

### Overview

- Introduction
- Packer techniques
- Automated Unpacking
- Manual Unpacking

```
push
                         edi
                call
                         sub_314623
                test
                         eax, eax
                         short loc_31306D
                         [ebp+arg_0], ebx
                         short loc 313066
                         eax, [ebp+var_70]
                         eax, [ebp+var_84]
                         short loc 313066
                         eax, [ebp+var_84]
                push
                         [ebp+arg_0], eax
                call
                         sub 31486A
                test
                         eax, eax
                         short loc 31306D
                         681
                lea
                         eax, [ebp+arg_0]
                         esi, 1D0h
                push
                         681
                push
                         [ebp+arg_4]
                call
                         sub 314623
                test
                         eax, eax
                         short loc_31306D
                         [ebp+arg_0], esi
                         short loc 31308F
loc 313066:
                                          ; CODE XREF: sub 312FD8
                                          : sub 312FD8+55
                push
                         0 Dh
                call
                         sub_31411B
loc_31306D:
                                          ; CODE XREF: sub 312FD8
                                          ; sub 312FD8+49
                call
                         sub 3140F3
                         eax, eax
                         short loc 31307D
                call
                         sub_3140F3
                         short loc_31308C
                THE
                                          ; CODE XREF: sub 312FD8
loc_31307D:
                call
                         sub_3140F3
                         eax, 80070000h
loc_31308C:
                                          ; CODE XREF: sub 312FD8
```

# What is a packed progra

- A program that is wrapped by another program
  - Typically also encrypted and/or compressed
- We've seen UPX before

```
call
                         sub 314623
                 test
                         eax, eax
                         short loc_31306D
                         [ebp+arg 0], esi
                         short loc 31308F
loc 313066:
                                          ; CODE XREF: sub 312FD8
                                          ; sub 312FD8+55
                push
                call
                         sub 31411B
loc_31306D:
                                          ; CODE XREF: sub 312FD8
                                          ; sub 312FD8+49
                call
                         sub 3140F3
                         eax, eax
                         short loc 31307D
                         sub_3140F3
                call
                         short loc 31308C
loc_31307D:
                                          ; CODE XREF: sub 312FD8
                         sub_3140F3
                         eax, 80070000h
```

[ebp+arg\_4]

push

push

edi sub\_314623

short loc\_31306D [ebpuarg\_0], ebx

short loc\_313066 eax, [ebp+var\_84]

## Why bother?

- Signature evasion
  - Old Anti-Virus technique
  - Packed <-/-> malware
- Reduces payload size
- Increases difficulty of analysis

```
call
                         sub_314623
                 test
                         eax, eax
                         short loc_31306D
                         [ebp+arg 0], ebx
                         short loc 313066
                         eax, [ebp+var 70]
                         eax, [ebp+var_84]
                         short loc 313066
                         eax, [ebp+var_84]
                         [ebp+arg_0], eax
                call
                         sub 31486A
                         eax, eax
                         short loc 31306D
                         681
                 lea
                         eax, [ebp+arg_0]
                         esi, 1D0h
                         881
                 push
                         [ebp+arg_4]
                call
                         sub 314623
                 test
                         eax, eax
                         short loc_31306D
                         [ebp+arg 0], esi
                         short loc 31308F
loc 313066:
                                          ; CODE XREF: sub 312FD8
                                          ; sub 312FD8+55
                push
                         0 Dh
                call
                         sub 31411B
loc_31306D:
                                          ; CODE XREF: sub 312FD8
                                          ; sub 312FD8+49
                call
                         sub 3140F3
                         eax, eax
                         short loc 31307D
                call
                         sub_3140F3
                         short loc_31308C
                                          ; CODE XREF: sub 312FD8
loc_31307D:
                         sub_3140F3
                         eax, 80070000h
loc_31308C:
                                          ; CODE XREF: sub 312FD8
```

push

edi

### Detection

```
push edi
call sub_314623
test eax, eax
jz short loc_31306D
cmp [ebp+arg_0], ebx
jnz short loc_313066
mov eax, [ebp+var_70]
cmp eax, [ebp+var_84]
jb short loc_313066
sub eax, [ebp+var_84]
push esi
push esi
push eax
```

- We've been over some methods already
  - -PEiD
  - PE Header: Size of Raw Data vs Virtual Siz
  - —limited strings / imports

```
[ebp+arg_4]
                call
                         sub 314623
                test
                         eax, eax
                         short loc_31306D
                         [ebp+arg 0], esi
                         short loc_31308F
loc 313066:
                                          ; CODE XREF: sub 312FD8
                                          : sub 312FD8+55
                push
                call
                         sub 31411B
loc_31306D:
                                          ; CODE XREF: sub 312FD8
                                          ; sub 312FD8+49
                call
                         sub 3140F3
                         eax, eax
                         short loc 31307D
                call
                         sub_3140F3
                         short loc_31308C
                                          ; CODE XREF: sub 312FD8
loc_31307D:
                call
                         sub_3140F3
```

short loc 31306D

loc\_31308C:

eax, 80070000h

### Detection

- Another common method
  - Entropy: Measure of randomness
  - Has many uses
    - Check if address had high entropy d now executable short loc 31306D
    - Can track it through memory
      - What routines touch this data?
      - Do they move it? Unpack it in place? Jump to it?

```
sub 31411B
                                          ; sub 312FD8+49
                         sub_3140F3
                         eax, eax
                         short loc 31307D
                         sub 3140F3
                         short loc 31308C
loc_31307D:
                                           : CODE XREF: sub 312FD8
                         sub_3140F3
                                           : CODE XREF: sub 312FD
                          [ebp+var 4], eax
```

push

edi sub 314623

short loc\_31306D [ebp+arg 0], ebx

short loc 313066 eax, [ebp+var\_70] eax, [ebp+var\_84] short loc 313066 eax, [ebp+var\_84]

