```
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
                                                                                    push
                                                                                          es1
                                                                                          [ebp+arg_0], eax
                                                                                    call
                                                                                          sub 31486A
                                                                                          eax, eax
                                                                                           short loc 31306D
                                                                                          eax, [ebp+arg_0]
          Covert Malware Laun
                                                                                    call
                                                                                          sub 314623
                                                                                    test
                                                                                          eax, eax
                                                                                           short loc_31306D
                                                                                           [ebp+arg_0], esi
                                                                                          short loc_31308F
                                    Malware Analysis
                                                                                                        ; CODE XREF: sub 312FD8
                                                                                                        : sub 312FD8+55
                                                                                          0 Dh
                                CSCI 4976 - Fall 2015
                                                                                          sub_31411B
                                                                                                        ; CODE XREF: sub 312FD8
                                                                                                        ; sub 312FD8+49
                                        Branden Clark
                                                                                          sub 3140F3
                                                                                    test
                                                                                          eax, eax
                                                                                          short loc 31307D
                                                                                    call
                                                                                          sub_3140F3
                                                                                          short loc_31308C
                                                                                    THE
                                                                                                        ; CODE XREF: sub 312FD8
                                                                       loc_31307D:
                                                                                          sub_3140F3
                                                                                          eax, 80070000h
Malware - 10/16/2015
                                            Covert Malware Launching
                                                                       loc_31308C:
                                                                                                        ; CODE XREF: sub 312FD8
```

push

edi

[ebp+var 4], eax

- IAT Hooking
- Inline Hooking
- DLL Injection
- Direct Injection
- Process Replacement
- Related

```
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
                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
```

push

edi

- IAT Import Address Table
 - Load addresses of DLLs can change
 - Windows loader dynamically resolves addresses of imports
 - Stores these addresses in the IAT

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

push

call

test

loc 313066:

loc_31306D:

loc_31307D:

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

eax, 80070000h

- Windows uses two methods...
 - Directly call the IAT function pointer...
 - CALL DWORD PTR DS: [401234]
 - call into a jmp table
 - CALL 401567
 - 401567: JMP DWORD PTR DS: 401234

eax, 80070000h

push

call

test

call

test

push

push

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]

short loc_31306D [ebp+arg_0], esi short loc_31308F

sub 31486A

esi, 1D0h

[ebp+arg_4]

sub 314623

eax, eax

881

eax, eax

loc 31308C:

; CODE XREF: sub 312FD8

- Code caves!
 - Not every byte is used
 - Steal some for yourself!
 - Shellcode
 - DLL Names
 - WinAPI names

```
• • •
```

```
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
                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:
                         sub_3140F3
                         eax, 80070000h
```

push

edi

- Hooking first method
 - -Statically: Have to replace all CALLs to the IA
 - Dynamically: Replace address in IAT
- Hooking second method
 - -Only have to replace the entry in the imp tabl

```
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

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

eax, [ebp+arg_0]

[ebp+arg_0], esi short loc 31308F

esi, 1D0h

[ebp+arg_4]

eax, eax

eax, 80070000h

Let's give it a shot!

```
push
                         edi
                         sub_314623
                test
                         eax, eax
                         short loc_31306D
                CID
                         [ebp+arg_0], ebx
                         short loc 313066
                         eax, [ebp+var_70]
                         eax, [ebp+var_84]
                         short loc 313066
                         eax, [ebp+var_84]
                         esi
                push
                         C51
                push
                         eax
                         [ebp+arg_0], eax
                call
                         sub_31486A
                test
                         eax, eax
                         short loc_31306D
                push
                         esi
                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
                         0 Dh
                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
                 THE C
loc_31307D:
                                          ; CODE XREF: sub 312FD8
                         sub_3140F3
                         eax, Offffn
                         eax, 80070000h
loc_31308C:
                                          ; CODE XREF: sub 312FD8
```

- IAT Hooking
- Inline Hooking
- DLL Injection
- Direct Injection
- Process Replacement
- Related

```
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
                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
```

push

edi

; CODE XREF: sub 312FD8

Inline Hooking

- Similar idea
- Insert a JMP into code
 - Beginning or end of function (or anywhere)
 - -Goes to your code
 - log stuff, modify arguments, skip the call, ...

