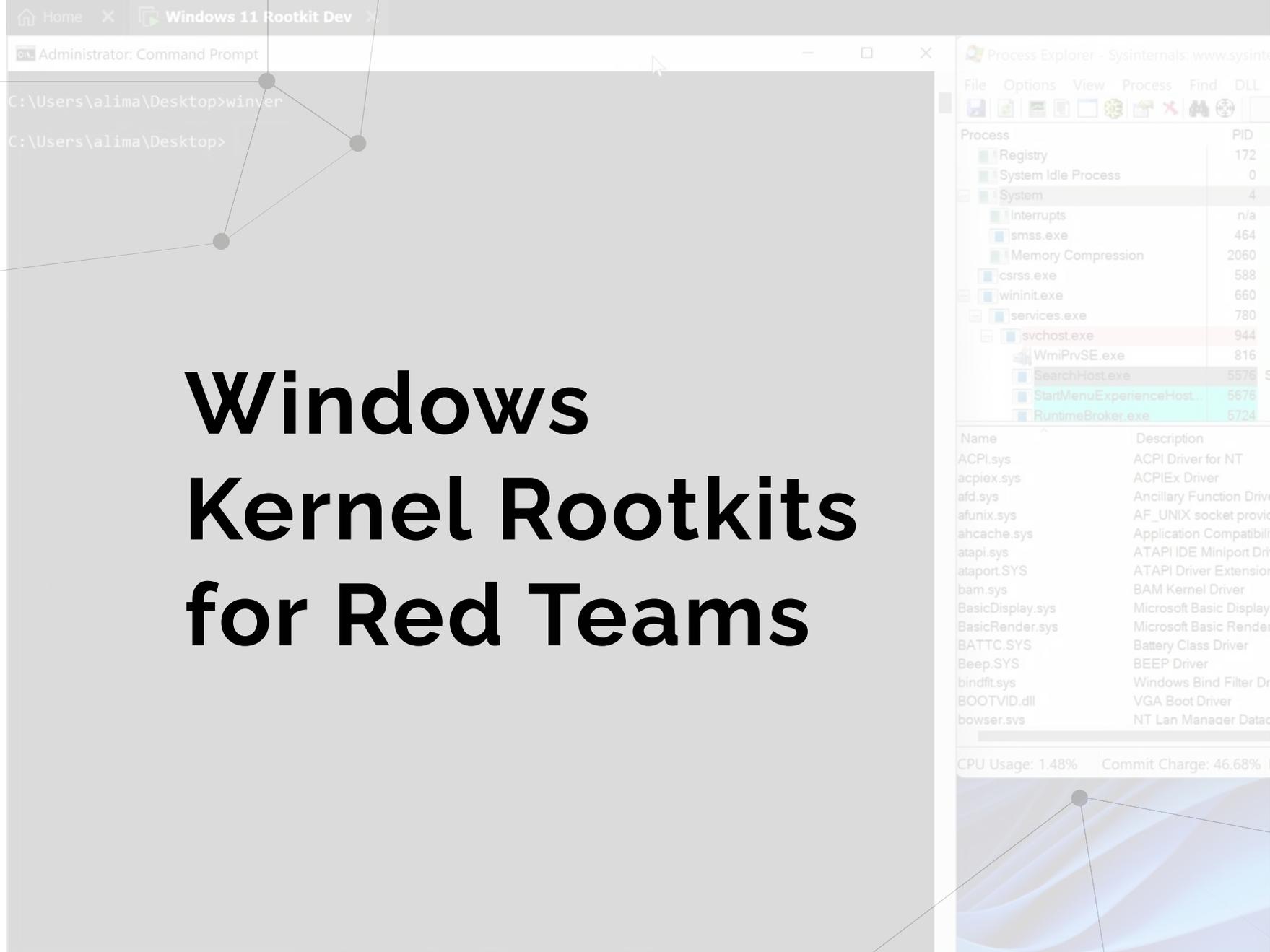


# Windows Kernel Rootkits for Red Teams



## > whoami

- Work @ PwC Norway
- Pentester | Red Teamer | Researcher
- Worked in Portugal (Lisbon), Australia (Melbourne), and now Norway (Oslo)
- Blogger + Youtube channel
- Certs: OSED, eCRE, SLAE64, etc
- Best friends: windbg, IDA, assembly



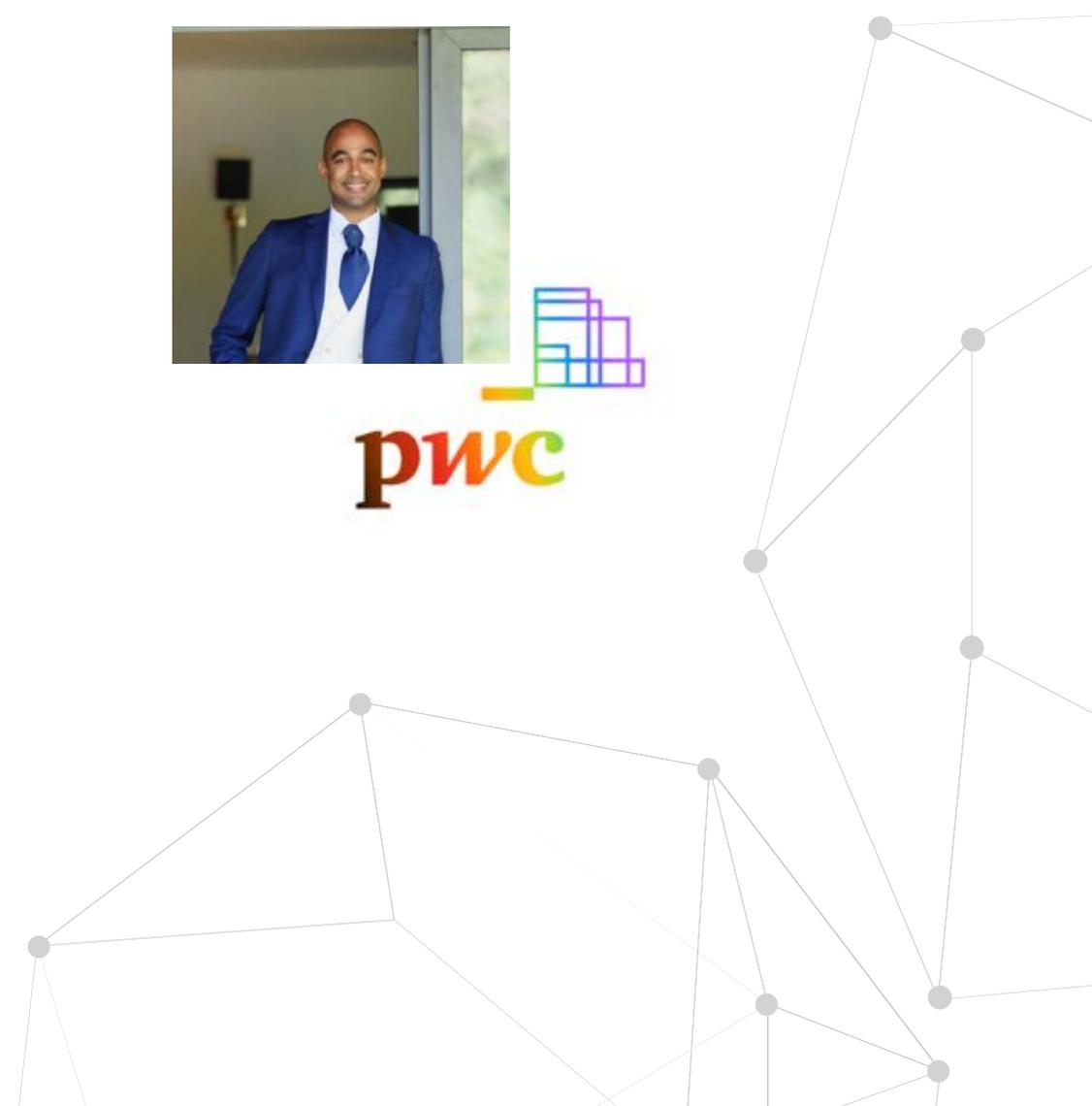
<https://twitter.com/0x4ndr3>



<https://www.youtube.com/@0x4ndr3>



<https://www.linkedin.com/in/aflima/>



● WHAT ARE WE GOING TO TALK ABOUT?

- Why kernel dev?
- Objective
- Kernel Code Execution
- Demo #1
- Intro to the Windows kernel
- Methodology for rootkit dev
- Hiding a process
- Demo #2
- Keylogger
- Demo #3
- Virtual Secure Mode (VSM)
- References

```
397 auto PIO_STACK_LOCATION
398 switch (stack->Par
399 case IOCTL_ROO
400 // Irp->As
401 ExecuteAtD
402 break;
403 case IOCTL_ROO
404 // Execute
405 ExecuteAtD
406 break;
407 case IOCTL_ROO
408 if (HideOn
409 ExFree
410 PsSetC
411 }
412 HideOnCrea
413 i = 0;
414 aux = ((PU
415 while (aux
416 HideOn
417 ++i;
418 aux =
419 }
420 ntStatus =
421 break;
422 case IOCTL_ROO
423 ExecuteAtD
424 break;
425 case IOCTL_ROO
426 LPE( toProces
427 break;
428 case IOCTL_ROO
```

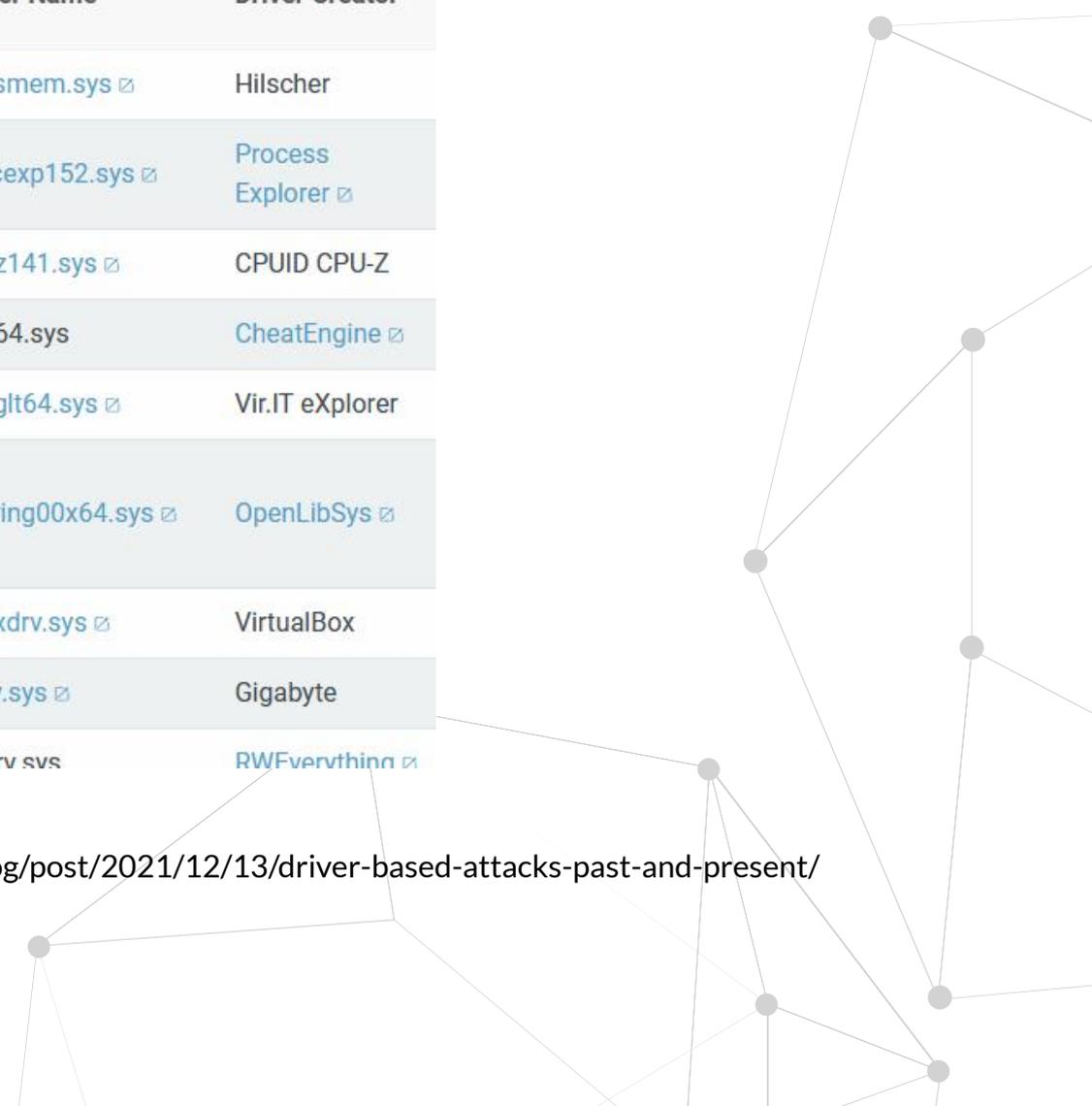
# → Why kernel dev?