[ebp+arg\_0], eax sub 31486A

short loc 31306D

eax, [ebp+arg\_0]

[ebp+arg 0], esi short loc 31308F

: sub 312FD8+55

### Overview

- Introduction
- Packer techniques
- Automated Unpacking
- Manual Unpacking

```
push
                         edi
                call
                         sub_314623
                 test
                         eax, eax
                         short loc_31306D
                         [ebp+arg_0], ebx
                         short loc 313066
                         eax, [ebp+var_70]
                         eax, [ebp+var_84]
                         short loc 313066
                         eax, [ebp+var_84]
                         C51
                push
                         [ebp+arg_0], eax
                call
                         sub 31486A
                 test
                         eax, eax
                         short loc_31306D
                 push
                         681
                 lea
                         eax, [ebp+arg_0]
                         esi, 1D0h
                 push
                         681
                 push
                         [ebp+arg_4]
                 push
                call
                         sub 314623
                test
                         eax, eax
                         short loc_31306D
                         [ebp+arg_0], esi
                         short loc 31308F
loc 313066:
                                          ; CODE XREF: sub 312FD8
                                          : sub 312FD8+55
                push
                         0 Dh
                call
                         sub_31411B
loc_31306D:
                                          ; CODE XREF: sub 312FD8
                                          ; sub 312FD8+49
                call
                         sub 3140F3
                         eax, eax
                         short loc 31307D
                call
                         sub_3140F3
                         short loc_31308C
                 THE
                                          ; CODE XREF: sub 312FD8
loc_31307D:
                call
                         sub_3140F3
                         eax, 80070000h
loc_31308C:
                                          ; CODE XREF: sub 312FD8
```

```
call sub_314623
test eax, eax
jz short loc_31306D
cmp [ebp+arg_0], ebx
jnz short loc_313066
mov eax, [ebp+var_70]
cmp eax, [ebp+var_84]
jb short loc_313066
sub eax, [ebp+var_84]
push esi
push esi
```

edi

push

Decrypts/Decompresses packed cod

```
eax, eax
        short loc_31306D
push
        esi
lea
        eax, [ebp+arg_0]
        cax
        esi, 1D0h
push
        881
push
        [ebp+arg_4]
push
        sub 314623
test
        eax, eax
        short loc_31306D
        [ebp+arg 0], esi
        short loc 31308F
                         ; CODE XREF: sub 312FD8
                         : sub 312FD8+55
push
        0 Dh
call
        sub_31411B
```

call

loc 313066:

loc\_31306D:

```
; CODE XREF: sub_312FD8
call sub_3140F3
and eax, Offfin
```

; CODE XREF: sub 312FD8

; sub 312FD8+49

sub\_3140F3 eax, eax

sub\_3140F3 short loc\_31308C

short loc\_31307D

- Decrypts/Decompresses packed co
- Loads code into memory

```
call
                         sub_314623
                 test
                         eax, eax
                         short loc_31306D
                         [ebp+arg 0], ebx
                         short loc 313066
                         eax, [ebp+var_70]
                         eax, [ebp+var_84]
                         short loc 313066
                         eax, [ebp+var_84]
                         short loc 31306D
                 lea
                         eax, [ebp+arg_0]
                         esi, 1D0h
                push
                         881
                push
                         [ebp+arg_4]
                 push
                call
                         sub 314623
                test
                         eax, eax
                         short loc_31306D
                         [ebp+arg 0], esi
                         short loc 31308F
loc 313066:
                                          ; CODE XREF: sub 312FD8
                                          : sub 312FD8+55
                push
                         0 Dh
                call
                         sub 31411B
loc_31306D:
                                          ; CODE XREF: sub 312FD8
                                          ; sub 312FD8+49
                call
                         sub 3140F3
                         eax, eax
                         short loc 31307D
                call
                         sub_3140F3
                         short loc_31308C
                 THE C
                                          ; CODE XREF: sub 312FD8
loc_31307D:
                         sub_3140F3
                         eax, 80070000h
```

push

edi

push edi
call sub\_314623
test eax, eax
jz short loc\_31306D
cmp [ebp+arg\_0], ebx
jnz short loc\_313066
mov eax, [ebp+var\_70]
cmp eax, [ebp+var\_84]
jb short loc\_313066
sub eax, [ebp+var\_84]
push esi
push esi

short loc 31306D

- Decrypts/Decompresses packed cod
- Loads code into memory
- Resolves imports of original executable

```
[ebp+arg_4]
                         edi
                 call
                         sub 314623
                 test
                         eax, eax
                         short loc_31306D
                         [ebp+arg 0], esi
                         short loc 31308F
loc 313066:
                                          ; CODE XREF: sub 312FD8
                                          : sub 312FD8+55
                push
                call
                         sub 31411B
loc_31306D:
                                          ; CODE XREF: sub 312FD8
                                          ; sub 312FD8+49
                call
                         sub 3140F3
                         eax, eax
                         short loc 31307D
                call
                         sub_3140F3
                         short loc 31308C
                 ij
loc_31307D:
                                          ; CODE XREF: sub 312FD8
                call
                         sub_3140F3
```

