PuppetMaster

anorganix of ARTeam

MAY 2006

Keywords

eSellerate, PupperMaster, OllyDbg, Product Activation

1. Brief Introduction

eSellerate is an industry-leading software commerce provider focused on providing the tools and solutions for software publishers to sell more of their products. Our premier services have more tools, features and functionality than any other e-commerce provider, giving you the freedom to choose the best way to sell your software.

World-class E-commerce Systems
Giving you complete control over all of your online commerce activities, eSellerate lets you easily create a sales strategy to help you sell more of your products. We provide multiple sales solutions and supply you with real-time tools to upload content, set prices, create promotional coupons and offers, and customize the look and feel of your order forms.

Leading Affiliate Program
eSellerate also provides an Affiliate Program that has re-defined the software affiliate sales industry. If you are a software developer looking to extend your products into a broader market or a merchant interested in selling some of the hottest software titles available, eSellerate has all the tools and resources at your disposal for highly successful sales campaigns. With direct purchase and "try before you buy" formats, our proprietary technology ensures that your shoppers will find what they want and that each party is guaranteed credit for their sales.

The Right Choice
So, if you are looking for some of the most unique, advanced, and successful commerce solutions available, from our in-app sales capabilities to the basic establishment of a Web Store, eSellerate is the right choice for you.

In addition, eSellerate supports: Split Payments, Coupon discounts, Product Activation, Cross-Selling, Up-Selling, Volume Pricing, Extended Download Service, Multiple Payment Methods, Multi-Currency Support, Phone/Fax Ordering (PFO), Complete Settlement Process, Serial Number Generation.

Find out more at:
http://www.esellerate.net

2. Things needed to get started

The tools:

Required Tools
» OllyDbg » PEiD 0.94 » Stripper 2.13 (for unpacking ASProtect)

…and the target:

Target Application & Protection	
» PuppetMaster	http://www.lim.com.au/PuppetMaster/

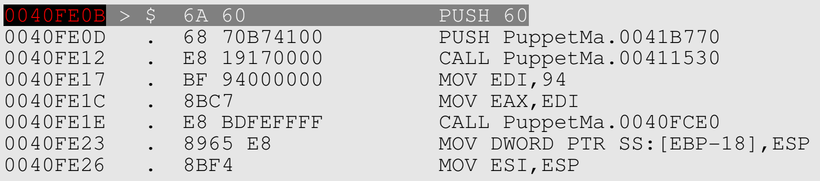
3. Getting a valid license for PuppetMaster

Download the program and install it. The first step is to open it in PEiD and notice that it's protected with ASProtect (ASProtect 2.0x Registered » Alexey Solodovnikov). I will not go over manual unpacking ASProtect, because this is not the purpose of this tutorial. Instead we will use Stripper 2.13 from Syd.

After unpacking is done, rename the original file to a different name, and the unpacked one to "PuppetMaster.exe". If doing otherwise, you will get some errors and we don't want that.

Fire up Olly and notice that the target is a typical Visual C++ app:

Target loaded in Olly



```
0040FE0B  > $  6A 60            PUSH 60
0040FE0D   .   68 70B74100      PUSH PuppetMa.0041B770
0040FE12   .   E8 19170000      CALL PuppetMa.00411530
0040FE17   .   BF 94000000      MOV EDI,94
0040FE1C   .   8BC7             MOV EAX,EDI
0040FE1E   .   E8 BDFEFFFF      CALL PuppetMa.0040FCE0
0040FE23   .   8965 E8          MOV DWORD PTR SS:[EBP-18],ESP
0040FE26   .   8BF4             MOV ESI,ESP
```

Let's run it and see what we can do to register it… Press F9 (Run) in Olly, then in the program click on "Preferences" and under the "Register" tab click on "Activate Manually".

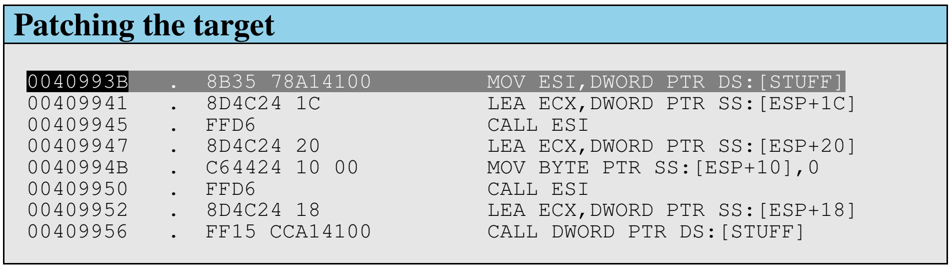
Enter a dummy serial number in the input-box, and you will receive a nice message saying that “The serial number entered does not appear to be valid”. OK, we need to bypass this check to see if we can reach the eSellerate Product Activation. We can find the message by setting BPs on the “MessageBoxA” API, and also by using the call stack, as shown below.

In computer science, a call stack is a special stack which stores information about the active subroutines of a computer program (the active subroutines are those which have been called but have not yet completed execution by returning). This kind of stack is also known as an execution stack, control stack, or function stack.