Year Published	Adversary/Malware	Driver Name	Driver Creator
2021	<a href="#">Candiru</a>	<a href="#">physmem.sys</a>	Hilscher
2021	<a href="#">Iron Tiger</a>	<a href="#">procexp152.sys</a>	<a href="#">Process Explorer</a>
2021	Iron Tiger	<a href="#">cpuz141.sys</a>	CPUID CPU-Z
2021	<a href="#">GhostEmperor</a>	<a href="#">dbk64.sys</a>	<a href="#">CheatEngine</a>
2021	<a href="#">ZINC</a>	<a href="#">viraglt64.sys</a>	Vir.IT eXplorer
2021	Various Cryptominers using XMRig	<a href="#">winring00x64.sys</a>	<a href="#">OpenLibSys</a>
2021	<a href="#">TunnelSnake</a>	<a href="#">vboxdrv.sys</a>	VirtualBox
2020	<a href="#">RobbinHood</a>	<a href="#">gdrv.sys</a>	Gigabyte
2020	<a href="#">Trickhot</a>	<a href="#">rwdrv.sys</a>	<a href="#">RWFEverything</a>

Many more...

Source: <https://www.rapid7.com/blog/post/2021/12/13/driver-based-attacks-past-and-present/>



```
397 auto PIO_STACK_LOCATION
398 switch (stack->Par
399     case IOCTL_R00
400         // Irp->As
401         ExecuteAtD
402         break;
403     case IOCTL_R00
404         // Execute
405         ExecuteAtD
406         break;
407     case IOCTL_R00
408         if (HideOn
409             ExFree
410             PsSetC
411         }
412         HideOnCrea
413         i = 0;
414         aux = ((PU
415         while (aux
416             HideOn
417             ++i;
418             aux =
419         }
420         ntStatus =
421         break;
422     case IOCTL_R00
423         ExecuteAtD
424         break;
425     case IOCTL_R00
426         LPE( toProces
427         break;
428     case IOCTL_R00
```

# → Why kernel dev?

Allows for:

- More advanced tool dev for Red Teams
- Advanced Blue Team training
- Better understanding of kernel exploit dev
- Opening of interesting new attack surface for bug hunting (i.e. Hyper-V)



```
397 auto PIO_STACK_LOCATION
398 switch (stack->Par
399     case IOCTL_R00
400         // Irp->As
401         ExecuteAtD
402         break;
403     case IOCTL_R00
404         // Execute
405         ExecuteAtD
406         break;
407     case IOCTL_R00
408         if (HideOn
409             ExFree
410             PsSetC
411         }
412         HideOnCrea
413         i = 0;
414         aux = ((PU
415         while (aux
416             HideOn
417             ++i;
418             aux =
419         }
420         ntStatus =
421         break;
422     case IOCTL_R00
423         ExecuteAtD
424         break;
425     case IOCTL_R00
426         LPE( toProces
427         break;
428     case IOCTL_R00
```

# → Objective

- Make you curious about all things kernel
- Show you interesting things you can do in it.



```
397 auto PIO_STACK_LOCATION
398 switch (stack->Par
399     case IOCTL_R00
400         // Irp->As
401         ExecuteAtD
402         break;
403     case IOCTL_R00
404         // Execute
405         ExecuteAtD
406         break;
407     case IOCTL_R00
408         if (HideOn
409             ExFree
410             PsSetC
411         }
412         HideOnCrea
413         i = 0;
414         aux = ((PU
415         while (aux
416             HideOn
417             ++i;
418             aux =
419         }
420         ntStatus =
421         break;
422     case IOCTL_R00
423         ExecuteAtD
424         break;
425     case IOCTL_R00
426         LPE( toProces
427         break;
428     case IOCTL_R00
```

# → Kernel code execution

Common ways:

- Sign your own driver: technically simpler but risky



# → Kernel code execution

Common ways:

- Sign your own driver: technically simpler but risky
- BYOVD: less risky, but technically trickier
  - known by the community: there are a lot!

```
397 auto PIO_STACK_LOCATION
398 switch (stack->Par
399     case IOCTL_ROO
400         // Irp->As
401         ExecuteAtD
402         break;
403     case IOCTL_ROO
404         // Execute
405         ExecuteAtD
406         break;
407     case IOCTL_ROO
408         if (HideOn
409             ExFree
410             PsSetO
411         }
412         HideOnCrea
413         i = 0;
414         aux = ((PU
415         while (aux
416             HideOn
417             ++i;
418             aux =
419         }
420         ntStatus =
421         break;
422     case IOCTL_ROO
423         ExecuteAtD
424         break;
425     case IOCTL_ROO
426         LPE( toProces
427         break;
428     case IOCTL_ROO
```

```
<Deny ID="ID_DENY_ATILLK_1F" FriendlyName="atillk64\d2182b6ef3255c7c1a69223cd3c
<Deny ID="ID_DENY_BANDAI_SHA1" FriendlyName="bandai.sys Hash Sha1" Hash="0F780B
<Deny ID="ID_DENY_BANDAI_SHA256" FriendlyName="bandai.sys Hash Sha256" Hash="7F
<Deny ID="ID_DENY_BANDAI_SHA1_PAGE" FriendlyName="bandai.sys Hash Page Sha1" Ha
<Deny ID="ID_DENY_BANDAI_SHA256_PAGE" FriendlyName="bandai.sys Hash Page Sha256
<Deny ID="ID_DENY_BS_RCI064_SHA1" FriendlyName="BS_RCI064 73327429c505d8c5fd690
<Deny ID="ID_DENY_BS_RCI064_SHA256" FriendlyName="BS_RCI064 73327429c505d8c5fd6
<Deny ID="ID_DENY_BS_RCI064_SHA1_PAGE" FriendlyName="BS_RCI064 5651466512138240
<Deny ID="ID_DENY_BS_RCI064_SHA256_PAGE" FriendlyName="BS_RCI064 56514665121382
<Deny ID="ID_DENY_CAPCOM_SHA1" FriendlyName="capcom.sys Hash Sha1" Hash="1D1CAF
<Deny ID="ID_DENY_CAPCOM_SHA256" FriendlyName="capcom.sys Hash Sha256" Hash="FA
<Deny ID="ID_DENY_CAPCOM_SHA1_PAGE" FriendlyName="capcom.sys Hash Page Sha1" Ha
<Deny ID="ID_DENY_CAPCOM_SHA256_PAGE" FriendlyName="capcom.sys Hash Page Sha256
<Deny ID="ID_DENY_DBUTIL_32_SHA1" FriendlyName="32-bit dell dbutil.sys Hash Sha
<Deny ID="ID_DENY_DBUTIL_32_SHA256" FriendlyName="32-bit dell dbutil.sys Hash S
<Deny ID="ID_DENY_DBUTIL_32_SHA1_PAGE" FriendlyName="32-bit dell dbutil.sys Has
<Deny ID="ID_DENY_DBUTIL_32_SHA256_PAGE" FriendlyName="32-bit dell dbutil.sys H
<Deny ID="ID_DENY_DBUTIL_64_SHA1" FriendlyName="64-bit dell dbutil.sys Hash Sha
<Deny ID="ID_DENY_DBUTIL_64_SHA256" FriendlyName="64-bit dell dbutil.sys Hash S
```

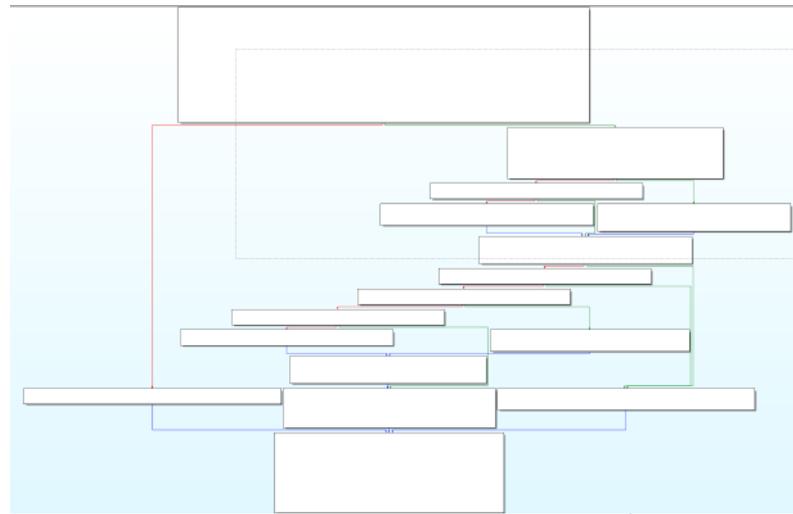
Source: <https://learn.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-control/microsoft-recommended-driver-block-rules>

# → Kernel code execution

Common ways:

- Sign your own driver
- BYOVD:
  - known by the community: there are a lot!
  - find your own ...

```
397 auto PIO_STACK_LOCATION
398 switch (stack->Par
399     case IOCTL_R00
400         // Irp->As
401         ExecuteAtD
402         break;
403     case IOCTL_R00
404         // Execute
405         ExecuteAtD
406         break;
407     case IOCTL_R00
408         if (HideOn
409             ExFree
410             PsSetC
411         }
412         HideOnCrea
413         i = 0;
414         aux = ((PU
415         while (aux
416             HideOn
417             ++i;
418             aux =
419         }
420         ntStatus =
421         break;
422     case IOCTL_R00
423         ExecuteAtD
424         break;
425     case IOCTL_R00
426         LPE( toProces
427         break;
428     case IOCTL_R00
```



# → Kernel code execution

Common ways:

- Sign your own driver
- BYOVD:
  - **known by the community**: there are a lot!
  - find your own ...



Why **BYOVD with a known vuln driver**?

- be able to emulate a common malicious technique
- be able to recommend better detection to Blue Teams

```
397 auto PIO_STACK_LOCATION
398 switch (stack->Par
399     case IOCTL_R00
400         // Irp->As
401         ExecuteAtD
402         break;
403     case IOCTL_R00
404         // Execute
405         ExecuteAtD
406         break;
407     case IOCTL_R00
408         if (HideOn
409             ExFree
410             PsSetC
411         }
412         HideOnCrea
413         i = 0;
414         aux = ((PU
415         while (aux
416             HideOn
417             ++i;
418             aux =
419         }
420         ntStatus =
421         break;
422     case IOCTL_R00
423         ExecuteAtD
424         break;
425     case IOCTL_R00
426         LPE( toProces
427         break;
428     case IOCTL_R00
```

# → Kernel code execution

Objective: disable DSE so I can load my own driver/rootkit

```
397 auto PIO_STACK_LOCATION
398 switch (stack->Par
399     case IOCTL_ROOT
400         // Irp->As
401         ExecuteAtD
402         break;
403     case IOCTL_ROOT
404         // Execute
405         ExecuteAtD
406         break;
407     case IOCTL_ROOT
408         if (HideOn
409             ExFree
410             PsSetC
411         }
412         HideOnCrea
413         i = 0;
414         aux = ((PU
415         while (aux
416             HideOn
417             ++i;
418             aux =
419         }
420         ntStatus =
421         break;
422     case IOCTL_ROOT
423         ExecuteAtD
424         break;
425     case IOCTL_ROOT
426         LPE( toProces
427         break;
428     case IOCTL_ROOT
```

CA. Select Administrator: Command Prompt

```
C:\Users\alima\Desktop>sc create rootkit type= kernel binPat
[SC] CreateService SUCCESS

C:\Users\alima\Desktop>sc start rootkit
[SC] StartService FAILED 577:

Windows cannot verify the digital signature for this file. A
might have installed a file that is signed incorrectly or dam
ware from an unknown source.

C:\Users\alima\Desktop>_
```



Your PC ran into a problem and needs to restart. We're just collecting some error info, and then we'll restart for you.

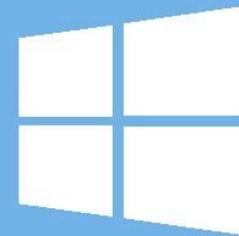
20% complete



For more information about this issue and possible fixes, visit <https://www.windows.com/stopcode>

If you call a support person, give them this info:

Stop code: CRITICAL\_PROCESS\_DIED



## DEMO #1 - bypassing DSE

Windows 11 Rootkit Dev

Administrator: Command Prompt

```
C:\Users\alima\Desktop>winver  
C:\Users\alima\Desktop>
```

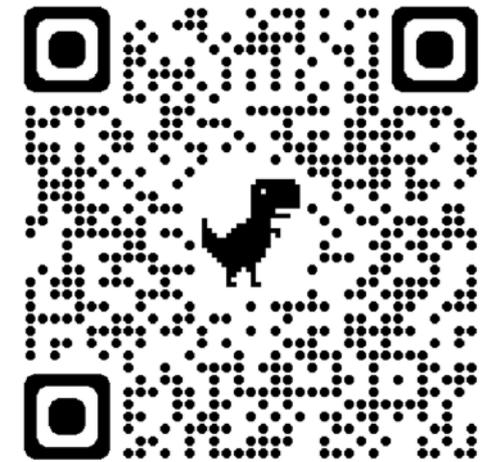
Process Explorer - Sysinternals: www.sysinternals.com

File Options View Process Find DLL

Process	PID
Registry	172
System Idle Process	0
System	4
Interrupts	n/a
smss.exe	464
Memory Compression	2060
csrss.exe	588
wininit.exe	660
services.exe	780
svchost.exe	944
WmiPrvSE.exe	816
SearchHost.exe	5576
StartMenuExperienceHost.exe	5676
RuntimeBroker.exe	5724

Name	Description
ACPI.sys	ACPI Driver for NT
acpiex.sys	ACPIEx Driver
afd.sys	Ancillary Function Driver
afunix.sys	AF_UNIX socket provider
ahcache.sys	Application Compatibility
atapi.sys	ATAPI IDE Miniport Driver
ataport.SYS	ATAPI Driver Extension
bam.sys	BAM Kernel Driver
BasicDisplay.sys	Microsoft Basic Display
BasicRender.sys	Microsoft Basic Render
BATTC.SYS	Battery Class Driver
Beep.SYS	BEEP Driver
bindflt.sys	Windows Bind Filter Driver
BOOTVID.dll	VGA Boot Driver
bowser.sys	NT Lan Manager Data

CPU Usage: 1.48% Commit Charge: 46.68%



Disclaimer: Win 11 22H2

The image shows a Windows 11 desktop environment. In the foreground, the 'About Windows' window is open, displaying the Windows 11 logo and version information. Below it, a Command Prompt window is open, showing the execution of a command to start a service, which has failed with an error message. The error message is highlighted in a white box.

