```
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]
                                                                                             push
                                                                                                    esi
                                                                                             push
                                                                                                    esi
                                                                                             push
                                                                                                    eax
                                                                                             push
                                                                                                    edi
                                                                                                    [ebp+arg_0], eax
                                                                                             MOV
                                                                                             call
                                                                                                    sub_31486A
                                                                                             test
                                                                                                    eax, eax
                                                                                                    short loc_31306D
                                                                                                    esi
                                                                                                    eax, [ebp+arg 0]
                Intro to Windows Kei
                                                                                                    [ebp+arg_4]
                                                                                                    sub 314623
                                                                                             test
                                                                                                    eax, eax
                                                                                                    short loc_31306D
                                                                                                    [ebp+arg_0], esi
                                                                                                    short loc_31308F
                                          Aaron Sedlacek
                                                                                                                   ; 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
                                                                              loc_31307D:
                                                                                                                   ; CODE XREF: sub 312FD8
                                                                                                    sub_3140F3
                                                                                                    eax, Offffn
                                                                                                    eax, 80070000h
Malware - 11/10/2015
                                                       Windows Kernel
                                                                              loc_31308C:
                                                                                                                   ; CODE XREF: sub 312FD8
                                                                                                    [ebp+var 4], eax
```

push

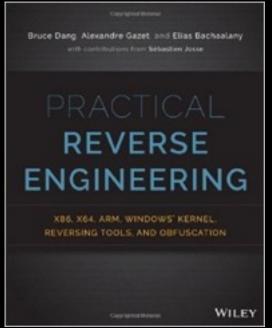
edi

Agenda

- Kernel Basics
- Windows API
- Windows Drivers & Devices
- Kernel Debugging

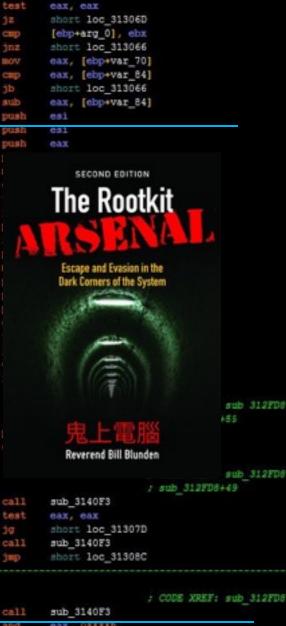
```
push
                         edi
                call
                         sub_314623
                 test
                         eax, eax
                         short loc_31306D
                         [ebp+arg_0], ebx
                         short loc 313066
                         eax, [ebp+var_70]
                         eax, [ebp+var_84]
                         short loc 313066
                         eax, [ebp+var_84]
                         C51
                push
                MOV
                         [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
                 test
                         eax, eax
                         short loc 31307D
                call
                         sub_3140F3
                         short loc_31308C
                 THE
loc_31307D:
                                          ; CODE XREF: sub 312FD8
                         sub_3140F3
                         eax, 80070000h
loc_31308C:
                                          ; CODE XREF: sub 312FD8
                         [ebp+var 4], eax
```

Changing Textbooks!



- ← Your kernel land field guide
- ← Highly recommended
- ← Ch. 3+4 are the focus of this lecture

The most common techniques → Focuses primarily on ring 0 → Also talks about ring -1,-2, and



loc_31307D:

and eax, Offern eax, 80070000h

push

call

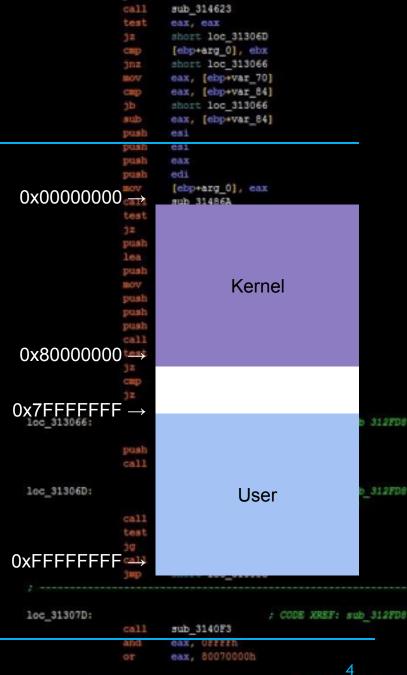
edi

sub 314623

100h

Memory Layout

- Virtual Address Space is divided into two portions
 - Kernel memory space is mostly the same in all processes
 - Kernel mode can access both spaces
 - User mode can only access user space



