AN EXAMPLE OF SERIAL FISHING: *AXMAN 2.12*

Tutorial by UmE

Introduction: in this tutorial I'll try to explain you how to find the correct serial number in AxMan 2.12 using the HMEMCPY API function. This tutorial is very simple and I've write it only for educational porpouse as a compendium of the Volatility's tutorials about serial fishing using HMEMCPY.

Necessary tools: SoftIce 3.24 or better

Program description: AxMan version 2.12, AxMan.exe, 141.824 bytes.

PARENTAL ADVISORY: this tutorial is cracking oriented!!!

Step 1: when you run the program you can notice an annoying nag screen that tells you that AxMan is shareware and you can use it for a trial period of 30 days (I think that the disclaimers are very boring!!). Click on the "Agree and register" button and a dialog will appear: insert your name (I've entered Ume), the Company name (I've entered Ume1) and the registration number (I've entered 12345).

Step 2: press Ctrl+D to enter in SoftIce and set a breakpoint on the HMEMCPY function (bpx HMEMCPY). As you know Windows use the HMEMCPY function to read and store the strings that you have entered in memory for use them later. Press Ctrl+D again to return to the operating system and press the "OK" button in the dialog…..TA DA!!!! You're in SoftIce again. This call to the HMEMCPY function reads the serial number that you've entered. Press Ctrl+D and you will be putted in SoftIce again (this time the function reads the company name). Press Ctrl+D for the last time and you'll be in SoftIce again: this is the good time (the function reads the name that you've entered).

Step 3: press F11 to return to the piece of code that has called the HMEMCPY function. You should be here:

```
173F:0B40  CALL         KERNEL!HMEMCPY
173F:0B45  PUSH         WORD PTR [DI]
173F:0B47  CALL         KERNEL!LOCALUNLOCK
173F:0B4C  MOV          AX,SI
173F:0B4E  POP          SI

 ------------------------------- USER (0A)-----------------------------------
```

HMEMCPY function send you on a piece of code that is not inside the program that we want to crack. In fact under the displayed code you can notice the written:

USER (0A)

You got to trace in SoftIce pressing F10 until that written change in

AXMAN!.text + 14AA

This tell you that now you're into the Axman.exe code. You might see the following line:

```
014F:004024AC  LEA       EAX,[EBP-18]
```

If you type d EBP-18 in SoftIce you will see:

```
0157:0065D02C 31 32 33 34 35 00 2E F4-02 00 A0 60 02 00 00 01  12345.....`....
0157:0065D03C 00 01 40 06 BF 05 BF 05-64 D0 65 00 63 36 F7 BF  ..@.....d.e.c6..
0157:0065D04C 70 09 00 00 11 01 00 00-01 00 00 00 60 09 00 00  p...........`...
0157:0065D05C 97 3E 96 60 57 01 00 00-78 D0 65 00 94 28 F9 BF  .>.`W...x.e..(..
0157:0065D06C BC 60 97 3E 97 3E 00 00-00 00 00 00 79 1A F7 BF  .`.>.>......y...
0157:0065D07C B6 60 00 00 9C FA 65 00-2E 19 F7 BF 97 3E 96 60  .`....e......>.`
0157:0065D08C 00 00 00 00 96 60 97 3E-02 00 00 00 00 00 02 02  .....`.>........
0157:0065D09C 00 00 F4 60 02 00 2E 3B-02 00 8F 16 2E F4 3F 27  ...`...;......?'
```

Wow!!! Your registration number!!!
Continue to press F10…

```
014F:004024AF  PUSH      EAX                 ←---- puts your SN in the stack
014F:004024B0  LEA       EAX,[EBP-80]
```

Type d EBP-80 and you'll see:

```
0157:0065CFC4 55 6D 65 00 00 00 4F 4B-00 60 00 00 99 28 F9 BF  Ume1..OK.`...(..
0157:0065CFD4 79 1A F7 BF 10 60 00 00-9C FA 65 00 2E 19 F7 BF  y....`....e.....
0157:0065CFE4 97 3E F0 5F 00 00 00 00-F0 5F 97 3E 00 00 00 00  .>._....._.>....
0157:0065CFF4 06 02 00 00 4E 60 02 00-2E 3B 03 0C 03 0C 03 0C  ....N`...;......
0157:0065D004 40 06 4D 09 2E F4 02 00-76 60 02 00 54 60 FB 3C  @.M.....v`..T`.<
0157:0065D014 A3 02 C0 C0 C0 00 6D 00-80 F4 24 09 24 09 B4 06  ......m...$.$...
0157:0065D024 BF 05 44 60 0E 0C 00 01-31 32 33 34 35 00 2E F4  ..D`....12345...
0157:0065D034 02 00 A0 60 02 00 00 01-00 01 40 06 BF 05 BF 05  ...`......@.....
```