**About Windows**

 **Windows 11**

Microsoft Windows  
Version 22H2 (OS Build 22621.675)  
© Microsoft Corporation. All rights reserved.

The Windows 11 Home operating system and its components are protected by trademark and other pending or registered rights in the United States and other countries.

This product is licensed under the [Microsoft Software License Terms](#) to:  
alima

**Select Administrator: Command Prompt**

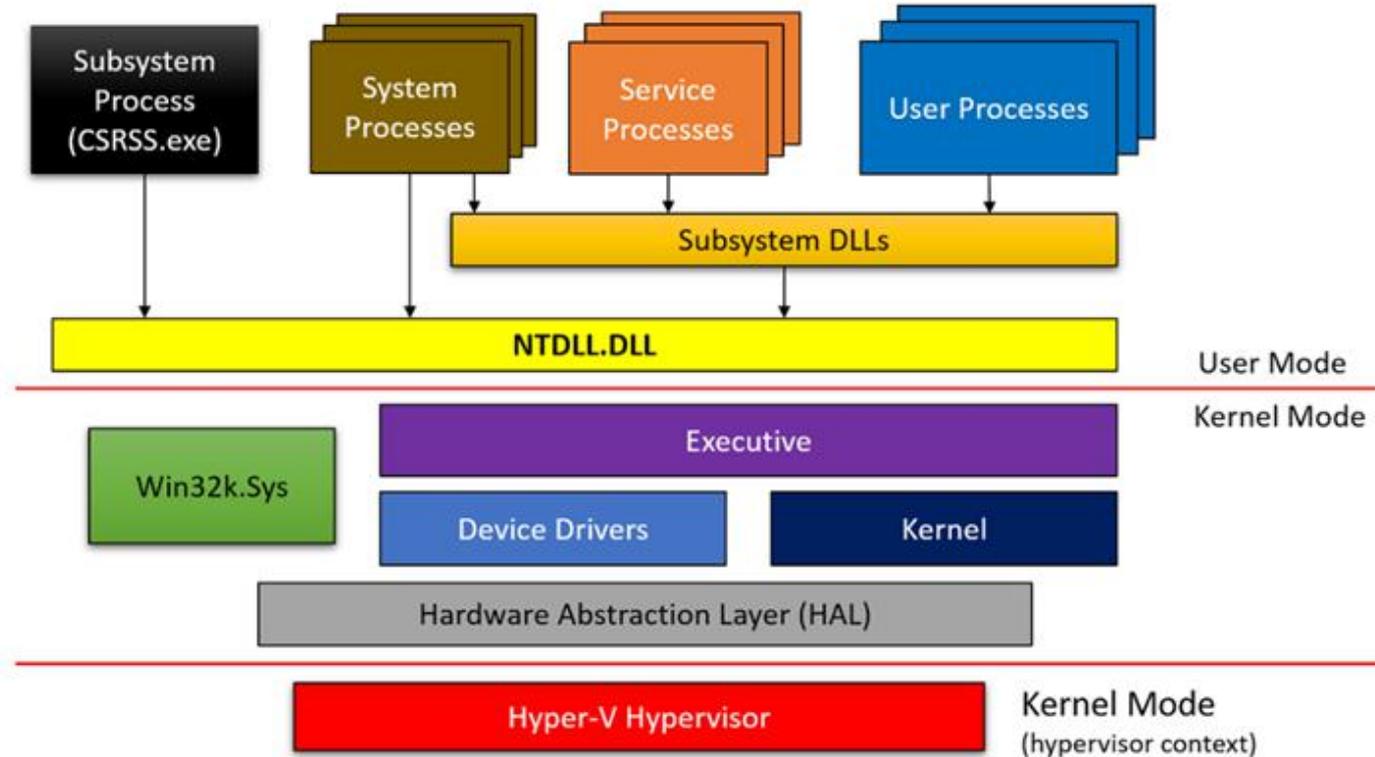
```
C:\Users\alima\Desktop>sc start uceanismkljpk  
[SC] StartService FAILED 2148204812:  
A certificate was explicitly revoked by its issuer.  
  
C:\Users\alima\Desktop>
```

From the attackers perspective:

Kernel exec	Loading driver	Exploitation
Signed driver	✓	N/A
BYOVD: known	 Blocked in Win 11 22H2	 HVCI could be an issue
BYOVD: unknown	✓	 HVCI could be an issue

# → Intro to Windows Kernel

```
397 auto P10_STACK_LOCATION
398 switch (stack->Par
399     case IOCTL_R00
400         // Irp->As
401         ExecuteAtD
402         break;
403     case IOCTL_R00
404         // Execute
405         ExecuteAtD
406         break;
407     case IOCTL_R00
408         if (HideOn
409             ExFree
410             PsSetO
411         }
412         HideOnCrea
413         i = 0;
414         aux = ((PU
415         while (aux
416             HideOn
417             ++i;
418             aux =
419         }
420         ntStatus =
421         break;
422     case IOCTL_R00
423         ExecuteAtD
424         break;
425     case IOCTL_R00
426         LPE( toProces
427         break;
428     case IOCTL_R00
```

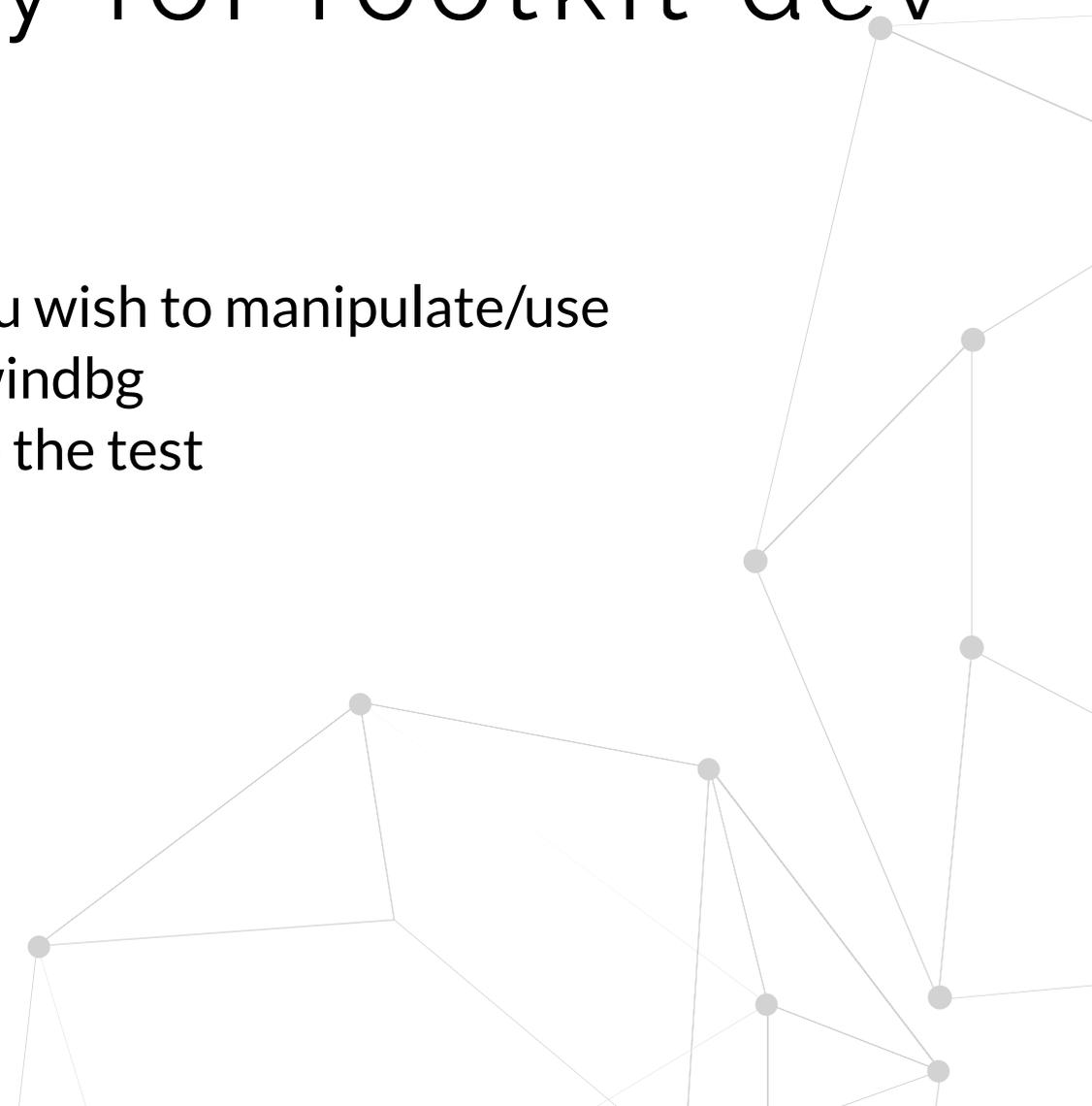


Source: Windows Kernel Programming, by Pavel Yosifovich at <http://leanpub.com/windowskernelprogramming>

```
397 auto PIO_STACK_LOCATION
398 switch (stack->Par
399     case IOCTL_R00
400         // Irp->As
401         ExecuteAtD
402         break;
403     case IOCTL_R00
404         // Execute
405         ExecuteAtD
406         break;
407     case IOCTL_R00
408         if (HideOn
409             ExFree
410             PsSetC
411         }
412         HideOnCrea
413         i = 0;
414         aux = ((PU
415         while (aux
416             HideOn
417             ++i;
418             aux =
419         }
420         ntStatus =
421         break;
422     case IOCTL_R00
423         ExecuteAtD
424         break;
425     case IOCTL_R00
426         LPE( toProces
427         break;
428     case IOCTL_R00
```

## → Methodology for rootkit dev

- Understand the feature you wish to manipulate/use
- Test manipulation live on windbg
- Write the code to replicate the test
- Compile
- Crash
- Restore snapshot & repeat



```
397 auto PIO_STACK_LOCATION
398 switch (stack->Par
399     case IOCTL_R00
400         // Irp->As
401         ExecuteAtD
402         break;
403     case IOCTL_R00
404         // Execute
405         ExecuteAtD
406         break;
407     case IOCTL_R00
408         if (HideOn
409             ExFree
410             PsSetO
411         }
412         HideOnCrea
413         i = 0;
414         aux = ((PU
415         while (aux
416             HideOn
417             ++i;
418             aux =
419         }
420         ntStatus =
421         break;
422     case IOCTL_R00
423         ExecuteAtD
424         break;
425     case IOCTL_R00
426         LPE( toProces
427         break;
428     case IOCTL_R00
```

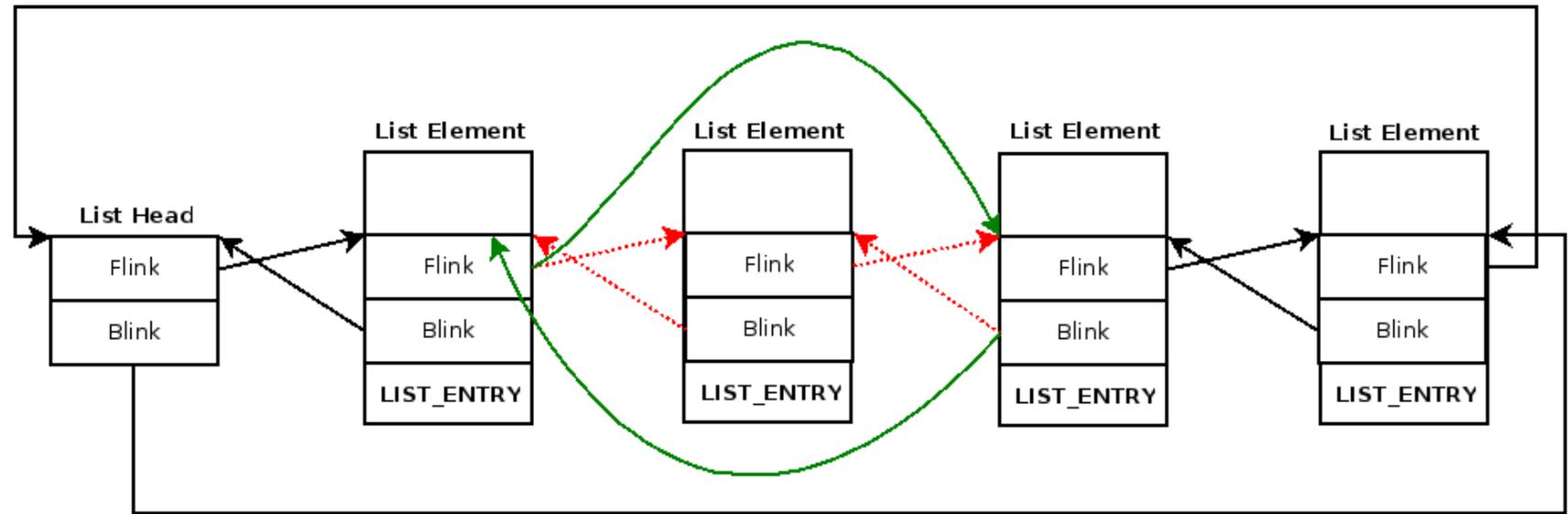
→ Hiding a process



```
397 auto PIO_STACK_LOCATION
398 switch (stack->Par
399     case IOCTL_R00
400         // Irp->As
401         ExecuteAtD
402         break;
403     case IOCTL_R00
404         // Execute
405         ExecuteAtD
406         break;
407     case IOCTL_R00
408         if (HideOn
409             ExFree
410             PsSetO
411         }
412     HideOnCrea
413     i = 0;
414     aux = ((PU
415     while (aux
416         HideOn
417         ++i;
418         aux =
419     }
420     ntStatus =
421     break;
422     case IOCTL_R00
423         ExecuteAtD
424         break;
425     case IOCTL_R00
426         LPE( toProce
427     break;
428     case IOCTL_R00
```

