
How to find a serials in Bomby

Cracker: **stealthFIGHTER**

Target: **Bomby v7.3**

Tools: Soft-Ice
Brain

Where: <http://www.sf-soft.de/>

Protection: Two serial numbers.

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

Step 1:

=====
Run Bomby > Help > Registration. There are two input boxes. Type anything (I entered 224466 and 113355). Push "OK" button >
These codes are...

=====
Go to Soft-Ice (Ctrl+D) and type: **BPX HMEMCPY (HighMEMoryCoPY)**. Go back (F5). Push "OK" button and Soft-Ice pops-up.

=====
We have 2 input boxes => press **F5** (if you press F5 two times you'll get the message) and **F11** to get to the caller. Now keep pressing **F12** until you get to the program code (it's about 10 times). You should be here:

=====
:00410DFF 6BC831 imul ecx, eax, 00000031
:00410E02 33D2 xor edx, edx
:00410E04 8A15E0F24100 mov dl, byte ptr [0041F2E0]
:00410E0A 8BDA mov ebx, edx
:00410E0C 03CB add ecx, ebx
:00410E0E 83C13E add ecx, 0000003E
:00410E11 3B4C240C **cmp ecx, dword ptr [esp+0C]** ; Compare our 1st fake s/n with 1st real s/n
:00410E15 7541 **jne 00410E58** ; If they are not same, jump to bad boy
:00410E17 6BC023 imul eax, 00000023
:00410E1A C1E203 shl edx, 03
:00410E1D 03C2 add eax, edx
:00410E1F 83C00E add eax, 0000000E
:00410E22 3B442410 **cmp eax, dword ptr [esp+10]** ; Compare our 2nd fake s/n with 2nd real s/n
:00410E26 7530 **jne 00410E58** ; If they are not same, jump to bad boy
=====

=====
Now at **00410E11** in the right-top corner you should see: **SS:XXXXXXXX=00036CD2**. Now type ? **36CD2** and you can see our 1st fake code (224466). Now type ? **ECX** and you should see our 1st real code. Note it!

=====
At **00410E22** in the right-top corner you should see: **SS:XXXXXXXX=0001BACB**. Now type ? **1BACB** and you can see our 2nd fake code (113355). Now type ? **EAX** and you should see our 2nd real code. Note it!

=====
Try to register again. It's correct!
=====



=====

If I make a mistake, please e-mail me

stealthfighter@another.com

You can also find me on the web:

=====

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

<http://nitrous.hop.to/>