

# Module 1

A journey from high level languages, through assembly, to the running process

[https://github.com/hasherezade/malware\\_training\\_voll](https://github.com/hasherezade/malware_training_voll)

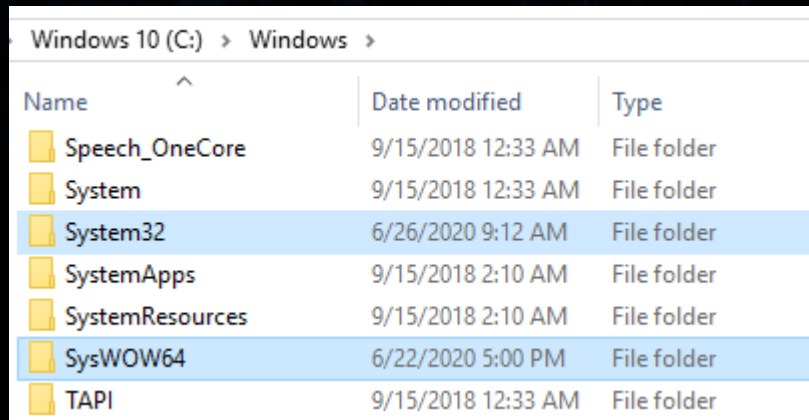
Wow64: 32 bit PE on 64 bit  
Windows





# WoW64: basics

- Backward compatibility: running 32 bit applications on 64 bit Windows
- 32 bit application must be isolated from the 64 bit environment
- WoW64 is a special subsystem that provides the 32 bit environment on Windows 64 bit



Windows 10 (C:) > Windows >		
Name	Date modified	Type
Speech_OneCore	9/15/2018 12:33 AM	File folder
System	9/15/2018 12:33 AM	File folder
System32	6/26/2020 9:12 AM	File folder
SystemApps	9/15/2018 2:10 AM	File folder
SystemResources	9/15/2018 2:10 AM	File folder
SysWOW64	6/22/2020 5:00 PM	File folder
TAPI	9/15/2018 12:33 AM	File folder



# Wow64: basics

- SysWow64 contains 32 bit equivalents of the DLLs that can be found in System32:

Windows 10 (C:) > Windows > System32			
Name	Date modified	Type	Size
ntasn1.dll	9/15/2018 12:28 AM	Application extens...	237 KB
ntdll.dll	3/19/2019 4:21 AM	Application extens...	1,949 KB
ntdsapi.dll	9/15/2018 12:28 AM	Application extens...	146 KB
ntlanman.dll	9/15/2018 12:28 AM	Application extens...	65 KB
ntlanui2.dll	9/15/2018 12:28 AM	Application extens...	20 KB
NtLmShared.dll	3/19/2019 4:21 AM	Application extens...	39 KB
ntmarta.dll	9/15/2018 12:28 AM	Application extens...	182 KB
ntoskrnl.exe	3/19/2019 4:21 AM	Application	9,457 KB
ntprint.dll	9/15/2018 12:28 AM	Application extens...	355 KB
ntprint.exe	9/15/2018 12:28 AM	Application	63 KB
ntshrui.dll	9/15/2018 12:28 AM	Application extens...	758 KB
ntvdm64.dll	9/15/2018 12:28 AM	Application extens...	19 KB
objsel.dll	9/15/2018 12:29 AM	Application extens...	648 KB
occache.dll	9/15/2018 12:29 AM	Application extens...	146 KB
ocsetapi.dll	9/15/2018 12:28 AM	Application extens...	163 KB
odbc32.dll	9/15/2018 12:29 AM	Application extens...	695 KB
odbcad32.exe	9/15/2018 12:29 AM	Application	72 KB
odbcbcpl.dll	9/15/2018 12:29 AM	Application extens...	47 KB
odbcconf.dll	9/15/2018 12:29 AM	Application extens...	29 KB

