CNC code Maker Free

by Apuromafo

Encontré que necesitaban ayuda y me propuse apoyar

CLS
17/08/2013

Hola, no tengo mucho tiempo pero Hoy vamos a revisar un programa “free” que daba soporte de un “código” para seguir usando y de paso actualizarlo, pero la pagina caducó o dejó de funcionar y luego el programa quedaba “locked” o inutilizable, este escrito es con fines educacionales, saludos Apuromafo

Historia:
BUEN DIA NECESITARIA CRACKEAR UN PEQUEÑO PROGRAMITA LLAMADO "CNC CODE MAKER" Q ES UN PROGRAMA DE CONTROL NUMERICO QUE ERA GRATIS Y HABIA Q CARGARLE CADA TANTO UN CODIGO DESDE LA WEB OFICIAL PARA QUE SIGA FUNCIONANADO. EL TEMA ES QUE CADUCO LA PAGINA WEB Y YA NO TENGO DE DONDE SACAR EL CODIGO ASI Q TENDRIA Q CRACKEAR EL SOFT

Así que manos a la obra ,espero les guste ^^

Descarga (desde el pasado)

http://web.archive.org/web/http://www.cncsimple.com/get.php?v=599&f=CncCodeMaker-v1.0RC1-build599.exe

Información relevante del programa:

Publisher description
Do you think the normal CAD/CAM systems like MasterCam, SmartCam, GibbsCam etc. are too complicated? Or maybe do you just need something simpler? CAD/CAM too expensive? Simple CNC Code Maker might be the right choice for you!
CNC Code Maker is a tool that let's you easily draw using the CAD part of the program and produce ISO G-codes, Heidenhain codes more in a simple way.
It will work both for milling, turning (lathes), laser, water-jets and other CNC-machines.

What's the cost of CNC Code Maker? - It's FREE!

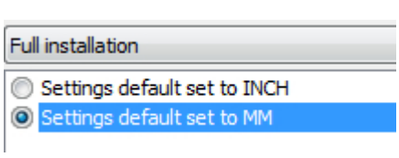
So what's the catch? - Really none, all we want from you is to come back to the website once a month to get a new battery-code. That's all.

Main Features:

- User-adaptable postprocessors
- Supplied ISO and heidenhain postprocessors
- DXF-file import/export
- Adjustable NC code output. Depth/start/stop etc

En palabras Simples tenemos algún check que vencer y claramente era free gratuito por ende no haremos tanto daño .

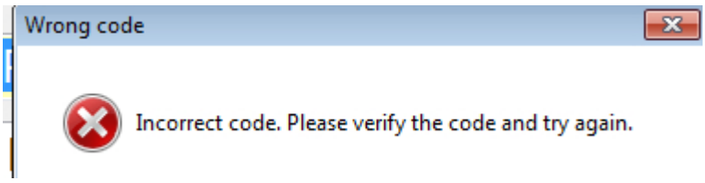
Instalo:



Adelantaré el programa, porque a primera vista no veo nada extraño.

Jaja que es esto

Sigamos:



o bien algunos crash al cerrar

Abrimos en ollydbg (leo claramente checking key ¿?)

```
00517D14  .  80795100    DD 00517980                    Entry point
00517D18  .  55          PUSH EBP
00517D19  .  8BEC        MOV EBP,ESP
00517D1B  .  83C4 E8     ADD ESP,-18
00517D1E  .  53          PUSH EBX
00517D1F  .  56          PUSH ESI
00517D20  .  57          PUSH EDI
00517D21  .  33C0        XOR EAX,EAX
00517D23  .  8945 EC     MOV DWORD PTR SS:[EBP-14],EAX
00517D26  .  8945 E8     MOV DWORD PTR SS:[EBP-18],EAX
00517D29  .  B8 A8795100 MOV EAX,005179A8
00517D2E  .  E8 85FBEEFF CALL 004078B8
00517D33  .  8B1D 34A95100 MOV EBX,DWORD PTR DS:[51A934]
00517D39  .  33C0        XOR EAX,EAX
00517D3B  .  55          PUSH EBP
00517D3C  .  68 BB7F5100 PUSH 00517FBB
00517D41  .  64:FF30     PUSH DWORD PTR FS:[EAX]
00517D44  .  64:8920     MOV DWORD PTR FS:[EAX],ESP     Installs SE handler 517FBB
00517D47  .  8B03        MOV EAX,DWORD PTR DS:[EBX]
00517D49  .  E8 4ED0F6FF CALL 00484D9C
00517D4E  .  8B03        MOV EAX,DWORD PTR DS:[EBX]
00517D50  .  BA D47F5100 MOV EDX,00517FD4               ASCII "Cnc Code Maker"
00517D55  .  E8 2ACCF6FF CALL 00484984
00517D5A  .  8B0D 30A65100 MOV ECX,DWORD PTR DS:[51A630]
00517D60  .  8B03        MOV EAX,DWORD PTR DS:[EBX]
00517D62  .  8B15 E0DE4E00 MOV EDX,DWORD PTR DS:[4EDEE0]
00517D68  .  E8 47D0F6FF CALL 00484DB4
00517D6D  .  8B0D 3CA55100 MOV ECX,DWORD PTR DS:[51A53C]
00517D73  .  8B03        MOV EAX,DWORD PTR DS:[EBX]
00517D75  .  8B15 58745100 MOV EDX,DWORD PTR DS:[517458]
00517D7B  .  E8 34D0F6FF CALL 00484DB4
00517D80  .  8B0D F8A55100 MOV ECX,DWORD PTR DS:[51A5F8]
00517D86  .  8B03        MOV EAX,DWORD PTR DS:[EBX]
00517D88  .  8B15 303B4C00 MOV EDX,DWORD PTR DS:[4C3B30]
00517D8E  .  E8 21D0F6FF CALL 00484DB4
00517D93  .  A1 3CA55100 MOV EAX,DWORD PTR DS:[51A53C]
00517D98  .  8B00        MOV EAX,DWORD PTR DS:[EAX]
00517D9A  .  E8 B19AF6FF CALL 00481850
00517D9F  .  A1 3CA55100 MOV EAX,DWORD PTR DS:[51A53C]
00517DA4  .  8B00        MOV EAX,DWORD PTR DS:[EAX]
00517DA6  .  BA EC7F5100 MOV EDX,00517FEC               ASCII "Checking key"
00517DAB  .  E8 74F8FFFF CALL 00517624
00517DB0  .  8B0D E8A95100 MOV ECX,DWORD PTR DS:[51A9E8]
00517DB6  .  8B03        MOV EAX,DWORD PTR DS:[EBX]
00517DB8  .  8B15 84D04E00 MOV EDX,DWORD PTR DS:[4ED084]
00517DBE  .  E8 F1CFF6FF CALL 00484DB4
00517DC3  .  8D55 E8     LEA EDX,[EBP-18]
00517DC6  .  33C0        XOR EAX,EAX
00517DC8  .  E8 13B2EEFF CALL 00402FE0
00517DCD  .  8B45 E8     MOV EAX,DWORD PTR SS:[EBP-18]
00517DD0  .  8D55 EC     LEA EDX,[EBP-14]
00517DD3  .  E8 6826EFFF CALL 0040A440                  CCncCodeMaker.0040A440
00517DD8  .  8D45 EC     LEA EAX,[EBP-14]
00517DDB  .  BA 04805100 MOV EDX,00518004               ASCII "CncCodeMaker.ini"
00517DE0  .  E8 97D9EEFF CALL 0040577C                  CCncCodeMaker.0040577C
00517DE5  .  8B4D EC     MOV ECX,DWORD PTR SS:[EBP-14]
00517DE8  .  B2 01       MOV DL,1
```

Buscamos las referencias

```
004ED2D6  ASCII "TKeyForm"                  ASCII "TKeyForm"
004ED2E9  ASCII "uKey"                      ASCII "uKey"
004ED2F8  ASCII "MATHNYJS3LKGRDZX"          ASCII "MATHNYJS3LKGRDZX"
004ED314  ASCII "LEFWVQNUPZKGRDAX"          ASCII "LEFWVQNUPZKGRDAX"
004ED78C  ASCII "/@"
004ED81D  MOV ECX,004ED92C                  ASCII "key.dat"
004ED92C  ASCII "key.dat"                   ASCII "key.dat"
004ED93C  ASCII "/@"
004ED998  MOV ECX,004EDAEC                  ASCII "key.dat"
004EDAEC  ASCII "key.dat"                   ASCII "key.dat"
004EDCD0  PUSH 004EDD80                     ASCII "Too old key"
004EDCD5  PUSH 004EDD8C                     ASCII "The code is too old. Please visit http://www.cncsimple.com to get a new one."
004EDCFD  PUSH 004EDDDC                     ASCII "Wrong code"
004EDD02  PUSH 004EDDE8                     ASCII "Incorrect code. Please verify the code and try again."
004EDD74  ASCII "$"
004EDD80  ASCII "Too old key",0             ASCII "Too old key"
004EDD8C  ASCII "The code is too "          ASCII "The code is too old. Please visit http://www.cncsimple.com to get a new one."
004EDDDC  ASCII "Wrong code",0              ASCII "Wrong code"
004EDDE8  ASCII "Incorrect code. "          ASCII "Incorrect code. Please verify the code and try again."
004EDE35  PUSH 004EDE50                     ASCII "http://www.cncsimple.com"
004EDE3A  PUSH 004EDE6C                     ASCII "open"
004EDE50  ASCII "http://www.cncsi"          ASCII "http://www.cncsimple.com"
004EDE6C  ASCII "open",0                    ASCII "open"
004EE050  ASCII "StatusBar"                 ASCII "StatusBar"
004EE060  ASCII "MainMenu1"                 ASCII "MainMenu1"
004EE070  ASCII "Arkiv1"                    ASCII "Arkiv1"
```

