



---

### COOKIE-TUTORIAL

---

After installing it check if the target is packed or not:

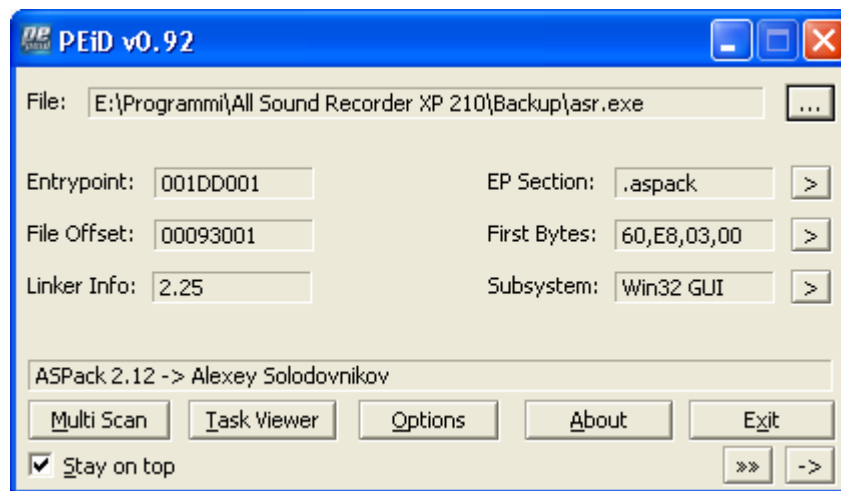


Fig. 1 Checking about the packer.

Use Stripper V2.07 final in order to unpack the target in easily way, then when you ve done it make another check to take a look about programming language:

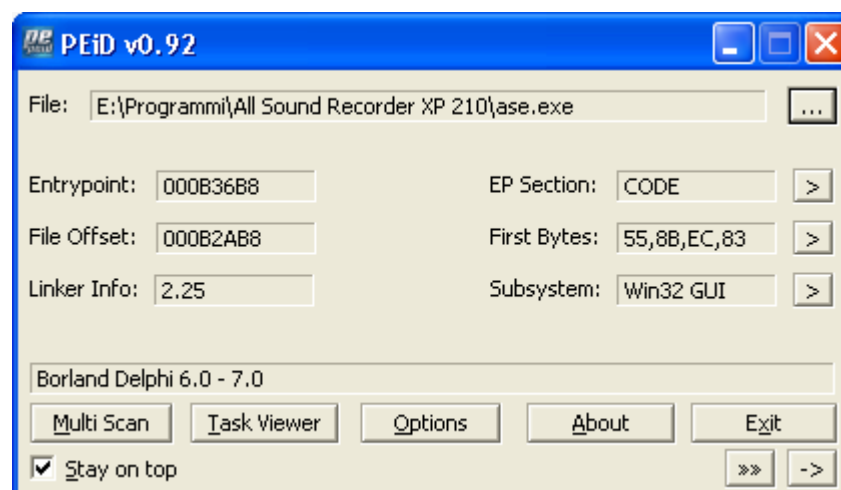


Fig. 2 Check about programming language after unpacking.

Now you can also check about some crypto signatures or CRC integrity check:

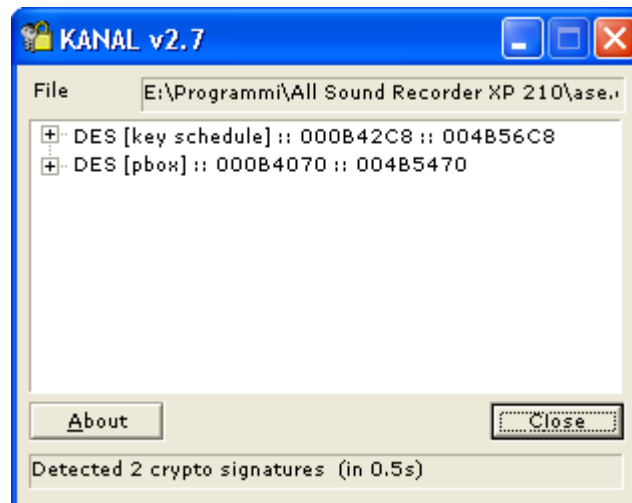


Fig. 3 Crypto signatures.

Load unpacked target into OllyDbg and use the *Search for -> All referenced text string* feature to search the *serial* text string:

0048D1E4	ASCII "open",0	
0048D248	MOV EAX,asi.0048D2B4	ASCII "Your serial number have not been accept,0/please contact "
0048D270	MOV EAX,asi.0048D2FC	ASCII "please input your name?"
0048D2B4	ASCII "Your serial numb"	
0048D2C4	ASCII "er have not been"	
0048D2D4	ASCII " accept.0/please"	
0048D2E4	ASCII " contact ",0	
0048D2FC	ASCII "please input You"	
0048D30C	ASCII "r name?",0	

Fig. 4 Searching about serial text string.

