



# *Lab 15: Identifying Packers using PEiD*

*Because teaching teaches  
teachers to teach*

# Packers

2

- 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

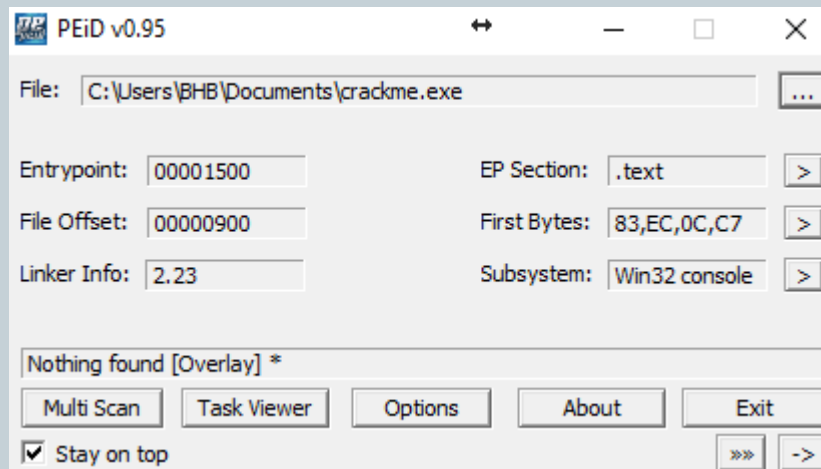
3

- 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

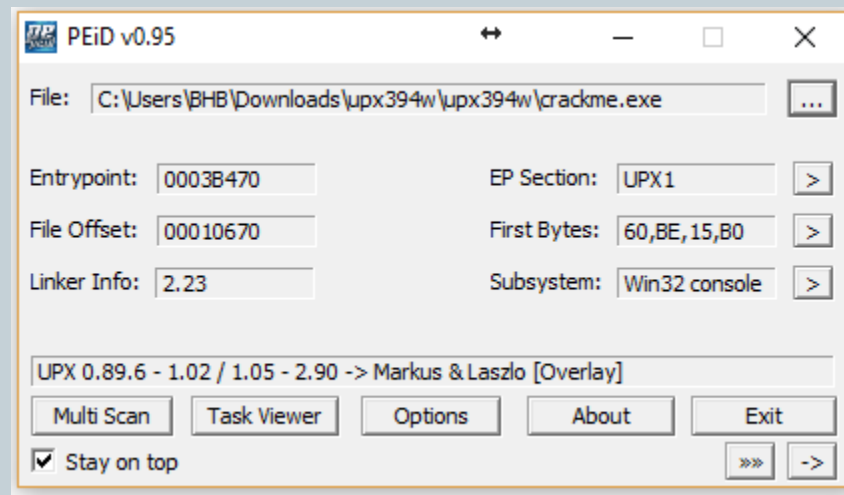
Packed 1 file: 0 ok, 1 error.

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

# Check a file packed again?

6

- crackme.exe is packed



# View code in IDA pro

7

- crackme.exe is not packed

```
; Attributes: bp-based frame
; int __cdecl main(int argc, const char **argv, const char **envp)
public _main
_main proc near
    argc= dword ptr 8
    argv= dword ptr 0Ch
    envp= dword ptr 10h

    push    ebp
    mov     ebp, esp
    push    edi
    push    esi
    push    ebx
    and     esp, 0FFFFFFFh
    sub     esp, 60h
    mov     dword ptr [esp+30h], offset _gxx_personality_sj0
    mov     dword ptr [esp+38h], offset dword_415744
    lea     eax, [esp+3Ch]
    mov     [eax], ebp
    mov     edx, offset loc_4015E3
    mov     [eax+4], edx
    mov     [eax+8], esp
    lea     eax, [esp+1Ch]
    mov     [esp], eax
    mov     [esp+4], fc
    call    __Unwind_SjLj_Register
    call    _main
    mov     dword ptr [esp+50h], 3A393291h
    mov     word ptr [esp+5Eh], 35h
    mov     dword ptr [esp+5Ah], 35343332h
    mov     word ptr [esp+58h], 36h
```

```
loc_40157C:
    mov     dword ptr [esp], offset aInputSerialNum ; "input serial number:"
    mov     dword ptr [esp+20h], 1
    call    _printf
    lea     eax, [esp+50h]
    mov     [esp], eax
    call    _gets
    lea     eax, [esp+50h]
    mov     [esp+4], eax
    lea     eax, [esp+50h]
    mov     [esp], eax
    call    _strcmp
    test    eax, eax
    jz      short loc_4015C0
```

```
mov     dword ptr [esp], offset aWrongSerialNum ; "wrong serial number:"
call    _puts
```

```
loc_4015C0:
    lea     eax, [esp+50h]
    mov     [esp+4], eax
    lea     eax, [esp+50h]
    mov     [esp], eax
    call    _strcmp
    test    eax, eax
    jz      short loc_40157C
```

```
mov     eax, 1
mov     [esp+10h], eax
jmp     short loc_4015F7
```

```
loc_4015E3:
    mov     eax, [esp+20h]
    mov     [esp], eax
    mov     dword ptr [esp+20h], 0FFFFFFFh
    call    __Unwind_SjLj_Resume
```

```
loc_4015F7:
    lea     eax, [esp+1Ch]
    mov     [esp], eax
    mov     [esp+4], fc
    call    __Unwind_SjLj_Unregister
    mov     eax, [esp+10h]
    lea     esp, [ebp-0Ch]
    pop     ebx
    pop     esi
    pop     edi
    pop     ebp
    retn
main endp
```

# View code in IDA pro

8

- crackme.exe is packed

## Warning



The imports segment seems to be destroyed. This MAY mean that the file was packed or otherwise modified in order to make it more difficult to analyze. If you want to see the imports segment in the original form, please reload it with the 'make imports section' checkbox cleared.

OK

☐ Don't display this message again