Luego en sus referencias

```
004EDCB4  $^ E9 9F6EF1FF    JMP 00404B58                    SE handling routine
004EDCB9  .  E8 0272F1FF    CALL 00404EC0
004EDCBE  >  68 D0070000    PUSH 7D0                        Time = 2000. ms
004EDCC3  .  E8 1815F2FF    CALL <JMP.&kernel32.Sleep>      KERNEL32.Sleep
004EDCC8  .  807D EB 00     CMP BYTE PTR SS:[EBP-15],0
004EDCCC  .v 74 2D          JE SHORT 004EDCFB
004EDCCE  .  6A 11          PUSH 11                         Type = MB_OKCANCEL|MB_ICONHAND|MB_DEFBUTTON1|MB_APPLM
004EDCD0  .  68 80DD4E00    PUSH 004EDD80                   Caption = "Too old key"
004EDCD5  .  68 8CDD4E00    PUSH 004EDD8C                   Text = "The code is too old. Please visit http://www.
004EDCDA  .  8B45 FC        MOV EAX,DWORD PTR SS:[EBP-4]
004EDCDD  .  E8 46DAF7FF    CALL 0046B728
004EDCE2  .  50             PUSH EAX                        hOwner
004EDCE3  .  E8 B4A7F1FF    CALL <JMP.&user32.MessageBoxA>  USER32.MessageBoxA
004EDCE8  .  83F8 02        CMP EAX,2                       CONST 2 => IDCANCEL
004EDCEB  .v 75 39          JNE SHORT 004EDD26
004EDCED  .  A1 34A95100    MOV EAX,DWORD PTR DS:[51A934]
004EDCF2  .  8B00           MOV EAX,DWORD PTR DS:[EAX]
004EDCF4  .  E8 2772F9FF    CALL 00484F20
004EDCF9  .v EB 2B          JMP SHORT 004EDD26
004EDCFB  >  6A 11          PUSH 11                         Type = MB_OKCANCEL|MB_ICONHAND|MB_DEFBUTTON1|MB_APPLM
004EDCFD  .  68 DCDD4E00    PUSH 004EDDDC                   Caption = "Wrong code"
004EDD02  .  68 E8DD4E00    PUSH 004EDDE8                   Text = "Incorrect code. Please verify the code and tr
004EDD07  .  8B45 FC        MOV EAX,DWORD PTR SS:[EBP-4]
004EDD0A  .  E8 19DAF7FF    CALL 0046B728
004EDD0F  .  50             PUSH EAX                        hOwner
004EDD10  .  E8 87A7F1FF    CALL <JMP.&user32.MessageBoxA>  USER32.MessageBoxA
004EDD15  .  83F8 02        CMP EAX,2                       CONST 2 => IDCANCEL
004EDD18  .v 75 0C          JNE SHORT 004EDD26
004EDD1A  .  A1 34A95100    MOV EAX,DWORD PTR DS:[51A934]
004EDD1F  .  8B00           MOV EAX,DWORD PTR DS:[EAX]
004EDD21  .  E8 FA71F9FF    CALL 00484F20
004EDD26  >  33C0           XOR EAX,EAX
```

