

-----  
How to find serial in ScareByte/TGC CrackMe Nr. 9  
-----

Cracker: **stealthFIGHTER**

Target: **Scarebyte CrackMe Nr. 9**

Tools: Soft-Ice  
Brain

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

Protection: Serial number, P-Code (VB crackme uses VB40032.dlls).

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

-----  
Step 1:  
-----

=====  
Run crackme > enter your registration details > press check > nothing happened. Go to Soft-Ice and type:  
**Bpx widechartomultibyte** [enter] (= this is VB breakpoint)

=====  
Go back and erase last digit from your s/n (s/n is calculated every time when you press some key) > Soft-Ice pops-up > press F5  
(i think 19x) then press F11 to get to caller > you're somewhere in VB40032.dll. Now type

=====

**s 0 L FFFFFFFF 56,57,8B,7C,24,10,8B,74,24,0C,8B,4C,24,14** [enter] ; This is in HEX.

=====  
In your **data window** you'll find this:  
=====

**:OF79B348** 56 57 8B 7C 24 10 8B 74 24 0C 8B 4C 24 14 .. .. VW.#\$.I\$.3.....

=====  
Now type **bpx OF79B348** [enter] (= > this is where we find the string). Now press F11 > Soft-Ice breaks just at this place:  
=====

**: OF79B348** PUSH ESI ; Push our fake s/n.  
**: 0F79B349** PUSH EDI ; Push our real s/n.

=====  
Stop at **PUSH ESI** and type **d ESI** and you'll see your fake s/n in **w.i.d.e.c.h.a.r.** At **PUSH EDI** type **d EDI** and you'll see in your  
data window your real s/n. (of course in widechar)

=====

CrackMe registered!

=====



=====

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

You can also find me on the web:

=====

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

---

---