Double click on the highlighted row, you land here:

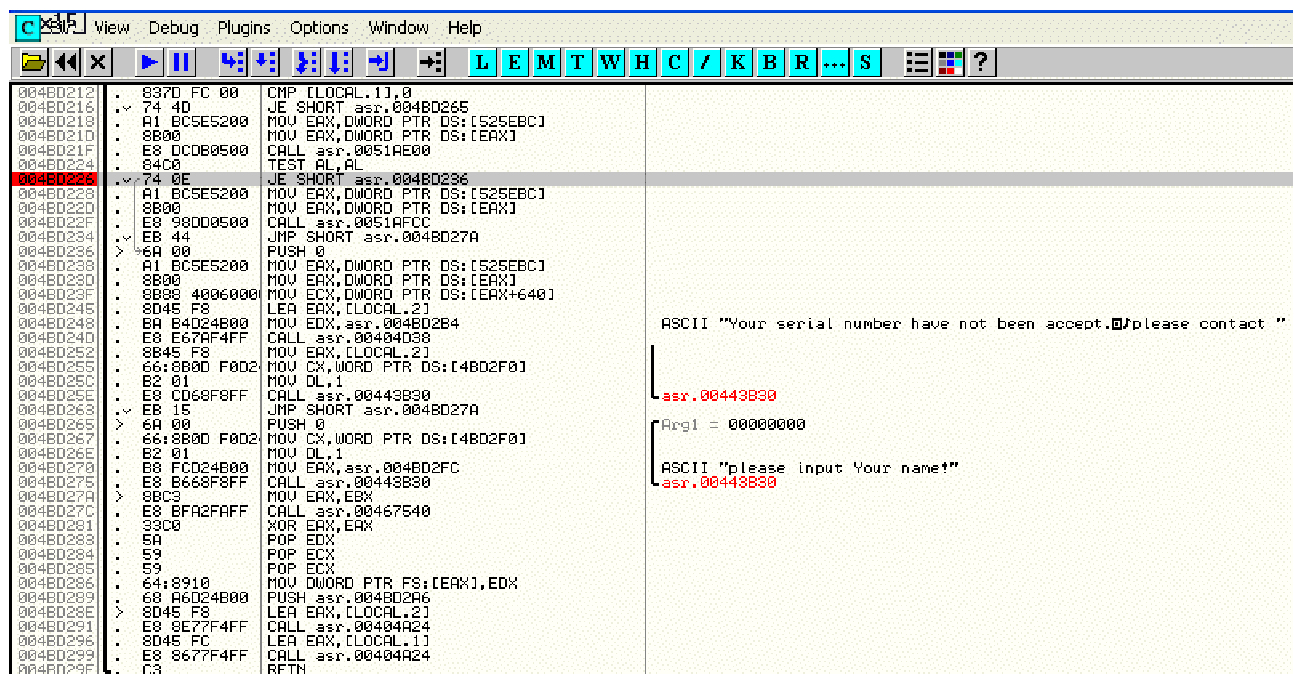


Fig. 5 Conditional jump about right serial.

Scroll up into the code, the conditional jump on 004BD226 is related to serial verification, now is time to enter into the CALL 0051AE00, make a F8 step analysis, scroll down until you reach

the 0051AF16 address, there is a check about serial which you've entered (pointed on EAX) with the right one (pointed to EDX):

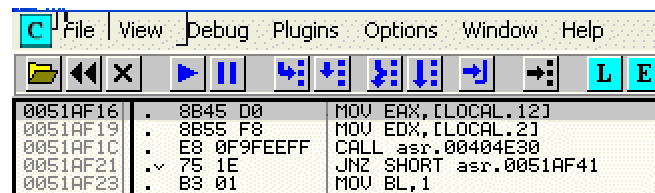


Fig. 6 Original code.

In order to make all serial accepted, simply change the EAX pointed serial to the right one then change the MOV EAX,[LOCAL.12] instruction with MOV EDX,[LOCAL.2], with this patch all serial which is entered is kept valid and program is still registered.

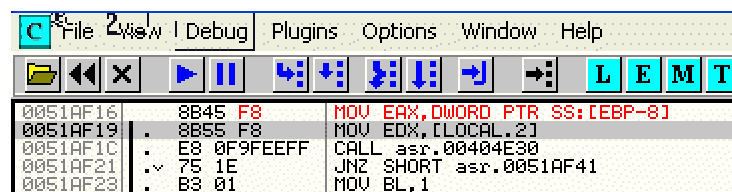


Fig. 7 Patch to accept each serial entered.

On the next start the program is still registered:



Fig. 8 About screen tell us about right registration.



Fig. 9 Main screen.

Work done!