push

edi

System Calls

- 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
- Kernel function that services I/O requests from users
- Stored in two structures:
 - (System)ServiceDescriptorTable (SDT, SSDT)
 - (System)ServiceDescriptorTableShadow (System)ServiceDescriptor(System)ServiceDescriptorTableShadow (System)ServiceDescriptor(System)ServiceDescriptor(System
 - The shadow table has the same information as the descriptor table
 - It also has an additional syscall table for GUI threads

```
call sub_3140F3
jmp short loc_31308C

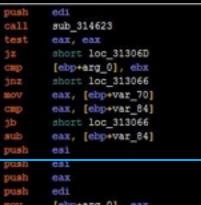
/ code xref: sub_312FD8

call sub_3140F3
```

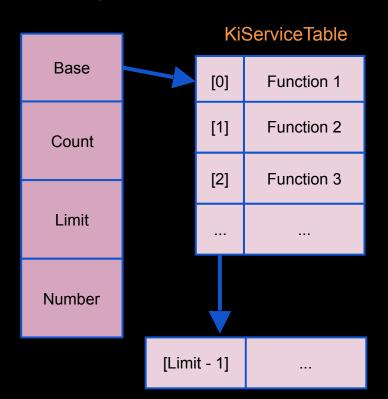
short loc 31307D

sub_3140F3

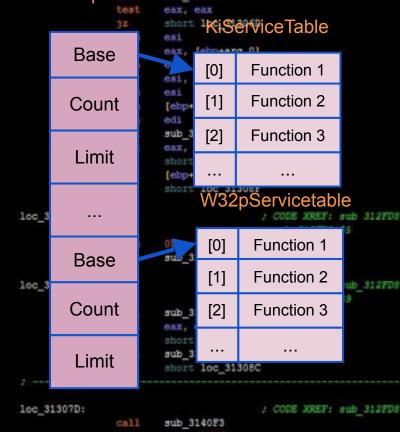
SSDT



KeServiceDescriptorTable



KeServiceDescriptorTableShadow



eax, 80070000h

Interrupts

- Interrupt Descriptor Table →
 - AKA the IDT
 - 256 entries
 - Each interrupt is associated with an index in this table
- Each _KIDT_ENTRY defines the interrupt handler
- The base address of the IDT is stored in a special register called the IDTR

mov eax, [ebp+var_70] cmp eax, [ebp+var_84] jb short loc_313066 sub eax, [ebp+var_84] push esi push esi	
0x0	_KIDT_ENTRY
0x1	_KIDT_ENTRY
	_KIDT_ENTRY
0xFF	_KIDT_ENTRY

```
7 sub 312FD8+49
sub_3140F3
short loc 31307D
sub 3140F3
short loc 31308C
```

loc_31307D:

push

edi

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

sub_3140F3

; CODE XREF: sub 312FD8

Traps

- push 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]
- Pre pentium 2 processors use perform syscalls
- eax, [ebp+arg_0] More modern processors use SYSEN
 - The arguments are passed on the stack instead
 - SYSENTER uses KiFastSystemCall(), which references the SSDT short loc 31308F
 - We will dig deeper into this later with MSR hooking
 - A trap frame is used to save registers before SYSENTER
 - This also saves the user-mode return address

```
: CODE XREF: sub 312FD6
                 ; sub 312FD8+49
sub 3140F3
eax, eax
short loc 31307D
sub 3140F3
short loc 31308C
                 : CODE XREF: sub 312FD8
```

CODE XREF: sub 312FD8

sub 312FD8+55

sub_3140F3

loc_31307D:

Interrupt Request Levels

- Just a number defined by the KIRQL struct
- (0) All user-mode code and most kernel code executes here
- (1) APC's are executed at this level
- (2) Highest in the system

Malware - 11/10/2015

- The thread dispatcher and DPC's run at this IRQL
- Higher IRQL's exist, but are typically associated with hardware

```
[ebp+arg_0], eax
 PASSIVE LEVEL (0)
   APC LEVEL (1)
DISPATCH LEVEL (2)
  sub_3140F3
  short loc 31307D
  short loc 31308C
                 ; CODE XREF: sub 312FD
```

loc_31307D:

sub 3140F3

Pools

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

- Kernel mode memory allocated at runtime
 - Paged pool
 - A page fault exception is generated when kernel code touches this memory while it is paged out
 - Non-paged pool
 - Can never be paged out to the hard drive, never triggers a page fault

```
; 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
```

loc_31308C:

Memory Descriptor Lists

- (MD) (S) (S)
- Data structure used to describe physical pages mapped by a virtual address
 - Describes one contiguous buffer
 - Once an MDL is built over a buffer, pages can be locked in memory (marked non-reusable)
- MDL's must be initialized, probed, and locked
 - MDL's are used to allow drivers to load and modify memory in kernel space

jmp short loc_31308C

Windows Kernel

loc_31307D:

short loc 31307D

Processes and Threads

```
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
```

- Threads and processes are defined by the ETHREAD and EPROCESS structures, respectively
 - ETHREAD and EPROCESS contain basic housekeeping info
 - ETHREAD contains a KTHREAD structure
 - EPROCESS contains a KPROCESS structure
 - KTHREAD and KPROCESS contain scheduling information
 - The PEB and TEB are analogous user-mode data structures

call sub_3140F3
and eax, OFFFFR
or eax, 80070000h

7 sub 312FD8+49

loc_31307D:

loc 31308C:

Thread Execution Contex

- Thread Contexts contain the address space, security token, etc.
 - a. Thread Context of a specific thread
 - IOCTL handler, APC's
 - b. System Context of a thread executing as System
 - DriverEntry(), work items, system threads
 - c.Arbitrary Context of the previous thread
 - DPC's, timers

short loc_313066 eax, [ebp+var 84]

Windows Kernel

sub 3140F3

Kernel Synchronization Mechanisms

- Events Indicate the state of an operation
 - A thread can wait for a particular event to occur
- Timers Indicate that a certain time interval has passed
- Spin locks and Mutexes Used for exclusive access to shared resources
 - Spin locks are used to protect resources that are accessed at DISPATCH_LEVEL or higher IRQL

```
test eax, eax
jg short loc_31307D
call sub_3140F3
jmp short loc_31308C
;
loc_31307D: ; CODE XREF: sub_312FD0
```

And eax, Serren
or eax, 80070000h

loc 31308C:

Agenda

- Kernel Basics
- Windows API
- Windows Drivers & Devices
- Kernel Debugging

```
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
                 test
                         eax, eax
                         short loc 31307D
                call
                         sub_3140F3
                         short loc_31308C
                 THE
                                          ; CODE XREF: sub 312FD8
loc_31307D:
                         sub_3140F3
                         eax, 80070000h
loc_31308C:
                                          ; CODE XREF: sub 312FD8
```

Asynchronous Execution

System Threads

- Drivers can create threads to execute functions
- Initialized with PsCreateSystemThread()

Work Items

- They are objects in a queue processed by a pool of system threads, they do not have their own thread
- Initialized by IoAllocateWorkItem()
- loQueueWorkItem() places the work item in the PRCB

```
call sub_3140F3
test eax, eax
jg short loc_31307D
call sub_3140F3
jmp short loc_31308C
;
loc_31307D: ; CODE XREF: sub_312FD0
call sub_3140F3
and eax, 0FFFFR
or eax, 80070000h
```

[ebp+var 4], eax

short loc_31306D [ebp+arg_0], ebx

eax, [ebp+var 84]

[ebp+arg_0], eax

[ebp+arg 4]

loc 31308C:

Asynchronous Procedure Ca

- The functions that are executed in particular thread context
 - Defined by the KAPC structure

Malware - 11/10/2015

- Executes at either PASSIVE_LEVEL or APC_LEVEL
- Initialized by KelnitializeApc() and inserted into a KTHREAD's queue with KelnsertQueueApc()
- APC's are frequently used by rootkits
 - Clean way to inject code into user-land from kernel-land

; CODE XREF: sub_312FD0

; sub 312FD8+49

[ebp+arg_0]

Windows Kernel

loc_31307D:

