

-----  
How to reverse LucisArt Adobe PhotoShop Plug-in  
-----

Cracker: **stealthFIGHTER**

Target: **LucisArt v1.0**

Tools: W32DASM  
Hiew  
Brain

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

Protection: Disabled "APPLY" function.

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

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

=====  
Run PhotoShop > Use the plug-in > apply plug-in > NAG pops-up: "**LucisArt Registration**: This copy of ...<blah blah>". Note this text.

=====  
Run W32DASM and disassembly **LUCISART.8BF** file. Click SDR window > search for the text > nothing. Go to **Search > Find text...** and enter **LucisArt Registration** and press [ENTER]. You should find only **1** string:

=====  
Name: **DialogID\_009A**, # of Controls=004, Caption:"**LucisArt Registration**", ClassName:"" ; Here you are!

001 - ControlID:0001, Control Class:"BUTTON" Control Text:"OK"  
002 - ControlID:FFFF, Control Class:"STATIC" Control Text:"This copy of LucisArt is not licensed and can only be used to ....."  
003 - ControlID:FFFF, Control Class:"STATIC" Control Text:"To see examples of what can be done with LucisArt and to ....."  
004 - ControlID:FFFF, Control Class:"STATIC" Control Text:"Thank you for trying LucisArt."

=====  
**DialogID\_009A** is the name of the NAG. Lets find it. Again go to **Search > Find text...** and enter **DialogID\_009A**. You find this (only one string):

=====  
Referenced by a CALL at Address:  
:10007E92 ; Note this!

```
:10009290 8B442404      mov eax, dword ptr [esp+04]
:10009294 8B0D287D0110      mov ecx, dword ptr [10017D28]
:1000929A 6A00              push 00000000
:1000929C 6840920010        push 10009240
:100092A1 50                push eax
```

Possible Reference to Dialog: **DialogID\_009A** ; Here you are!

=====  
Press [Shift+F12] (=Goto Code Location) and enter **10007E92**. You should be here:

=====  
Referenced by a (U)nconditional or (C)onditional Jump at Address:  
: **10007E1B(C)** ; Note this!

```
:10007E91 57                push edi
:10007E92 E8F9130000        call 10009290 ; You land here!
:10007E97 A1B87D0110        mov eax, dword ptr [10017DB8]
:10007E9C 83C404            add esp, 00000004
:10007E9F 8B08              mov ecx, dword ptr [eax]
:10007EA1 6A02              push 00000002
```

=====

The **CALL 10009290** calls window "LucisArt Registration: This copy...." If we NOP it we don't get the window only, but the filter won't be apply. If you scroll up you will see **(C)onditional jump (10007E1B)**. Press [Shift+F12] and enter **10007E1B**. You should be here:

=====

:10007DF9 FF1528010110	Call dword ptr [10010128]	
:10007DFF A1B87D0110	mov eax, dword ptr [10017DB8]	
:10007E04 6A00	push 00000000	
:10007E06 50	push eax	
:10007E07 E926FFFFFF	jmp 10007D32	
:10007E0C 85ED	test ebp, ebp	
:10007E0E 0F85CA020000	jne 100080DE	
:10007E14 E8A7CAFFFF	call 100048C0	; Are we registered?
:10007E19 84C0	test al, al	
:10007E1B 7474	je 10007E91	; Here you are!
:10007E1D 8B0DB87D0110	mov ecx, dword ptr [10017DB8]	
:10007E23 68B47D0110	push 10017DB4	
:10007E28 57	push edi	
:10007E29 51	push ecx	

=====

If we are registered we don't jump. If we are not registered we jump to bad cracker. So if we change **JE** to **JNE** we don't jump to bad cracker. Double click on **JE 10007E91** and note the offset (7E1B).

=====

Run HIEW > open **LUCISART.8BF** > press twice [ENTER] to decode mode. Press F5 and enter the offset. Press F3 and change **74** to **75** and save file (F9).

=====

Try to apply the filter again > you did it!

=====

=====



=====

If I make a mistake, please e-mail me  
**stealthFIGHTER@another.com**  
You can also find me on the web:

=====

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

