Lab3 Report Dimitry

Pedump:

First we will view the MZ header for the provided executable.

```
root@DCOM-2:/mnt/c/Users/Administrator/Desktop/lab3_dimitry# pedump --mz lab3.exe

=== MZ Header ===

                    signature:                    "MZ"
          bytes_in_last_block:       144          0x90
               blocks_in_file:         3             3
                   num_relocs:         0             0
             header_paragraphs:         4             4
          min_extra_paragraphs:         0             0
          max_extra_paragraphs:     65535        0xffff
                           ss:         0             0
                           sp:       184          0xb8
                     checksum:         0             0
                           ip:         0             0
                           cs:         0             0
            reloc_table_offset:        64          0x40
                overlay_number:         0             0
                     reserved0:         0             0
                        oem_id:         0             0
                      oem_info:         0             0
                     reserved2:         0             0
                     reserved3:         0             0
                     reserved4:         0             0
                     reserved5:         0             0
                     reserved6:         0             0
                        lfanew:       240          0xf0
```

We can see that this is in fact a MZ header file.

Now we will inspect the DOS stub.

```
root@DCOM-2:/mnt/c/Users/Administrator/Desktop/lab3_dimitry# pedump --dos-stub lab3.exe

=== DOS STUB ===

00000000: 0e 1f ba 0e 00 b4 09 cd  21 b8 01 4c cd 21 54 68  |........!..L.!Th|
00000010: 69 73 20 70 72 6f 67 72  61 6d 20 63 61 6e 6e 6f  |is program canno|
00000020: 74 20 62 65 20 72 75 6e  20 69 6e 20 44 4f 53 20  |t be run in DOS |
00000030: 6d 6f 64 65 2e 0d 0d 0a  24 00 00 00 00 00 00 00  |mode....$.......|
```

This program cannot be run in DOS mode after all.

```
root@DCOM-2:/mnt/c/Users/Administrator/Desktop/lab3_dimitry# pedump --pe lab3.exe

=== PE Header ===

                    signature:            "PE\x00\x00"

# IMAGE_FILE_HEADER:
                      Machine:        332         0x14c  x86
              NumberOfSections:          5             5
                 TimeDateStamp:    "2018-02-09 03:28:57"
           PointerToSymbolTable:          0             0
                NumberOfSymbols:          0             0
           SizeOfOptionalHeader:        224          0xe0
                Characteristics:        258         0x102  EXECUTABLE_IMAGE, 32BIT_MACHINE

# IMAGE_OPTIONAL_HEADER32:
                        Magic:        267         0x10b  32-bit executable
                LinkerVersion:                      9.0
                   SizeOfCode:       3584         0xe00
         SizeOfInitializedData:       5120        0x1400
       SizeOfUninitializedData:          0             0
           AddressOfEntryPoint:       6229        0x1855
                     BaseOfCode:       4096        0x1000
                     BaseOfData:       8192        0x2000
                      ImageBase:    4194304      0x400000
              SectionAlignment:       4096        0x1000
                 FileAlignment:        512         0x200
        OperatingSystemVersion:                     5.0
                  ImageVersion:                     0.0
              SubsystemVersion:                     5.0
                     Reserved1:          0             0
                   SizeOfImage:      24576        0x6000
                 SizeOfHeaders:       1024         0x400
                      CheckSum:      24762        0x60ba
                     Subsystem:          2             2  WINDOWS_GUI
            DllCharacteristics:      33088        0x8140  DYNAMIC_BASE, NX_COMPAT
                                                          TERMINAL_SERVER_AWARE
           SizeOfStackReserve:    1048576      0x100000
            SizeOfStackCommit:       4096        0x1000
           SizeOfHeapReserve:    1048576      0x100000
            SizeOfHeapCommit:       4096        0x1000
                  LoaderFlags:          0             0
          NumberOfRvaAndSizes:         16          0x10
```

This provides us with some useful info. We find out that this is a 32 bit executable. We get the size of code, bss and data sections. File alignment is default at 512 bytes. Pedump is telling us that this application has graphical elements via the subsystem.