A call stack is often used for several related purposes, but the main reason for having one is to keep track of the point to which each active subroutine should return control when it finishes executing. If, for example, a subroutine “DrawSquare” calls a subroutine “DrawLine” from four different places, the code of “DrawLine” must have a way of knowing which place to return to. This is typically done by code for each call within “DrawSquare” putting the address of the instruction after the particular call statement (the “return address”) into the call stack.

Now that we know what the Call Stack is, we can use it by pressing F12 (Pause) in Olly and then Alt+K. Now, double-click on “USER32.MessageBoxTimeoutW” and scroll down a little until you see a return instruction. Put a breakpoint (F2) on the RET and resume the target (F9). Now the program is running and if you press OK in the mesage-box and Olly should break on the RET. Remove the breakpoint (F2 again) and press F8 until you get back in the target code (~5 times).

We arrive here:



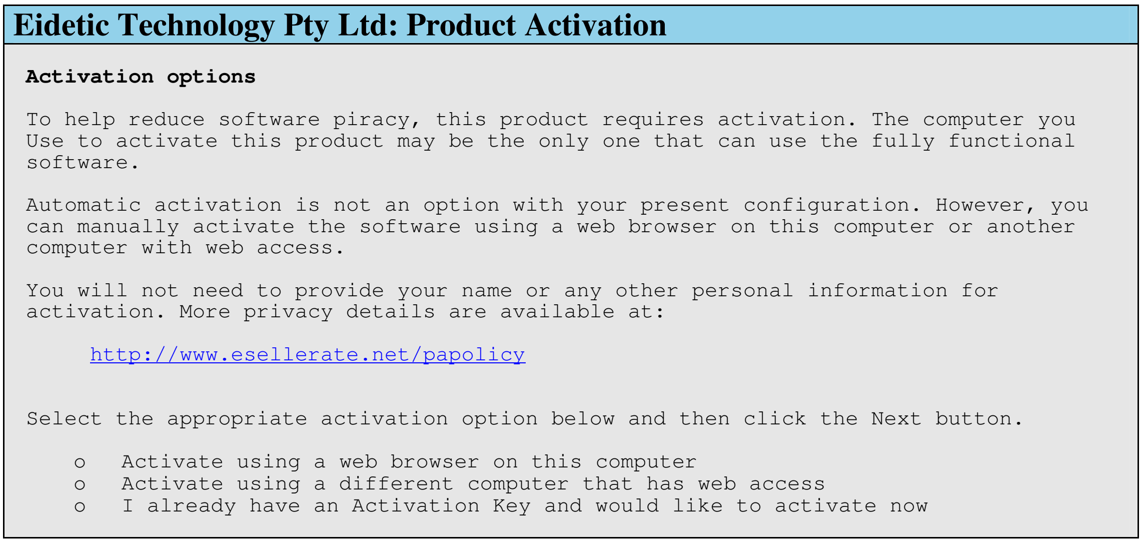
Patching the target

```
0040993B    .  8B35 78A14100        MOV ESI,DWORD PTR DS:[STUFF]
00409941    .  8D4C24 1C            LEA ECX,DWORD PTR SS:[ESP+1C]
00409945    .  FFD6                 CALL ESI
00409947    .  8D4C24 20            LEA ECX,DWORD PTR SS:[ESP+20]
0040994B    .  C64424 10 00         MOV BYTE PTR SS:[ESP+10],0
00409950    .  FFD6                 CALL ESI
00409952    .  8D4C24 18            LEA ECX,DWORD PTR SS:[ESP+18]
00409956    .  FF15 CCA14100        CALL DWORD PTR DS:[STUFF]
```

Scroll up a little and notice a JNZ at 00409901. So if this jump is not taken, the program will show the “Invalid Code” message. Let’s patch it to JMP to bypass the message-box, press F9 to continue execution, click on the “Activate” button again and this time the message is gone. We are one step closer to our goal.

NOTE: it seems that the program uses this serial verification restrict the “access” to the eSellerate Activation sequence. Now that we patched this check we can see our “Installation ID”, which is the crucial element in getting a valid “Activation Key”.

Notice that the program still requires activation:



Eidetic Technology Pty Ltd: Product Activation

Activation options

To help reduce software piracy, this product requires activation. The computer you Use to activate this product may be the only one that can use the fully functional software.

Automatic activation is not an option with your present configuration. However, you can manually activate the software using a web browser on this computer or another computer with web access.

You will not need to provide your name or any other personal information for activation. More privacy details are available at:

http://www.esellerate.net/papolicy

Select the appropriate activation option below and then click the Next button.

○ Activate using a web browser on this computer
○ Activate using a different computer that has web access
○ I already have an Activation Key and would like to activate now

Select the first option ("Activate using a web browser on this computer") and click "Next". In the new window click on the activation link (http://activate.esellerate.net) and the click on "Submit" in the web-browser page. This page acts like a key-generator for eSellerate productes, but it would be useless if we would not have the "Installation ID".

