
How to make a keygen for Alteros 3D

Cracker: **stealthFIGHTER**

Target: **Alteros 3D v1.0**

Tools: SoftIce
Delphi
Brain

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

Protection: Name/serial

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

Step 1:

=====
Run Alteros > press big blue button :) > Options > Registration > type your name and s/n > Register > bad cracker. Go to SoftIce and type **bp x hmemcpy**. Go back > Register > we're in SoftIce. Press 3x F5 and F11 to get to the caller. Now press F12 about 11x till you're in program code. You should be here:
=====

:004A3D8B E884FFF5FF	call 00403D14
:004A3D90 85C0	test eax, eax
:004A3D92 7E13	jle 004A3DA7
:004A3D94 BA01000000	mov edx, 00000001

Referenced by a (U)nconditional or (C)onditional Jump at Address:
:004A3DA5(C)

:004A3D99 8B4DFC	mov ecx, dword ptr [ebp-04]
:004A3D9C 0FB64C11FF	movzx ecx, byte ptr [ecx+edx-01]
:004A3DA1 03F1	add esi, ecx
:004A3DA3 42	inc edx
:004A3DA4 48	dec eax
:004A3DA5 75F2	jne 004A3D99

Referenced by a (U)nconditional or (C)onditional Jump at Address:
:004A3D92(C)

:004A3DA7 8975EC	mov dword ptr [ebp-14], esi
:004A3DAA DB45EC	fild dword ptr [ebp-14]
:004A3DAD E8E2EBF5FF	call 00402994
:004A3DB2 69C041010000	imul eax, 00000141
:004A3DB8 8BF0	mov esi, eax
:004A3DBA 3B75F8	cmp esi, dword ptr [ebp-08]
:004A3DBD 7562	jne 004A3E21

=====
Explanation:
=====

call 00403D14	; Check, how long is our name
test eax, eax	
jle 004A3DA7	; Move length of our name into EAX; type ? EAX and you'll see the length

=====

```

=====
mov ecx, dword ptr [ebp-04]      ; Move our name into ECX; type D ECX and you'll see your name
movzx ecx, byte ptr [ecx+edx-01] ; Move HEX value of our first character of our name into ECX
add esi, ecx                     ; Store value into ESI
inc edx                         ; Type ? ESI and you'll see your first character or your name
dec eax                         ; Decrease length of our name
jne 004A3D99                    ; If it was the last character of our name, continue, if not jump back to mov ecx,
                                ; dword ptr [ebp-04] and move HEX value of the next character of our name
                                ; into ESI

```

=====

This loop ends, when the sum of all HEX values of all characters our name is stored in ESI. When the loop ends, type ? **ESI** and you'll see the sum value.

=====

Example how we got the sum:
 As a name I typed: stealthFIGHTER
 The loop in **ASCII**:
 =====

$s+t+e+a+l+t+h+F+I+G+H+T+E+R = \text{sum in ESI}$

=====

The loop in **HexaDecimal**:
 =====

$73+74+65+61+6C+74+68+46+49+47+48+54+45+52 = 4FE$

=====

The sum of all HEX values is 4FE. At **jne 004A3D99** you'll see the sum in **ESI**. Now type ? **ESI** and you'll get **Decimal** value of our sum (? **4FE = 1278**).

=====

End of example.
 =====

```

call 00402994                  ; Move sum to EAX
imul eax, 00000141             ; Multiply sum (value in EAX) with 141 (this number is in HEX) and store it in EAX
mov esi, eax                   ; Move result to ESI
cmp esi, dword ptr [ebp-08]    ; Compare real serial in ESI with fake serial in dword ptr [ebp-08]
jne 004A3E21                   ; If they are not same, jump to bad cracker

```

=====

Example of multiplication (**imul eax, 00000141**):
 My sum of my name is **4FE** in HEX (**1278** in Decimal).
 Multiplication in **HexaDecimal**:
 =====

$EAX = EAX * 141$
 $EAX = 4FE * 141$
 $EAX = 6427E$; When you type ? **6427E** you'll get **410238**

=====

Multiplication in **Decimal**:
 =====

$EAX = EAX * 321$; When you type ? **141** you'll get **321**
 $EAX = 1278 * 321$
 $EAX = 410238$; Type ? **ESI** (at **cmp esi, dword ptr [ebp-08]**) and you'll get real serial

=====

Now the keygen:
 =====

1. Read name
 2. Make a sum of the Decimal(or HexaDecimal) values of all characters of name
 3. Multiply sum with 321(in Decimal) or 141(in HexaDecimal)
 4. Display serial
- =====

=====

Now the source code (core only),(in Delphi, i use v3.0):

=====

```
Procedure TForm1.KeyGen;
```

```
// -- Variations --
```

```
Var name: String;
```

```
fs, i, counter : Integer;
```

```
// -- KeyGen code
```

```
If Length(Edit1.Text) <> 0 Then
```

```
Begin
```

```
name := Edit1.Text;
```

```
counter := 0;
```

```
For i := 1 To Length(Name) Do
```

```
counter := counter + Ord(Name[i]);
```

```
fs := 321;
```

```
Edit2.Text := IntToStr(counter * fs);
```

```
End
```

```
; Set counter to 0
```

```
; This line and the line below is similar to movzx ecx, byte ptr [ecx+edx-01]
```

```
; (continue: this is converting of our name into Decimal format)
```

```
; A constant in Decimal (141 in HEX)
```

```
; Multiplication; similar to imul eax, 00000141
```

=====

The information that we are registered is in \Alteros 3D\settings.ini. To unregister the program erase settings.ini.

=====

All done!

=====



=====

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/>]--

=====