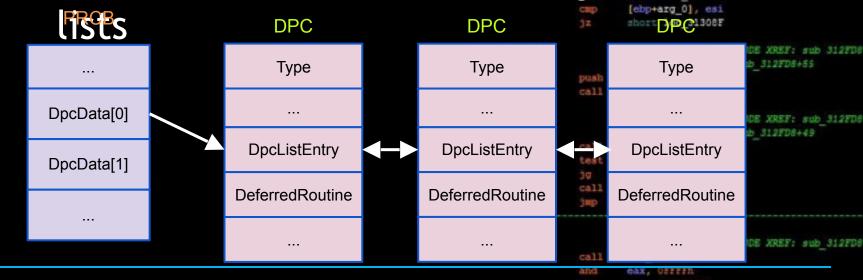
17 loc_31308C: ; CODE XREF: sub

short loc 31307D

short loc 31308C

Deferred Procedure Calls

- Routines executed at DISPATCH TEX
 - Used to quickly execute short tasks
 - KelnitializeDpc() and KelnsertQueueDpc()
 - Rootkits use DPC's to access global linked



Malware - 11/10/2015

Windows Kernel

loc 31308C: : CODE XREF: sub 312FD8 [ebp+var 4], eax

Callback Functions

```
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
```

- Drivers can register callbacks for certain system events
- Usually related to processes and threads
 - PsSetCreateProcessNotifyRoutine()
 - PsSetCreateThreadNotifyRoutine()
 - PsSetLoadImageNotifyRoutine()

```
push esi
push [ebp+arg_4]
push edi
call sub_314623
test eax, eax
jz short loc_31306D
cmp [ebp+arg_0], esi
jz short loc_31308F

; CODE XREF: sub_312FD8
push ODh
call sub_31411B
```

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

loc 313066:

loc_31307D:

I/O Request Packet (IRP)

- IRP's are used to describe I/O requests to kernel components
 - Each IRP describes a request and is passed through multiple devices until it is completed
 - MajorFunction and MinorFunction
 - Predefined lists that define all request types
 - File read request → IRP_MJ_READ
 - File write request → IRP_MJ_WRITE

```
VRITE

push
call
sub_314118

loc_31306D:

; CODE XREF: sub_312FD8

; sub_312FD8+55

; sub_312FD8+69

call
sub_3140F3
test
eax, eax
jg short loc_31307D
call
sub_3140F3
jmp short loc_31308C

;
loc_31307D:
; CODE XREF: sub_312FD8

; sub_312FD8+69

call
sub_3140F3
and
cax, OFFFFR
or
eax, 80070000h
```

edi sub 314623

short loc_31306D [ebp+arg_0], ebx

[ebp+var 84]

[ebp+var 84]

eax, [ebp+arg_0]

short loc 31306D

sub 314623

Malware - 11/10/2015 Windows Kernel

loc_31308C:

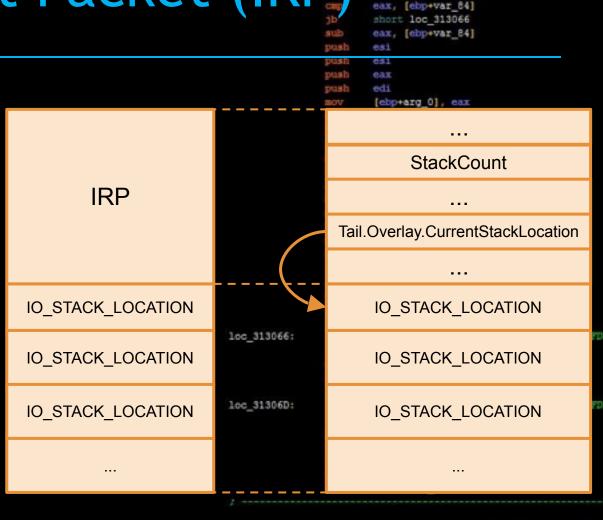
; CODE XREF: sub_312FD(
[ebp+var 4], eax

I/O Request Packet (IRP)

One IO_STACK_LOCATION structure allocated per device in the device stack

Each device is responsible for preparing the next IO_STACK_LOCATION

CurrentStackLocation pointer moves upward, towards the IRP



push

sub 314623

short loc_31306D [ebp+arg_0], ebx

[ebp+var 70]

loc_31307D:

d cax, Offern

x, 80070000h

; CODE XREF: sub 312FD8

Completion Routines

```
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
```

- Devices are layered on top of each other
 - Higher level drivers can pass requests to lower ones
 - OWhichever layer completes the request by calling loCompleteRequest() → executes the completion routine
- Completion routines are registered using

IoSetCompletionRoutine()