# → Hiding a process

```
Command X
3: kd> dt nt!_eprocess
+0x000 Pcb : _KPROCESS
+0x438 ProcessLock : _EX_PUSH_LOCK
+0x440 UniqueProcessId : Ptr64 Void
+0x448 ActiveProcessLinks : LIST_ENTRY
+0x458 RundownProtect : _EX_RUNDOWN_REF
+0x460 Flags2 : Uint4B
+0x460 JobNotReallyActive : Pos 0, 1 Bit
+0x460 AccountingFolded : Pos 1, 1 Bit
```



```
397 auto PIO_STACK_LOCATION
398 switch (stack->Par
399     case IOCTL_ROO
400         // Irp->As
401         ExecuteAtD
402         break;
403     case IOCTL_ROO
404         // Execute
405         ExecuteAtD
406         break;
407     case IOCTL_ROO
408         if (HideOn
409             ExFree
410             PsSetC
411         }
412         HideOnCrea
413         i = 0;
414         aux = ((PU
415         while (aux
416             HideOn
417             ++i;
418             aux =
419         }
420         ntStatus =
421         break;
422     case IOCTL_ROO
423         ExecuteAtD
424         break;
425     case IOCTL_ROO
426         LPE( toProces
427         break;
428     case IOCTL_ROO
```

# → Hiding a process

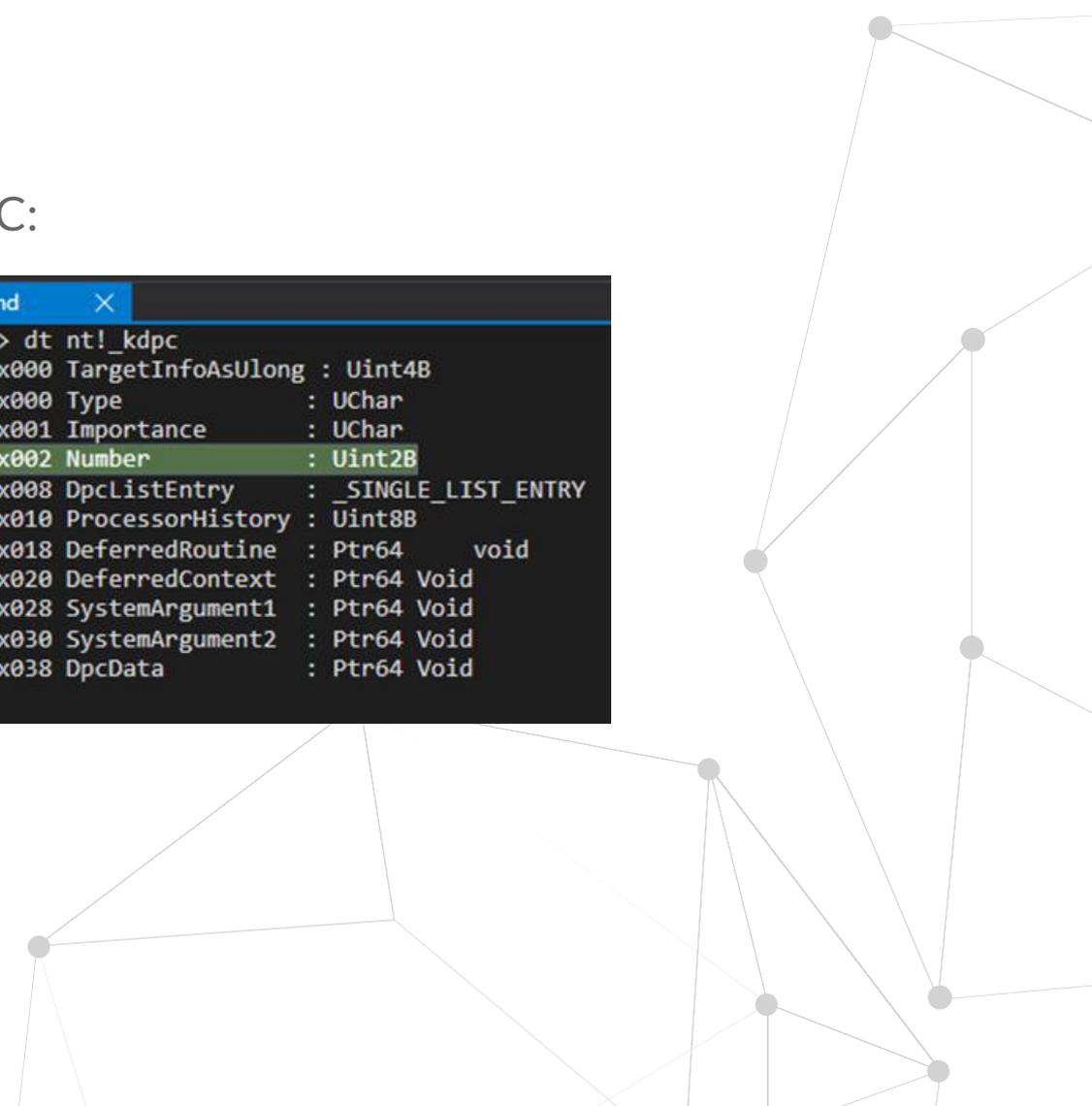
Locking the OS for sensitive actions

IRQL:

- HIGH\_LEVEL
- Device IRQL
- DISPATCH\_LEVEL = 2
- APC\_LEVEL = 1
- PASSIVE\_LEVEL = 0

DPC:

```
Command X
3: kd> dt nt!_kdpc
+0x000 TargetInfoAsUlong : Uint4B
+0x000 Type : UChar
+0x001 Importance : UChar
+0x002 Number : Uint2B
+0x008 DpcListEntry : _SINGLE_LIST_ENTRY
+0x010 ProcessorHistory : Uint8B
+0x018 DeferredRoutine : Ptr64 void
+0x020 DeferredContext : Ptr64 Void
+0x028 SystemArgument1 : Ptr64 Void
+0x030 SystemArgument2 : Ptr64 Void
+0x038 DpcData : Ptr64 Void
```



```
397 auto PIO_STACK_LOCATION
398 switch (stack->Par
399     case IOCTL_ROO
400         // Irp->As
401         ExecuteAtD
402         break;
403     case IOCTL_ROO
404         // Execute
405         ExecuteAtD
406         break;
407     case IOCTL_ROO
408         if (HideOn
409             ExFree
410             PsSetC
411         }
412     HideOnCrea
413     i = 0;
414     aux = ((PU
415     while (aux
416         HideOn
417         ++i;
418         aux =
419     }
420     ntStatus =
421     break;
422     case IOCTL_ROO
423         ExecuteAtD
424         break;
425     case IOCTL_ROO
426         LPE( toProces
427     break;
428     case IOCTL_ROO
```

# → Hiding a process

Locking the OS for sensitive actions

```
113 void ExecuteAtDispatchLevel(void (*sensitiveFunc)(PVOID64, PVOID64), PVOID64 arg1, PVOID64 arg2) {
114     KIRQL irql;
115     PKDPC dpcPtr;
116
117     // 1. Raise the IRQL of curr CPU core to DISPATCH_LEVEL
118     KdPrint(("[Driver entry]:\tRaising IRQL...\n"));
119     irql = RaiseIRQL();
120     KdPrint(("[Driver entry]:\tIRQL = DISPATCH_LEVEL\n"));
121
122     // 2. Create + queue DPCs to raise the IRQL of the other CPU cores
123     KdPrint(("[Driver entry]:\tAcquiring lock...\n"));
124     dpcPtr = AcquireLock();
125     KdPrint(("[Driver entry]:\tLock acquired\n"));
126
127     // 3. Perform sensitive task -> ex: hide process
128     KdPrint(("[Driver entry]:\tExecuting sensitive action(s)...\n"));
129     (*sensitiveFunc)(arg1, arg2);
130
131     KdPrint(("[Driver entry]:\tEnding sensitive action(s)\n"));
132
133     // 4. Signal DPCs in the other cores to stop spinning and exit
134     KdPrint(("[Driver entry]:\tReleasing lock...\n"));
135     ReleaseLock(dpcPtr);
136     KdPrint(("[Driver entry]:\tLock released\n"));
137
138     // 5. Lower IRQL of curr core back to original IRQL
139     KdPrint(("[Driver entry]:\tRestoring IRQL...\n"));
140     LowerIRQL(PrevIrql);
141     KdPrint(("[Driver entry]:\tIRQL restored.\n"));
142
143 }
```



Original idea: Greg Hoglund & Jamie Butler

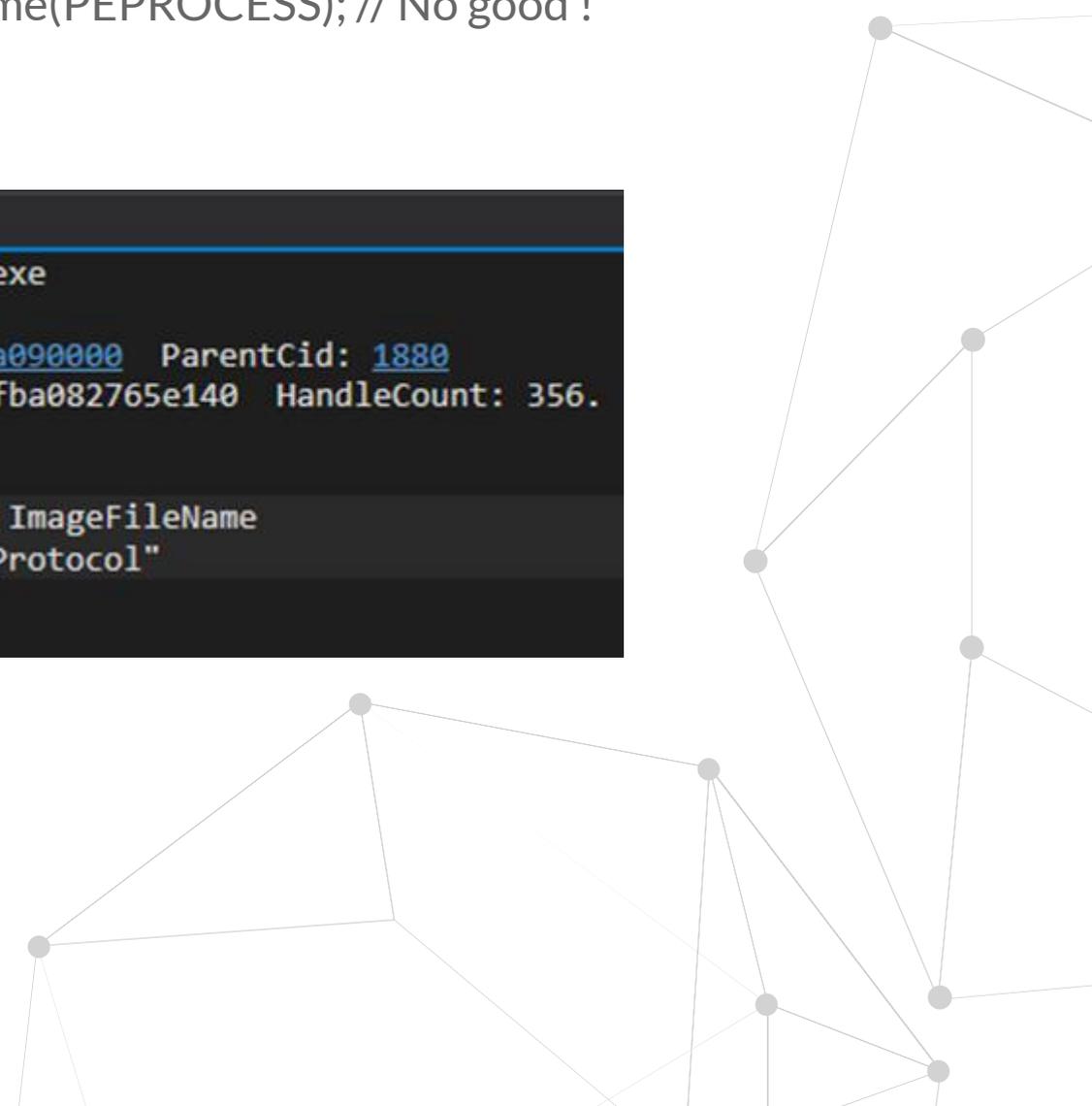
```
397 auto PIO_STACK_LOCATION
398 switch (stack->Par
399     case IOCTL_ROO
400         // Irp->As
401         ExecuteAtD
402         break;
403     case IOCTL_ROO
404         // Execute
405         ExecuteAtD
406         break;
407     case IOCTL_ROO
408         if (HideOn
409             ExFree
410             PsSetC
411         }
412         HideOnCrea
413         i = 0;
414         aux = ((PU
415         while (aux
416             HideOn
417             ++i;
418             aux =
419         }
420         ntStatus =
421         break;
422     case IOCTL_ROO
423         ExecuteAtD
424         break;
425     case IOCTL_ROO
426         LPE( toProce
427         break;
428     case IOCTL_ROO
```