Al subir encontrando un comienzo de rutina

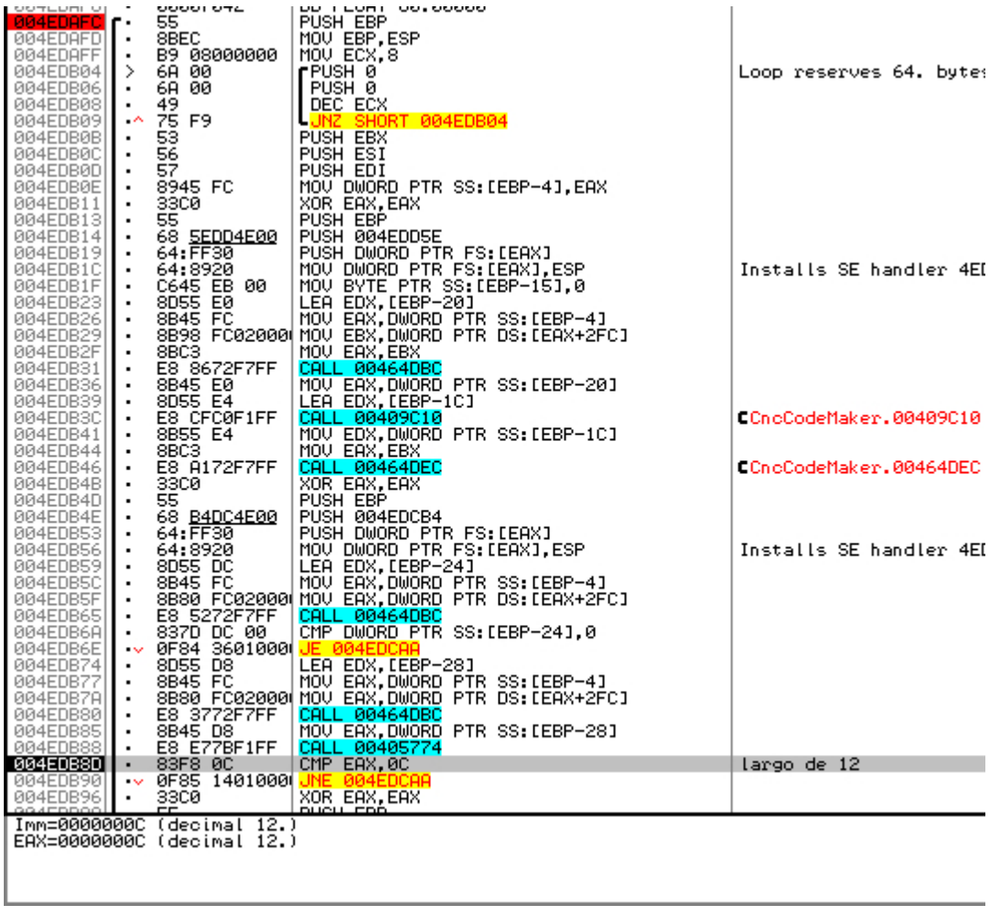
```
IAE8  .  07000000     DD 00000007
IAEC  .  6B 65 79 2E  ASCII "key.dat"                 ASCII "key.dat"
IAF3     00           DB 00
IAF4  .  0050C347     DD FLOAT 100000.0
IAF8  .  00007042     DD FLOAT 60.00000
IAFC  .  55           PUSH EBP
IAFD  .  8BEC         MOV EBP,ESP
IAFF  .  B9 08000000  MOV ECX,8
IB04  >  6A 00        PUSH 0                            Loop reserves 64. bytes on the stack
IB06  .  6A 00        PUSH 0
IB08  .  49           DEC ECX
IB09  .^ 75 F9        JNZ SHORT 004EDB04
IB0B  .  53           PUSH EBX
IB0C  .  56           PUSH ESI
IB0D  .  57           PUSH EDI
IB0E  .  8945 FC      MOV DWORD PTR SS:[EBP-4],EAX
IB11  .  33C0         XOR EAX,EAX
IB13  .  55           PUSH EBP
IB14  .  68 5EDD4E00  PUSH 004EDD5E
IB19  .  64:FF30      PUSH DWORD PTR FS:[EAX]
IB1C  .  64:8920      MOV DWORD PTR FS:[EAX],ESP        Installs SE handler 4EDD5E
IB1F  .  C645 EB 00   MOV BYTE PTR SS:[EBP-15],0
IB23  .  8D55 E0      LEA EDX,[EBP-20]
IB26  .  8B45 FC      MOV EAX,DWORD PTR SS:[EBP-4]
IB29  .  8B98 FC020000 MOV EBX,DWORD PTR DS:[EAX+2FC]
```