eax, 80070000h

- push edi
  call sub\_314623
  test eax, eax
  jz short loc\_31306D
  cmp [ebp+arg\_0], ebx
  jnz short loc\_313066
  mov eax, [ebp+var\_70]
  cmp eax, [ebp+var\_84]
  jb short loc\_313066
  sub eax, [ebp+var\_84]
  push esi
  push esi
- Decrypts/Decompresses packed cod
- Loads code into memory
- Resolves imports of original executable
- Transfer execution to OEP (Original Entry Point)

```
loc 313066:
                                          ; CODE XREF: sub 312FD8
                                          ; sub 312FD8+55
                push
                call
                         sub 31411B
loc_31306D:
                                          ; CODE XREF: sub 312FD8
                                          ; sub 312FD8+49
                         sub 3140F3
                         eax, eax
                         short loc 31307D
                         sub 3140F3
                         short loc 31308C
loc_31307D:
                                          ; CODE XREF: sub 312FD8
                         sub_3140F3
```

eax, 80070000h

push edi sub 314623 test eax, eax short loc\_31306D [ebp+arg 0], ebx short loc 313066 eax, [ebp+var 70] eax, [ebp+var 84] short loc 313066 eax, [ebp+var\_84]

eax, [ebp+arg\_0]

[ebp+arg\_4]

sub 314623

- Decrypts/Decompresses packed code
- Loads code into memory
- Resolves imports of original executable
- Transfer execution to OEP

```
test
        eax, eax
        short loc 31306D
        [ebp+arg 0], esi
        short loc 31308F
```

Usually anti-analysis at one or all of these

steps

loc 313066:

loc\_31307D:

loc\_31308C:

```
; CODE XREF: sub 312FD8
                ; sub 312FD8+49
sub 3140F3
eax, eax
short loc 31307D
sub 3140F3
short loc 31308C
                ; CODE XREF: sub 312FD8
```

sub\_3140F3

# Unpacking the code

- Any method you can imagine
  - Plaintext
  - Compression
  - -XOR
  - -AES
  - **—** ...
- Sometimes this is as far as you need

```
short loc_31306D
                         [ebp+arg_0], esi
                         short loc 31308F
                                          ; CODE XREF: sub 312FD8
                                          ; sub 312FD8+55
                call
                         sub 31411B
loc_31306D:
                                          ; CODE XREF: sub 312FD8
                                          ; sub 312FD8+49
                call
                         sub 3140F3
                         eax, eax
                         short loc 31307D
                call
                         sub_3140F3
                         short loc 31308C
                 ij
loc_31307D:
                                          ; CODE XREF: sub 312FD8
                         sub_3140F3
```

push

call

test

call

test

push

lea

push

call

test

edi

sub\_314623

short loc\_31306D

[ebp+arg\_0], ebx short loc\_313066 eax, [ebp+var\_70] eax, [ebp+var\_84] short loc\_313066 eax, [ebp+var\_84]

[ebp+arg\_0], eax

short loc 31306D

eax, [ebp+arg\_0]

sub 31486A

eax, eax

esi, 1D0h

[ebp+arg\_4]

sub 314623

eax, eax

881

eax, eax

eax, 80070000h

# Unpacking the code

- Location of unpacked code
  - -Same section (as stub)
  - New section
  - Heap
  - **—**???

```
[ebp+arg 0], ebx
                         short loc 313066
                         eax, [ebp+var_70]
                         eax, [ebp+var_84]
                         short loc 313066
                         eax, [ebp+var_84]
                 push
                         C51
                 push
                         [ebp+arg_0], eax
                call
                         sub 31486A
                 test
                         eax, eax
                         short loc 31306D
                         681
                 lea
                         eax, [ebp+arg_0]
                         esi, 1D0h
                push
                         681
                 push
                         [ebp+arg_4]
                call
                         sub 314623
                test
                         eax, eax
                         short loc_31306D
                         [ebp+arg 0], esi
                         short loc_31308F
loc 313066:
                                          ; CODE XREF: sub 312FD8
                                          : sub 312FD8+55
                push
                         0 Dh
                call
                         sub 31411B
loc_31306D:
                                          ; CODE XREF: sub 312FD8
                                          ; sub 312FD8+49
                call
                         sub 3140F3
                         eax, eax
                         short loc 31307D
                call
                         sub_3140F3
                         short loc_31308C
                 ij
                                          ; CODE XREF: sub 312FD8
loc_31307D:
                call
                         sub_3140F3
                         eax, 80070000h
```

push

call

test

edi

sub\_314623

short loc\_31306D

eax, eax

[ebp+var 4], eax

# Resolving Imports - Lame

lame [ebp+arg\_0], ebx short loc\_313066 eax, [ebp+var\_70] eax, [ebp+var\_84] short loc\_313066 sub eax, [ebp+var\_84]

push

call

test

edi

C51

sub\_314623

short loc 31306D

[ebp+arg\_0], eax

eax, [ebp+arg\_0]

eax, eax

- Keep original import table intact
- Windows' Loader will resolve imports

```
esi, 1D0h
                 push
                         881
                 push
                         [ebp+arg_4]
                call
                         sub 314623
                test
                         eax, eax
                         short loc_31306D
                         [ebp+arg 0], esi
                         short loc 31308F
loc 313066:
                                          ; CODE XREF: sub 312FD8
                                          : sub 312FD8+55
                push
                call
                         sub 31411B
loc_31306D:
                                          ; CODE XREF: sub 312FD8
                                          ; sub 312FD8+49
                call
                         sub 3140F3
                 test
                         eax, eax
                         short loc 31307D
                call
                         sub_3140F3
                         short loc 31308C
                 ij
loc_31307D:
                                          ; CODE XREF: sub 312FD8
                call
                         sub_3140F3
```