Windows 10 (C:) > Windows > SysWOW64			
Name	Date modified	Type	Size
ntasn1.dll	9/15/2018 12:29 AM	Application extens...	174 KB
ntdll.dll	3/19/2019 4:21 AM	Application extens...	1,636 KB
ntdsapi.dll	9/15/2018 12:29 AM	Application extens...	96 KB
ntlanman.dll	9/15/2018 12:29 AM	Application extens...	56 KB
ntlanui2.dll	9/15/2018 12:29 AM	Application extens...	17 KB
NtLmShared.dll	3/19/2019 4:21 AM	Application extens...	33 KB
ntmarta.dll	9/15/2018 12:29 AM	Application extens...	150 KB
ntprint.dll	9/15/2018 12:29 AM	Application extens...	310 KB
ntprint.exe	9/15/2018 12:29 AM	Application	61 KB
ntshrui.dll	9/15/2018 12:29 AM	Application extens...	656 KB
ntvdm64.dll	9/15/2018 12:29 AM	Application extens...	16 KB
objsel.dll	9/15/2018 12:29 AM	Application extens...	544 KB
occache.dll	9/15/2018 12:29 AM	Application extens...	125 KB
ocsetapi.dll	9/15/2018 12:29 AM	Application extens...	162 KB
odbc32.dll	9/15/2018 12:29 AM	Application extens...	591 KB
odbcad32.exe	9/15/2018 12:29 AM	Application	71 KB
odbcbcpl.dll	9/15/2018 12:29 AM	Application extens...	39 KB
odbcconf.dll	9/15/2018 12:29 AM	Application extens...	24 KB



# WoW64: basics

- But Ntoskrnl.exe has only one version – native (64 bit on 64 bit system)

Windows 10 (C:) > Windows > System32			
Name	Date modified	Type	Size
ntasn1.dll	9/15/2018 12:28 AM	Application extens...	237 KB
ntdll.dll	3/19/2019 4:21 AM	Application extens...	1,949 KB
ntdsapi.dll	9/15/2018 12:28 AM	Application extens...	146 KB
ntlanman.dll	9/15/2018 12:28 AM	Application extens...	65 KB
ntlanui2.dll	9/15/2018 12:28 AM	Application extens...	20 KB
NtlmShared.dll	3/19/2019 4:21 AM	Application extens...	39 KB
ntmarta.dll	9/15/2018 12:28 AM	Application extens...	182 KB
ntoskrnl.exe	3/19/2019 4:21 AM	Application	9,457 KB
ntprint.dll	9/15/2018 12:28 AM	Application extens...	355 KB
ntprint.exe	9/15/2018 12:28 AM	Application	63 KB
ntshrui.dll	9/15/2018 12:28 AM	Application extens...	758 KB
ntvdm64.dll	9/15/2018 12:28 AM	Application extens...	19 KB
objsel.dll	9/15/2018 12:29 AM	Application extens...	648 KB
occache.dll	9/15/2018 12:29 AM	Application extens...	146 KB
ocsetapi.dll	9/15/2018 12:28 AM	Application extens...	163 KB
odbc32.dll	9/15/2018 12:29 AM	Application extens...	695 KB
odbcad32.exe	9/15/2018 12:29 AM	Application	72 KB
odbcbcpl.dll	9/15/2018 12:29 AM	Application extens...	47 KB
odbcconf.dll	9/15/2018 12:29 AM	Application extens...	29 KB

