
How to reverse HTML Autorunner

Cracker: **stealthFIGHTER**

Target: **HTML Autorunner v1.15**

Tools: W32Dasm
HIEW
Brain

Where: http://www.win-software.com/

Protection: NAG

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

Step 1:

==========
In the directory with the **CDSTART.EXE** you should have **autorun.inf** and **index.html** file. Inside the autorun.inf you should have these lines:

[autorun]
open=index.html

Now run the CDSTART.EXE >> NAG >>"This software has not been ... blah" >> Look at the caption of the window: "**Copyright Notice**" >> note this text. Run W32Dasm and disassemble CDSTART.EXE and search for text Copyright Notice >> text found on line 32:
==========

Name: **DialogID_0069**, # of Controls=013, Caption: "**Copyright Notice**", ClassName: "DialogAsMain"

==========
DialogID_0069 = Our dialog window with **Copyright Notice** caption. Now search for the text DialogID_0069 >> text found on line 2191:
==========

Referenced by a (U)nconditional or (C)onditional Jump at Address:
:00401E98(C)

```
:00401E9F 33C0              xor eax, eax
:00401EA1 A0988B4000        mov al, byte ptr [00408B98]
:00401EA6 85C0              test eax, eax
:00401EA8 7518              jne 00401EC2                ; If we're registered => jump
:00401EAA 6A00              push 00000000               ; if not => Nag
:00401EAC 685A224000        push 0040225A
:00401EB1 6A00              push 00000000

Possible Reference to Dialog: DialogID_0069             ; Our DialogID

:00401EB3 6A69              push 00000069
:00401EB5 8B0D7C894000      mov ecx, dword ptr [0040897C]
:00401EBB 51                push ecx

Reference To: USER32.DialogBoxParamA, Ord:0093h

:00401EBC FF1524714000      Call dword ptr [00407124]   ; Here you get the Nag
```
==========

==========
If we change the jump (**jne 00401EC2**) so, that it jumps every time - we don't get the Nag >> note the offset of the jump (1EA8) >> Run HIEW >> decode mode >> F5 (enter offset) >> change from:

7518

to

7418

>> F9 >> Run again >> No Nag.
======
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/]**=-

==========