# Resolving Imports - Easy

- Packed stub only imports GetProcAddress and LoadLibrary
- Iterates original executables import table
- Creates the import table from results
- The most common method

```
[ebp+arg 0], esi
                         short loc 31308F
loc 313066:
                                          ; CODE XREF: sub 312FD8
                                          ; sub 312FD8+55
                push
                call
                         sub 31411B
loc_31306D:
                                          ; CODE XREF: sub 312FD8
                                          ; sub 312FD8+49
                         sub 3140F3
                         eax, eax
                         short loc 31307D
                         sub 3140F3
                         short loc 31308C
loc_31307D:
                                          ; CODE XREF: sub 312FD8
                         sub_3140F3
```

short loc 31306D

push

edi sub 314623

short loc\_31306D [ebp+arg\_0], ebx

eax, [ebp+var\_70] eax, [ebp+var\_84] short loc\_313066 eax, [ebp+var\_84]

# Resolving Imports - Hard

No imports

```
short loc 313066
                         eax, [ebp+var_70]
                         eax, [ebp+var_84]
                         short loc 313066
                         eax, [ebp+var_84]
                push
                         esi
                         C51
                push
                         eax
                         [ebp+arg_0], eax
                call
                         sub_31486A
                test
                         eax, eax
                         short loc_31306D
                push
                         681
                lea
                         eax, [ebp+arg_0]
                         cax
                         esi, 1D0h
                push
                         681
                push
                         [ebp+arg_4]
                push
                         sub 314623
                test
                         eax, eax
                         short loc_31306D
                         [ebp+arg 0], esi
                         short loc 31308F
loc 313066:
                                          ; CODE XREF: sub 312FD8
                                          : sub 312FD8+55
                push
                         0 Dh
                call
                         sub_31411B
loc_31306D:
                                          ; CODE XREF: sub 312FD8
                                          ; sub 312FD8+49
                call
                         sub_3140F3
                test
                         eax, eax
                         short loc 31307D
                call
                         sub_3140F3
                         short loc_31308C
                 THE
loc_31307D:
                                          ; CODE XREF: sub 312FD8
                         sub_3140F3
                         eax, Offffn
                         eax, 80070000h
```

[ebp+var 4], eax

push

call

test

edi

sub\_314623

short loc\_31306D [ebp+arg\_0], ebx

eax, eax

# Resolving Imports - Hard

No imports

Malware - 11/03/2015

Get address of kernel32 from PEB

```
eax, [ebp+arg_0]
// find base addr of kernel32.dll
 mov ebx, fs:[edx + 0x30]; ebx = ADDRESS of PEB
 mov ecx, [ebx + 0xc]
                            ;ecx = pointer to loader data
 mov ecx, [ecx + 0x1c]
                             ;ecx = first entry in initialization order list
                                                                                       DE XREF: sub 312FD8
                         ;ecx = second entry in list (kernelab.dll)
 mov ecx, [ecx]
                                                                                       312FD8+55
                         ;ecx = third entry in list (kernel32.dll)
 mov ecx, [ecx]
                             ;ebp = base ADDRESS of kernel32.dll
 mov ebp, [ecx + 0x08]
                                                                                       E XREF: sub 312FD8
                                                                                        312FD8+49
                                                                call
                                                                      sub 3140F3
                                                                      short loc 31308C
                                                   loc_31307D:
                                                                                    ; CODE XREF: sub 312FD8
                                                                      sub 3140F3
```

loc\_31308C:

Packers and Unpacking

push

edi sub\_314623 eax, eax

short loc\_31306D [ebp+arg\_0], ebx

short loc\_313066 eax, [ebp+var\_70] eax, [ebp+var\_84] short loc\_313066 eax, [ebp+var\_84]

[ebp+arg\_0], eax sub\_31486A eax, eax

short loc 31306D

eax, 80070000h

[ebp+var 4], eax

; CODE XREF: sub 312FD8

# Resolving Imports - Hard

- Walk kernel32.dll's export table
- Find address of GetProcAddress and LoadLibrary
- Two options

Malware - 11/03/2015

- Repeat common method using newfound function short loc 31308F pointers
- Use LoadLibrary on required DLLs Walk their export tables, too

```
sub 312FD8+55
call
        sub 31411B
                         ; CODE XREF: sub 312FD8
                         ; sub 312FD8+49
        sub 3140F3
        eax, eax
        short loc 31307D
        sub 3140F3
        short loc 31308C
                         : CODE XREF: sub 312FD8
        sub 3140F3
```

loc\_31307D:

push

edi

short loc 31306D [ebp+arg 0], ebx

[ebp+arg\_0], eax

eax, [ebp+arg\_0]

esi, 1D0h

[ebp+arg\_4]

sub 314623

loc 31306D

[ebp+var 84] short loc 313066 [ebp+var 84]

### Overview

- Introduction
- Packer techniques
- Automated Unpacking
- Manual Unpacking

```
push
                         edi
                call
                         sub_314623
                test
                         eax, eax
                         short loc_31306D
                         [ebp+arg_0], ebx
                         short loc 313066
                         eax, [ebp+var_70]
                         eax, [ebp+var_84]
                         short loc 313066
                         eax, [ebp+var_84]
                         C51
                push
                         [ebp+arg_0], eax
                call
                         sub 31486A
                test
                         eax, eax
                         short loc_31306D
                         681
                lea
                         eax, [ebp+arg_0]
                         esi, 1D0h
                push
                         681
                push
                         [ebp+arg_4]
                call
                         sub 314623
                test
                         eax, eax
                         short loc_31306D
                         [ebp+arg_0], esi
                         short loc 31308F
loc 313066:
                                          ; CODE XREF: sub 312FD8
                                          : sub 312FD8+55
                push
                         0 Dh
                call
                         sub_31411B
loc_31306D:
                                          ; CODE XREF: sub 312FD8
                                          ; sub 312FD8+49
                call
                         sub 3140F3
                         eax, eax
                         short loc 31307D
                call
                         sub_3140F3
                         short loc_31308C
                THE
                                          ; CODE XREF: sub 312FD8
loc_31307D:
                call
                         sub_3140F3
                         eax, 80070000h
                                                      20
loc_31308C:
                                          ; CODE XREF: sub 312FD8
```