 Rootkits often set completion routines to manipulate lower level drivers for nefarious purposes!

```
; CODE XREF: sub_312FD
call sub_3140F3
and eax, Office
or eax, 80070000h
```

Malware - 11/10/2015 Windows Kernel

loc_31307D:

sub 312FD8+55

; sub 312FD8+49

Agenda

- Kernel Basics
- Windows API
- Windows Drivers & Devices
- Kernel Debugging

```
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
                         C51
                push
                MOV
                         [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
                 test
                         eax, eax
                         short loc 31307D
                call
                         sub_3140F3
                         short loc_31308C
                 THE
loc_31307D:
                                          ; CODE XREF: sub 312FD8
                         sub_3140F3
                         eax, 80070000h
loc_31308C:
                                          ; CODE XREF: sub 312FD8
```

Windows Driver Kit (WD

short loc 31306D ebp+arg 0], ebx [ebp+var 84]

push

edi sub 314623

- You all have Visual Studio Professional for free! short loc 31306D
 - eax, [ebp+arg_0] https://www.dreamspark.com
 - Download it and get it running, need it for the windows API short loc 31306D [ebp+arg 0], esi

```
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

short loc 31308F

loc_31308C:

Driver Basics

- short loc 313066 eax, [ebp+var 70] eax, [ebp+var 84] short loc 313066 eax, [ebp+var_84] DriverEntry [ebp+arg_0], eax
 - Think of a driver as a DLL for the kernel
 - The DriverEntry function is immediately executed when a driver is loaded
 - Initializes any driver-specific settings an routines short loc 31306D [ebp+arg 0], esi
- **Driver Objects**
 - One per driver, tracks driver data for the kernel

loc 31306D:

- **Device Objects**
 - One per device, contains device-specific data

Windows Kernel

sub 3140F3 short loc 31308C loc_31307D: ; CODE XREF: sub 312FD: sub 3140F3 loc 31308C: [ebp+var 4], eax

short loc 31308F

push

edi sub 314623

short loc_31306D

[ebp+arg 0], ebx

Driver Basics

- IRP Handling
 - DriverEntry makes routines for each MajorFunction
 - METHOD_BUFFERED I/O
 - User buffer is copied into a non-paged pool in AssociatedIrp.SystemBuffer, which gets copied back to userland upon IoCompleteRequest
- METHOD_IN_DIRECT/METHOD_OUT_DIRECT_I/O.
 - Driver gets an MDL describing the user buffer
- Neither The raw data is passed to the driver

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 4]

IOCTL

- IRP MJ DEVICE CONTROL
 - Special IRP MajorFunction type
 - The driver switches over an IOCTL code
 - See skeleton-rootkit for usage

```
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
                         [ebp+arg_0], eax
                 call
                         sub 31486A
                         eax, eax
                         short loc 31306D
                         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
                                          ; CODE XREF: sub 312FD8
```

Agenda

- Kernel Basics
- Windows API
- Windows Drivers & Devices
- Kernel Debugging

```
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
                MOV
                         [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
                 test
                         eax, eax
                         short loc 31307D
                call
                         sub_3140F3
                         short loc_31308C
                 THE
                                          ; CODE XREF: sub 312FD8
loc_31307D:
                         sub_3140F3
                         eax, 80070000h
loc_31308C:
                                          ; CODE XREF: sub 312FD8
                         [ebp+var 4], eax
```

Requirements

1. Two virtual machines

a.One running your debuggerb.One being debugged

2.WinDBG

a. Our chosen debugger for this course

```
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
                 lea
                         eax, [ebp+arg_0]
                         esi, 1D0h
                         681
                         [ebp+arg_4]
                         sub 314623
                         cax, cax
                         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
```

push

call

test

edi

sub_314623

short loc_31306D [ebp+arg_0], ebx

eax, eax

loc_31308C:

Set Up

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

- Your two virtual machines must be connected
 - eax, [ebp+arg_0] Depending on your host operating system, you use a virtual network, serial port, etc. [ebp+arg_4]

sub 314623 eax, eax

short loc 31306D [ebp+arg_0], esi short loc 31308F

- Symbols
 - https://support.microsoft.com/en-us/kb/311503

loc_31308C:

```
call
                         sub 31411B
loc_31306D:
                                          ; CODE XREF: sub 312FD6
                                          ; 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
```

[ebp+var 4], eax

; CODE XREF: sub 312FD8

