B64300	DD unpacked.0043B644	ASCII "ArmAccess.DLL"
0043B73C	24B74300	DD unpacked.0043B724	ASCII "InstallKey"
0043B740	00	DB 00	
0043B741	00	DB 00	
0043B742	04	DB 04	
0043B743	00	DB 00	
0043B744	24735D00	DD unpacked.005D7324	
0043B748	00	DB 00	
0043B749	00	DB 00	
0043B74A	00	DB 00	
0043B74B	00	DB 00	
0043B74C	00	DB 00	
0043B74D	00	DB 00	
0043B74E	00	DB 00	
0043B74F	00	DB 00	
0043B750	\$ A1 2C735D00	MOV EAX,DWORD PTR DS:[5D732C]	
0043B755	. 0BC0	OR EAX,EAX	
0043B757	. v74 02	JE SHORT unpacked.0043B75B	
0043B759	. FFE0	JMP EAX	
0043B75B	> 68 38B74300	PUSH unpacked.0043B738	
0043B760	. B8 44854100	MOV EAX,<JMP.&MSUBUM60.DLLFunctionCall>	
0043B765	. FFD0	CALL EAX	
0043B767	. FFE0	JMP EAX	
0043B769	00	DB 00	

0043B76D	00	DB 00	
0043B76E	00	DB 00	
0043B76F	00	DB 00	
0043B770	. 53 68 6F 77 5	ASCII "ShowReminderMess"	
0043B780	. 61 67 65 00	ASCII "age",0	
0043B784	44B64300	DD unpacked.0043B644	ASCII "ArmAccess.DLL"
0043B788	70B74300	DD unpacked.0043B770	ASCII "ShowReminderMessage"
0043B78C	00	DB 00	
0043B78D	00	DB 00	
0043B78E	04	DB 04	
0043B78F	00	DB 00	
0043B790	30735D00	DD unpacked.005D7330	
0043B794	00	DB 00	
0043B795	00	DB 00	
0043B796	00	DB 00	
0043B797	00	DB 00	
0043B798	00	DB 00	
0043B799	00	DB 00	
0043B79A	00	DB 00	
0043B79B	00	DB 00	
0043B79C	. A1 38735D00	MOV EAX,DWORD PTR DS:[5D7338]	
0043B7A1	. 0BC0	OR EAX,EAX	
0043B7A3	. v74 02	JE SHORT unpacked.0043B7A7	
0043B7A5	. FFE0	JMP EAX	
0043B7A7	> 68 84B74300	PUSH unpacked.0043B784	
0043B7AC	. B8 44854100	MOV EAX,<JMP.&MSUBUM60.DLLFunctionCall>	
0043B7B1	. FFD0	CALL EAX	
0043B7B3	. FFE0	JMP EAX	
0043B7B5	00	DB 00	

0043B640	0E	DB 0E	
0043B641	00	DB 00	
0043B642	00	DB 00	
0043B643	00	DB 00	
0043B644	. 41 72 6D 41 6	ASCII "ArmAccess.DLL",0	
0043B652	00	DB 00	
0043B653	00	DB 00	
0043B654	08	DB 08	
0043B655	00	DB 00	
0043B656	00	DB 00	
0043B657	00	DB 00	
0043B658	. 45 6E 76 69 7	ASCII "Environ",0	
0043B660	44B64300	DD unpacked.0043B644	ASCII "ArmAccess.DLL"
0043B664	58B64300	DD unpacked.0043B658	ASCII "Environ"
0043B668	00	DB 00	
0043B669	00	DB 00	
0043B66A	04	DB 04	
0043B66B	00	DB 00	
0043B66C	00735D00	DD unpacked.005D7300	
0043B670	00	DB 00	
0043B671	00	DB 00	
0043B672	00	DB 00	
0043B673	00	DB 00	
0043B674	00	DB 00	
0043B675	00	DB 00	
0043B676	00	DB 00	
0043B677	00	DB 00	
0043B678	\$ A1 08735D00	MOV EAX,DWORD PTR DS:[5D7308]	
0043B67D	. 0BC0	OR EAX,EAX	
0043B67F	. 74 02	JE SHORT unpacked.0043B683	
0043B681	. FFE0	JMP EAX	
0043B683	> 68 60B64300	PUSH unpacked.0043B660	
0043B688	. B8 44854100	MOV EAX,<JMP.&MSUBUM60.DllFunctionCall>	
0043B68D	. FFD0	CALL EAX	
0043B68F	. FFE0	JMP EAX	
0043B691	00	DB 00	

Coloco el significado o la importancia de las 3 en un anexo al final.

Me pongo a trazar un poco y encuentro esto

Esto es un codigo para chequear el USERNAME, en otras palabras un procedimiento para una lista negra o black list desde el usuario en armadillo