# → Hiding a process

Hiding a process (by name) | Red Team operational considerations  
PUCHAR PsGetProcessImageFileName(PEPROCESS); // No good !

```
Command X
0: kd> !process 0 0 SearchProtocolHost.exe
PROCESS ffff908ddfe6d080
    SessionId: 0 Cid: 10ec Peb: 363a090000 ParentCid: 1880
    DirBase: b0b33002 ObjectTable: fffffba082765e140 HandleCount: 356.
    Image: SearchProtocolHost.exe

0: kd> dt nt!_eprocess ffff908ddfe6d080 ImageFileName
+0x5a8 ImageFileName : [15] "SearchProtocol"
```



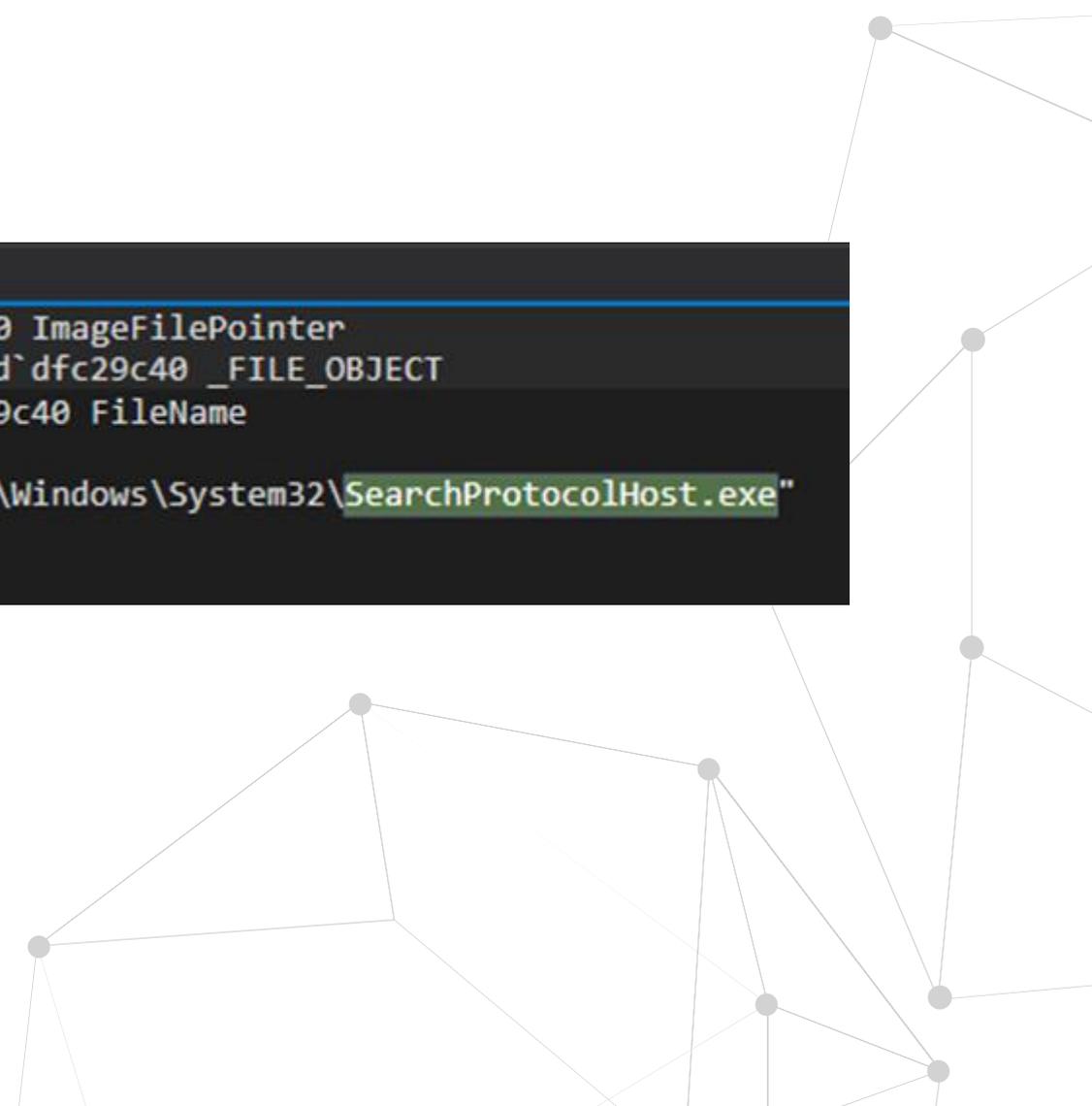
```
397 auto PIO_STACK_LOCATION
398 switch (stack->Par
399     case IOCTL_R00
400         // Irp->As
401         ExecuteAtD
402         break;
403     case IOCTL_R00
404         // Execute
405         ExecuteAtD
406         break;
407     case IOCTL_R00
408         if (HideOn
409             ExFree
410             PsSetC
411         }
412     HideOnCrea
413     i = 0;
414     aux = ((PU
415     while (aux
416         HideOn
417         ++i;
418         aux =
419     }
420     ntStatus =
421     break;
422     case IOCTL_R00
423         ExecuteAtD
424         break;
425     case IOCTL_R00
426         LPE( toProce
427     break;
428     case IOCTL_R00
```

# → Hiding a process

Hiding a process (by name) | Red Team operational considerations

Grabbing the UNICODE "full name":

```
Command X
0: kd> dt nt!_eprocess ffff908ddfe6d080 ImageFilePointer
+0x5a0 ImageFilePointer : 0xffff908d`dfc29c40 _FILE_OBJECT
0: kd> dt _FILE_OBJECT 0xffff908d`dfc29c40 FileName
nt!_FILE_OBJECT
+0x058 FileName : _UNICODE_STRING "\Windows\System32\SearchProtocolHost.exe"
```





Your PC ran into a problem and needs to restart. We're just collecting some error info, and then we'll restart for you.

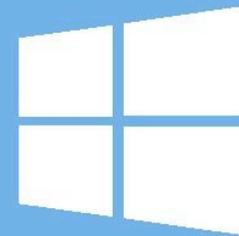
20% complete



For more information about this issue and possible fixes, visit <https://www.windows.com/stopcode>

If you call a support person, give them this info:

Stop code: CRITICAL\_PROCESS\_DIED



**DEMO #2 - hiding procs  
and other cool stuff**



internals: www.sysinternals.com [Lab\alima] (...)

Process Find Users Help

<Filter by name>

PID	CPU	Private Bytes	Working Set	Description
5520	< 0.01	3,684 K	8,144 K	System Guard
1876		2,124 K	10,428 K	Host Process f
1388		2,232 K	7,768 K	Host Process f
1728				
1924				
3460				
784				
904				
648				
728				
912				
848				
3844				
6720				
6776				
7084				
7760				
6764				
7592				
2668				

Administrator: Command Prompt - Injector.exe

```
C:\Users\alima\Desktop>Injector.exe

Kernel injection by 0x4ndr3 @ PwC Norway:
[.] Rootkit already loaded.

Rootkit> help_
```

CPU Usage: 6.67% Commit Charge: 18.35%

The taskbar at the bottom of the screen shows the Start button, File Explorer, Task View, Microsoft Edge, Google Chrome, Mozilla Firefox, Microsoft Word, and a user profile picture. There is also a search icon and a task view icon.

```
397 auto PIO_STACK_LOCATION
398 switch (stack->Par
399     case IOCTL_R00
400         // Irp->As
401         ExecuteAtD
402         break;
403     case IOCTL_R00
404         // Execute
405         ExecuteAtD
406         break;
407     case IOCTL_R00
408         if (HideOn
409             ExFree
410             PsSetO
411         }
412         HideOnCrea
413         i = 0;
414         aux = ((PU
415         while (aux
416             HideOn
417             ++i;
418             aux =
419         }
420         ntStatus =
421         break;
422     case IOCTL_R00
423         ExecuteAtD
424         break;
425     case IOCTL_R00
426         LPE( toProces
427         break;
428     case IOCTL_R00
```

→ Keylogger



# → Keylogger

Identifying the keyboard driver:

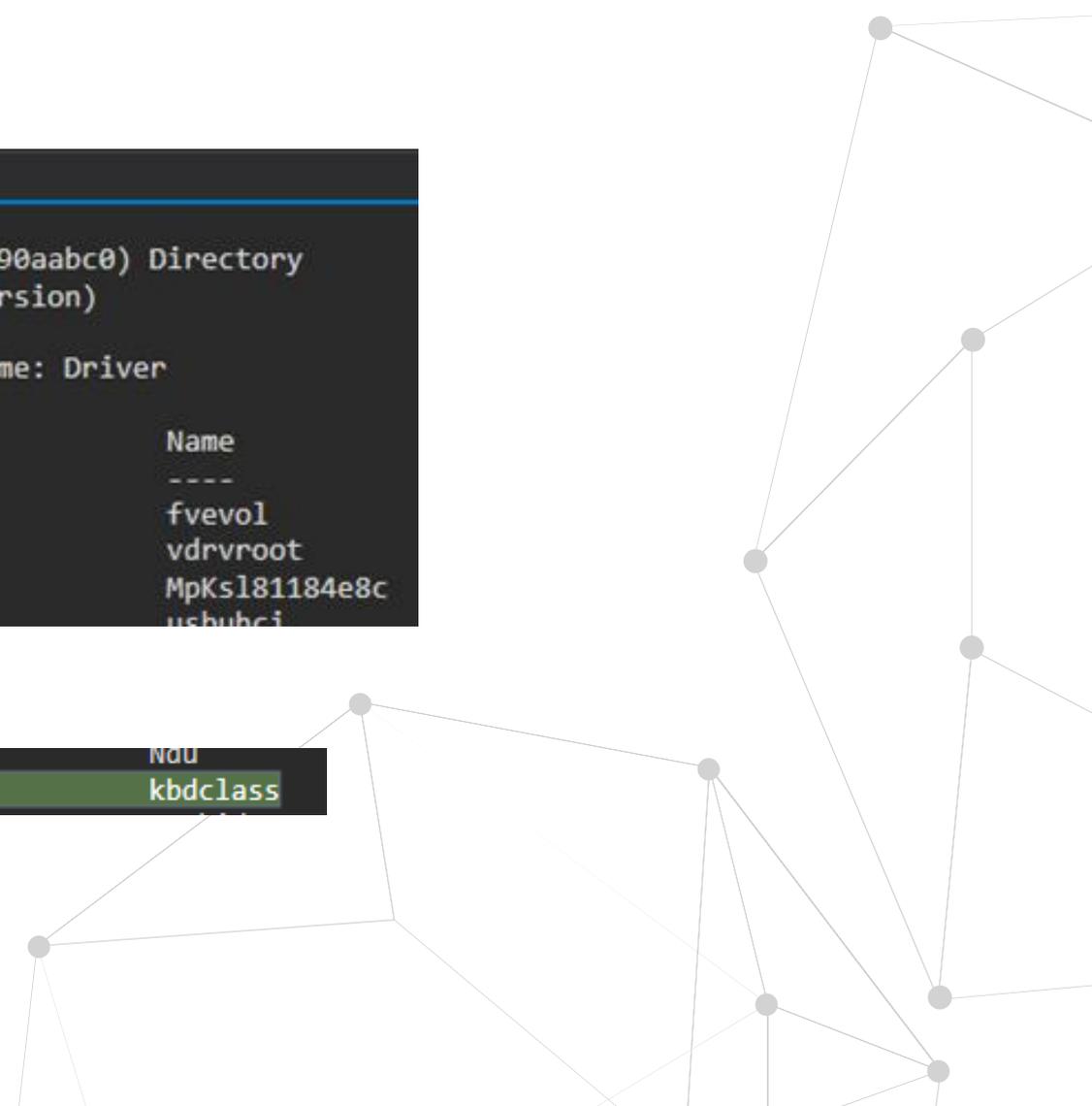
```
397 auto PIO_STACK_LOCATION
398 switch (stack->Par
399 case IOCTL_R00
400 // Irp->As
401 ExecuteAtD
402 break;
403 case IOCTL_R00
404 // Execute
405 ExecuteAtD
406 break;
407 case IOCTL_R00
408 if (HideOn
409 ExFree
410 PsSetC
411 }
412 HideOnCrea
413 i = 0;
414 aux = ((PU
415 while (aux
416 HideOn
417 ++i;
418 aux =
419 }
420 ntStatus =
421 break;
422 case IOCTL_R00
423 ExecuteAtD
424 break;
425 case IOCTL_R00
426 LPE( toProces
427 break;
428 case IOCTL_R00
```

```
Command x
0: kd> !object \driver
Object: fffffba08272ffe60 Type: (ffff908dd90aabc0) Directory
ObjectHeader: fffffba08272ffe30 (new version)
HandleCount: 0 PointerCount: 125
Directory Object: fffffba082723bdc0 Name: Driver

Hash Address Type Name
----
00 fffff908dd9d13db0 Driver fvevol
ffff908dd9b907c0 Driver vdrvroot
01 fffff908de01c5e50 Driver MpKs181184e8c
ffff908ddb3bfa30 Driver ushubci
```