```
push
                                                                                                    call
                                                                                                            sub_314623
                                                                                                    test
                                                                                                            eax, eax
                                                                                                            short loc_31306D
                                                                                                    CHIP
                                                                                                            [ebp+arg_0], ebx
                                                                                                            short loc_313066
                                                                                                            eax, [ebp+var_70]
                                                                                                    MOV
                                                                                                            eax, [ebp+var_64]
                                                                                                    CHD
                                                                                                            short loc 313066
                                                                                                    sub
                                                                                                            eax, [ebp+var_84]
                                                                                                    push
                                                                                                            esi
                                                                                                    push
                                                                                                            esi
                                                                                                    push
                                                                                                            eax
                                                                                                    push
                                                                                                            edi
                                                                                                            [ebp+arg_0], eax
                                                                                                    MOV
                                                                                                    call
                                                                                                            sub_31486A
                                                                                                    test
                                                                                                            eax, eax
                                                                                                            short loc_31306D
                                                                                                    push
                                                                                                            esi
                                                                                                            eax, [ebp+arg_0]
                                                                                                    push
                                                                                                            cax
                                                                                                    MOV
                                                                                                            esi, 1D0h
                                                                                                    push
                                                                                                            681
                                                                                                    push
                                                                                                            [ebp+arg_4]
                                        Demo Driver!
                                                                                                    push
                                                                                                            edi
                                                                                                            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
                                                                                                            short loc 31307D
                                                                                                    call
                                                                                                            sub_3140F3
                                                                                                            short loc_31308C
                                                                                                    THE
                                                                                                                            ; CODE XREF: sub 312FD8
                                                                                    loc_31307D:
                                                                                                            sub_3140F3
                                                                                                            cax, Offifh
                                                                                                            eax, 80070000h
Malware - 11/10/2015
                                                           Windows Kernel
                                                                                                                                       31
                                                                                     loc_31308C:
                                                                                                                            ; CODE XREF: sub 312FD8
                                                                                                            [ebp+var 4], eax
```

edi

```
push
                                                                                                             edi
                                                                                                     call
                                                                                                             sub_314623
                                                                                                     test
                                                                                                             eax, eax
                                                                                                             short loc_31306D
                                                                                                     CID
                                                                                                             [ebp+arg_0], ebx
                                                                                                             short loc_313066
                                                                                                             eax, [ebp+var_70]
                                                                                                             eax, [ebp+var_64]
                                                                                                     CHD
                                                                                                             short loc 313066
                                                                                                     sub
                                                                                                             eax, [ebp+var_84]
                                                                                                     push
                                                                                                             esi
                                                                                                     push
                                                                                                             esi
                                                                                                     push
                                                                                                             eax
                                                                                                     push
                                                                                                             edi
                                                                                                     MOV
                                                                                                             [ebp+arg_0], eax
                                                                                                     call
                                                                                                             sub_31486A
                                                                                                     test
                                                                                                             eax, eax
                                                                                                             short loc_31306D
                                                                                                     push
                                                                                                             esi
                                                                                                             eax, [ebp+arg_0]
                                              Questions?
                                                                                                             cax
                                                                                                     MOV
                                                                                                             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
                                                                                                             short loc 31307D
                                                                                                     call
                                                                                                             sub_3140F3
                                                                                                             short loc_31308C
                                                                                                     THE
                                                                                                                             ; CODE XREF: sub 312FD8
                                                                                     loc_31307D:
                                                                                                             sub_3140F3
                                                                                                             cax, Offffh
                                                                                                             eax, 80070000h
Malware - 11/10/2015
                                                            Windows Kernel
                                                                                     loc_31308C:
                                                                                                                             ; CODE XREF: sub 312FD8
                                                                                                             [ebp+var 4], eax
```

References

```
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
```

1. Dang, Bruce, and Alexandre Gazet. *Practical Reverse Engineering: X86, X64, ARM, Windows Kernel, Reversing Tools, and Obfuscation.* Print.

```
short loc_31306D
                push
                         esi
                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
                         sub 3140F3
                 test
                         eax, eax
                         short loc 31307D
                call
                         sub_3140F3
                         short loc_31308C
                 ij
                                          ; CODE XREF: sub 312FD8
loc_31307D:
                         sub_3140F3
                         eax, 80070000h
```