In a few seconds, you should be given a valid Activation Key of the form "xxxxxxx-xxxx-xxxxxx-xxxx-xxxxxx-xxxxxx-xxxx-xxxxxx-xxxx-xxxxxx". Switch to the running target and click on the "Next" button… in the new window enter your Activation Key from the web-browser page. When finished, click on "Activate" and the on the "Done" button.

The program should be registered now. You don't have to save the changes made in Olly, because we used that just to get to the eSellerate Activation process. You can even delete the unpacked file and put back the ASProtected one. All you have to do now is enjoy using the full version… ☺

4. Another approach: patching the program

We can also patch the program to thinks it's registered, without even using the eSellerate engine approach. From the eSellerate SDK, I found out that every program that uses the eSellerate system, also uses a "PublisherID" and "ActivationID", and they have approximately the same structure. Open the unpacked program in Olly, do a right-click and select "Search for » All referenced text strings". Now to look for string references that start with "ACT" or "PUB" (for example: ACT434528799 / PUB0830764619) and double-click on the first one that you find (start searching from the top of the list).

You should be here:

Patching the registration check

```
00404CC0  /$  51                      PUSH ECX
00404CC1  |.  56                      PUSH ESI
00404CC2  |.  8BF1                    MOV ESI,ECX
00404CC4  |.  C646 0C 00              MOV BYTE PTR DS:[ESI+C],0
00404CC8  |.  A1 80A14100             MOV EAX,DWORD PTR DS:[STUFF]
00404CCD  |.  50                      PUSH EAX
00404CCE  |.  68 80AC4100             PUSH PuppetMa.0041AC80
00404CD3  |.  8D4C24 0C               LEA ECX,DWORD PTR SS:[ESP+C]
00404CD7  |.  51                      PUSH ECX
00404CD8  |.  8D4E 58                 LEA ECX,DWORD PTR DS:[ESI+58]
00404CDB  |.  E8 E0FAFFFF             CALL PuppetMa.004047C0
00404CE0  |.  8B4424 04               MOV EAX,DWORD PTR SS:[ESP+4]
00404CE4  |.  8B48 04                 MOV ECX,DWORD PTR DS:[EAX+4]
00404CE7  |.  85C9                    TEST ECX,ECX
00404CE9  |.  74 38                   JE SHORT PuppetMa.00404D23
00404CEB  |.  83C0 08                 ADD EAX,8
00404CEE  |.  50                      PUSH EAX
00404CEF  |.  68 64A84100             PUSH PuppetMa.0041A864
00404CF4  |.  68 44A84100             PUSH PuppetMa.0041A844
00404CF9  |.  E8 AE980000             CALL PuppetMa.0040E5AC
00404CFE  |.  85C0                    TEST EAX,EAX
00404D00  |.  74 1D                   JE SHORT PuppetMa.00404D1F
00404D02  |.  8B5424 04               MOV EDX,DWORD PTR SS:[ESP+4]
00404D06  |.  6A 00                   PUSH 0
00404D08  |.  83C2 08                 ADD EDX,8
00404D0B  |.  52                      PUSH EDX
00404D0C  |.  68 64A84100             PUSH PuppetMa.0041A864
00404D11  |.  68 44A84100             PUSH PuppetMa.0041A844
00404D16  |.  E8 43980000             CALL PuppetMa.0040E55E
00404D1B  |.  85C0                    TEST EAX,EAX
00404D1D  |.  75 04                   JNZ SHORT PuppetMa.00404D23
00404D1F  |>  C646 0C 01              MOV BYTE PTR DS:[ESI+C],1
00404D23  |>  8D4C24 04               LEA ECX,DWORD PTR SS:[ESP+4]
00404D27  |.  FF15 CCA14100           CALL DWORD PTR DS:[STUFF]
00404D2D  |.  5E                      POP ESI
00404D2E  |.  59                      POP ECX
00404D2F  \.  C3                      RETN
```

Let's place a breakpoint (F2) on the PUSH ECX at 404CC0 and press F9 to run the program. When Olly breaks, start tracing with F8 until you reach the JE at 404CE9. If this jumps then the program will be unregistered, so let's NOP is. Also, as a safety measure, NOP the JE at 404D00 too, and don't forget to NOP the JNZ at 404D1D also. When running the program we notice that it's registered.

5. Conclusions

The same result was obtained in 2 different ways. Personally I would choose the first one, not only because it's cleaner (you get to keep the original exe), but also it's more exciting than the plain patching operation of a program.

Well, this is the end of this story, I hope all the things said here will be useful to understand future versions of eSellerate. I suggest as usual to use this material for learning purposes only, and not for cracking programs. **Thank you for reading this tutorial!**

Disclaimer

All the code provided with this tutorial is free for public use, just make a greets to the authors and the ARTeam if you find it useful. Don't use these concepts for making illegal operation, all the info here reported are only meant for studying and to help having a better knowledge of application code security techniques.

6. Greetings

Thank you Pilli for your support! You are the best!
Thanks to all my friends from ARTeam – some of the coolest people I ever met!

[ARTeam] [EXETools] [all the RO scene] [bLaCk-eye] [vybez_mR]