Your company name……

Press F10 twice…

```
014F:004024B3  PUSH      EAX              ←- puts your company name in stack
014F:004024B4  LEA       EAX,[EBP-00E8]
```

Type d EBP-00E8 and you'll see:

```
0157:0065CFB6 8F 16 CC 60 85 63 5F 17-02 00 34 07 76 20 55 6D  Ume..c_...4.v Um
0157:0065CFC6 65 00 00 00 4F 4B 00 60-00 00 99 28 F9 BF 79 1A  e...OK.`...(..y.
0157:0065CFD6 F7 BF 10 60 00 00 9C FA-65 00 2E 19 F7 BF 97 3E  ...`....e......>
0157:0065CFE6 F0 5F 00 00 00 00 F0 5F-97 3E 00 00 00 00 06 02  ._....._.>......
0157:0065CFF6 00 00 4E 60 02 00 2E 3B-03 0C 03 0C 03 0C 40 06  ..N`...;......@.
0157:0065D006 4D 09 2E F4 02 00 76 60-02 00 54 60 FB 3C A3 02  M.....v`..T`.<..
0157:0065D016 C0 C0 C0 00 6D 00 80 F4-24 09 24 09 B4 06 BF 05  ....m...$.$.....
0157:0065D026 44 60 0E 0C 00 01 31 32-33 34 35 00 2E F4 02 00  D`....12345.....
```

Your Name…..

Now, if you continue to trace the program with F10 you'll see:

```
014F:004024BA  PUSH          EAX          ← puts your name in stack
014F:004024BB  CALL          00402546     ← compute the right SN
014F:004024C1  ADD           ESP, 08      ← update the stack
014F:004024C3  TEST          EAX, EAX     ← test the two SN (entered and right)
014F:004024C7  JGE           00……         ← jump if the SN entered is OK
```

The function at 004024BB is very interesting because it's before the critical test. We think that in this function the program compute the right serial number based on the datas that you've entered. In fact with the PUSH EAX instruction showed before we pass to the function the parameters to analyze. If we trace that function we can see:

```
014F:00402546  PUSH          EBP
014F:00402547  MOV           EBP,ESP
014F:00402549  SUB           ESP,18
014F:0040254C  LEA           EAX,[EBP-18]
014F:00402561  PUSH          DWORD PTR [EBP+10]
014F:00402564  PUSH          EAX
014F:00402565  CALL          00408480
014F:0040256A  POP           ECX
014F:0040256B  NEG           EAX
014F:0040256D  POP           ECX
014F:0040254C  LEA           EAX,[EBP-18]          ← very interesting!!!
```

We remember that before the function call the memory location EBP-18 holds the registration number that we have entered. Try to type d EBP-18 now and you'll get:

```
0157:0065CF24 31 31 36 2D 35 34 37 2D-38 38 30 00 44 D0 65 00  116-547-880.D.e.
0157:0065CF34 AC 24 40 00 00 00 00 00-44 D0 65 00 C0 24 40 00  .$@.....D.e..$@.
0157:0065CF44 5C CF 65 00 C4 CF 65 00-2C D0 65 00 4C D0 65 00  \.e...e.,.e.L.e.
0157:0065CF54 BC 60 00 00 98 D0 65 00-55 6D 65 00 01 00 F7 BF  .`....e.Ume.....
0157:0065CF64 C2 5F 97 3E 00 00 00 00-30 00 3C 01 5C 00 49 01  ._.>....0.<.\.I.
0157:0065CF74 00 00 BF 05 2E F4 FE 05-BF 05 0B 00 6C 5F 97 3E  ............l_.>
0157:0065CF84 42 00 00 00 00 00 00 00-AA 5F E7 A2 5F 04 00 00  B........_.._...
0157:0065CF94 00 00 02 00 C2 5F B8 5F-9C 47 5F 04 00 00 00 00  ....._._.G_.....
```

The right registration number!!!!! 116-547-880!!

Have you understan how it works? I hope so…..

I hope that this tutorial could be useful for someone.

That's all for now….greetings to Volatitlity and all the Immortal Descendants.

Contact me at ume15@hotmail.com