## **Automated Unpacking**

```
push
        edi
call
        sub_314623
test
        eax, eax
        short loc_31306D
        [ebp+arg 0], ebx
        short loc 313066
        eax, [ebp+var 70]
        eax, [ebp+var_84]
        short loc 313066
        eax, [ebp+var_84]
```

short loc 31306D

ax, [ebp+arg\_0]

- Sometimes an official tool is available
  - -e.g. UPX

Malware - 11/03/2015

- Usually reliable unless tampered
  - Change metadata
  - Corkami UPX trap

```
[ebp+arg_4]
                 call
                         sub 314623
                 test
                         eax, eax
                         short loc_31306D
                         [ebp+arg 0], esi
                         short loc 31308F
loc 313066:
                                          ; CODE XREF: sub 312FD8
                                          ; sub 312FD8+55
                push
                call
                         sub 31411B
loc_31306D:
                                          ; CODE XREF: sub 312FD8
                                          ; sub 312FD8+49
                call
                         sub 3140F3
                         eax, eax
                         short loc 31307D
                         sub_3140F3
                         short loc 31308C
loc_31307D:
                                          ; CODE XREF: sub 312FD8
                         sub_3140F3
                         eax, 80070000h
```

## **Automated Unpacking**

- push edi sub 314623 short loc 31306D [ebp+arg 0], ebx short loc 313066 eax, [ebp+var 70] eax, [ebp+var 84] short loc 313066 [ebp=var\_84]
- Other times, people write scripts tools
  - OllyScript / ODbgScript
  - Python
  - PEExplorer
    - NSPack, UPack, UPX
- Don't always work
- Sometimes tailored towards a specific executable or packer version

```
short loc 31306D
        eax, [ebp+arg_0]
        esi, 1D0h
        [ebp+arg_4]
        sub 314623
test
        eax, eax
        short loc 31306D
        [ebp+arg 0], esi
        short loc 31308F
                         : sub 312FD8+55
```

or custom

```
; sub 312FD8+49
short loc 31307D
```

[ebp+var 4], eax

sub 31411B

```
sub 3140F3
short loc 31308C
```

loc 313066:

loc\_31307D:

### Overview

- Introduction
- Packer techniques
- Automated Unpacking
- Manual Unpacking

```
push
                         edi
                call
                         sub_314623
                 test
                         eax, eax
                         short loc_31306D
                         [ebp+arg 0], ebx
                         short loc 313066
                         eax, [ebp+var_70]
                         eax, [ebp+var_84]
                         short loc 313066
                         eax, [ebp+var_84]
                         [ebp+arg_0], eax
                call
                         sub 31486A
                 test
                         eax, eax
                         short loc_31306D
                         681
                 lea
                         eax, [ebp+arg_0]
                         esi, 1D0h
                 push
                         681
                 push
                         [ebp+arg_4]
                 call
                         sub 314623
                test
                         eax, eax
                         short loc_31306D
                         [ebp+arg_0], esi
                         short loc 31308F
loc 313066:
                                          ; CODE XREF: sub 312FD8
                                          : sub 312FD8+55
                push
                         0 Dh
                call
                         sub_31411B
loc_31306D:
                                          ; CODE XREF: sub 312FD8
                                          ; sub 312FD8+49
                call
                         sub 3140F3
                         eax, eax
                         short loc 31307D
                         sub_3140F3
                         short loc_31308C
                                          ; CODE XREF: sub 312FD8
loc_31307D:
                call
                         sub_3140F3
                         eax, 80070000h
loc_31308C:
                                          ; CODE XREF: sub 312FD8
```

#### push edi sub\_314623 eax, eax short loc 31306D [ebp+arg 0], ebx When automated technic eax, [ebp+var\_84] esi You can't always just run a tool eax, eax flag short loc 31306D 681 lea eax, [ebp+arg\_0] esi, 1D0h push 881 push [ebp+arg\_4] call sub 314623 test eax, eax short loc\_31306D [ebp+arg 0], esi short loc 31308F loc 313066: ; CODE XREF: sub 312FD8 : sub 312FD8+55 push 0 Dh call sub 31411B loc\_31306D: ; CODE XREF: sub 312FD8 ; sub 312FD8+49 call sub 3140F3 eax, eax short loc 31307D call sub\_3140F3 short loc\_31308C THE C loc\_31307D: ; CODE XREF: sub 312FD8 sub\_3140F3 eax, 80070000h Malware - 11/03/2015 24

[ebp+var 4], eax

# When automated techniques fail

- You can't always just run a tool and get the flag
- Difficulty and time required varies greatly
  - Packer
  - Packer options chosen
  - Unpacking method
  - Multiple levels of packing?

```
[ebp+arg_4]
                         sub 314623
                 test
                         eax, eax
                         short loc 31306D
                         [ebp+arg 0], esi
                         short loc 31308F
loc 313066:
                                          ; CODE XREF: sub 312FD8
                                          ; sub 312FD8+55
                push
                call
                         sub 31411B
loc_31306D:
                                          ; CODE XREF: sub 312FD8
                                          ; sub 312FD8+49
                         sub 3140F3
                         eax, eax
                         short loc 31307D
                         sub 3140F3
                         short loc 31308C
loc_31307D:
                                          ; CODE XREF: sub 312FD8
                         sub_3140F3
```

push

## When automated techni

Two methods

Malware - 11/03/2015

- Write a tool to undo each step perforn [ebp+arg 0] packer esi, 1D0h
  - No one does this
- Run the packed program to OEP, dump from memory short loc 31308F

loc 313066:

loc 31308C:

Much, much more common

```
; sub 312FD8+55
                         sub 31411B
loc_31306D:
                                          ; CODE XREF: sub 312FD8
                                          ; sub 312FD8+49
                         sub 3140F3
                         short loc 31307D
                         sub 3140F3
                         short loc 31308C
loc_31307D:
                                          ; CODE XREF: sub 312FD8
                         sub 3140F3
```

[ebp+arg\_0], eax

[ebp+arg\_4] sub 314623

- Find OEP
- Reconstruct import table

```
test
                         eax, eax
                         short loc_31306D
                         [ebp+arg_0], ebx
                         short loc 313066
                         eax, [ebp+var_70]
                         eax, [ebp+var_84]
                         short loc 313066
                         eax, [ebp+var_84]
                push
                         C51
                push
                         [ebp+arg_0], eax
                call
                         sub_31486A
                test
                         eax, eax
                         short loc_31306D
                push
                         681
                lea
                         eax, [ebp+arg_0]
                         cax
                         esi, 1D0h
                push
                         681
                push
                         [ebp+arg_4]
                push
                         sub 314623
                test
                         eax, eax
                         short loc_31306D
                         [ebp+arg_0], esi
                         short loc_31308F
loc 313066:
                                          ; CODE XREF: sub 312FD8
                                          : sub 312FD8+55
                push
                         0 Dh
                call
                         sub_31411B
loc_31306D:
                                          ; CODE XREF: sub 312FD8
                                          ; sub 312FD8+49
                call
                         sub_3140F3
                         eax, eax
                         short loc_31307D
                call
                         sub_3140F3
                         short loc_31308C
                THE
                                          ; CODE XREF: sub 312FD8
loc_31307D:
                         sub_3140F3
                         eax, 80070000h
```

push

edi sub\_314623

- Find OEP
- Reconstruct import table

### Easy, right?

```
loc 313066:
                                          ; CODE XREF: sub 312FD8
                                          : sub 312FD8+55
                push
                         0 Dh
                call
                         sub_31411B
loc_31306D:
                                          ; CODE XREF: sub 312FD8
                                          ; sub 312FD8+49
                call
                         sub 3140F3
                         eax, eax
                         short loc_31307D
                call
                         sub_3140F3
                         short loc_31308C
                THE
                                          ; CODE XREF: sub 312FD8
loc_31307D:
                         sub_3140F3
```

eax, 80070000h

[ebp+var 4], eax

push

test

push

push

call

test

push

lea

push

push

push

test

edi sub\_314623

C51

eax, eax

short loc\_31306D [ebp+arg\_0], ebx

short loc\_313066 eax, [ebp+var\_70] eax, [ebp+var\_84] short loc\_313066 eax, [ebp+var\_84]

[ebp+arg\_0], eax

short loc\_31306D

eax, [ebp+arg\_0]

short loc\_31306D [ebp+arg\_0], esi short loc\_31308F

sub\_31486A

eax, eax

esi, 1D0h

[ebp+arg\_4]

sub 314623

eax, eax

681

681

- Tail jumps
  - Jump from unpacking stub to OEP
  - Really visible in simple unpacking stubs
    - jmp BB goes nowhere
  - Doesn't have to be a jmp
    - push/ret
    - SEH
    - call
    - 。???

```
eax, [ebp+var_84]
                         [ebp+arg_0], eax
                         sub 31486A
                         eax, eax
                         short loc 31306D
                         eax, [ebp+arg_0]
                         esi, 1D0h
                         681
                 push
                         [ebp+arg_4]
                 call
                         sub 314623
                 test
                         eax, eax
                         short loc_31306D
                         [ebp+arg 0], esi
                         short loc 31308F
loc 313066:
                                          ; CODE XREF: sub 312FD8
                                          : sub 312FD8+55
                push
                         0 Dh
                call
                         sub 31411B
loc_31306D:
                                          ; CODE XREF: sub 312FD8
                                          ; sub 312FD8+49
                call
                         sub 3140F3
                         eax, eax
                         short loc 31307D
                call
                         sub_3140F3
                         short loc_31308C
                                          ; CODE XREF: sub 312FD8
loc_31307D:
                         sub_3140F3
                         eax, 80070000h
loc_31308C:
```

[ebp+var 4], eax

push

call

test

edi

sub\_314623

short loc\_31306D [ebp+arg 0], ebx

short loc 313066 eax, [ebp+var 70] eax, [ebp+var 84] short loc 313066

eax, eax

- Section hop
  - OEP can be in a different section than unpacking stub

```
sub_314623
                test
                        eax, eax
                        short loc_31306D
                         [ebp+arg_0], ebx
                        short loc 313066
                        eax, [ebp+var_70]
                        eax, [ebp+var_84]
                        short loc 313066
                        eax, [ebp+var_84]
                        C51
                         [ebp+arg_0], eax
                call
                        sub 31486A
                         eax, eax
                      the 100_31306D
                        eax, [ebp+arg_0]
                        esi, 1D0h
                push
                        681
                push
                         [ebp+arg_4]
                push
                call
                        sub 314623
                test
                        eax, eax
                        short loc_31306D
                        [ebp+arg_0], esi
                        short loc 31308F
loc 313066:
                                         ; CODE XREF: sub 312FD8
                                         : sub 312FD8+55
                push
                        0 Dh
                call
                        sub_31411B
loc_31306D:
                                         ; CODE XREF: sub 312FD8
                                         ; sub 312FD8+49
                call
                        sub_3140F3
                        eax, eax
                         short loc 31307D
                call
                        sub_3140F3
                        short loc_31308C
                THE
                                         ; CODE XREF: sub 312FD8
loc_31307D:
                        sub_3140F3
                        eax, 80070000h
                                                     30
                                         ; CODE XREF: sub 312FD8
```