We can view the data directory.

```
root@DCOM-2:/mnt/c/Users/Administrator/Desktop/lab3_dimitry# pedump --data-directory lab3.exe

=== DATA DIRECTORY ===

  EXPORT        rva:0x       0   size:0x        0
  IMPORT        rva:0x    22ac   size:0x       64
  RESOURCE      rva:0x    4000   size:0x      34c
  EXCEPTION     rva:0x       0   size:0x        0
  SECURITY      rva:0x       0   size:0x        0
  BASERELOC     rva:0x    5000   size:0x      1d8
  DEBUG         rva:0x    2130   size:0x       1c
  ARCHITECTURE  rva:0x       0   size:0x        0
  GLOBALPTR     rva:0x       0   size:0x        0
  TLS           rva:0x       0   size:0x        0
  LOAD_CONFIG   rva:0x    2198   size:0x       40
  Bound_IAT     rva:0x       0   size:0x        0
  IAT           rva:0x    2000   size:0x      110
  Delay_IAT     rva:0x       0   size:0x        0
  CLR_Header    rva:0x       0   size:0x        0
                rva:0x       0   size:0x        0
```

We will also check the Sections.

```
root@DCOM-2:/mnt/c/Users/Administrator/Desktop/lab3_dimitry# pedump --sections lab3.exe

=== SECTIONS ===

  NAME          RVA      VSZ   RAW_SZ  RAW_PTR  nREL  REL_PTR nLINE LINE_PTR     FLAGS
  .text        1000      d9e      e00      400     0        0     0        0  60000020  R-X CODE
  .rdata       2000      880      a00     1200     0        0     0        0  40000040  R-- IDATA
  .data        3000      3a4      200     1c00     0        0     0        0  c0000040  RW- IDATA
  .rsrc        4000      34c      400     1e00     0        0     0        0  40000040  R-- IDATA
  .reloc       5000      270      400     2200     0        0     0        0  42000040  R-- IDATA DISCARDABLE
```

So far nothing seems out of the ordinary.

Now we will check the resources.

```
root@DCOM-2:/mnt/c/Users/Administrator/Desktop/lab3_dimitry# pedump --resources lab3.exe

=== RESOURCES ===

FILE_OFFSET    CP  LANG     SIZE  TYPE          NAME
     0x1eb8  1252 0x409       60  MENU          THREADMENU
     0x1ef4  1252 0x409      598  MANIFEST      #1
```

This application appears to have no resources and is threaded.

Now we will check the imports.

MODULE_NAME	HINT	ORD	FUNCTION_NAME
KERNEL32.dll	8b		CreateMutexA
KERNEL32.dll	377		ReleaseMutex
KERNEL32.dll	43		CloseHandle
KERNEL32.dll	a3		CreateThread
KERNEL32.dll	1aa		GetCurrentProcessId
KERNEL32.dll	1ad		GetCurrentThreadId
KERNEL32.dll	266		GetTickCount
KERNEL32.dll	421		Sleep
KERNEL32.dll	2d1		IsDebuggerPresent
KERNEL32.dll	415		SetUnhandledExceptionFilter
KERNEL32.dll	43e		UnhandledExceptionFilter
KERNEL32.dll	1a9		GetCurrentProcess
KERNEL32.dll	42d		TerminateProcess
KERNEL32.dll	239		GetStartupInfoA
KERNEL32.dll	2ba		InterlockedCompareExchange
KERNEL32.dll	2bd		InterlockedExchange
KERNEL32.dll	24f		GetSystemTimeAsFileTime
KERNEL32.dll	354		QueryPerformanceCounter
KERNEL32.dll	464		WaitForSingleObject
USER32.dll	1d6		LoadIconA
USER32.dll	220		PostQuitMessage
USER32.dll	14a		GetMessageA
USER32.dll	25e		SendMessageA
USER32.dll	e		BeginPaint
USER32.dll	2d5		TranslateMessage
USER32.dll	1f8		MessageBoxA
USER32.dll	67		CreateWindowExA
USER32.dll	11f		GetDlgItem
USER32.dll	95		DefWindowProcA
USER32.dll	2b8		ShowWindow
USER32.dll	a8		DispatchMessageA
USER32.dll	2e9		UpdateWindow
USER32.dll	1d2		LoadCursorA
USER32.dll	233		RegisterClassA
USER32.dll	d5		EndPaint
GDI32.dll	29f		TextOutA
MSVCR90.dll	13f		_controlfp_s
MSVCR90.dll	20b		_invoke_watson
MSVCR90.dll	173		_except_handler4_common
MSVCR90.dll	546		sprintf
MSVCR90.dll	115		_amsg_exit
MSVCR90.dll	9f		__getmainargs
MSVCR90.dll	12c		_cexit
MSVCR90.dll	17c		_exit
MSVCR90.dll	66		_XcptFilter
MSVCR90.dll	225		_ismbblead
MSVCR90.dll	4cc		exit
MSVCR90.dll	160		_decode_pointer
MSVCR90.dll	204		_initterm
MSVCR90.dll	205		_initterm_e
MSVCR90.dll	13c		_configthreadlocale
MSVCR90.dll	e3		__setusermatherr
MSVCR90.dll	10b		_adjust_fdiv
MSVCR90.dll	cb		__p__commode
MSVCR90.dll	cf		__p__fmode
MSVCR90.dll	16a		_encode_pointer
MSVCR90.dll	e0		__set_app_type
MSVCR90.dll	14b		_crt_debugger_hook
MSVCR90.dll	fd		_acmdln
MSVCR90.dll	43		?terminate@@YAXXZ
MSVCR90.dll	3e6		_unlock
MSVCR90.dll	96		__dllonexit

From experience with win32 I can say that something odd is going on here based on imports. The process wants to create threads and new windows by calling CreateWindExA. There is a possibility that this is a simple win32 application.

Let's check for a packer.

```
root@DCOM-2:/mnt/c/Users/Administrator/Desktop/lab3_dimitry# pedump --packer lab3.exe

=== Packer / Compiler ===

  MS Visual C++ v8.0
```

Nothing too suspicious on this front.

WinDbg

After opening the executable we see this output.

```
Microsoft (R) Windows Debugger Version 10.0.18239.1000 X86
Copyright (c) Microsoft Corporation. All rights reserved.

CommandLine: C:\Users\Administrator\Desktop\lab3_dimitry\lab3.exe

************* Path validation summary **************
Response                         Time (ms)     Location
Deferred                                       srv*
Symbol search path is: srv*
Executable search path is:
ModLoad: 00270000 00276000   lab3.exe
ModLoad: 77c40000 77dd0000   ntdll.dll
ModLoad: 76110000 761f0000   C:\WINDOWS\SysWOW64\KERNEL32.DLL
ModLoad: 75d20000 75f04000   C:\WINDOWS\SysWOW64\KERNELBASE.dll
ModLoad: 75b20000 75cad000   C:\WINDOWS\SysWOW64\USER32.dll
ModLoad: 752d0000 752e7000   C:\WINDOWS\SysWOW64\win32u.dll
ModLoad: 752a0000 752c2000   C:\WINDOWS\SysWOW64\GDI32.dll
ModLoad: 75810000 75974000   C:\WINDOWS\SysWOW64\gdi32full.dll
ModLoad: 74f10000 74f8d000   C:\WINDOWS\SysWOW64\msvcp_win.dll
ModLoad: 75050000 7516e000   C:\WINDOWS\SysWOW64\ucrtbase.dll
ModLoad: 6db30000 6dbd3000   C:\WINDOWS\WinSxS\x86_microsoft.vc90.crt_1fc8b3b9a1e18e3b_9.0.30729.9415_none_508df7e2bcbccb90\MSVCR90.dll
(2108.f4): Break instruction exception - code 80000003 (first chance)
eax=00000000 ebx=00000000 ecx=c34a0000 edx=00000000 esi=00b77000 edi=77c4d724
eip=77ce80c9 esp=00d3f438 ebp=00d3f464 iopl=0         nv up ei pl zr na pe nc
cs=0023  ss=002b  ds=002b  es=002b  fs=0053  gs=002b             efl=00000246
ntdll!LdrpDoDebuggerBreak+0x2b:
77ce80c9 cc              int     3
```

This time all the symbols loaded successfully.

Here we can extract the following info.

Base	End	Name
00270000	00276000	lab3.exe
77c40000	77dd0000	ntdll.dll
76110000	761f0000	KERNEL32.DLL
75d20000	75f04000	KERNELBASE.dll
6db30000	6dbd3000	C:\WINDOWS\WinSxS\ \x86_microsoft.vc90.crt_1fc8b3b9a1e18e3b_9 .0.30729.9415_none_508df7e2bcbccb90\MSVCR90.dll

These were the most suspicious DLLs I found. Many of these provide low level access to system level functions.

Using the lm command we get another printout of similar information.

```
0:000> lm
start    end        module name
00270000 00276000   lab3       (no symbols)
6db30000 6dbd3000   MSVCR90    (deferred)
74f10000 74f8d000   msvcp_win   (deferred)
75050000 7516e000   ucrtbase   (deferred)
752a0000 752c2000   GDI32      (deferred)
752d0000 752e7000   win32u     (deferred)
75810000 75974000   gdi32full   (deferred)
75b20000 75cad000   USER32     (deferred)
75d20000 75f04000   KERNELBASE   (deferred)
76110000 761f0000   KERNEL32   (deferred)
77c40000 77dd0000   ntdll      (pdb symbols)          C:\ProgramData\Dbg\sym\wntdll.pdb\D3AE91CEDD9309EF777F2FD5120010BE1\wntdll.pdb
```

Listing the lab3 we see that there is no information in the resource tables.

```
0:000> lmDvmlab3
Browse full module list
start    end        module name
00270000 00276000   lab3       (no symbols)
    Loaded symbol image file: C:\Users\Administrator\Desktop\lab3_dimitry\lab3.exe
    Image path: lab3.exe
    Image name: lab3.exe
    Browse all global symbols  functions  data
    Timestamp:        Thu Feb  8 19:28:57 2018 (5A7D1579)
    CheckSum:         000060BA
    ImageSize:        00006000
    Translations:     0000.04b0 0000.04e4 0409.04b0 0409.04e4
    Information from resource tables:
```

Next we will examine the file headers for the main executable.

```
0:000> !dh 00270000 -f

File Type: EXECUTABLE IMAGE
FILE HEADER VALUES
     14C machine (i386)
       5 number of sections
5A7D1579 time date stamp Thu Feb  8 19:28:57 2018

       0 file pointer to symbol table
       0 number of symbols
      E0 size of optional header
     102 characteristics
            Executable
            32 bit word machine

OPTIONAL HEADER VALUES
     10B magic #
    9.00 linker version
     E00 size of code
    1400 size of initialized data
       0 size of uninitialized data
    1855 address of entry point
    1000 base of code
         ----- new -----
00270000 image base
    1000 section alignment
     200 file alignment
       2 subsystem (Windows GUI)
    5.00 operating system version
    0.00 image version
    5.00 subsystem version
    6000 size of image
     400 size of headers
```

```
    60BA checksum
00100000 size of stack reserve
00001000 size of stack commit
00100000 size of heap reserve
00001000 size of heap commit
    8140  DLL characteristics
            Dynamic base
            NX compatible
            Terminal server aware
       0 [       0] address [size] of Export Directory
    22AC [      64] address [size] of Import Directory
    4000 [     34C] address [size] of Resource Directory
       0 [       0] address [size] of Exception Directory
       0 [       0] address [size] of Security Directory
    5000 [     1D8] address [size] of Base Relocation Directory
    2130 [      1C] address [size] of Debug Directory
       0 [       0] address [size] of Description Directory
       0 [       0] address [size] of Special Directory
       0 [       0] address [size] of Thread Storage Directory
    2198 [      40] address [size] of Load Configuration Directory
       0 [       0] address [size] of Bound Import Directory
    2000 [     110] address [size] of Import Address Table Directory
       0 [       0] address [size] of Delay Import Directory
       0 [       0] address [size] of COR20 Header Directory
       0 [       0] address [size] of Reserved Directory
```

From this output we can see some of the Virtual addresses and sizes of different data directories. Import directory, resource directory, base relocation directory, debug directory, load configuration directory and import address table directory are used.