0052BB3F	CC	INT3	
0052BB40	55	PUSH EBP	
0052BB41	8BEC	MOV EBP,ESP	
0052BB43	83EC 08	SUB ESP,8	
0052BB46	68 96844100	PUSH BracketT.00418496	
0052BB4B	64:A1 00000000	MOV EAX,DWORD PTR FS:[0]	JMP to MSUBUM60.__vbaExceptionHandler
0052BB51	50	PUSH EAX	
0052BB52	64:8925 00000000	MOV DWORD PTR FS:[0],ESP	
0052BB59	81EC 9C000000	SUB ESP,9C	
0052BB5F	53	PUSH EBX	
0052BB60	56	PUSH ESI	
0052BB61	57	PUSH EDI	
0052BB62	8965 F8	MOV DWORD PTR SS:[EBP-8],ESP	
0052BB65	C745 FC 58C14000	MOV DWORD PTR SS:[EBP-4],BracketT.0040C39F6	
0052BB6C	39F6	XOR ESI,ESI	
0052BB6E	68 10EF4300	PUSH BracketT.0043EF10	UNICODE "USERNAME"
0052BB73	8D45 EC	LEA EAX,DWORD PTR SS:[EBP-14]	
0052BB76	50	PUSH EAX	
0052BB77	8975 EC	MOV DWORD PTR SS:[EBP-14],ESI	
0052BB7A	8975 E8	MOV DWORD PTR SS:[EBP-18],ESI	
0052BB7D	8975 E4	MOV DWORD PTR SS:[EBP-1C],ESI	
0052BB80	8975 D4	MOV DWORD PTR SS:[EBP-2C],ESI	
0052BB83	8975 C4	MOV DWORD PTR SS:[EBP-3C],ESI	
0052BB86	8975 B4	MOV DWORD PTR SS:[EBP-4C],ESI	
0052BB89	8975 A4	MOV DWORD PTR SS:[EBP-5C],ESI	
0052BB8C	8975 94	MOV DWORD PTR SS:[EBP-6C],ESI	
0052BB8F	8975 84	MOV DWORD PTR SS:[EBP-7C],ESI	
0052BB92	89B5 58FFFFFF	MOV DWORD PTR SS:[EBP-A8],ESI	
0052BB98	FF15 80124000	CALL DWORD PTR DS:[401280]	MSUBUM60.__vbaStrToAnsi
0052BB9E	50	PUSH EAX	
0052BB9F	E8 04FAF0FF	CALL BracketT.0043B678	
0052BBA4	8BD0	MOV EDI,EAX	
0052BBA6	8D4D E8	LEA ECX,DWORD PTR SS:[EBP-18]	
0052BBA9	FF15 B4124000	CALL DWORD PTR DS:[4012B4]	MSUBUM60.__vbaStrMove
0052BBAF	FF15 A0104000	CALL DWORD PTR DS:[4010A0]	MSUBUM60.__vbaSetSystemError
0052BBB5	8B4D E8	MOV ECX,DWORD PTR SS:[EBP-18]	
0052BBB8	51	PUSH ECX	
0052BBB9	8D55 E4	LEA EDX,DWORD PTR SS:[EBP-1C]	
0052BBBC	52	PUSH EDX	
0052BBBD	FF15 BC114000	CALL DWORD PTR DS:[4011BC]	MSUBUM60.__vbaStrToUnicode

Esto es gracias a las llamadas de entorno que realiza armadillo

Ahora verifica unos nombres

0052BBF1	83C4 10	ADD ESP,10	
0052BBF4	50	PUSH EAX	
0052BBF5	68 5C974400	PUSH BracketT.0044975C	UNICODE "Thomas Tarr"
0052BBFA	FFD7	CALL EDI	
0052BBFC	85C0	TEST EAX,EAX	
0052BBFE	0F84 F3000000	JS BracketT.0052BCF7	
0052BC04	8B8D 58FFFFFF	MOV ECX,DWORD PTR SS:[EBP-A8]	
0052BC0A	51	PUSH ECX	
0052BC0B	68 78974400	PUSH BracketT.00449778	UNICODE "Jacqueline Hughes"
0052BC10	FFD7	CALL EDI	
0052BC12	85C0	TEST EAX,EAX	
0052BC14	0F84 D0000000	JS BracketT.0052BCF7	
0052BC1A	8B95 58FFFFFF	MOV EDX,DWORD PTR SS:[EBP-A8]	
0052BC20	52	PUSH EDX	
0052BC21	68 A0974400	PUSH BracketT.004497A0	UNICODE "Matthew Hummel"
0052BC26	FFD7	CALL EDI	
0052BC28	85C0	TEST EAX,EAX	
0052BC2A	0F84 C7000000	JS BracketT.0052BCF7	
0052BC2C	8B85 58FFFFFF	MOV EAX,DWORD PTR SS:[EBP-A8]	
0052BC36	50	PUSH EAX	
0052BC37	68 C4974400	PUSH BracketT.004497C4	UNICODE "Roman Beran"
0052BC3C	FFD7	CALL EDI	
0052BC3E	85C0	TEST EAX,EAX	
0052BC40	0F84 B1000000	JS BracketT.0052BCF7	
0052BC46	8B8D 58FFFFFF	MOV ECX,DWORD PTR SS:[EBP-A8]	
0052BC4C	51	PUSH ECX	
0052BC4D	68 88984400	PUSH BracketT.00449888	UNICODE "Allan Pang"
0052BC52	FFD7	CALL EDI	
0052BC54	85C0	TEST EAX,EAX	
0052BC56	0F85 A7010000	JNZ BracketT.0052BE03	
0052BC5C	3935 BC535D00	CMPL DWORD PTR DS:[5D53BC],ESI	
0052BC62	75 10	JNZ SHORT BracketT.0052BC74	

Si son esos usuarios

0052BD18	8945 AC	MOV DWORD PTR SS:[EBP-54],EAX	
0052BD1B	8945 BC	MOV DWORD PTR SS:[EBP-44],EAX	
0052BD1E	C745 8C 70984400	MOV DWORD PTR SS:[EBP-74],BracketT.0044	UNICODE "WARNING !"
0052BD25	895D 84	MOV DWORD PTR SS:[EBP-7C],EBX	
0052BD28	FFD7	CALL EDI	
0052BD2A	8D55 94	LEA EDX,DWORD PTR SS:[EBP-6C]	
0052BD2D	8D4D D4	LEA ECX,DWORD PTR SS:[EBP-2C]	
0052BD30	C745 9C 0C984400	MOV DWORD PTR SS:[EBP-64],BracketT.0044	UNICODE "Bracket Trader cannot be used on this computer."
0052BD37	895D 94	MOV DWORD PTR SS:[EBP-6C],EBX	
0052BD3A	FFD7	CALL EDI	
0052BD3C	8D45 A4	LEA EAX,DWORD PTR SS:[EBP-5C]	
0052BD3F	50	PUSH EAX	
0052BD40	8D4D B4	LEA ECX,DWORD PTR SS:[EBP-4C]	
0052BD43	51	PUSH ECX	
0052BD44	8D55 C4	LEA EDX,DWORD PTR SS:[EBP-3C]	
0052BD47	52	PUSH EDX	
0052BD48	6A 30	PUSH 30	
0052BD4A	8D45 D4	LEA EAX,DWORD PTR SS:[EBP-2C]	
0052BD4D	50	PUSH EAX	
0052BD4E	FF15 E0104000	CALL DWORD PTR DS:[4010E0]	MSUBUM60.rtcMsgBox
0052BD54	8D4D A4	LEA ECX,DWORD PTR SS:[EBP-5C]	

Ahora sigamos en las otras

005D0101	PUSH BracketT.00454520	UNICODE "" attempted to "	
005D01F8	MOV DWORD PTR SS:[EBP-144],BracketT.004	UNICODE "read"	
005D0219	MOV DWORD PTR SS:[EBP-134],BracketT.004	UNICODE "write"	
005D0268	MOV DWORD PTR SS:[EBP-154],BracketT.004	UNICODE "" data at address '0x"	
005D03C2	MOV DWORD PTR SS:[EBP-114],BracketT.004	UNICODE "ExceptionFilter"	
005D0512	MOV EDX,BracketT.0043F244	UNICODE "http://www.bracket-trader.com/register/register.html"	
005D0759	PUSH BracketT.0043EF10	UNICODE "USERNAME"	
005D07BC	PUSH BracketT.004545E4	UNICODE "DEFAULT"	
005D0859	PUSH BracketT.00443348	UNICODE "EXPIRED"	
005D088E	PUSH BracketT.0043ED70	UNICODE "True"	
005D08D9	PUSH BracketT.00454644	UNICODE "Click the Help menu for registration instructions"	
005D0928	PUSH BracketT.004546AC	UNICODE "Not Yet Registered"	
005D09A0	PUSH BracketT.00454608	UNICODE "Registered Version"	
005D09EC	PUSH BracketT.0043EF10	UNICODE "USERNAME"	
005D0A10	PUSH BracketT.00454704	UNICODE "Registered to "	
005D0AC5	PUSH BracketT.00446A40	UNICODE "PAIDFOR"	
005D0AFA	PUSH BracketT.00454728	UNICODE "Beta"	
005D0B45	PUSH BracketT.00454738	UNICODE "Beta Version"	
005D0B87	PUSH BracketT.00454758	UNICODE "Ver 07.0130a90 API "	

5d09a0

005AF54	PUSH BracketT.0043ACE0	UNICODE "Error"
005AF54	PUSH BracketT.0043AD10	UNICODE "("
005AF54	PUSH BracketT.00452DA8	UNICODE ") in procedure comboSymbol_Click of Form frmMain"
005AF54	MOV EDI,BracketT.00452D2C	UNICODE "comboSymbol_Click"
005AF54	MOV EDI,BracketT.0043C658	UNICODE "frmMain"
005AF171	PUSH BracketT.00443848	UNICODE "EXPIRED"
005AF1A6	PUSH BracketT.0043ED70	UNICODE "True"
005AF27B	PUSH BracketT.00452E10	UNICODE "Click 'Register Bracket Trader' in the Help menu to get your key"
005AF51D	PUSH BracketT.0044377C	UNICODE "LIMIT"
005AF523	PUSH BracketT.00443788	UNICODE "SELL"
005AF628	PUSH BracketT.0043DEE4	UNICODE "201012"
005AF87B	MOV EAX,BracketT.0043DAE4	UNICODE "FALSE"
005AF889	PUSH BracketT.0043D930	UNICODE "STPLMT"

004A69C6	PUSH BracketT.0043F7EC	UNICODE "1,3000"
004A69C6	PUSH BracketT.0043F920	UNICODE "Closing Feature Tester, wait..."
004A69C6	PUSH BracketT.0043F964	UNICODE "Trying to Reconnect to IB"
004A658C	MOV DWORD PTR SS:[EBP-90],BracketT.0043F964	UNICODE "Error!"
004A65AF	MOV DWORD PTR SS:[EBP-80],BracketT.0043F964	UNICODE "You must enter a name and a key."
004A65FC	MOV DWORD PTR SS:[EBP-80],BracketT.0043F964	UNICODE "Registration Successful !!"
004A691C	PUSH BracketT.0043FA48	UNICODE "Key is valid, and has been stored."
004A6921	PUSH BracketT.0043AC00	UNICODE "J0"
004A6938	PUSH BracketT.0043FA94	UNICODE "Thank you for supporting Bracket Trader."
004A68D7	MOV DWORD PTR SS:[EBP-90],BracketT.0043F964	UNICODE "Error!"
004A68FA	MOV DWORD PTR SS:[EBP-80],BracketT.0043F964	UNICODE "The name/key you entered does not appear to be valid. Please try again"
004A6E8E	MOV DWORD PTR SS:[EBP-98],BracketT.0043F964	UNICODE "00"
004A6EC7	MOV DWORD PTR SS:[EBP-A8],BracketT.0043F964	UNICODE "00"
004A6EFA	MOV DWORD PTR SS:[EBP-B8],BracketT.0043F964	UNICODE "00"

Y por ultimo veo los registrados

005D09EA	8BF8	MOV EDI,EAX	UNICODE "USERNAME"
005D09EC	68 10EF4300	PUSH <unpacked.off_43EF10>	
005D09F1	8D45 D8	LEA EAX,DWORD PTR SS:[EBP-28]	
005D09F4	50	PUSH EAX	
005D09F5	FFD3	CALL EBX	
005D09F7	50	PUSH EAX	
005D09F8	E8 7BACE6FF	CALL <unpacked.sub_43B678>	
005D09FD	8BD0	MOV EDX,EAX	
005D09FF	8D4D D4	LEA ECX,DWORD PTR SS:[EBP-2C]	
005D0A02	FF15 94114000	CALL DWORD PTR DS:[<dwor_62F194>]	MSUBUM60.__vbaStrMove
005D0A08	FF15 70114000	CALL DWORD PTR DS:[<dwor_62F170>]	MSUBUM60.__vbaSetSystemError
005D0A0E	8B1F	MOV EBX,DWORD PTR DS:[EDI]	
005D0A10	68 04474500	PUSH unpacked.00454704	UNICODE "Registered to "
005D0A15	8B4D D4	MOV ECX,DWORD PTR SS:[EBP-2C]	
005D0A18	51	PUSH ECX	
005D0A19	8D55 D0	LEA EDX,DWORD PTR SS:[EBP-30]	
005D0A1C	52	PUSH EDX	
005D0A1D	FF15 A4114000	CALL DWORD PTR DS:[<dwor_62F1A4>]	MSUBUM60.__vbaStrToUnicode
005D0A23	50	PUSH EAX	
005D0A24	FF15 78114000	CALL DWORD PTR DS:[<dwor_62F178>]	MSUBUM60.__vbaStrCat

Y vemos la variables UserNAME y PAIDFOR

Osea tenemos 2 variables necesarias para el usuario registrado: Username y Paidfor

005D0AB8	FF15 B0104000	CALL DWORD PTR DS:[<dwor_62F0B0>]	MSUBUM60.__vbaFreeObj
005D0ABE	C745 FC 0F0000	MOV DWORD PTR SS:[EBP-4],0F	
005D0AC5	68 406A4400	PUSH <unpacked.off_446A40>	UNICODE "PAIDFOR"
005D0ACA	8D4D D8	LEA ECX,DWORD PTR SS:[EBP-28]	
005D0ACD	51	PUSH ECX	
005D0ACE	FF15 A0114000	CALL DWORD PTR DS:[<dwor_62F1A0>]	MSUBUM60.__vbaStrToAnsi
005D0AD4	50	PUSH EAX	
005D0AD5	E8 9EABE6FF	CALL <unpacked.sub_43B678>	
005D0ADA	8BD0	MOV EDX,EAX	
005D0ADC	8D4D D4	LEA ECX,DWORD PTR SS:[EBP-2C]	
005D0ADF	FF15 94114000	CALL DWORD PTR DS:[<dwor_62F194>]	MSUBUM60.__vbaStrMove
005D0AE5	FF15 70114000	CALL DWORD PTR DS:[<dwor_62F170>]	MSUBUM60.__vbaSetSystemError
005D0AEB	8B55 D4	MOV EDX,DWORD PTR SS:[EBP-2C]	
005D0AEE	52	PUSH EDX	
005D0AEF	8D45 D0	LEA EAX,DWORD PTR SS:[EBP-30]	
005D0AF2	50	PUSH EAX	
005D0AF3	FF15 A4114000	CALL DWORD PTR DS:[<dwor_62F1A4>]	MSUBUM60.__vbaStrToUnicode
005D0AF9	50	PUSH EAX	
005D0AFA	68 28474500	PUSH unpacked.00454728	UNICODE "Beta"
005D0AFF	FF15 7C114000	CALL DWORD PTR DS:[<dwor_62F17C>]	MSUBUM60.__vbaStrCmp
005D0B05	8BF8	MOV EDI,EAX	
005D0B07	F7DF	NEG EDI	
005D0B09	1BFF	SAR ESI,ESI	

Vamos a los help: no conozco este productor de pdf, pero igual es llamativo los botones y el productor de pdf

PDF Producer: wPDF3 by WPCubed GmbH

Luego decompilo, pues mas comentarios no puedo hacer

Para crear un map luego de desempacado:

Herramientas:

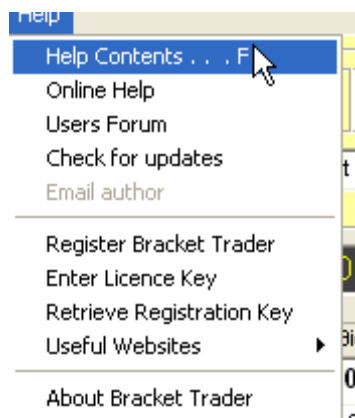
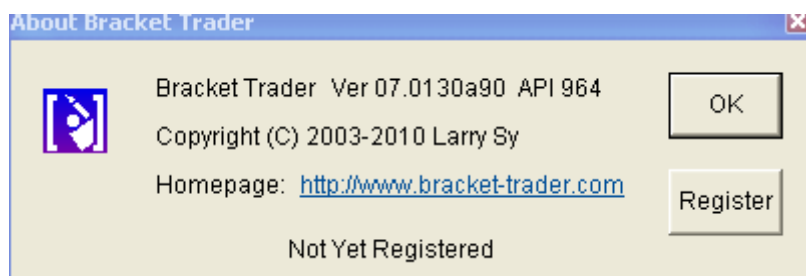
WB Decompiler Pro 7.6 ->producir IDC

IDA 5.X->cargar IDC y exportar como map

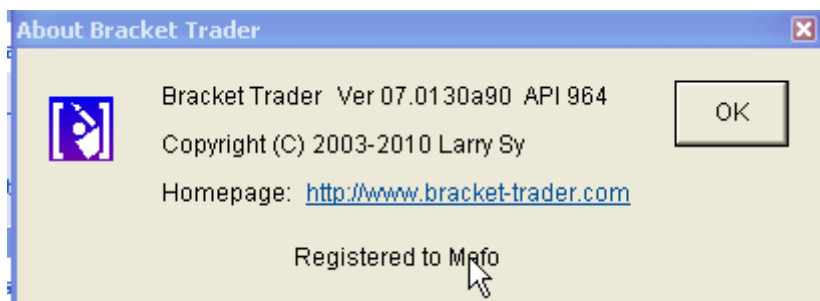
Olly 1.1+>Plugin para importar los map.

Sigamos

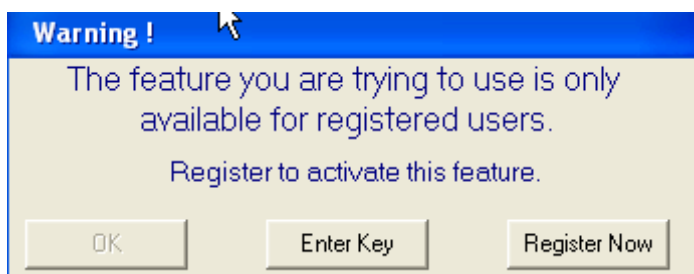
Bajado el active x, que pide, al colocar about en el original:



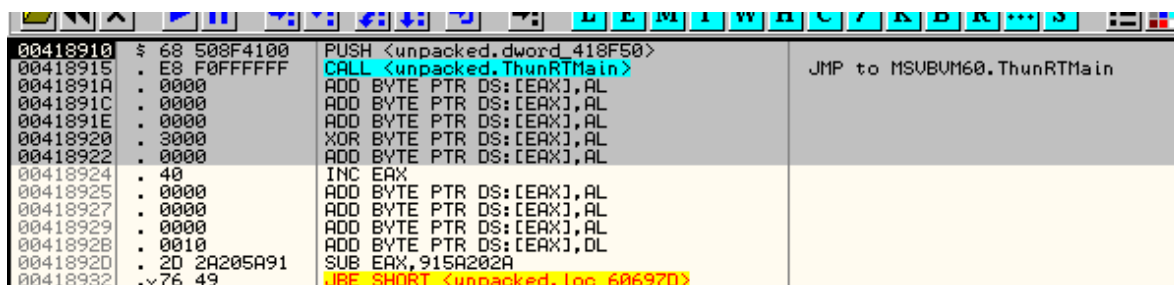
El desempacado con la dll de armadillo v8



Pero coloco la opcion de tools y me muestra que esto es trial:



Ahora en el desempacado tengo



Coloco go to GetEnvironmentVariableA

Coloco bp y vemos ;, este no proviene de armadillo



Este tampoco



Este si

0011F810	025D17CC	CALL to GetEnvironmentVariableA from ArmAcces.025D17C6
0011F814	0018E22C	VarName = "USERNAME"
0011F818	0011F824	Buffer = 0011F824
0011F81C	0000FFFF	BufSize = FFFF (65535)
0011F820	0012FAF4	

0011F810 025D17CC /CALL to GetEnvironmentVariableA from ArmAcces.025D17C6

0011F814 0018E22C |VarName = "USERNAME"

0011F74C 025D17CC /CALL to GetEnvironmentVariableA from ArmAcces.025D17C6

0011F750 0018E22C |VarName = "USERNAME"

0011F810 025D17CC /CALL to GetEnvironmentVariableA from ArmAcces.025D17C6

0011F814 0018E22C |VarName = "Systemroot"

0011F71C 025D17CC /CALL to GetEnvironmentVariableA from ArmAcces.025D17C6

0011F720 001C2D2C |VarName = "PAIDFOR"

0011F680 025D17CC /CALL to GetEnvironmentVariableA from ArmAcces.025D17C6

0011F684 001C2D2C |VarName = "windir"

0011F680 025D17CC /CALL to GetEnvironmentVariableA from ArmAcces.025D17C6

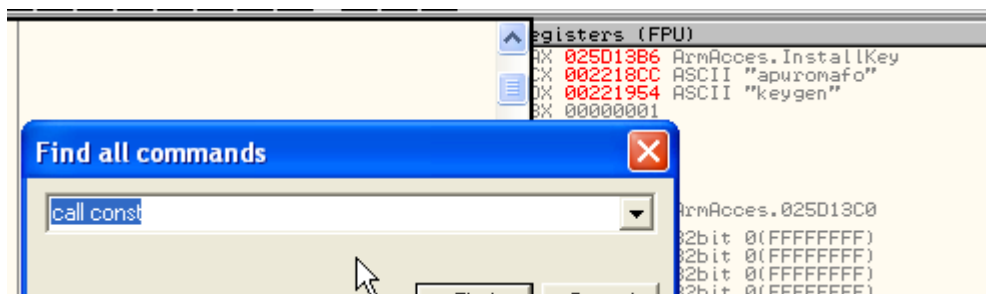
0011F684 001C575C |VarName = "windir"

0011F680 025D17CC /CALL to GetEnvironmentVariableA from ArmAcces.025D17C6

0011F684 001C2D7C |VarName = "windir"

O bien coloco el add, y vere esto:

Y voy a la dll...



Y entre depuracion el valor de al, es importante, si al es 1, muestra que es valido y puedes seguir, pero..si reinicias la aplicacion, denuevo es la misma realidad, no se puede usar full, asi que los registros de armadillos pueden ser engañados, pero al reinicio verificara denuevo..

Al iniciar comienzo a analizar un poco el DLL Function call y veo que descarga de internet:

Descarga de internet:

0043AA7B	00	DB 00	
0043AA7C	5CA44300	DD <unpacked.aUrlmon>	ASCII "urlmon"
0043AA80	68AA4300	DD <unpacked.aUrlDownloadTo>	ASCII "URLDownloadToFileA"
0043AA84	00	DB 00	
0043AA85	00	DB 00	
0043AA86	04	DB 04	
0043AA87	00	DB 00	
0043AA88	74725D00	DD unpacked.005D7274	
0043AA8C	00	DB 00	
0043AA8D	00	DB 00	
0043AA8E	00	DB 00	
0043AA8F	00	DB 00	
0043AA90	00	DB 00	
0043AA91	00	DB 00	
0043AA92	00	DB 00	
0043AA93	00	DB 00	
0043AA94	\$ A1 7C725D00	MOV EAX,DWORD PTR DS:[5D727C]	
0043AA99	. 0BC0	OR EAX,EAX	
0043AA9B	. <74 02	JE SHORT <unpacked.loc_43AA9F>	
0043AA9D	. FFE0	JMP EAX	
0043AA9F	> 68 7CA44300	PUSH <unpacked.off_43AA7C>	
0043AAA4	. B8 44854100	MOV EAX,<unpacked.DllFunctionCall>	JMP to MSVBVM60.DllFunctionCall
0043AAA9	. FFD0	CALL EAX	
0043AAB8	. FFE0	JMP EAX	urlmon.URLDownloadToFileA
0043AABD	00	DB 00	
0043AABE	00	DB 00	
0043AABF	00	DB 00	
0043AAB0	09	DB 09	

Y la variable:

0012F6FC 0018E31C ASCII "http://www.bracket-trader.com/vercheck20070130a90.htm"

0012F700 0018E254 ASCII "\\version.htm"

Y tiene tambien mensajes de corruptos:

0052AD69	68 08934400	PUSH unpacked.00449308	UNICODE "WARNING: This copy of Bracket
0052AD6E	68 00AC4300	PUSH unpacked.0043AC00	UNICODE "¡"
0052AD73	FF15 78114000	CALL DWORD PTR DS:[&MSUBUM60.__vbaStrC	MSUBUM60.__vbaStrCat
0052AD79	8B00	MOV EDX,EAX	
0052AD7B	8D4D 04	LEA ECX,DWORD PTR SS:[EBP-2C]	
0052AD7E	FF15 94114000	CALL DWORD PTR DS:[&MSUBUM60.__vbaStrM	MSUBUM60.__vbaStrMove
0052AD84	50	PUSH EAX	
0052AD85	68 B88C4300	PUSH unpacked.00438CB8	
0052AD8A	FF15 78114000	CALL DWORD PTR DS:[&MSUBUM60.__vbaStrC	MSUBUM60.__vbaStrCat
0052AD90	8B00	MOV EDX,EAX	
0052AD92	8D4D 00	LEA ECX,DWORD PTR SS:[EBP-30]	
0052AD95	FF15 94114000	CALL DWORD PTR DS:[&MSUBUM60.__vbaStrM	MSUBUM60.__vbaStrMove
0052AD98	50	PUSH EAX	
0052AD9C	68 00AC4300	PUSH unpacked.0043AC00	UNICODE "¡"
0052ADA1	FF15 78114000	CALL DWORD PTR DS:[&MSUBUM60.__vbaStrC	MSUBUM60.__vbaStrCat
0052ADA7	8B00	MOV EDX,EAX	
0052ADA9	8D4D CC	LEA ECX,DWORD PTR SS:[EBP-34]	
0052ADAC	FF15 94114000	CALL DWORD PTR DS:[&MSUBUM60.__vbaStrM	MSUBUM60.__vbaStrMove
0052ADB2	50	PUSH EAX	
0052ADB3	68 F4934400	PUSH unpacked.004493F4	UNICODE "The program will end after you
0052ADB8	FF15 78114000	CALL DWORD PTR DS:[&MSUBUM60.__vbaStrC	MSUBUM60.__vbaStrCat
0052ADBE	8945 9C	MOV DWORD PTR SS:[EBP-64],EAX	
0052ADC1	C745 94 08000000	MOV DWORD PTR SS:[EBP-6C],8	
0052ADC8	8D85 64FFFFFF	LEA EAX,DWORD PTR SS:[EBP-9C]	
0052ADCE	50	PUSH EAX	
0052ADCF	8D8D 74FFFFFF	LEA ECX,DWORD PTR SS:[EBP-8C]	
0052ADD5	51	PUSH ECX	
0052ADD6	8D55 84	LEA EDX,DWORD PTR SS:[EBP-7C]	
0052ADD9	52	PUSH EDX	
0052ADDA	6A 30	PUSH 30	
0052ADDC	8D45 94	LEA EAX,DWORD PTR SS:[EBP-6C]	
00449308	unpacked.00449308 (UNICODE "WARNING: This copy of Bracket Trader is corrupt. Reinstall with a		

00449308	PUSH EDI	(Initial CPU selection)
0052AD69	PUSH unpacked.00449308	UNICODE "WARNING: This copy of Bracket Trader is corrupt. Reinstall with a fresh
005D0F18	PUSH unpacked.00449308	UNICODE "WARNING: This copy of Bracket Trader is corrupt. Reinstall with a fresh
005D2EC4	PUSH unpacked.00449308	UNICODE "WARNING: This copy of Bracket Trader is corrupt. Reinstall with a fresh

1->sin dll de armadillo

2->sin poder acceder al internet explorer 6

3->Missing Component

Inyeccion de variables y con eso deberia ejecutar como registrado:

1)agregamos una seccion con topo (crackskit) y cambiamos para que coloque 00 y no Nop, creando una nueva seccion, haciendolo escribible, de tamaño 1000, y luego al abrir haremos saltar al OEP, desde la seccion,injertamos la variable con otra tool

2) agregamos las variables con MultimateAssembler 1.2 -> <http://rammichael.com/>

Y tenemos

<707000>

PUSHAD

PUSHFD

MOV EBX,kernel32.SetEnvironmentVariableA

PUSH @apuromafo

PUSH @apuromafo2

CALL EBX

PUSH @apuromafo3

PUSH @apuromafo4

CALL EBX

....push 5 /6 call ebx..

POPFD

POPAD

JMP 00418910 //lugar donde retorna

Y las variables como sigue

@apuromafo: "key"

ADD BYTE PTR DS:[EAX],AL

@apuromafo2: "USERKEY"

ADD BYTE PTR DS:[EAX],AL

@apuromafo4: "VERSION"

ADD BYTE PTR DS:[EAX],AL

@apuromafo5: "True"

ADD BYTE PTR DS:[EAX],AL

@apuromafo6: "PAIDFOR"

ADD BYTE PTR DS:[EAX],AL

@apuromafo8: "KEYCREATED"

ADD BYTE PTR DS:[EAX],AL

@apuromafo10:"V8"

ADD BYTE PTR DS:[EAX],AL

@apuromafo12: "EXTRAINFO"

@apuromafo14: "ALTUSERNAME"

ADD BYTE PTR DS:[EAX],AL

@apuromafo15: "Apuromafo CLS"

ADD BYTE PTR DS:[EAX],AL

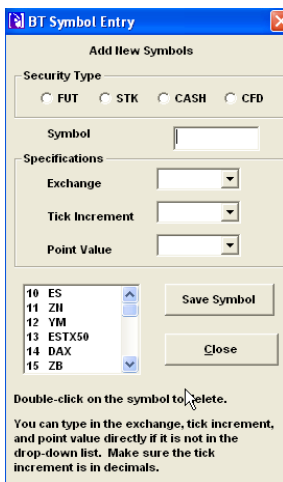
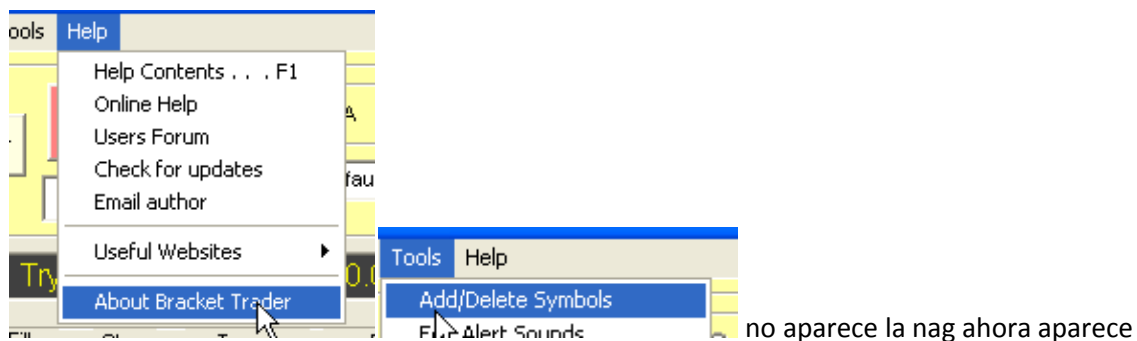
@apuromafo16: "USERNAME"

ADD BYTE PTR DS:[EAX],AL

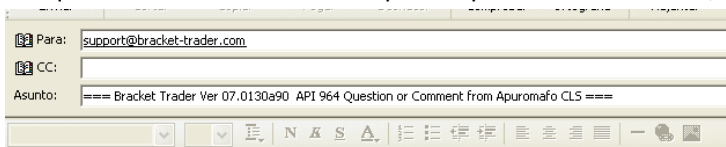
Asi que usamos MulimateAssembler y ensamblamos en el lugar, pero como somos mas ordenados



Y al pulsar los botones no pide una nueva registracion Y ahora el menu lateral



Y si quiero colocar un mail de soporte aprovecha la version , y mi nombre en el asunto



Question or Comment:

Por lo que damos fin a este escrito, no olviden leer el anexo, puede ser de ayuda .

Saludos Apuromafo

Anexo

Leo las apis en armadillo 8 y lo coloco como anexo:

InstallKey

Purpose:

Checks a name/key pair, and (if valid and not already expired) stores it as the new key.

Declarations:

C/C++:

```
typedef bool (__stdcall *InstallKeyFn)(const char *name, const char *code);
```

Delphi:

```
Function InstallKey (name,code:PAnsiChar) : Boolean; stdcall; external  
'armaccess.dll';
```

Visual BASIC:

```
Declare Function InstallKey Lib "ArmAccess.DLL" (ByVal Name$, ByVal Code$)  
as Byte
```

FoxPro:

```
DECLARE INTEGER InstallKey IN ArmAccess.DLL STRING Name, STRING  
Code
```

Parameters:

- name**: The "name" the key is made for. This can be blank (an empty string) only for nameless keys. The name must use 8-bit ASCII encoding. Do not pass a name that uses
 - Unicode or UTF-8 encoding.
- code**: The key to install.

Returns:

Returns non-zero if the key is valid and installed (see notes below for expired-key exception), or zero if it isn't.

Notes:

When this function was called with an expired key in versions prior to 4.01, it still returned non-zero but the key was never installed. You had to check the EXPIRED environment variable to see whether it was correctly installed or not. Now this function returns zero any time the key is not installed, for any reason.

If the program attempts to (re)install the currently-installed key, it is ignored, and the function simply returns non-zero to say that it's valid.

This function is not intended for use with client/server keys. To install client/server keys, your users must use the SERVER REGISTER command-line option.

For Delphi versions prior to Delphi 2009, you may need to make the following adjustment to ensure compatibility: Change all PAnsiChar types to PChar.

This function is operationally identical to the older [CheckCode](#) function.

ShowReminderMessage

Purpose:

Displays (or redisplay) the configured show-before Reminder Message for the **current certificate**.

Declarations:

C/C++:

```
typedef void (__stdcall *ShowReminderMessageFn)(HWND parent);
```

Delphi:

```
Procedure ShowReminderMessage(parent:HWND); stdcall; external  
'armaccess.dll';
```

Visual BASIC:

```
Declare Sub ShowReminderMessage lib "ArmAccess.DLL" (ByVal ParentWindow  
as Long)
```

FoxPro:

```
DECLARE INTEGER ShowReminderMessage IN ArmAccess.DLL INTEGER  
ParentWindowHandle
```

Parameters:

- parent:** The handle (HWND) of the window to use as the parent window for the new
- window. This parameter can be zero if no parent window is required.

Returns:

Nothing.

Notes:

If the show-before Reminder Message is not configured for this certificate, this function does nothing.

/Enviroment -> GetEnvironmentVariable -> Using with Visual BASIC /

The easiest way to retrieve environment variables in Visual BASIC 5.0 or later is to use SoftwarePassport/Armadillo's ArmEnviron\$ function. You can also do it by way of the Windows API function **GetEnvironmentVariable**, but we no longer recommend that; ArmEnviron\$ is much easier to deal with and has no conversion and comparison problems.

To make Visual BASIC programs work with SoftwarePassport/Armadillo's ArmEnviron\$ function, rather than the Environ\$ function built into Visual BASIC itself (which cannot access the SoftwarePassport/Armadillo-generated environment variables), add the following line to any module file:

```
Public Declare Function ArmEnviron Lib "ArmAccess.DLL" Alias "Environ" (ByVal  
    Name$) As String
```

Then use ArmEnviron\$ in place of Environ\$. For more information on retrieving environment variables, please refer to the Visual BASIC documentation.

Possible Problems

One possible problem is caused by setting Intercept None. SoftwarePassport/Armadillo must intercept the MSVBVM?0.DLL file appropriate to your version of VB (MSVBVM50.DLL or MSVBVM60.DLL) to provide access to the virtual ArmAccess.DLL's functions. If you set it to Intercept None, or remove those entries from the default interception list, then it won't be able to.

If you continue to have problems, please check the version of the MSVBVM60.DLL file that the affected customer is using. The version that ships with Windows Millennium (marked 6.0.84.95 or 6.00.8495, with a comment of "May 10, 1999") has issues with SoftwarePassport/Armadillo. Version 6.0.92.37 (or 6.0.9237), with a comment of "May 29, 2001", works. Some versions of installation programs (such as Wise Install v7) won't always update files properly -- we're told that the current version (at the time of this writing, Wise Install v9) works as it should.

If all else fails, you can select the "Store Environment Variables Externally" option, and use VB's built-in Environ\$ command. You may not be able to update the variables after your program starts, and they'll be visible to anyone with the right tools, but it will work.

Example

The following example simply retrieves the USERNAME environment variable, and stores it in the User variable. To retrieve a different variable, simply replace the name.

```
Public Declare Function ArmEnviron Lib "ArmAccess.DLL" Alias "Environ" (ByVal  
    Name$) As String  
Dim User as String
```

```
User = ArmEnviron$("USERNAME")
```