
How to get a full version of Ulead Type.Plug-in

Cracker: **iNFiNiTY**

Target: **Ulead Type.Plug-in Trial Version**

Tools: W32DASM
Hiew
Brain

Where: http://www.ulead.com/webutilities

Protection: Time limit and NAG.

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

Step 1:

======
Install plug-in and run Photoshop. Use **Ulead Type.Plug-in** > NAG pops-up > push "OK" > main window pops-up > click on the **About** button > it is the same NAG we see at the beginning!
======
Go to the plugin's directory and find file **Tp_about.dll**. I think it is file containing the NAG.
======
Open W32DASM and disassemble **Tp_about.dll**. Click on the SDR window > shit! – only bullshit. Click on the **Exports** button. There is a pair of strings only. But one is interesting: **IsFullVersion** > that we have full version of this plug-in in our hands. Double click on it. You should be here:
======

```
Exported fn(): IsFullVersion - Ord:0003h                    ; You'll land here
:100038D0 83EC04            sub esp, 00000004
:100038D3 833D6CB1001000    cmp dword ptr [1000B16C], 00000000
:100038DA 750F              jne 100038EB                    ; If we have full version > jump


:100038DC E86FFFFFFF        call 10003850                   ; Some internal check procedure
:100038E1 85C0              test eax, eax
:100038E3 7506              jne 100038EB                    ; If not jump to bad cracker
:100038E5 33C0              xor eax, eax
:100038E7 83C404            add esp, 00000004
:100038EA C3                ret



* Referenced by a (U)nconditional or (C)onditional Jump at Addresses:
:100038DA(C), :100038E3(C)

:100038EB 8D442400          lea eax, dword ptr [esp]
:100038EF 6A00              push 00000000
:100038F1 8B4C240C          mov ecx, dword ptr [esp+0C]
:100038F5 50                push eax
:100038F6 6A01              push 00000001

* Possible StringData Ref from Data Obj ->"SpecialBuild"     ; Here it builds full version
                                |
:100038F8 6878B10010        push 1000B178
:100038FD 51                push ecx
:100038FE E85DF5FFFF        call 10002E60                   ; Another check procedure
:10003903 83C414            add esp, 00000014
:10003906 85C0              test eax, eax
:10003908 741D              je 10003927                     ; Jump to bad cracker
:1000390A 817C240014050000  cmp dword ptr [esp], 00000514
```

```
:10003912 7513                  jne 10003927                    ; Jump to bad cracker
:10003914 B801000000            mov eax, 00000001
:10003919 83C404                add esp, 00000004
:1000391C C70568D80010010000    mov dword ptr [1000D868], 00000001
:10003926 C3                    ret                             ; We need the program to pass this RET!
```

======
The first jump (**750F jne 100038EB**) is executed if we have full version. We should patch it. Note the offset (**2CDA**). Run HIEW and open **Tp_about.dll.** Press two times [ENTER] to select decode mode. Press **F5** and enter the offset. Press **F3** and change
======

750F JNE to> **EB0F JMPS**

======
Press **F9** to update. Go to Photoshop and try the plug-in > shit! > message (due some internal check procedure) saying us we have corrupted plug-in or some like this. Go back to W32DASM. Below the **jne 100038EB** you could see call of the checking routine: **E86FFFFFFF call 10003850.** Note the offset (**2CDC**).
======
Go to the HIEW and enter the offset. We have to **NOP** the call (=this means NO oPeration). Change:
======

E86FFFFFFF call 10003850 to> **9090909090 NOP 10003850**

======
Try plug-in now > the same bullshit. Back to W32DASM. Below the call there is a jump (**7506 jne 100038EB**). But we **cannot NOP** it because we want the "**SpecialBuild**" procedure would be executed. (if we change it it will jump to bad cracker and we are back with trial version)
======
Scroll down > Below "**SpecialBuild**" there are two jumps (**741D je 10003927** and **7513 jne 10003927**). Note their offsets (**2D08**, **2D12**). Think a bit. The "**SpecialBuild**" procedure must be executed > it must pass the **RET** (**10003926 C3 ret**) below the 2 jumps. So we cannot change them to 75 and 74 but we must **NOP**ed them again. (If you don't understand, mail me).
======
Go to HIEW (for the last time I hope) and enter the 1st offset and change:
======

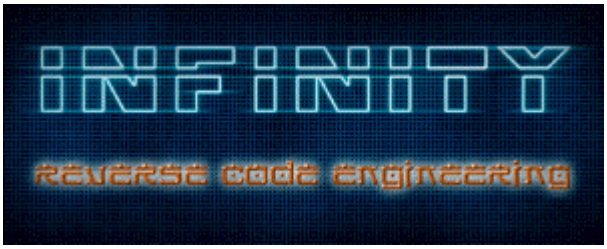
741D je to> **9090 NOP**

======
Press **F9** to update. Enter the 2nd offset and change:
======

7513 jne to> **9090 NOP**

======
Press **F9** to update the file.
======
Try the plug-in > NO NAG. Change the date > NO NAG. Press "About" button > we have FULL VERSION!
======

==========



==========
==========
If I make a mistake, please e-mail me
to: **infinity@2000net.com**
You can also find me on the web:
==========
----==[**http://nitrous.hop.to/**]==----
-==[**http://infinity2001.cjb.net**]==-
==========

==========
Or at Public Tutorial Search Engine
==========
---==[**http://pubtsem1.cjb.net/**]==---
==========
==========
[Thanks to all crackers on the web!]
==========