Now we will take a closer look at the IAT and the Export Directory.

```
0:000> dps 00270000+2000
00272000  752a5790 GDI32!TextOutAStub
00272004  00000000
00272008  7617f5f0 KERNEL32!CreateMutexA
0027200c  7617f6d0 KERNEL32!ReleaseMutex
00272010  7617f560 KERNEL32!CloseHandle
00272014  761243e0 KERNEL32!CreateThreadStub
00272018  7617f510 KERNEL32!GetCurrentProcessId
0027201c  76128560 KERNEL32!GetCurrentThreadId
00272020  7617ea30 KERNEL32!GetTickCountStub
00272024  76126490 KERNEL32!SleepStub
00272028  76125660 KERNEL32!IsDebuggerPresentStub
0027202c  76126450 KERNEL32!SetUnhandledExceptionFilterStub
00272030  76126600 KERNEL32!UnhandledExceptionFilterStub
00272034  7617f500 KERNEL32!GetCurrentProcess
00272038  76126510 KERNEL32!TerminateProcessStub
0027203c  76163760 KERNEL32!GetStartupInfoA
00272040  761270d0 KERNEL32!InterlockedCompareExchangeStub
00272044  76127110 KERNEL32!InterlockedExchangeStub
00272048  76125260 KERNEL32!GetSystemTimeAsFileTimeStub
0027204c  76125ad0 KERNEL32!QueryPerformanceCounterStub
00272050  7617f750 KERNEL32!WaitForSingleObject
00272054  00000000
00272058  6dbaa95b MSVCR90!_controlfp_s
0027205c  6db9cb33 MSVCR90!_invoke_watson [f:\dd\vctools\crt_bld\self_x86\crt\src\invarg.c @ 137]
00272060  6dba1850 MSVCR90!_except_handler4_common
00272064  6db62e73 MSVCR90!sprintf [f:\dd\vctools\crt_bld\self_x86\crt\src\sprintf.c @ 99]
00272068  6db52157 MSVCR90!_amsg_exit [f:\dd\vctools\crt_bld\self_x86\crt\src\crt0dat.c @ 460]
0027206c  6db52793 MSVCR90!__getmainargs [f:\dd\vctools\crt_bld\self_x86\crt\src\crtlib.c @ 148]
00272070  6db5248b MSVCR90!_cexit [f:\dd\vctools\crt_bld\self_x86\crt\src\crt0dat.c @ 426]
00272074  6db52470 MSVCR90!_exit [f:\dd\vctools\crt_bld\self_x86\crt\src\crt0dat.c @ 419]
00272078  6db9cf88 MSVCR90!_XcptFilter [f:\dd\vctools\crt_bld\self_x86\crt\src\winxfltr.c @ 206]
0027207c  6db704e0 MSVCR90!_ismbblead [f:\dd\vctools\crt_bld\self_x86\crt\src\ismbbyte.c @ 171]
```

Looks like the application creates threads and uses a mutex to manage some kind of multi-threaded operation.

Now all that is left is to check the exports for some of the suspicious DLLs.

We listed them at the start but let's put them here again for convenience.

Base	End	Name
00270000	00276000	lab3.exe
77c40000	77dd0000	ntdll.dll
76110000	761f0000	KERNEL32.DLL
75d20000	75f04000	KERNELBASE.dll
6db30000	6dbd3000	C:\WINDOWS\WinSxS\ \x86_microsoft.vc90.crt_1fc8b3b9a1e18e3b_9 .0.30729.9415_none_508df7e2bcbccb90\MSVCR90.dll

Lab3.exe
Turns out it has no exports which makes sense. It is the main application.

Ntdll.dll

IMAGE_EXPORT_DIRECTORY:

```
0:000> dd 77c40000+100CF0
77d40cf0  00000000 bf2f8c99 00000000 00106a1a
77d40d00  00000008 0000094d 0000094d 00100d18
77d40d10  0010324c 00105780 0002b8c0 0003e540
77d40d20  000412c0 000b4c10 000b4cb0 000b4cc0
77d40d30  000b4ce0 0002c7d0 0007edd0 0002c890
77d40d40  000b4cf0 000b4d20 000b4e10 000b4e40
77d40d50  00024760 00024720 000b4e80 000b4fd0
77d40d60  000246e0 000b4ff0 000b5000 000b5050
```

AddressOfNames:

```
0:000> dd 77c40000+0010324c
77d4324c  00106ac8 00106ad3 00106add 00106ae9
77d4325c  00106b12 00106b30 00106b5c 00106b83
77d4326c  00106b95 00106bad 00106bce 00106bfb
77d4327c  00106c1a 00106c36 00106c51 00106c78
77d4328c  00106c92 00106caf 00106cd8 00106cf2
77d4329c  00106d0b 00106d25 00106d3d 00106d69
77d432ac  00106d81 00106d93 00106da7 00106dc0
77d432bc  00106dd5 00106de5 00106e00 00106e14
```

