
How to reverse Photo/Graphic Patterns Demo [Auto F/X]

Cracker: **stealthFIGHTER**

Target: **Photo/Graphic Patterns Demo for Adobe Photoshop**

Tools: W32Dasm
HIEW
Brain

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

Protection: Disabled "Apply" function, NAGs

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

Step 1:

=====
Run AP and try to apply the Photo/Graphic Patterns filter >> "Apply is disabled ...blah..." message.
Run W32Dasm and disassemble the file **AFXPGP.8bf** >> then search for the text "**disabled**" >> only 1 string >> here:
=====

* Referenced by a (U)nconditional or (C)onditional Jump at Address:
:10005D0B(C)

```
:10005D1D 8B45E4      mov eax, dword ptr [ebp-1C]
:10005D20 50              push eax
:10005D21 E8C66D0200    call 1002CAEC
:10005D26 83C404      add esp, 00000004
:10005D29 8B4510      mov eax, dword ptr [ebp+10]
:10005D2C C60000      mov byte ptr [eax], 00
:10005D2F 8B45E4      mov eax, dword ptr [ebp-1C]
:10005D32 50              push eax
:10005D33 E8207F0200    call 1002DC58
:10005D38 83C404      add esp, 00000004
:10005D3B 8B4D14      mov ecx, dword ptr [ebp+14]
:10005D3E 668901      mov word ptr [ecx], ax
:10005D41 8B4508      mov eax, dword ptr [ebp+08]
:10005D44 50              push eax
:10005D45 6A11      push 00000011
```

* Possible StringData Ref. from Data Obj -> "Apply is **disabled** in the demo "
-> "version. Order the full version "
-> "today!"

; When we want to apply the plug-in, we get
; this message

```
:10005D47 6868250310      push 10032568
:10005D4C E8DFB8FFFF      call 10001630
:10005D51 83C40C      add esp, 0000000C
:10005D54 8B4508      mov eax, dword ptr [ebp+08]
:10005D57 50              push eax
:10005D58 E8A3E60100      call 10024400
:10005D5D 83C404      add esp, 00000004
:10005D60 668B45F8      mov ax, word ptr [ebp-08]
:10005D64 E972000000      jmp 10005DDB
:10005D69 8B450C      mov eax, dword ptr [ebp+0C]
:10005D6C 50              push eax
:10005D6D E851750000      call 1000D2C3
```

; Here is executed the bitmap window(NAG)

; This **JMP** kicks us to the end of the call
; and the plug-in is not executed
; (see below – it is in the same colour)

```

:10005D72 83C404      add esp, 00000004
:10005D75 50          push eax
:10005D76 E858FEFFFF  call 10005BD3      ; Check, if we chose some effects
:10005D7B 83C404      add esp, 00000004
:10005D7E 85C0        test eax, eax
:10005D80 0F8534000000  jne 10005DBA      ; If not, message pops-up
:10005D86 8B4510        mov eax, dword ptr [ebp+10]
:10005D89 C60000        mov byte ptr [eax], 00
:10005D8C 8B45E4        mov eax, dword ptr [ebp-1C]
:10005D8F 50          push eax
:10005D90 E8C37E0200  call 1002DC58
:10005D95 83C404      add esp, 00000004
:10005D98 8B4D14        mov ecx, dword ptr [ebp+14]
:10005D9B 668901        mov word ptr [ecx], ax
:10005D9E 8B4508        mov eax, dword ptr [ebp+08]
:10005DA1 50          push eax
:10005DA2 6A11        push 00000011

```

* Possible StringData Ref from Data Obj -> "**Please choose an effect before** " ; He he, but when we want to apply the
-> "**applying the filter.**" ; plug-in without choosing an effect we
; get this message.

```

:10005DA4 68B0250310      push 100325B0
:10005DA9 E882B8FFFF  call 10001630
:10005DAE 83C40C        add esp, 0000000C
:10005DB1 668B45F8        mov ax, word ptr [ebp-08]
:10005DB5 E921000000  jmp 10005DDB

```

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

```

:10005D80(C)

:10005DBA 8B4510        mov eax, dword ptr [ebp+10]
:10005DBD C60001        mov byte ptr [eax], 01
:10005DC0 8B45E4        mov eax, dword ptr [ebp-1C]
:10005DC3 50          push eax
:10005DC4 E88F7E0200  call 1002DC58
:10005DC9 83C404      add esp, 00000004
:10005DCC 8B4D14        mov ecx, dword ptr [ebp+14]
:10005DCF 668901        mov word ptr [ecx], ax
:10005DD2 668B45F8        mov ax, word ptr [ebp-08]
:10005DD6 E900000000  jmp 10005DDB

```

* Referenced by a (U)nconditional or (C)onditional Jump at Addresses:

:10005D64(U), :10005DB5(U), :10005DD6(U)

```

:10005DDB 5F          pop edi
:10005DDC 5E          pop esi
:10005DDD 5B          pop ebx
:10005DDE C9          leave
:10005DDF C3          ret

```

=====

If we don't want to be kicked to the end of the call (we want the plug-in to be executed) we must **NOP** the **JMP**. If we NOP the plug-in it will continue in executing. Note the offset (5164) and run HIEW >> decode mode >> F5 >> enter offset >> and change bytes from:

E972000000

to:

9090909090

Save your work [F9] and try to apply the filter again (don't forget to choose some effect) >> Bad cracker message ... NAG ... and then filter is executed! Now we want to piss off the "Apply is disabled..." message and the bitmap window. When you push the "APPLY" button you're here in the code:

=====

```

=====
:10005D44 50          push eax
:10005D45 6A11        push 00000011          ; Here you pushed the APPLY button

* Possible StringData Ref. from Data Obj -> "Apply is disabled in the demo " ; and the message box pops-up
  -> "version. Order the full version "
  -> "today!"

:10005D47 6868250310  push 10032568
:10005D4C E8DFB8FFFF  call 10001630
:10005D51 83C40C      add esp, 0000000C
:10005D54 8B4508      mov eax, dword ptr [ebp+08]
:10005D57 50          push eax
:10005D58 E8A3E60100    call 10024400          ; Here is executed the bitmap window
:10005D5D 83C404      add esp, 00000004
:10005D60 66B45F8     mov ax, word ptr [ebp-08]
:10005D64 E972000000    jmp 10005DDB          ; You should have this already NOPed!
:10005D69 8B450C      mov eax, dword ptr [ebp+0C] ; Here the plug-in continue in executing
:10005D6C 50          push eax

```

So that when we jump from **push 00000011** (at 10005D45) to **mov eax, dword ptr [ebp+0C]** (at 10005D69) we won't see any messages or other windows >> once you're at 10005D45 note the offset (5145) >> run HIEW >> decode mode >> F5 >> enter offset >> F3 >> F2 >> and type:

JMP 000005169

>> [ENTER] >> [ESC] >> F9 to save your work. Apply plug-in again >> great! – no bullshit. Now the last piece – NAG at the beginning. If you look at the code after the bad message (Apply is disabled...blah) there are two **CALLs** >> right here:

```

=====
* Possible StringData Ref. from Data Obj -> "Apply is disabled in the demo " ; and the message box pops-up
  -> "version. Order the full version "
  -> "today!"

:10005D47 6868250310  push 10032568
:10005D4C E8DFB8FFFF  call 10001630
:10005D51 83C40C      add esp, 0000000C
:10005D54 8B4508      mov eax, dword ptr [ebp+08]
:10005D57 50          push eax
:10005D58 E8A3E60100    call 10024400          ; Here is executed the bitmap window
:10005D5D 83C404      add esp, 00000004
:10005D60 66B45F8     mov ax, word ptr [ebp-08]
:10005D64 E972000000    jmp 10005DDB          ; You should have this already NOPed!

```

I don't know what does the 1st but the 2nd executes the bitmap window >> so in W32Dasm push call button and you should be here:

Referenced by a CALL at Addresses:

```

: 10005940 , :10005D58 , :1000773E , :10007ECC          ; These 4 calls execute the window bitmaps
                                                         ; (at the beginning or after "Apply is dis..."
                                                         ; message)
:10024400 55          push ebp          ; Here is place for our offensive
:10024401 8BEC      mov ebp, esp
:10024403 83EC04     sub esp, 00000004
:10024406 53          push ebx
:10024407 56          push esi
:10024408 57          push edi

```

```

:10024409 6A00          push 00000000
:1002440B 68D0450210    push 100245D0
:10024410 8B4508          mov eax, dword ptr [ebp+08]
:10024413 50              push eax

```

=====

When some of these 4 calls are executed you get the ugly NAG (or window bitmap telling you that we have the demo). But when we replace **PUSH EBP** (at 10024400) with **RET** (RET = RETURN FROM THE CALL) we won't get the NAG, because the calls are returned immediately >> double click on **PUSH EBP** and note the offset (23800) >> run HIEW >> decode mode >> F5 >> enter offset [enter] >> F3 >> F2 >> and replace

PUSH EBP

With

RET

>> [enter] >> [esc] >> F9 to save our work. Try to apply filter again ... great. If you were not successful drop me email.

=====

All done!

=====



=====

If I you found 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/>]=--

=====