Windows 10 (C:) > Windows > SysWOW64			
Name	Date modified	Type	Size
ntasn1.dll	9/15/2018 12:29 AM	Application extens...	174 KB
ntdll.dll	3/19/2019 4:21 AM	Application extens...	1,636 KB
ntdsapi.dll	9/15/2018 12:29 AM	Application extens...	96 KB
ntlanman.dll	9/15/2018 12:29 AM	Application extens...	56 KB
ntlanui2.dll	9/15/2018 12:29 AM	Application extens...	17 KB
NtlmShared.dll	3/19/2019 4:21 AM	Application extens...	33 KB
ntmarta.dll	9/15/2018 12:29 AM	Application extens...	150 KB
ntprint.dll	9/15/2018 12:29 AM	Application extens...	310 KB
ntprint.exe	9/15/2018 12:29 AM	Application	61 KB
ntshrui.dll	9/15/2018 12:29 AM	Application extens...	656 KB
ntvdm64.dll	9/15/2018 12:29 AM	Application extens...	16 KB
objsel.dll	9/15/2018 12:29 AM	Application extens...	544 KB
occache.dll	9/15/2018 12:29 AM	Application extens...	125 KB
ocsetapi.dll	9/15/2018 12:29 AM	Application extens...	162 KB
odbc32.dll	9/15/2018 12:29 AM	Application extens...	591 KB
odbcad32.exe	9/15/2018 12:29 AM	Application	71 KB
odbcbcpl.dll	9/15/2018 12:29 AM	Application extens...	39 KB
odbcconf.dll	9/15/2018 12:29 AM	Application extens...	24 KB

# Wow64: basics

- The following 64 bit DLLs are loaded in every 32 bit process running on Wow64:
  - WoW64Cpu.dll – an emulator to run 32 bit code on 64 bit processor
  - Wow64.dll – core emulation infrastructure, thanks to Ntoskrnl.exe entry-point functions
  - Wow64Win.dll – thanks to Win32k.sys entry-point functions
  - Ntdll.dll (64bit version)

```
[*] Scanning: C:\Windows\SysWow64\CoreUIComponents.dll
[*] Scanning: C:\Windows\SysWow64\SHCore.dll
[*] Scanning: C:\Windows\SysWow64\advapi32.dll
[*] Scanning: C:\Windows\SysWow64\CoreMessaging.dll
[*] Scanning: C:\Windows\SysWow64\ntmarta.dll
[*] Scanning: C:\Windows\SysWow64\WinTypes.dll
[*] Scanning: C:\Windows\System32\ntdll.dll
[*] Scanning: C:\Windows\System32\wow64.dll
[*] Scanning: C:\Windows\System32\wow64win.dll
[*] Scanning: C:\Windows\System32\wow64cpu.dll
Scanning workingset: 216 memory regions.
[*] Workingset scanned in 109 ms
```





# Wow64: basics

- Each 32 bit process running on Wow64 has 2 versions of NTDLL
  - 32-bit (from SysWow64) and 64 bit (from System32)