[...]

```
ffff908dd084e8f0 Driver Ndu
ffff908ddb367d50 Driver kbdclass
```



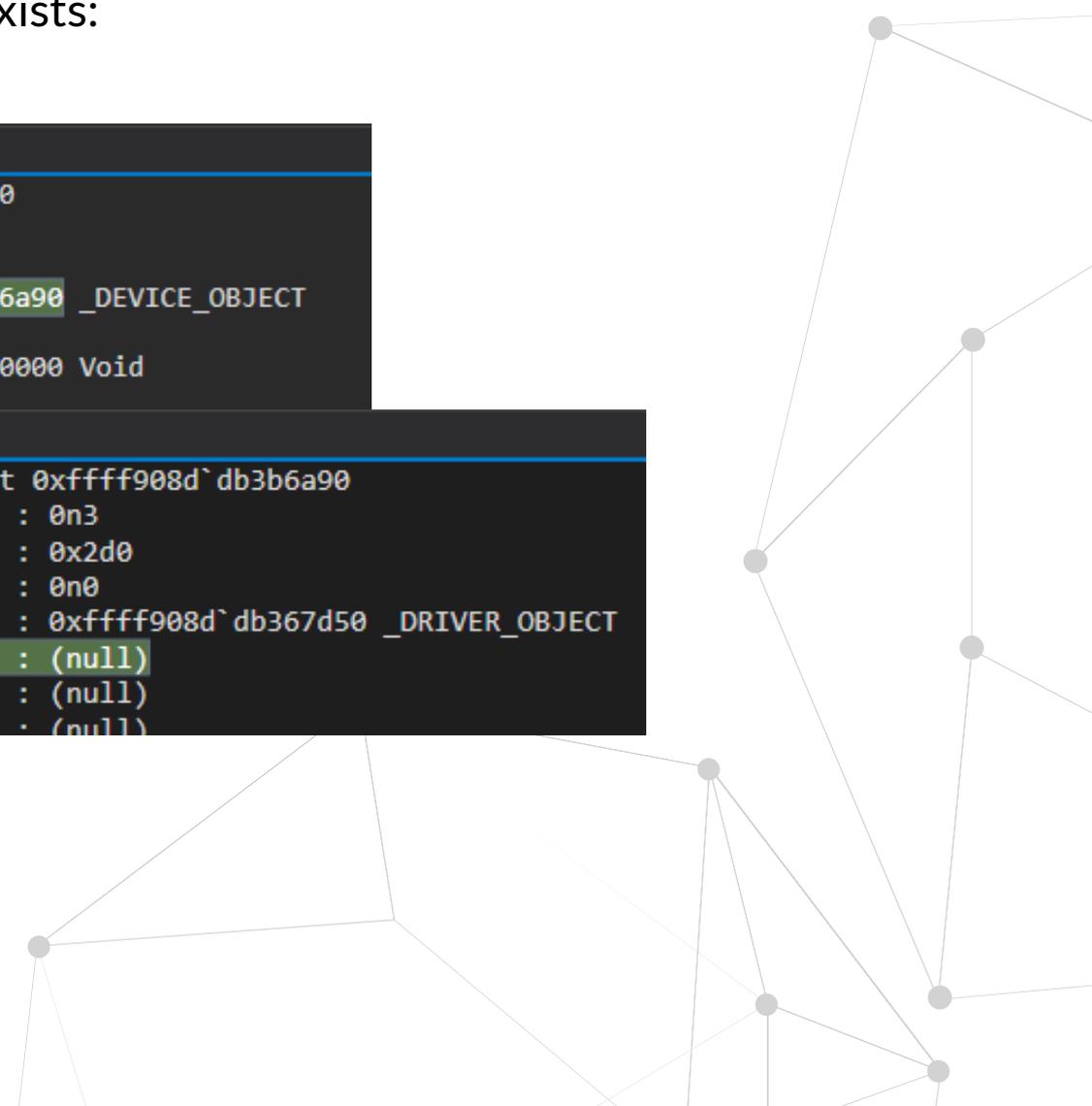
# → Keylogger

Device list when only one session exists:

```
397 auto PIO_STACK_LOCATION
398 switch (stack->Par
399     case IOCTL_R00
400         // Irp->As
401         ExecuteAtD
402         break;
403     case IOCTL_R00
404         // Execute
405         ExecuteAtD
406         break;
407     case IOCTL_R00
408         if (HideOn
409             ExFree
410             PsSetC
411         }
412         HideOnCrea
413         i = 0;
414         aux = ((PU
415         while (aux
416             HideOn
417             ++i;
418             aux =
419         }
420         ntStatus =
421         break;
422     case IOCTL_R00
423         ExecuteAtD
424         break;
425     case IOCTL_R00
426         LPE( toProces
427         break;
428     case IOCTL_R00
```

```
Command X
0: kd> dt nt!_driver_object fffff908ddb367d50
+0x000 Type : 0n4
+0x002 Size : 0n336
+0x008 DeviceObject : 0xffff908d`db3b6a90 _DEVICE_OBJECT
+0x010 Flags : 0x412
+0x018 DriverStart : 0xfffff805`34780000 Void
+0x020 DriverSize : 0x14000
+0x028 DriverS
+0x030 Driver
+0x038 Driver
+0x048 Hardwa
```

```
Command X
0: kd> dt nt!_device_object 0xffff908d`db3b6a90
+0x000 Type : 0n3
+0x002 Size : 0x2d0
+0x004 ReferenceCount : 0n0
+0x008 DriverObject : 0xffff908d`db367d50 _DRIVER_OBJECT
+0x010 NextDevice : (null)
+0x018 AttachedDevice : (null)
+0x020 CurrentIrp : (null)
```

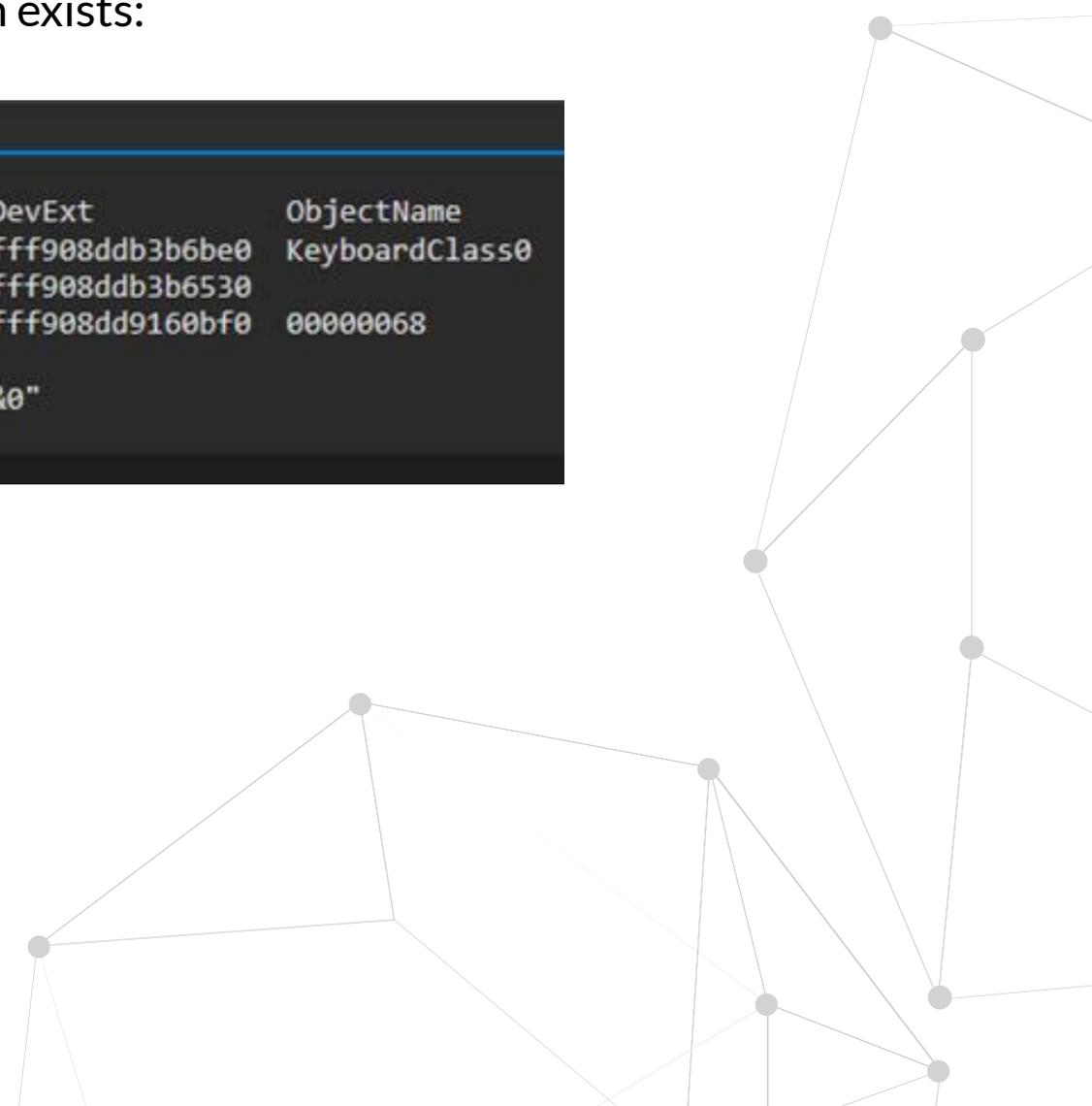


# → Keylogger

Device stack when only one session exists:

```
Command X
0: kd> !devstack 0xffff908d`db3b6a90
!DevObj      !DrvObj      !DevExt      ObjectName
> fffff908ddb3b6a90  \Driver\kbdclass  fffff908ddb3b6be0  KeyboardClass0
  fffff908ddb3b63e0  \Driver\i8042prt  fffff908ddb3b6530
  fffff908dd9be0cf0  \Driver\ACPI      fffff908dd9160bf0  00000068
!DevNode fffff908dd9c9e730 :
DeviceInst is "ACPI\PNP0303\4&25ee97c0&0"
ServiceName is "i8042prt"
```

```
397 auto PIO_STACK_LOCATION
398 switch (stack->Par
399     case IOCTL_R00
400         // Irp->As
401         ExecuteAtD
402         break;
403     case IOCTL_R00
404         // Execute
405         ExecuteAtD
406         break;
407     case IOCTL_R00
408         if (HideOn
409             ExFree
410             PsSetC
411         }
412         HideOnCrea
413         i = 0;
414         aux = ((PU
415         while (aux
416             HideOn
417             ++i;
418             aux =
419         }
420         ntStatus =
421         break;
422     case IOCTL_R00
423         ExecuteAtD
424         break;
425     case IOCTL_R00
426         LPE( toProces
427         break;
428     case IOCTL_R00
```



# → Keylogger

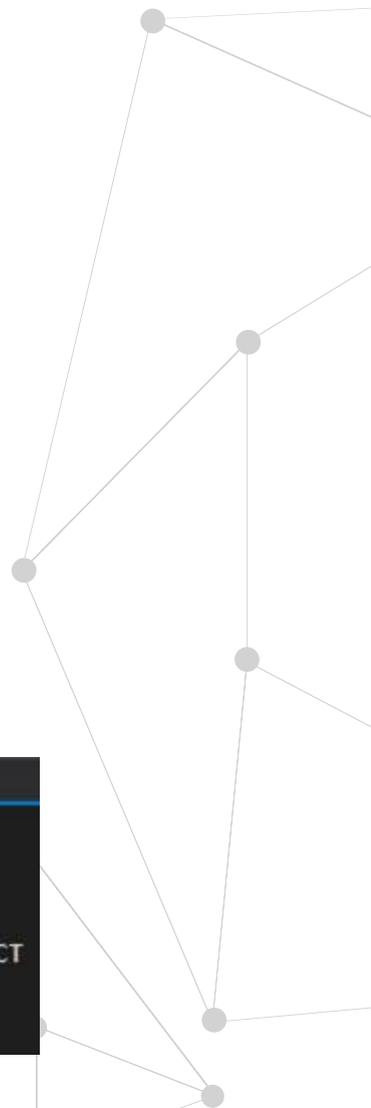
After a new RDP session: one keyboard device for each session

```
397 auto PIO_STACK_LOCATION
398 switch (stack->Par
399     case IOCTL_ROO
400         // Irp->As
401         ExecuteAtD
402         break;
403     case IOCTL_ROO
404         // Execute
405         ExecuteAtD
406         break;
407     case IOCTL_ROO
408         if (HideOn
409             ExFree
410             PsSetC
411         }
412         HideOnCrea
413         i = 0;
414         aux = ((PU
415         while (aux
416             HideOn
417             ++i;
418             aux =
419         }
420         ntStatus =
421         break;
422     case IOCTL_ROO
423         ExecuteAtD
424         break;
425     case IOCTL_ROO
426         LPE( toProces
427         break;
428     case IOCTL_ROO
```

```
Command X
0: kd> dt nt!_driver_object fffff908ddb367d50
+0x000 Type : 0n4
+0x002 Size : 0n336
+0x008 DeviceObject : 0xffff908d`e390ac90 _DEVICE_OBJECT
+0x010 Flags : 0x412
+0x018 DriverStart : 0xffffffff805`34780000 Void
+0x020 DriverSize : 0x14000
+0x028 DriverSection : 0xffff908d`db342230 Void
+0x030 DriverExtension : 0xffff908d`db367ea0 _DRIVER_EXTENSION
+0x038 DriverName : UNICODE_STRING "\Driver\kbdclass"
```

```
Command X
0: kd> dt nt!_device_object 0xffff908d`e390ac90
+0x000 Type : 0n3
+0x002 Size : 0x2d0
+0x004 ReferenceCount : 0n0
+0x008 DriverObject : 0xffff908d`db367d50 _DRIVER_OBJECT
+0x010 NextDevice : 0xffff908d`db3b6a90 _DEVICE_OBJECT
+0x018 AttachedDevice : (null)
```

```
Command X
0: kd> dt nt!_device_object 0xffff908d`db3b6a90
+0x000 Type : 0n3
+0x002 Size : 0x2d0
+0x004 ReferenceCount : 0n0
+0x008 DriverObject : 0xffff908d`db367d50 _DRIVER_OBJECT
+0x010 NextDevice : (null)
+0x018 AttachedDevice : (null)
```



