
How to code a keygen for Yoda's lame CrackMe

Cracker: **stealthFIGHTER**

Target: **Yoda's lame CrackMe**

Tools: Soft-Ice
Delphi
Brain

Where: <http://crackme.cjb.net/>

Protection: Name/serial (fake button)

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

Step 1:

=====

The **check!** button is fake. When you push the button every time pops up the same error message => the serial is calculated when each key is pressed in 2nd input box => we will use **HMEMCPY** breakpoint in Soft-Ice.
Write your name and serial >> go to Soft-Ice and type **bpx hmemcpy** and go back >> now type into the 2nd input box some number >> Soft-Ice pops up >> press 15 times [F12] till you are in crackme code >> you should be here:

=====

```
CALL 00403364          ; Set length of our name
CMP  EAX, 04           ; Compare it with 4
JLE                      ; If the length = 4 or if it is < 4 then jump
```

=====

Continue by pressing [F10] till you are here (I will rip off interesting code only)(note - the ':' means some lines above):

=====

```
MOVZX ESI, BYTE PTR [EAX]      ; Move first char of our name into ESI
:                               ; Type ? ESI and you should see the char
MOVZX EDI, BYTE PTR [EAX+01]   ; Move second char of our name into EDI
:                               ; Type ? EDI and you should see the char
MOVZX EAX, BYTE PTR [EAX+03]   ; Move fourth char of our name into EAX
:                               ; Here is the char moved into [EBP-08]
MOZXV EAX, BYTE PTR [EAX+04]   ; Move the fifth char of our name into EAX
:                               ; Type ? EAX and you should see the char
ADD EDI, ESI                  ; EDI = EDI + ESI (fist char plus second char)
:
ADD EAX, [EBP-08]              ; EAX = EAX + [EBP-08] (fourth char plus fifth char)
:
IMUL EDI, EAX                  ; EDI = EDI * EAX (multiply those sums)
:
MOV ESI, EDI                  ; Move EDI to ESI
:                               <-----
LEA EAX, [EBP-14]              ;
CALL 00405614                  ; Get the path of the crackme (e. g. C:\Windows\temp)
MOV EAX, [EBP-14]              ;
CALL 00403364                  ; Get length of the path and put into EAX (EAX = length of the path)
IMUL ESI                      ; EAX = EAX * ESI (Multiply the length of the path with ESI -----)
:                               ; Type ? EAX and you should see your right serial
CALL 00403474                  ; Compare our serials (type d eax and you should see your right serial)
JNZ 004258E0                  ; If they are not same then jump
```

=====

=====
All done!
=====



=====

If I you found 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/>]--

=====