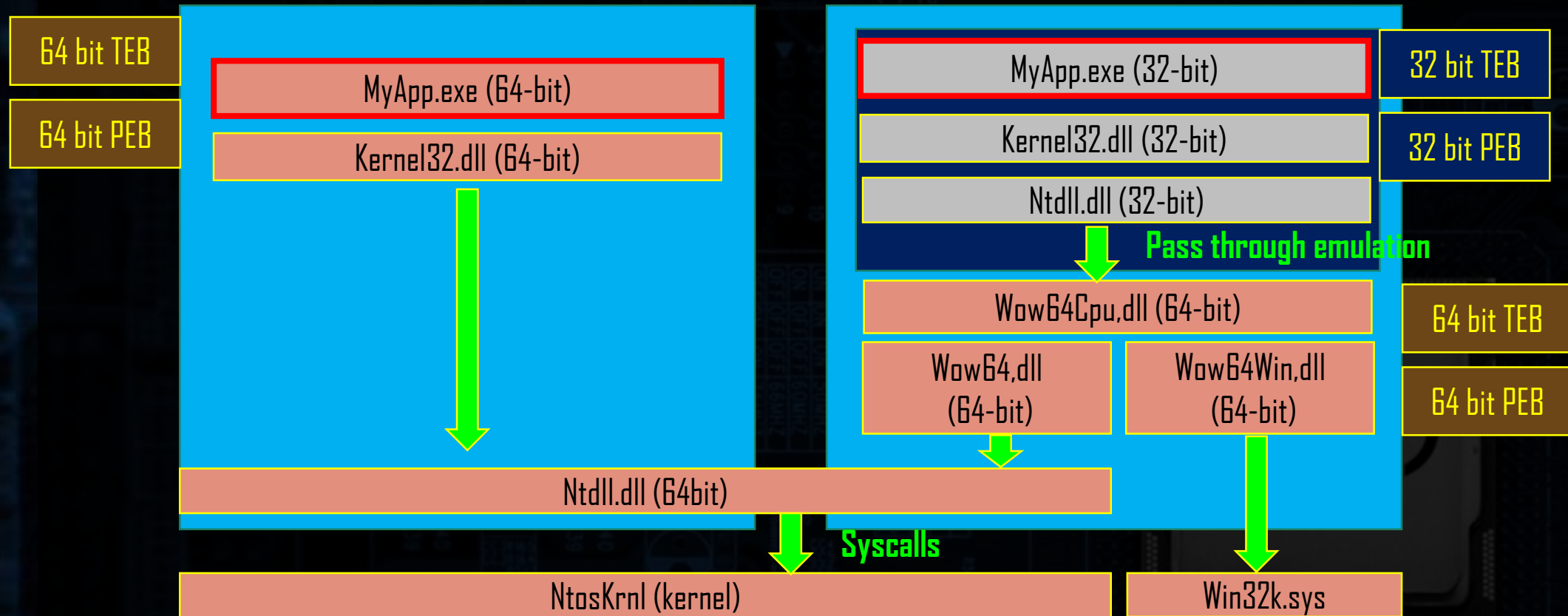
NTDLL.DLL (32 bit version)

```
[*] Scanning: C:\Users\IEUser\Desktop\demo1.exe  
[*] Scanning: C:\Windows\SysWow64\ntdll.dll  
[*] Scanning: C:\Windows\SysWow64\kernel32.dll  
[*] Scanning: C:\Windows\SysWow64\KERNELBASE.dll  
[*] Scanning: C:\Windows\SysWow64\user32.dll  
[*] Scanning: C:\Windows\SysWow64\win32u.dll  
[*] Scanning: C:\Windows\SysWow64\gdi32.dll  
[*] Scanning: C:\Windows\SysWow64\gdi32full.dll
```

NTDLL.DLL (64 bit version)

```
[*] Scanning: C:\Windows\SysWow64\CoreUIComponents.dll  
[*] Scanning: C:\Windows\SysWow64\SHCore.dll  
[*] Scanning: C:\Windows\SysWow64\advapi32.dll  
[*] Scanning: C:\Windows\SysWow64\CoreMessaging.dll  
[*] Scanning: C:\Windows\SysWow64\ntmarta.dll  
[*] Scanning: C:\Windows\SysWow64\WinTypes.dll  
[*] Scanning: C:\Windows\System32\ntdll.dll  
[*] Scanning: C:\Windows\System32\wow64.dll  
[*] Scanning: C:\Windows\System32\wow64win.dll  
[*] Scanning: C:\Windows\System32\wow64cpu.dll  
Scanning workingset: 216 memory regions.  
[*] Workingset scanned in 109 ms
```