push

edi

- Section hop
  - OEP can be in a different section than unpacking stub
  - -Olly can set a memory breakpoint on the other sections
  - —Will automatically break as soon as execution changes sections

```
; CODE XREF: sub 312FD8
                                          : sub 312FD8+55
                push
                call
                         sub 31411B
loc_31306D:
                                          ; CODE XREF: sub 312FD8
                                          ; sub 312FD8+49
                call
                         sub 3140F3
                         eax, eax
                         short loc 31307D
                         sub_3140F3
                         short loc 31308C
loc_31307D:
                                          ; CODE XREF: sub 312FD8
                         sub_3140F3
```

eax, 80070000h

push

call

test

call

edi

sub\_314623

short loc\_31306D [ebp+arg\_0], ebx

short loc\_313066 eax, [ebp+var\_70] eax, [ebp+var\_84] short loc\_313066 eax, [ebp+var\_84]

[ebp+arg\_0], eax

the 10c\_31306D eax, [ebp+arg\_0]

sub 31486A

esi, 1D0h

eax, eax

- PUSHA/POPA
  - PUSHA is used to save register state stub
  - POPA is used to restore register state at end of stub

```
test
                         eax, eax
                         short loc_31306D
                         [ebp+arg 0], esi
                         short loc_31308F
loc 313066:
                                          ; CODE XREF: sub 312FD8
                                          : sub 312FD8+55
                push
                         0 Dh
                call
                         sub_31411B
loc_31306D:
                                          ; CODE XREF: sub 312FD8
                                          ; sub 312FD8+49
                call
                         sub 3140F3
                         eax, eax
                         short loc 31307D
                call
                         sub_3140F3
                         short loc_31308C
                THE
                                          ; CODE XREF: sub 312FD8
loc_31307D:
                         sub_3140F3
                         eax, 80070000h
```

push

call

test

call

edi

sub\_314623

short loc\_31306D [ebp+arg\_0], ebx

short loc\_313066 eax, [ebp+var\_70] eax, [ebp+var\_84] short loc\_313066 eax, [ebp+var\_84]

[ebp+arg\_0], eax

eax, [ebp+arg\_0]

sub 31486A

esi, 1D0h

eax, eax

### PUSHA/POPA

- PUSHA is used to save register state at stub
- POPA is used to restore register state at end of stub
- -Put a memory breakpoint on one of the register values on the stack
- Will break when POPA pops the value
- Usually really close to OEP

```
loc 313066:
                                          ; sub 312FD8+55
                         sub 31411B
loc_31306D:
                                          ; CODE XREF: sub 312FD8
                                          ; sub 312FD8+49
                         sub 3140F3
                         eax, eax
                         short loc 31307D
                         sub 3140F3
                         short loc 31308C
loc_31307D:
                                          ; CODE XREF: sub 312FD8
                         sub 3140F3
loc_31308C:
                                          : CODE XREF: sub 312FD8
                         [ebp+var 4], eax
```

push

call

edi sub\_314623 eax, eax

short loc\_31306D [ebp+arg\_0], ebx

short loc\_313066 eax, [ebp+var\_70] eax, [ebp+var\_84] short loc\_313066 eax, [ebp+var\_84]

[ebp+arg\_0], eax

eax, [ebp+arg 0]

- API call
  - Fixing the import table is usually close of the stub
  - Break on LoadLibrary/GetProcAddress
  - Search nearby

```
[ebp+arg_0], eax
                call
                         sub 31486A
                         eax, [ebp+arg_0]
                         esi, 1D0h
                         881
                         [ebp+arg_4]
                         sub 314623
                 test
                         eax, eax
                         short loc_31306D
                         [ebp+arg 0], esi
                         short loc 31308F
loc 313066:
                                          ; CODE XREF: sub 312FD8
                                          : sub 312FD8+55
                push
                         0 Dh
                call
                         sub 31411B
loc_31306D:
                                          ; CODE XREF: sub 312FD8
                                          ; sub 312FD8+49
                call
                         sub 3140F3
                         eax, eax
                         short loc 31307D
                         sub_3140F3
                         short loc_31308C
loc_31307D:
                                          ; CODE XREF: sub 312FD8
                         sub_3140F3
                         eax, 80070000h
loc_31308C:
                                          ; CODE XREF: sub 312FD8
```

push

call

test

edi

sub\_314623

short loc\_31306D [ebp+arg 0], ebx

short loc 313066 eax, [ebp+var 70] eax, [ebp+var\_84] short loc 313066 eax, [ebp+var\_84]

eax, eax

- API call
  - Windows makes identifiable API calls in start
    - e.g. GetModuleHandle, GetCommandLine
  - Break on one of these functions
  - -OEP is usually at the top of the parent

```
short loc 31308F
loc 313066:
                                          ; CODE XREF: sub 312FD8
                                          ; sub 312FD8+55
                push
                         0 Dh
                call
                         sub 31411B
loc_31306D:
                                          ; CODE XREF: sub 312FD8
                                          ; sub 312FD8+49
                call
                         sub 3140F3
                         eax, eax
                         short loc 31307D
                call
                         sub_3140F3
                         short loc 31308C
loc_31307D:
                                          ; CODE XREF: sub 312FD8
                         sub_3140F3
                         eax, 80070000h
```

push

call

test

call

edi

sub\_314623

short loc\_31306D [ebp+arg\_0], ebx

short loc\_313066 eax, [ebp+var\_70] eax, [ebp+var\_84] short loc\_313066 eax, [ebp+var\_84]

