FPT University

Lab 15: Identifying Packers using PEiD

Because teaching teaches
teachers to teach

Packers

- Malware writers often attempt to pack or obfuscate their malware to make it harder to detect and to analyze.
- On the bright side, if the malware is packed it cannot infect your computer. That would seem to be the end of the story, except that we have something called run-time packers.

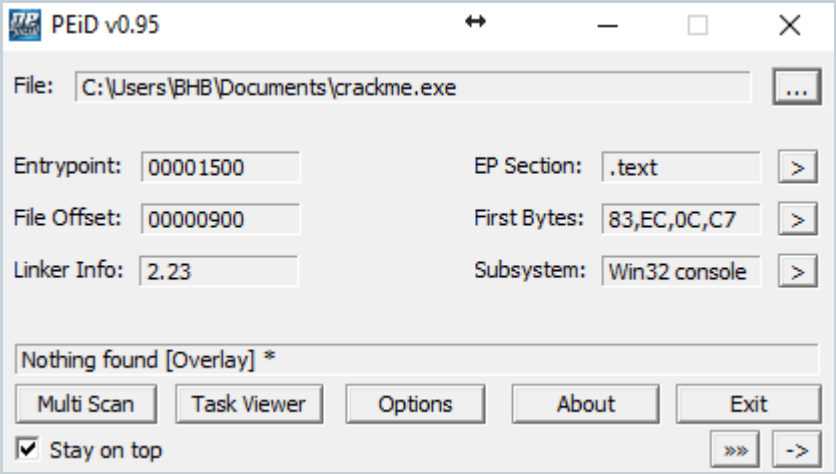
PEiD

- PEiD is a GUI tool for Windows that you can use to detect packers.
- The PEiD signatures are stored in a plain-text file that you can extend with new signatures and/or parse with your own tools.

Check a file packed?

4

- crackme.exe is not packed



Pack a file

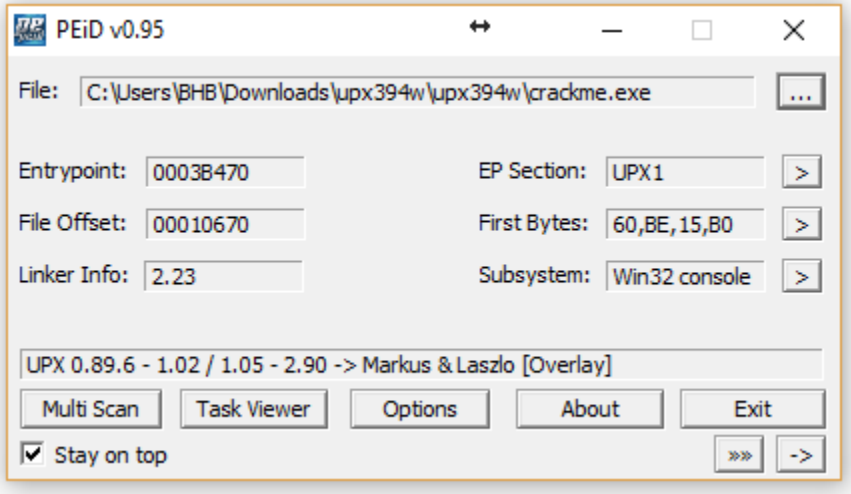
5

```
C:\Users\BHB\Downloads\upx394w\upx394w>upx.exe crackme.exe
                       Ultimate Packer for eXecutables
                          Copyright (C) 1996 - 2017
UPX 3.94w       Markus Oberhumer, Laszlo Molnar & John Reiser   May 12th 2017

        File size         Ratio      Format      Name
   --------------------   ------   -----------   -----------
upx: crackme.exe: AlreadyPackedException: already packed by UPX

Packed 1 file: 0 ok, 1 error.

C:\Users\BHB\Downloads\upx394w\upx394w>
```

Check a file packed again?