```
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
```

push

call test 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

short loc 31306D

[ebp+arg_4]

[ebp+arg_0], esi short loc 31308F

sub_3140F3

eax, 80070000h

- IAT Hooking
- Inline Hooking
- DLL Injection
- Direct Injection
- Process Replacement
- Related

```
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
                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
loc_31307D:
                                          ; CODE XREF: sub 312FD8
                call
                         sub 3140F3
                         eax, 80070000h
```

push

edi

Injection

```
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 eax
```

- That's cool and all, but how do we modify the memory of the other processes?
 - Just ask Windows!
 - WriteProcessMemory,CreateRemoteThread are key

```
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
                call
```

eax, 80070000h

loc 31308C:

Injection

- Why is it useful for malware?
 - Injected code runs in context of target
 - Helps abuse whitelists
 - Firewall rules
 - · IPS
 - Anti-virus

```
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, [ebp+arg 0]
                         esi, 1D0h
                         881
                         [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
loc_31307D:
                                          ; CODE XREF: sub 312FD8
                         sub_3140F3
                         eax, 80070000h
```

[ebp+var 4], eax

; CODE XREF: sub 312FD8

push

edi

DLL Injection

- 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]
- Windows....Load my DLL into this other process for me!
- LoadLibrary: Load DLL into my address space and execute DLLMain
- What if we tell another process to LoadLibrary? loc 313066:

```
; 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, [ebp+arg 0]

[ebp+arg_4]

sub 314623

loc 31308C:

eax, 80070000h

DLL Injection

Malware - 10/16/2015

- CreateRemoteThread(hVictimProcess,... oadLibrary Address, pDllNameInVictimProcess,...,...); short loc 31306D
 - We need some information first
 - Handle to target process
 - Address of LoadLibrary IN TARGET P
 - Address DLL name/path IN TARGET PROCESS
 - -Luckily what you can't obtain you can stick there yourself

loc_31307D:

 DllMain of loaded DLL is automatically called on load short loc 31308C

sub 3140F3

push

short loc 31306D [ebp+arg_0], ebx

[ebp+arg_0]

[ebp+arg 4]

DLL Injection

Awesome demo on Spotify

```
test
                         eax, eax
                         short loc_31306D
                CID
                         [ebp+arg_0], ebx
                         short loc 313066
                         eax, [ebp+var_70]
                         eax, [ebp+var_84]
                         short loc 313066
                         eax, [ebp+var_84]
                         esi
                push
                         C51
                push
                         eax
                MOV
                         [ebp+arg_0], eax
                call
                         sub 31486A
                 test
                         eax, eax
                         short loc_31306D
                push
                         esi
                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
                                          ; CODE XREF: sub 312FD8
loc_31307D:
                         sub_3140F3
                         eax, 80070000h
```

push

edi sub_314623

loc_31308C:

- IAT Hooking
- Inline Hooking
- DLL Injection
- Direct Injection
- Process Replacement
- Related

```
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
                         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
                 THE C
                                          ; CODE XREF: sub 312FD8
loc_31307D:
                call
                         sub 3140F3
                         eax, 80070000h
                                                      16
```

Direct Injection

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

[ebp+arg_0]

- Windows...Write and execute cod another process for me!
- Similar idea
 - Instead of writing DLL name/path and calling LoadLibrary
 - Write your shellcode and call it directly short loc_31308F
- Disadvantages
 - Have to dynamically resolve any of your dependencies
 - data, imports, resources

```
call sub_31411B

YOUT

; CODE XREF: sub_312FD8

; sub_312FD8+49

call sub_3140F3
test eax, eax

jg short loc_31307D
call sub_3140F3
jmp short loc_31308C
```

/ sub 312FD8+55

```
call sub_3140F3
and eax, Offern
or eax, 80070000h
```

loc_31307D:

- IAT Hooking
- Inline Hooking
- DLL Injection
- Direct Injection
- Process Replacement
- Related

```
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
                         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
```

```
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
```

- In case you're too cool for DLL injection
- Completely replace a process' address space
- Similar advantages to injection
 - Keeps privileges
 - Whitelist abuse
 - Maintain file path

— ...