# Wow64: basics





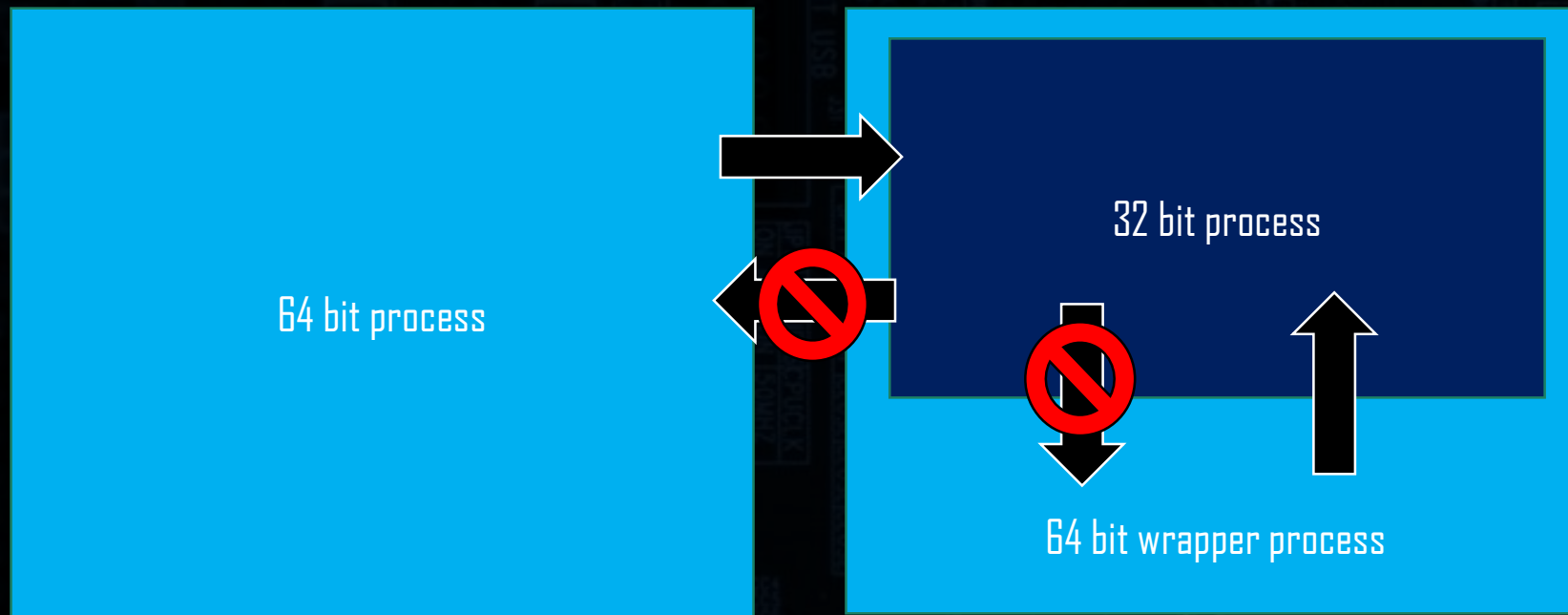
# WoW64: basics

- Try scanning a demo\_1.exe with PE-sieve: 64 bit version, and then 32 bit version
- Observe that:
  - The 32 bit version can access only the 32 bit modules
  - The 64 bit version can access both 32 and 64 bit modules