# → Keylogger

After keylogger devices attach to the keyboard device:

```
397 auto PIO_STACK_LOCATION
398 switch (stack->Par
399     case IOCTL_ROO
400         // Irp->As
401         ExecuteAtD
402         break;
403     case IOCTL_ROO
404         // Execute
405         ExecuteAtD
406         break;
407     case IOCTL_ROO
408         if (HideOn
409             ExFree
410             PsSetC
411         }
412         HideOnCrea
413         i = 0;
414         aux = ((PU
415         while (aux
416             HideOn
417             ++i;
418             aux =
419         }
420         ntStatus =
421         break;
422     case IOCTL_ROO
423         ExecuteAtD
424         break;
425     case IOCTL_ROO
426         LPE( toProces
427         break;
428     case IOCTL_ROO
```

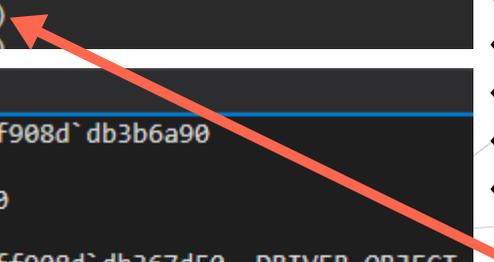
```
Command X
0: kd> dt nt!_driver_object ffff908ddb367d50
+0x000 Type : 0n4
+0x002 Size : 0n336
+0x008 DeviceObject : 0xffff908d`e390ac90 _DEVICE_OBJECT
+0x010 Flags : 0x412
+0x018 DriverStart : 0xfffff805`34780000 Void
+0x020 DriverSize : 0x14000
+0x028 DriverSection : 0xffff908d`db342230 Void
+0x030 DriverExtension : 0xffff908d`db367ea0 _DRIVER_EXTENSION
+0x038 DriverName : _UNICODE_STRING "\Driver\kbdclass"
+0x048 HardwareDatabase : 0xfffff805`2d52e088 _UNICODE_STRING "\
```

```
Command X
0: kd> dt nt!_device_object 0xffff908d`e390ac90
+0x000 Type : 0n3
+0x002 Size : 0x2d0
+0x004 ReferenceCount : 0n0
+0x008 DriverObject : 0xffff908d`db367d50 _DRIVER_OBJECT
+0x010 NextDevice : 0xffff908d`db3b6a90 _DEVICE_OBJECT
+0x018 AttachedDevice : (null)
+0x020 CurrentIrp : (null)
```

```
Command X
0: kd> dt nt!_device_object 0xffff908d`db3b6a90
+0x000 Type : 0n3
+0x002 Size : 0x2d0
+0x004 ReferenceCount : 0n0
+0x008 DriverObject : 0xffff908d`db367d50 _DRIVER_OBJECT
+0x010 NextDevice : (null)
+0x018 AttachedDevice : (null)
+0x020 CurrentIrp : (null)
```

```
Command X
0: kd> dt nt!_driver_object ffff908ddb367d50
+0x000 Type : 0n4
+0x002 Size : 0n336
+0x008 DeviceObject : 0xffff908d`e30722f0 _DEVICE_O
+0x010 Flags : 0x412
+0x018 DriverStart : 0xfffff805`34780000 Void
+0x020 DriverSize : 0x14000
```

```
Command X
0: kd> dt nt!_device_object 0xffff908d`e30722f0
+0x000 Type : 0n3
+0x002 Size : 0x2d0
+0x004 ReferenceCount : 0n0
+0x008 DriverObject : 0xffff908d`db367d50 _DRIVER_O
+0x010 NextDevice : 0xffff908d`db3b6a90 _DEVICE_O
+0x018 AttachedDevice : 0xffff908d`e22c54b0 _DEVICE_O
+0x020 CurrentIrp : (null)
+0x028 Timer : (null)
```



[...]

# → Keylogger

Before and after the keylogger devices attach to the keyboard device:

```
397 auto PIO_STACK_LOCATION
398 switch (stack->Par
399     case IOCTL_ROO
400         // Irp->As
401         ExecuteAtD
402         break;
403     case IOCTL_ROO
404         // Execute
405         ExecuteAtD
406         break;
407     case IOCTL_ROO
408         if (HideOn
409             ExFree
410             PsSetC
411         }
412         HideOnCrea
413         i = 0;
414         aux = ((PU
415         while (aux
416             HideOn
417             ++i;
418             aux =
419         }
420         ntStatus =
421         break;
422     case IOCTL_ROO
423         ExecuteAtD
424         break;
425     case IOCTL_ROO
426         LPE( toProces
427         break;
428     case IOCTL_ROO
```

```
Command X
0: kd> !devstack 0xffff908d`db3b6a90
!DevObj      !DrvObj      !DevExt      ObjectName
> ffff908ddb3b6a90  \Driver\kbdclass  ffff908ddb3b6be0  KeyboardClass0
  ffff908ddb3b63e0  \Driver\i8042prt  ffff908ddb3b6530
  ffff908dd9be0cf0  \Driver\ACPI      ffff908dd9160bf0  00000068
!DevNode ffff908dd9c9e730 :
DeviceInst is "ACPI\PNP0303\4&25ee97c0&0"
ServiceName is "i8042prt"
```



```
Command X
0: kd> !devstack 0xffff908d`e30722f0
!DevObj      !DrvObj      !DevExt      ObjectName
  ffff908de22c54b0  \Driver\TopKeylogger  ffff908de22c5600
> ffff908de30722f0  \Driver\kbdclass  ffff908de3072440  KeyboardClass2
  ffff908ddfabd2d0  \Driver\terminpt  ffff908ddfabd420
  ffff908ddf0bb520  \Driver\umbus     ffff908de3743f10  000000c1
!DevNode ffff908de079d660 :
DeviceInst is "TERMINPUT_BUS\UMB\2&2c22bcc9&0&Session1Keyboard0"
ServiceName is "terminpt"
```

[...]



Your PC ran into a problem and needs to restart. We're just collecting some error info, and then we'll restart for you.

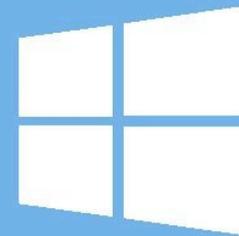
20% complete



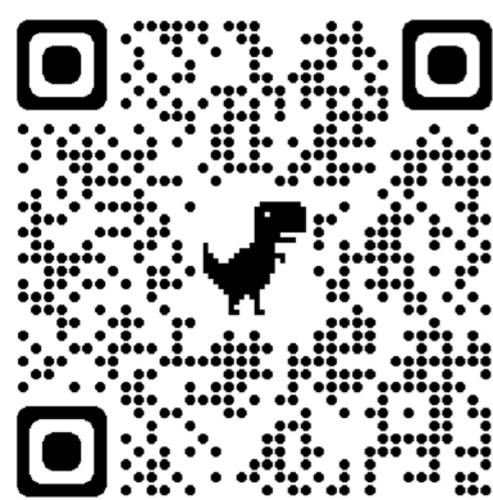
For more information about this issue and possible fixes, visit <https://www.windows.com/stopcode>

If you call a support person, give them this info:

Stop code: CRITICAL\_PROCESS\_DIED



**DEMO #3 - Using the keylogger  
as command & control**



Process Explorer - Sysinternals: www.sysinternals.com [Lab\alima] (...)

File Options View Process Find Users Help

<Filter by name>

Process	PID	CPU	Private Bytes	Working Set	Description
svchost.exe	3720		3,836 K	16,100 K	Host Process f
svchost.exe	7208		3,460 K	11,700 K	Host Process f
SgrmBroker.exe	8172	< 0.01	3,664 K	8,552 K	System Guard
svchost.exe	6828				
svchost.exe	6412				
svchost.exe	4776				
svchost.exe	4252				
lsass.exe	784				
fontdrvhost.exe	904				
csrss.exe	648				
winlogon.exe	728				
fontdrvhost.exe	912				
dwm.exe	848				
explorer.exe	3844				
SecurityHealthSystray.exe	6720				
vmtoolsd.exe	6776				
OneDrive.exe	7084				
cmd.exe	7760				
conhost.exe	6764				
Injector.exe	3820				
procexp64.exe	4620				

CPU Usage: 10.36% Commit Charge: 18.36%

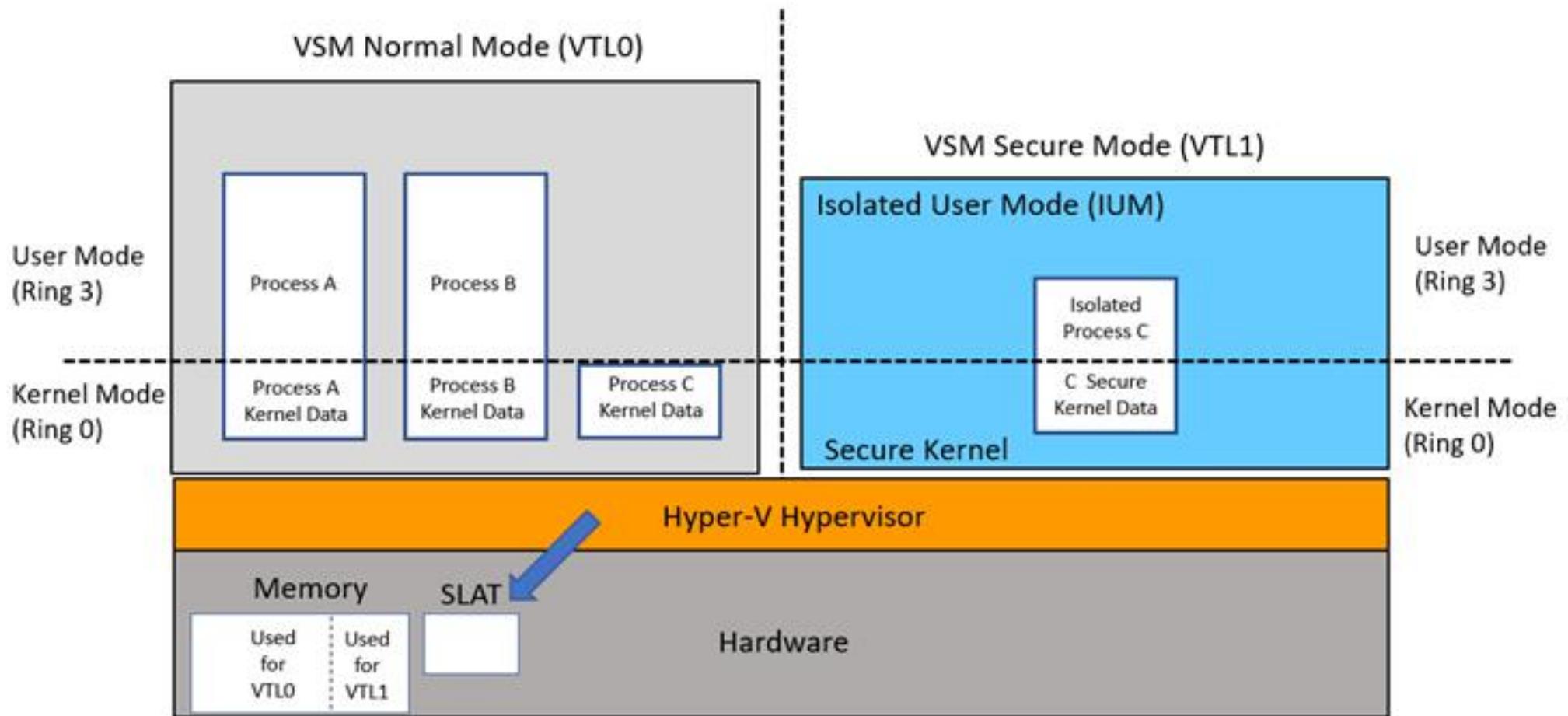
Administrator: Command Prompt - Injector.exe

```
C:\Users\alima\Desktop>Injector.exe
Kernel injection by 0x4ndr3 @ PwC Norway:
[.] Rootkit already loaded.

Rootkit> help
[+] Commands in place:
[.] > hidepid PID           : hides process with PID provided.
[.] > hidepname name.exe    : hides process with name provided.
[.] > hidecreate name.exe   : hides processes called name.exe on
[.] > hidedriver name.sys   : hides driver with name provided.
[.] > lpe PID               : give SYSTEM privs to process with PID
[.] > keylog (enable|disable) : enables or disables keylogger.

Rootkit> _
```

