
How to find a serial in Online

Cracker: **stealthFIGHTER**

Target: **Online v1.1**

Tools: W32DASM
Brain

Where: <http://www.microlynxsystems.com/>

Protection: Program is looking for one registration number. As easy as killing bunnies with axes.

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

Step 1:

=====
Start Online - registration nag pops-up. Press <Register> button and fill it -> <OK> -> Incorrect registration code. Please try again.
Note this text.

=====
Run W32Dasm and open Online.exe in it. Now click on SDR button (String Data Reference) and find the text of the message. Double click on it. You should be here:

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

:00465DE9(C) ; Conditional jump!

```
:00465E42 6A00          push 00000000
:00465E44 668B0D6C5F4600  mov cx, word ptr [00465F6C]
:00465E4B B202          mov dl, 02
```

Possible StringData Ref from Code Obj -> "Incorrect registration number. "

-> "Please try again." ; We land here!

=====
Now click on the **Goto code location** and enter **00465DE9** (this is the conditional jump). You should be here:
=====

Possible StringData Ref from Code Obj -> "Online Registration"

```
:00465DCE B8B05E4600      mov eax, 00465EB0
:00465DD3 E8ACB9FEFF      call 00451784
:00465DD8 84C0          test al, al
:00465DDA 747B          je 00465E57
:00465DDC 8B45FC          mov eax, dword ptr [ebp-04]
```

Possible StringData Ref from Code Obj -> "Onl11REG0"

; Looks like a serial?

```
:00465DDF BACC5E4600      mov edx, 00465ECC
:00465DE4 E84FDF99FF      call 00403D38
:00465DE9 7557          jne 00465E42
:00465DEB 6A00          push 00000000
:00465DED 668B0DD85E4600  mov cx, word ptr [00465ED8]
:00465DF4 B203          mov dl, 03
```

; Call fake s/n.

; You land here.

=====

=====

Good for now. The program compare our fake s/n with **OnI11REG0**. If it's bad, jump to bad boy. (jne 00465E42). So note the real reg. number and try to register again. 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>]=----

=====