Tenemos rutinas para ver

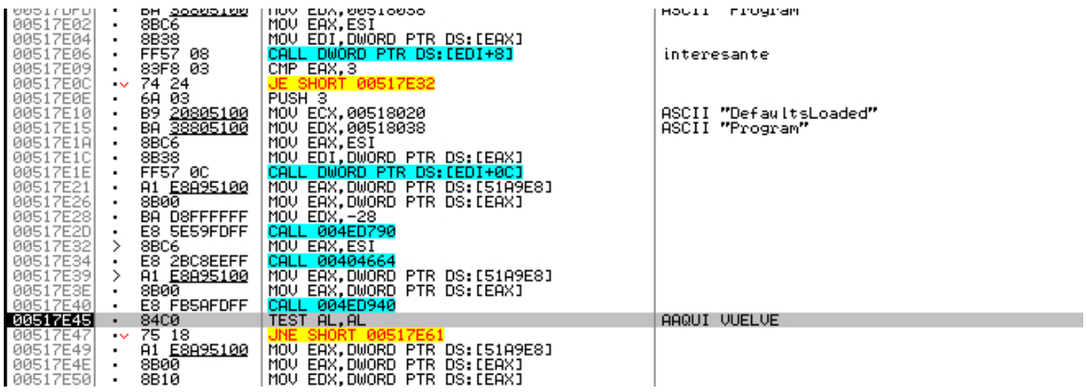
```
004ED259     11           DB 11
004ED25A     00           DB 00
004ED25B  .  48D64E00     DD 004ED648                     Entry point
004ED25F  .  0A           DB 0A
004ED260  .  46 6F 72 6D  ASCII "FormCreate"              ASCII "FormCreate"
004ED26A     15           DB 15
004ED26B     00           DB 00
004ED26C  .  FCDA4E00     DD 004EDAFC                     Entry point
004ED270  .  0E           DB 0E
004ED271  .  62 74 6E 52  ASCII "btnRefuelClick"          ASCII "btnRefuelClick"
004ED27F     13           DB 13
004ED280     00           DB 00
004ED281  .  20DE4E00     DD 004EDE20                     Entry point
004ED285  .  0C           DB 0C
004ED286  .  42 75 74 74  ASCII "Button1Click"           ASCII "Button1Click"
004ED292     12           DB 12
004ED293     00           DB 00
004ED294  .  2CDE4E00     DD 004EDE2C                     Entry point
004ED298  .  0B           DB 0B
004ED299  .  4C 61 62 65  ASCII "Label4Click"            ASCII "Label4Click"
004ED2A4     0F           DB 0F
004ED2A5     00           DB 00
004ED2A6  .  74DE4E00     DD 004EDE74                     Entry point
004ED2AA  .  08           DB 08
004ED2AB  .  46 6F 72 6D  ASCII "FormShow"                ASCII "FormShow"
004ED2B3  .  08           DB 08
004ED2B4  .  54 4B 65 79  ASCII "TKeyForm"                ASCII "TKeyForm"
004ED2BC     04           DB 04
004ED2BD     00           DB 00
004ED2BE  .  D8684500     DD 004568D8
004ED2C2  .  74714500     DD 00457174
```

Siguiendo con ello observo si hay algo que me llame la atención

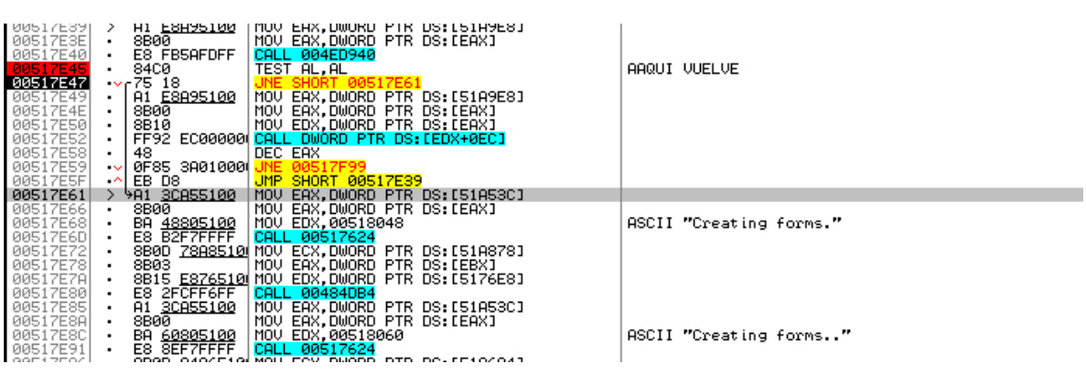
Ahora su funcionamiento del serial ingresado solicita que sea de un largo de 12decimal