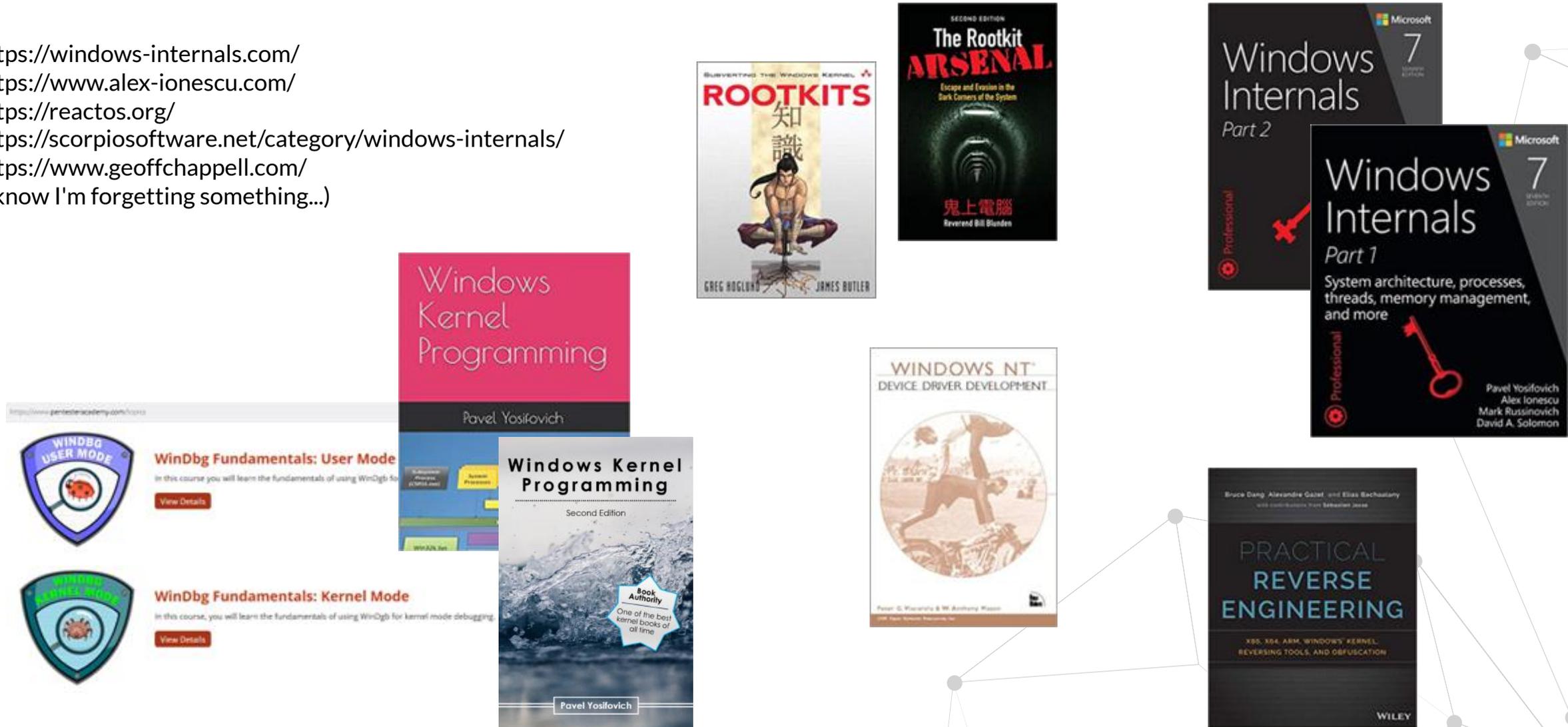
# → Virtual Secure Mode (VSM)



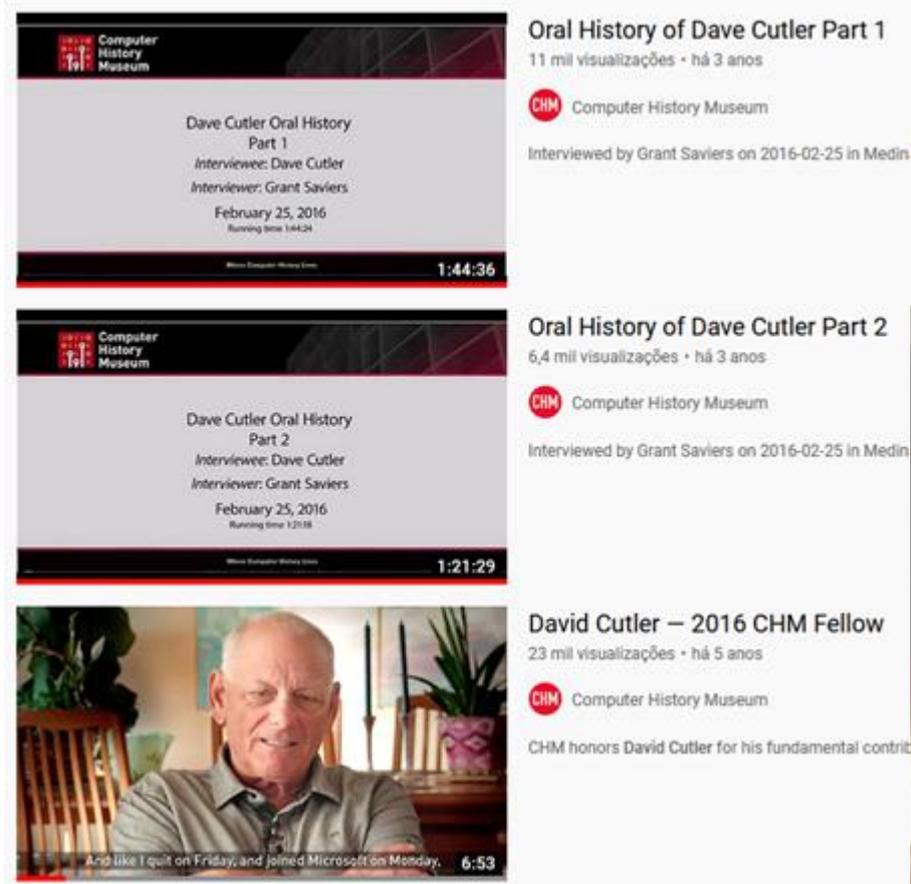
Source: <https://learn.microsoft.com/en-us/windows/win32/procthread/isolated-user-mode--ium--processes>

# → References and great studying resources

<https://windows-internals.com/>  
<https://www.alex-ionscu.com/>  
<https://reactos.org/>  
<https://scorpiosoft.net/category/windows-internals/>  
<https://www.geoffchappell.com/>  
(I know I'm forgetting something...)



# → References and great studying resources

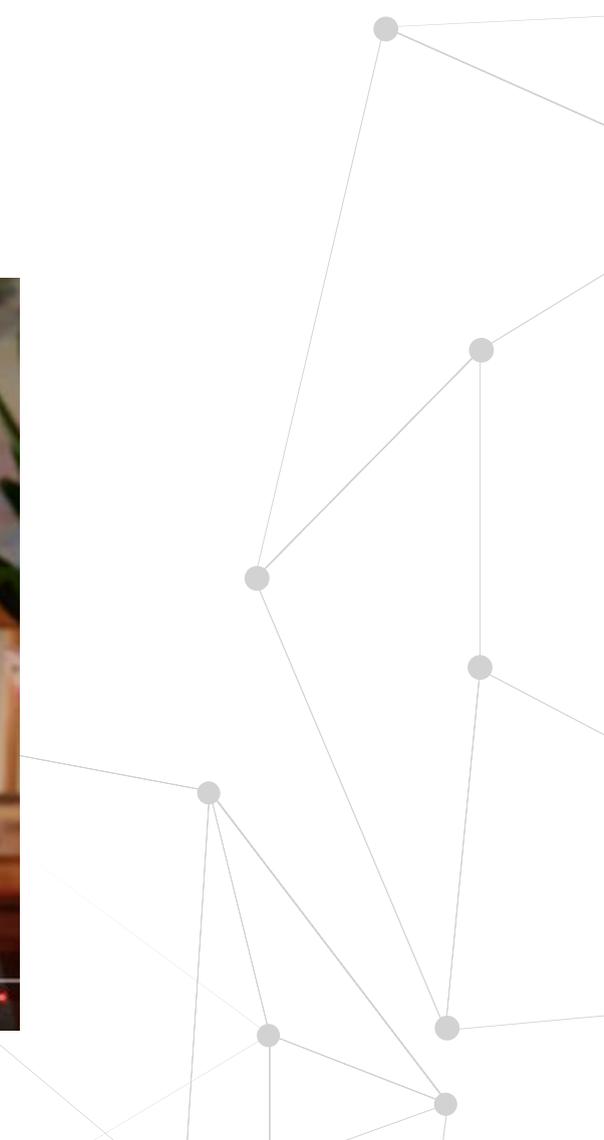
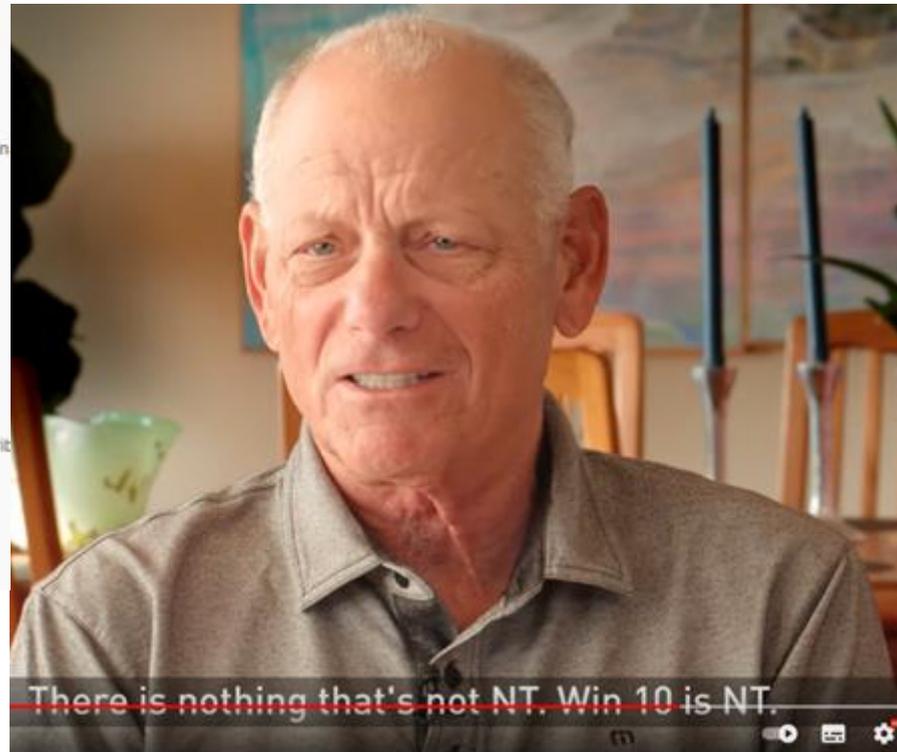


The image shows three video thumbnails from the Computer History Museum. Each thumbnail includes the museum's logo, the video title, the interviewer's name, the date of the interview, and the running time. The first two are parts of an oral history with Dave Cutler, and the third is a video honoring him as a 2016 fellow.

**Oral History of Dave Cutler Part 1**  
11 mil visualizações · há 3 anos  
Computer History Museum  
Interviewed by Grant Saviers on 2016-02-25 in Medin  
Dave Cutler Oral History Part 1  
Interviewee: Dave Cutler  
Interviewer: Grant Saviers  
February 25, 2016  
Running time: 1:44:24  
1:44:36

**Oral History of Dave Cutler Part 2**  
6,4 mil visualizações · há 3 anos  
Computer History Museum  
Interviewed by Grant Saviers on 2016-02-25 in Medin  
Dave Cutler Oral History Part 2  
Interviewee: Dave Cutler  
Interviewer: Grant Saviers  
February 25, 2016  
Running time: 1:21:28  
1:21:29

**David Cutler – 2016 CHM Fellow**  
23 mil visualizações · há 5 anos  
Computer History Museum  
CHM honors David Cutler for his fundamental contrit  
And like I quit on Friday, and joined Microsoft on Monday.  
6:53



# → References and great studying resources

 [Windows, Part IV - Dave Probert](#) [0:32:17] [2005/04/05]  
Here's the final part of the interview we did

 [Windows, Part III - Dave Probert](#) [0:15:10] [2005/04/05]  
Here's part III of [Dave Probert's](#) discussion c

 [Windows, Part II - Dave Probert](#) [0:19:36] [2005/04/01]  
In this second part of the video with Window  
Dave Probert  
Architect, Windows Kernel

 [Windows, Part I - Dave Probert](#) [0:23:17] [2005/04/01]  
[Dave Probert](#) is an architect on the Window

[https://walkingcat.github.io/ch9-index/Shows\\_Going+Deep.html](https://walkingcat.github.io/ch9-index/Shows_Going+Deep.html)



# THANK YOU



<https://twitter.com/0x4ndr3>



<https://www.youtube.com/@0x4ndr3>



<https://www.linkedin.com/in/aflima/>

