# HOW TO REVERSE *WinWeather 3.0*

## *Tutorial by UmE*

***Introduction***: in this tutorial I'll try to explain you how to reverse WinWeather 3.0. It has a time trial protection (30 days) and a nag screen to kill!! ☺

***Necessary tools:*** Wdasm 8.9, SoftIce 3.24 or better.

***Program description:*** WinWeather version 3.0, Weather.exe, 1.021.472 bytes.

***PARENTAL ADVISORY: this tutorial is cracking oriented!!!***

***Step 1***: when you start the program for the first time you'll see a nag screen that tells you that WinWeather is shareware and you can use it for a 30 days time trial period; if you push the "Continue free trial" button the program start. Let's change our system date putting it one month forward. Run the program again and a message box will appear telling you: "Your free trial period is over!…." Another nag screen gives you two choices: "Order for only…." Or "Exit…". Let's see what we can do!! ☺

***Step 2***: press Ctrl+D to enter in SoftIce and set a breakpoint on the GETLOCALTIME function (syntax: bpx getlocaltime, I've tried the getsystemtime function before but it don't works). Press Ctrl+D to return to the operating system and run the program….istantly you'll be in SoftIce again. Notice that if you have any application in use there will be a lot of call to the GETLOCALTIME function because it's commonly used by a lot of programs. At every call (in my case I've had 3 calls) you got to push F11 in SoftIce to see where is the caller. When you'll see under the caller code a line like this,

----------WEATHER!CODE+…..----------

you know you're in the right place: you're inside WinWeather code!!! Ok, now let's trace the code…..we can see:

```
014F:00454FAF  MOVZX     EAX,WORD PTR [EBP-04] <-Retrives the currents seconds
014F:00454FB3  PUSH      EAX
014F:00454FB4  MOVZX     EAX,WORD PTR [EBP-06] <-Retrives the currents minutes
014F:00454FB8  PUSH      EAX
014F:00454FB9  MOVZX     EAX,WORD PTR [EBP-08] <-Retrives the currents hours
014F:00454FBD  PUSH      EAX
014F:00454FBE  MOVZX     EAX,WORD PTR [EBP-0A] <-Retrives the day (1,2,…,31)
014F:00454FC2  DEC       EAX
014F:00454FC3  PUSH      EAX
014F:00454FC4  MOVZX     EAX,WORD PTR [EBP-0E] <-Retrives the month (1,2,…,12)
014F:00454FC8  DEC       EAX
014F:00454FC9  PUSH      EAX
014F:00454FCA  MOVZX     EAX,WORD PTR [EBP-10] <-Retrives the year
014F:00454FCE  ADD       EAX,FFFFF894
014F:00454FD3  PUSH      EAX
014F:00454FD4  CALL      00454E24
```

You can see what the program retrives by typeing: d ebp-… .Notice that what you read is in exadecimal format (year 1999 is 7CFh)
Now if we continue to treace we find:

```
014F:0041013F  SUB       EAX,EDX
014F:00410141  MOV       ECX,00015180
014F:00410146  CDQ
014F:00410147  IDIV      ECX
014F:00410149  MOV       EDX,0000001E                <-Put 1E in EDX (1Eh=30dec)
014F:0041014E  SUB       EDX,EAX                     <-Sub EAX from EDX
014F:00410150  MOV       [004700EC],EDX              <-Moves EDX in 004700EC
014F:00410156  CMP       DWORD PTR [004700EC],00     <-Compares 004700EC & 0
014F:0041015D  JLE       0041016C                    <-Jump if 004700EC is less
                                                       than 0
```

From this piece of code we can understand that EAX contains the number of days that you've used WinWeather. For example if you've used it for 35 days you have:

EAX=35
EDX= 1E (30 in decimal)
004700EC= EDX-EAX = -5

and the program jumps to 0041016C ("Your free trial period is over!!").
Notice that if the JLE is not verifed you have:

```
014F:0041015F  CMP       EAX, 1E
014F:00410106  JG        0041016C
```

This means that there is another control if the number of days you've used winweather is greater than 30. Just nop the two conditional jumps and the program will work forever!!!.
Let's kill the nag screen!!!
We got to intercept the call that generates the nag screen so open Wdasm and dissamble the program. Go to "Functions" → "Imports…" menu and see which function is call in the USER32 DLL…..the nag screen is a typical window generated by the function CREATEDIALOG…… In the list of the functions called by user32.dll we can see CREATEDIALOGPARAMA. Let's enter in SoftIce and place a breakpoint on the createdialogparama. Run the program……you're in SoftIce. Push F11 and see the address where the function is called. Return in Wdasm and go to the address that you've seen before in SoftIce. You now are in:

```
* Referenced by a CALL at Addresses:
|:00412559   , :0042193A   , :00422206   , :004380AD
|
:0044BB40 55                  push ebp
:0044BB41 8BEC                mov ebp, esp
:0044BB43 83C4F8              add esp, FFFFFFF8
:0044BB46 8B4508              mov eax, dword ptr [ebp+08]
:0044BB49 C7401401000000      mov [eax+14], 00000001
:0044BB50 8B1568BB4700        mov edx, dword ptr [0047BB68]
:0044BB56 8955F8              mov dword ptr [ebp-08], edx
:0044BB59 8B156CBB4700        mov edx, dword ptr [0047BB6C]
:0044BB5F 8955FC              mov dword ptr [ebp-04], edx
:0044BB62 8945F8              mov dword ptr [ebp-08], eax
:0044BB65 8B5510              mov edx, dword ptr [ebp+10]
```

```
:0044BB68 8955FC              mov dword ptr [ebp-04], edx
:0044BB6B 8D55F8              lea edx, dword ptr [ebp-08]
:0044BB6E 52                  push edx
:0044BB6F FF3564BB4700        push dword ptr [0047BB64]
:0044BB75 FF750C              push [ebp+0C]
:0044BB78 FF7010              push [eax+10]
:0044BB7B FF356A004700        push dword ptr [0047006A]

* Reference To: USER32.DialogBoxParamA, Ord:0000h          <-This is the call!!
                        |
:0044BB81 E85F4A0100          Call 004605E5
:0044BB86 59                  pop ecx
:0044BB87 59                  pop ecx
:0044BB88 5D                  pop ebp
:0044BB89 C3                  ret
```

Looking above we can see that this piece of code is referenced by 4 calls. Just nop the calls and the nag screen is killed!

Ok, that's all for now!!! I hope that this tutorial could be useful for someone!!

Greetings to Volatitlity and all the Immortal Descendants!

Contact me at ume15@hotmail.com