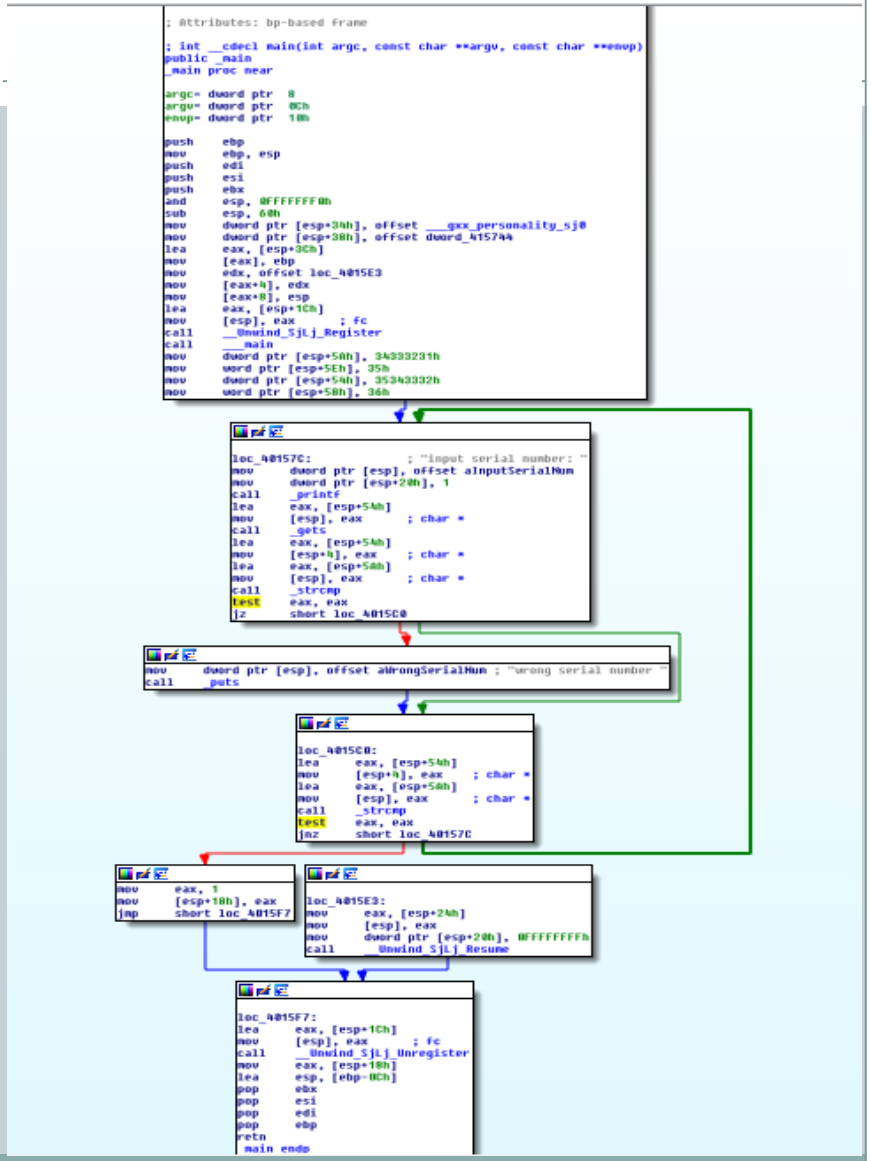
6

- crackme.exe is packed



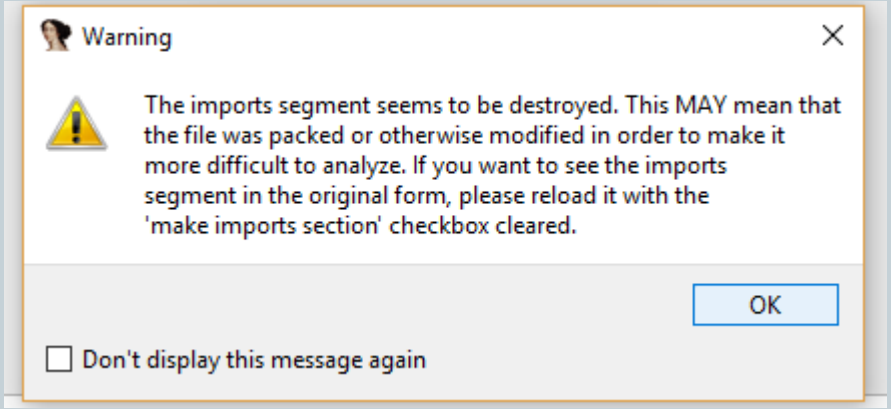
View code in IDA pro