[ebp+arg 0], eax

eax, [ebp+arg\_0]

short loc\_31306D [ebp+arg 0], esi

[ebp+arg\_4]

sub\_314623

sub 31486A

eax, eax

- VERA
  - Awesome visualization tool that uses PIN

Main Application Code

Application Initialization

Execution Start

Unpacking Code

loc\_31307D:

loc\_31308C:

short loc\_31308C

push

test

sub\_314623

short loc\_31306D [ebp+arg\_0], ebx

short loc\_313066 eax, [ebp+var\_70] eax, [ebp+var\_84] short loc\_313066 eax, [ebp+var\_84]

[ebp+arg\_0], eax sub\_31486A

eax, [ebp+arg\_0]

eax, eax

# Fixing Imports

- OllyDbg is pretty good at it
- ImpREC is very good at it
- You really want to avoid doing it by hand
  - Have to look up each address and fill in the pointer in the IAT

```
short loc 31308F
loc 313066:
                                          ; CODE XREF: sub 312FD8
                                          : sub 312FD8+55
                push
                call
                         sub 31411B
loc_31306D:
                                          ; CODE XREF: sub 312FD8
                                          ; sub 312FD8+49
                call
                         sub 3140F3
                         eax, eax
                         short loc 31307D
                call
                         sub 3140F3
                         short loc 31308C
loc_31307D:
                                          ; CODE XREF: sub 312FD8
                call
                         sub_3140F3
```

eax, 80070000h

push

call

test

edi

sub\_314623

short loc\_31306D [ebp+arg\_0], ebx

short loc\_313066 eax, [ebp+var\_70] eax, [ebp+var\_84] short loc\_313066 eax, [ebp+var\_84]

[ebp+arg\_0], eax sub\_31486A

short loc 31306D

short loc\_31306D [ebp+arg 0], esi

eax, eax

# Fixing PE header

push edi
call sub\_314623
test eax, eax
jz short loc\_31306D
cmp [ebp+arg\_0], ebx
jnz short loc\_313066
mov eax, [ebp+var\_70]
cmp eax, [ebp+var\_84]
jb short loc\_313066
sub eax, [ebp+var\_84]
push esi
push esi
push eax

short loc 31306D

[ebp+arg\_4]

[ebp+arg\_0]

- Sometimes the PE header doesn't right
- Sometimes you have no PE header
  - -e.g. Dumping from heap
- LordPE is a great tool for dealing with this
  - -Fix, compare, analyze headers

# Tips

```
push edi
call sub_314623
test eax, eax
jz short loc_313060
cmp [ebp+arg_0], ebx
jnz short loc_313066
mov eax, [ebp+var_70]
cmp eax, [ebp+var_84]
jb short loc_313066
sub eax, [ebp+var_84]
push esi
push esi
push eax
```

 PMA Chapter 18 has some great ti several common packers

```
short loc 31306D
                 lea
                         eax, [ebp+arg_0]
                         cax
                         esi, 1D0h
                push
                         881
                push
                         [ebp+arg_4]
                 push
                call
                         sub 314623
                test
                         eax, eax
                         short loc_31306D
                         [ebp+arg 0], esi
                         short loc_31308F
loc 313066:
                                          ; CODE XREF: sub 312FD8
                                          : sub 312FD8+55
                push
                         0 Dh
                call
                         sub_31411B
loc_31306D:
                                          ; CODE XREF: sub 312FD8
                                          ; sub 312FD8+49
                call
                         sub 3140F3
                         eax, eax
                         short loc 31307D
                call
                         sub_3140F3
                         short loc_31308C
                 ij
loc_31307D:
                                          ; CODE XREF: sub 312FD8
                         sub_3140F3
```

eax, 80070000h

### References

```
push
        edi
        sub_314623
test
        eax, eax
        short loc_31306D
        [ebp+arg_0], ebx
        short loc 313066
        eax, [ebp+var_70]
        eax, [ebp+var_84]
        short loc 313066
        eax, [ebp+var_84]
```

1. Sikorski, Michael, and Andrew Honig. Practical Malware Analysis the Hands-on Guide to Dissecting Malicious Software. San Francisco: No Starch, 2012. Print. short loc\_31306D

```
cax
                         esi, 1D0h
                push
                         881
                push
                         [ebp+arg_4]
                 push
                call
                         sub 314623
                test
                         eax, eax
                         short loc_31306D
                         [ebp+arg 0], esi
                         short loc 31308F
loc 313066:
                                          ; CODE XREF: sub 312FD8
                                          : sub 312FD8+55
                push
                         0 Dh
                call
                         sub_31411B
loc_31306D:
                                          ; CODE XREF: sub 312FD8
                                          ; sub 312FD8+49
                call
                         sub 3140F3
                         eax, eax
                         short loc 31307D
                call
                         sub_3140F3
                         short loc_31308C
                                          ; CODE XREF: sub 312FD8
loc_31307D:
                call
                         sub_3140F3
```

push

lea

esi

eax, [ebp+arg\_0]

loc\_31308C:

eax, Offffh eax, 80070000h