
How to reverse |VerTex|'s/TGC Crackme 03

Cracker: **stealthFIGHTER**

Target: | **VerTex** | 's Crackme 03

Tools: W32Dasm
Hiew
ProcDump
Brain

Where: <http://move.to/tgc>

Protection: Packed, Anti-Soft-Ice, Anti-W32Dasm, Serial number

Sorry for my English, it's not my mother language.

Step 1:

=====
Run crackme > Soft-Ice detected > run Procdump > unpack it > save it. Open W32Dasm and disassemble it. Click on SDR button.
You should find these strings: **nUMEGa SOFTICE (Win95 or WinNT)**
URSoft W32Dasm was found!

=====
Double click on the first. You'll land here:
=====

:0040100C E8C7030000	call 004013D8	
:00401011 85C0	test eax, eax	
:00401013 7518	jne 0040102D	
:00401015 6A10	push 00000010	; First check.

Possible StringData Ref from Data Obj -> "Error!"

:00401017 6858214000	push 00402158
----------------------	---------------

Possible StringData Ref from Data Obj -> "nUMEGa SOFTICE (Win95 or WinNT) "
-> "found!"

:0040101C 68BD204000	push 004020BD
:00401021 6A00	push 00000000

Reference To: USER32.MessageBoxA, Ord:0000h

:00401023 E87E040000	Call 004014A6
----------------------	---------------

Reference To: KERNEL32.ExitProcess, Ord:0000h

:00401028 E8A5050000	Call 004015D2
----------------------	---------------

Referenced by a (U)nconditional or (C)onditional Jump at Address:
:00401013(C)

Possible StringData Ref from Data Obj -> "URSoft W32Dasm Ver 8.9 Program "
-> "Disassembler/Debugger"

:0040102D 6852204000	push 00402052
:00401032 6A00	push 00000000

Reference To: USER32.FindWindowA, Ord:0000h

```

:00401034 E855040000      |
:00401039 83F800          |
:0040103C 7418            |
:0040103E 6A10            |
                        Call 0040148E
                        cmp eax, 00000000
                        je 00401056
                        push 00000010
; Second check!

```

Possible StringData Ref from Data Obj -> "Error!"

```

:00401040 6858214000      |
                        push 00402158

```

Possible StringData Ref from Data Obj -> "URSoft W32Dasm was found!"

```

:00401045 6811214000      |
                        push 00402111

```

=====

First check: If we have Soft-Ice loaded > we don't jump and we get the message > we must change **JNE** to **JE**. (if you don't know how to do it read my tutorials).

Once you changed it (W32Dasm is still running) run crackme > another message > Second check!

=====

Second check: When we have W32Dasm running > we get the message > **EAX=1**. If we don't have W32Dasm loaded > we don't get the message > **EAX=0**,

=====

But we cannot change **JE** to **JNE** because when you close W32Dasm and run the crackme you'll get the message > execute the call and you should be here:

=====

```

:0040148E FF2530324000      |
                        Jmp dword ptr [00403230]

```

=====

Note the offset (**A8E**) and run HIEW > select decode mode (press twice [ENTER]) > press F5 and enter the offset > press F3 and F2 to and type:

```

mov eax, 0 [ENTER]
ret      [ENTER]

```

Press F9 to update the file. Now we every time get **EAX=0** so we don't get the message.

=====

Now run the crackme > all checks defeated!

=====

Serial: Enter something > That was wrong... > note it > go to W32Dasm > click on SDR button > find the message > double click on it > you are here:

=====

Reference To: KERNEL32.CompareStringA, Ord:0000h

```

:0040130A E8CF020000      |
:0040130F 83F802          |
:00401312 741D            |
:00401314 6A10            |
                        Call 004015DE
                        cmp eax, 00000002
                        je 00401331
                        push 00000010
; Bad cracker!

```

Possible StringData Ref from Data Obj -> "Tha Game Cracker"

```

:00401316 685F214000      |
                        push 0040215F

```

Possible StringData Ref from Data Obj -> "That was the wrong password" ; You are here!

=====

EAX=1 > compared with **2** > we don't jump > bad cracker.

Double click on **cmp eax, 00000002** and note the offset (90F).

=====

Go to HIEW and change:

```

cmp eax, 00000002 to cmp eax, 00000001

```

=====

Enter anything > Well done!

=====

CrackMe cracked!

=====

=====



=====

If I make a mistake, please e-mail me
stealthFIGHTER@another.com

You can also find me on the web:

=====