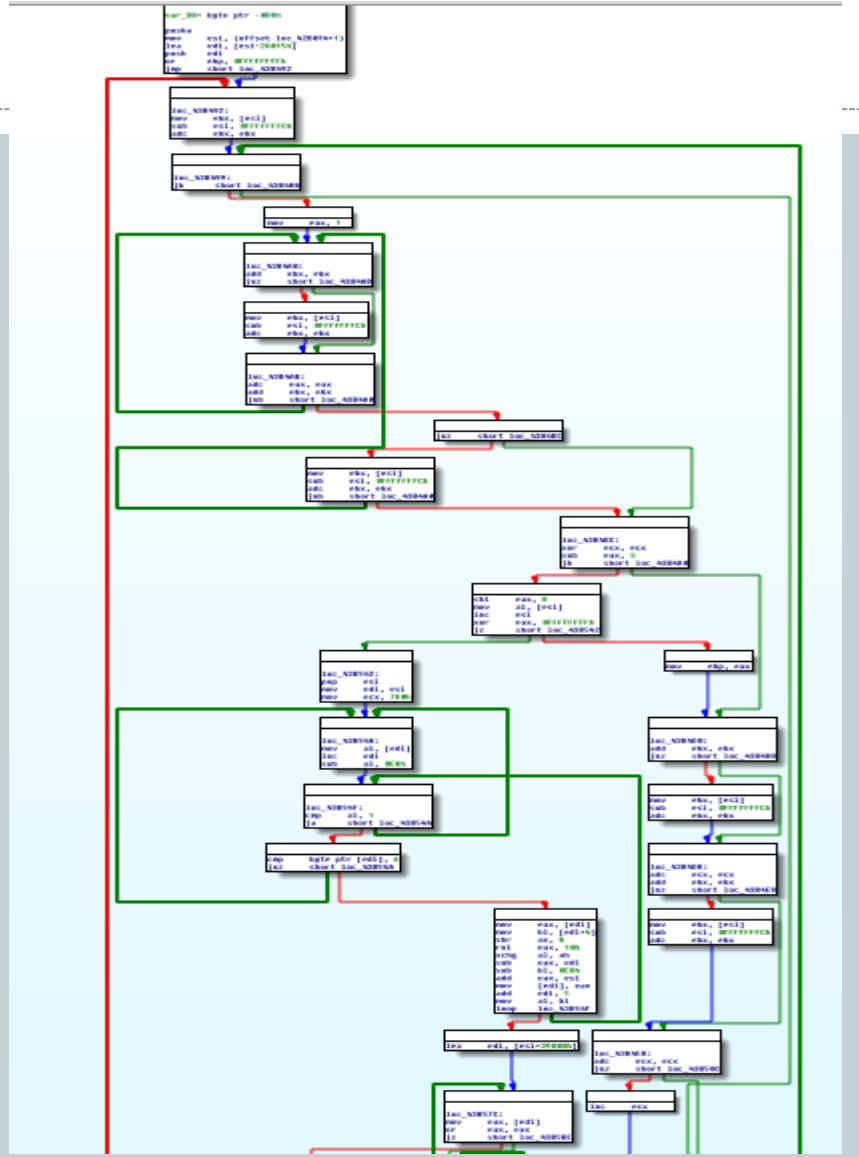
- crackme.exe is not packed



View code in IDA pro

- crackme.exe is packed





Q & A