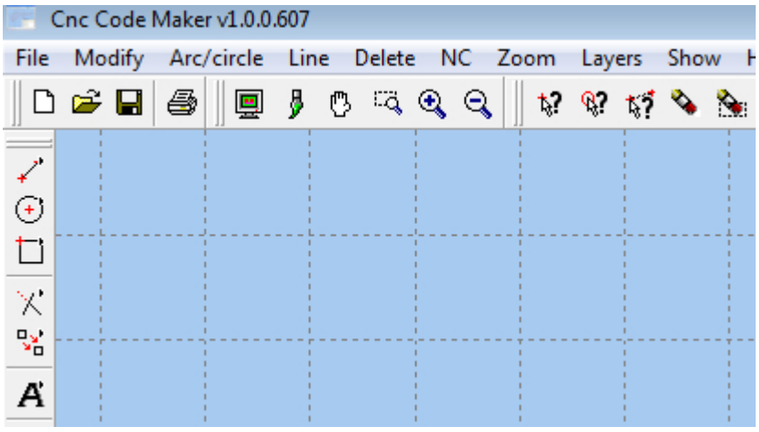
LUEGO DE JUGAR UN POCO CON LA ESTRUCTURA del serial logro salir de ahí probando cosas como AAAAAAAAAAAA o bien con otras letras LEFWVQNUPZ , luego de salir de ahí tengo una idea y no caigo en los mensajes (evitando los saltos)



Luego si queremos que correctamente proceda debemos llegar siempre a que salte desde su vuelta, para ello necesitamos que eax valga un valor distinto de 0:



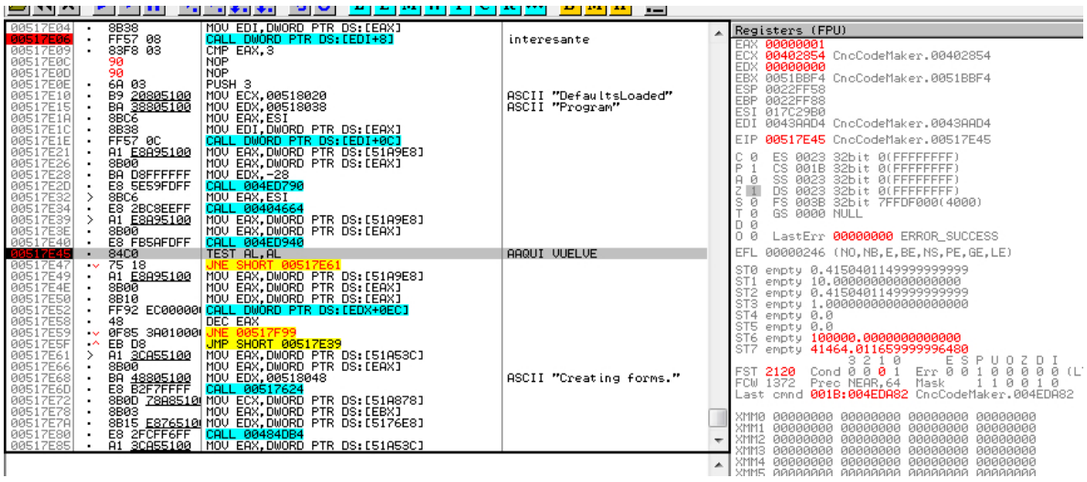
Luego estamos otra vez con el programa funcional(porque forzamos el salto)

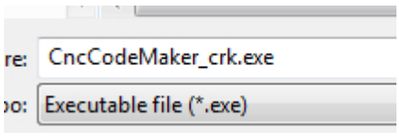


Ahora con otro intento (reiniciamos la aplicación)

Si nopeo (aplico NOP) en la comparación con el 3, claramente me figura 1 en eax y no necesito parchar más (hasta cuando vuelva a expirar en teoría, pero ya no expirará)

(pues saltará 00517E47 a 00517E61 y continuará el programa como si nada)



Guardo los cambios del nop 

y

claramente corre bien, si adelanto o atraso el reloj el _crk corre de lo más bien este programa no expirará
Programa derrotado, no fue tan complicado. Saludos a la lista de Crackslatinos y amigos ^^

Saludos Apuromafo