# Wow64

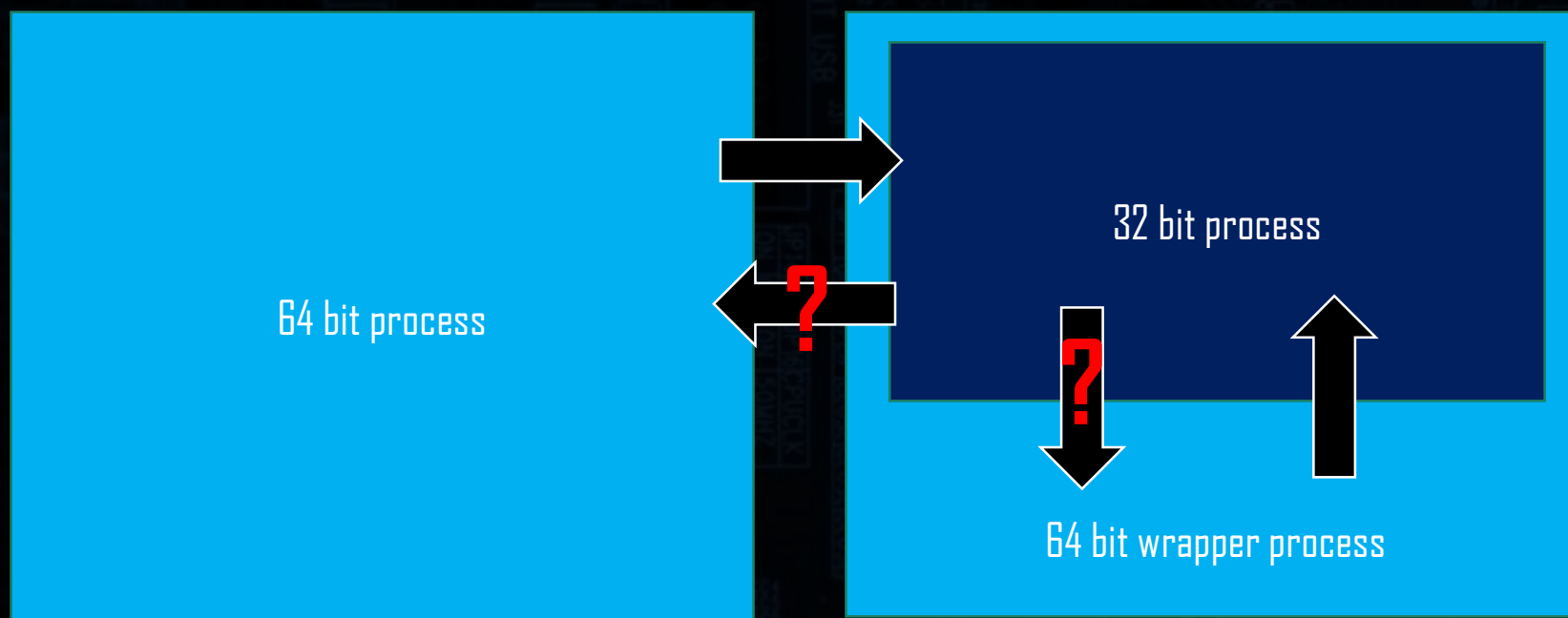
- Wow64 can be compared to a Sandbox





# Wow64

- How to break this isolation?



# How is the isolation made?

- The 32 bit and 64 bit code execution is accessible via different address of the code segment
  - 32 bit: 0x23
  - 64 bit: 0x33
- How to change the segment?
  - Typical return ( RET ): uses address and implicit (default) segment
  - Far return ( RETF ): uses address and explicit segment



# Heaven's Gate

- A technique described first by Roy G Biv

```
.text:00402A30      get_ntdll      proc far                ; CODE XREF:
.text:00402A30                                           ; sub_402D40+
.text:00402A30
.text:00402A30      var_5E8        = dword ptr -5E8h
.text:00402A30      var_10         = qword ptr -10h
.text:00402A30
.text:00402A30 55                push     ebp
.text:00402A31 8B EC            mov     ebp, esp
.text:00402A33 81 EC D4 05 00+   sub     esp, 5D4h
.text:00402A39 53                push     ebx
.text:00402A3A 56                push     esi
.text:00402A3B 0F 57 C0          xorps   xmm0, xmm0
.text:00402A3E 57                push     edi
.text:00402A3F 66 0F 13 45 F0    movl    [ebp+var_10], xmm0
.text:00402A44 6A 33             push     33h
.text:00402A46 E8 00 00 00 00    call    $+5
.text:00402A4B 83 04 24 05       add     [esp+5E8h+var_5E8], 5
.text:00402A4F CB                retf     ; enter 64
.text:00402A4F      get_ntdll      endp ; sp-analysis failed
```

# Heaven's Gate

- Changing segment allows to use 64 bit registers and use the 64 bit code
- Still, we need more work:
  - Get the handle to the 64 bit version of NTDLL
    - How? Using the 64 bit PEB!
  - Load other 64 bit DLLs with its help, in order to be able to use the 64 bit API



# Heaven's Gate in action

- Implemented by Rewolf's Wow64Ext library
  - <https://github.com/rwfp/rwfp-wow64ext/>
- Let's have a look at the real-life example: a miner with a Heaven's Gate
  - <https://blog.malwarebytes.com/threat-analysis/2018/01/a-coin-miner-with-a-heavens-gate/>



# Further readings...

- WOW64 Subsystem Internals and Hooking Techniques – by Stephen Eckels from FireEye:
  - <https://www.fireeye.com/blog/threat-research/2020/11/wow64-subsystem-internals-and-hooking-techniques.html>