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

loc 313066:

loc_31306D:

```
    Outline
```

- 1.CreateProcess(...,...,CREATE_SUSPEND
- 2. Unmap current sections
- 3. Alloc new sections
- 4. Write new section contents
- 5. Set EIP to entry point
- 6. Resume process
- Look for this API sequence

```
eax, [ebp+arg_0]
        esi, 1D0h
        [ebp+arg_4]
        sub 314623
test
        eax, eax
        short loc_31306D
        [ebp+arg 0], esi
        short loc 31308F
                         ; CODE XREF: sub 312FD8
```

push

test

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

```
; sub 312FD8+55
push
        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
```

[ebp+var 4], eax

loc_31307D:

loc 313066:

loc_31306D:

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

edi

push

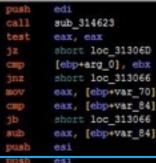
- You can also use Process Explorer.
 - Properties -> Strings -> (Image vs. Memory) 313060
- The difference is usually very apparent

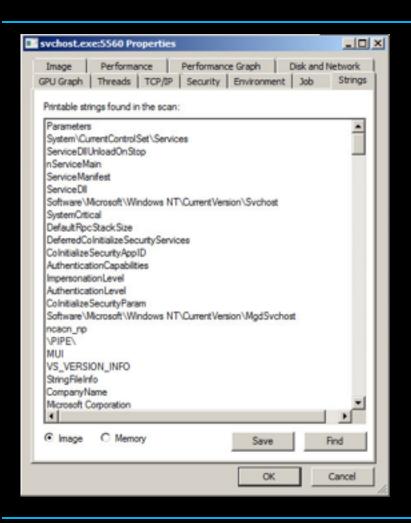
```
edi
                 call
                         sub 314623
                 test
                         eax, eax
                         short loc_31306D
                         [ebp+arg 0], esi
                         short loc 31308F
loc 313066:
                                          ; 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
loc_31307D:
                                          ; CODE XREF: sub 312FD8
                call
                         sub_3140F3
```

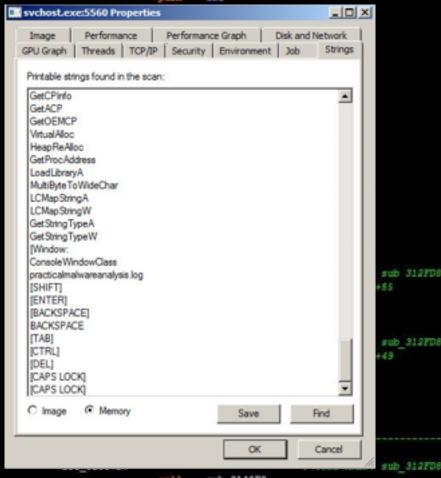
eax, 80070000h

[ebp+arg_4]

loc 31308C:







loc 31308C:

- IAT Hooking
- Inline Hooking
- DLL Injection
- Direct Injection
- Process Replacement
- Related

```
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
                         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
                                          ; CODE XREF: sub 312FD8
```

Windows Hooks

- 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
- Windows has an event/message system
 - Executes callbacks when things occur
 - If you register the handler in your DLL....
 - Then each process is forced to load your DLL to run the handler
- Another way to get your DLL loaded into other processes
- We did something similar for the keylogger we gave you...

short loc_31307D sub_3140F3 short loc_31308C

Covert Malware Launching

Windows APC

```
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_0]

- APC Asynchronous Procedure Ca
 - QueueUserAPC
 - Alternative to CreateRemoteThread
 - Rather than create a new thread for execution
 - Just have an existing thread execute your code when it can
 - When it is waiting (WaitFor..., Sleep, etc)
- Just have it call LoadLibrary or sthg...

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
                 test
                         eax, eax
                         short loc 31307D
                call
                         sub_3140F3
                         short loc_31308C
                                          ; CODE XREF: sub 312FD8
loc_31307D:
                call
                         sub_3140F3
```

eax, Offffh eax, 80070000h

push

lea

esi

eax, [ebp+arg_0]

loc_31308C: