
How to make a keygen for 2Sweet's Crackme 2.c

Cracker: **stealthFIGHTER**

Target: **2Sweet's Crackme 2.c**

Tools: SoftIce
Delphi
Brain

Where: <http://2sweet.tsx.org/>

Protection: Name/serial

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

Step 1 (finding a valid serial):

=====
Run CrackMe >>> Enter your name/serial >>> go to the SoftIce and type **bpx hmemcpy** [ENTER] and go back >>> push **Check** button. (We are kicked into SoftIce. CrackMe breaks twice cause we have 2 input boxes). Press F11 to see the caller. You should be here:
=====

:00442219	MOV	EAX, [EBP-04]	
:0044221C	CALL	00403BF8	
:00442221	CALL	004078C4	
:00442226	MOV	ECX, EBX	
:00442228	MOV	EBX, 00000001	; EBX=1; here will be stored our name(it starts at 1)
:0044222D	MOV	EAX, 00000001	; EAX=1; here will be stored length of name(it starts at 1)
:00442232	CMP	EAX, ECX	
:00442234	JG	00442245	
:00442236	MOV	EDX, [EBP-04]	; At this time EDX=1
:00442239	MOVZX	EDX, BYTE PTR [EAX+EDX-01]	; Move first char of the name into EDX
:0044223E	INC	EAX	; Increase counter
:0044223F	ADD	EBX, EDX	; Add first char to EBX
:00442241	CMP	EAX, ECX	; Was it last char?
:00442243	JLE	0044223C	; If not jump back to MOV EDX, [EBP-04]
:00442245	MOV	EAX, EBX	; Move final value of name in EAX(EAX=ASCII name + 1)
:00442247	SHL	EAX, 04	; SHL the value in EAX
:0044224A	ADD	EAX, EBX	; EAX=EAX+EBX
:0044224C	MOV	EBX, EAX	; ? EAX = Real serial

Step 2 (coding a keygen):

- =====
1. Input name
2. Make a sum of all chars of the name
3. Add 1 to sum
4. SHL sum, 04
5. Add (SHL sum, 04) to sum
6. Display serial
=====

Ending: Source is in this package. Remember, its very hard for me to explain it because English is not my mother language!

=====
CrackMe keygened!
=====



=====

If I make a mistake, please e-mail me
to: **stealthfighter@another.com**
You can also find me on the web:

=====

-----=[<http://nitrous.hop.to/>]-----

=[<http://stealthfighter.cjb.net/>]=-

=====