List of String Names

```
0:000> da ntdll+00106ac8
77d46ac8  "A_SHAFinal"
0:000> da ntdll+00106b12
77d46b12  "AlpcFreeCompletionListMessage"
0:000> da ntdll+00106b95
77d46b95  "AlpcGetMessageAttribute"
0:000> da ntdll+00106c1a
77d46c1a  "AlpcMaxAllowedMessageLength"
```

```
0:000> da ntdll+00106c92
77d46c92  "AlpcUnregisterCompletionList"
0:000> da ntdll+00106d0b
77d46d0b  "CsrAllocateMessagePointer"
0:000> da ntdll+00106d81
77d46d81  "CsrCaptureTimeout"
0:000> da ntdll+00106dd5
77d46dd5  "CsrGetProcessId"
```

This is really suspicious. The process is exporting cryptographic functions.

Script:

r? @$t0 = ((int *) (0x77D4324C))

.for (r @$t1 = 0; @$t1 < 100; r @$t1 = @$t1 + 1) {da ntdll+(@@c++(@$t0[@$t1]));}

Running the customized script, I got:

```
0:000> $$><C:\Users\Administrator\Desktop\lab3_dimitry\script.wds
77d46ac8  "A_SHAFinal"
77d46ad3  "A_SHAInit"
77d46add  "A_SHAUpdate"
77d46ae9  "AlpcAdjustCompletionListConcurre"
77d46b09  "ncyCount"
77d46b12  "AlpcFreeCompletionListMessage"
77d46b30  "AlpcGetCompletionListLastMessage"
77d46b50  "Information"
77d46b5c  "AlpcGetCompletionListMessageAttr"
77d46b7c  "ibutes"
77d46b83  "AlpcGetHeaderSize"
77d46b95  "AlpcGetMessageAttribute"
77d46bad  "AlpcGetMessageFromCompletionList"
77d46bcd  ""
77d46bce  "AlpcGetOutstandingCompletionList"
77d46bee  "MessageCount"
77d46bfb  "AlpcInitializeMessageAttribute"
77d46c1a  "AlpcMaxAllowedMessageLength"
77d46c36  "AlpcRegisterCompletionList"
77d46c51  "AlpcRegisterCompletionListWorker"
77d46c71  "Thread"
77d46c78  "AlpcRundownCompletionList"
77d46c92  "AlpcUnregisterCompletionList"
77d46caf  "AlpcUnregisterCompletionListWork"
77d46ccf  "erThread"
77d46cd8  "ApiSetQueryApiSetPresence"
77d46cf2  "CsrAllocateCaptureBuffer"
77d46d0b  "CsrAllocateMessagePointer"
77d46d25  "CsrCaptureMessageBuffer"
77d46d3d  "CsrCaptureMessageMultiUnicodeStr"
77d46d5d  "ingsInPlace"
77d46d69  "CsrCaptureMessageString"
77d46d81  "CsrCaptureTimeout"
77d46d93  "CsrClientCallServer"
77d46da7  "CsrClientConnectToServer"
77d46dc0  "CsrFreeCaptureBuffer"
77d46dd5  "CsrGetProcessId"
77d46de5  "CsrIdentifyAlertableThread"
77d46e00  "CsrSetPriorityClass"
77d46e14  "CsrVerifyRegion"
77d46e24  "DbgBreakPoint"
77d46e32  "DbgPrint"
77d46e3b  "DbgPrintEx"
77d46e46  "DbgPrintReturnControlC"
77d46e5d  "DbgPrompt"
77d46e67  "DbgQueryDebugFilterState"
77d46e80  "DbgSetDebugFilterState"
77d46e97  "DbgUiConnectToDbg"
77d46ea9  "DbgUiContinue"
77d46eb7  "DbgUiConvertStateChangeStructure"
```

```
77d46ed7  ""
77d46ed8  "DbgUiConvertStateChangeStructure"
77d46ef8  "Ex"
77d46efb  "DbgUiDebugActiveProcess"
77d46f13  "DbgUiGetThreadDebugObject"
77d46f2d  "DbgUiIssueRemoteBreakin"
77d46f45  "DbgUiRemoteBreakin"
77d46f58  "DbgUiSetThreadDebugObject"
77d46f72  "DbgUiStopDebugging"
77d46f85  "DbgUiWaitStateChange"
77d46f9a  "DbgUserBreakPoint"
77d46fac  "EtwCheckCoverage"
77d46fbd  "EtwCreateTraceInstanceId"
77d46fd6  "EtwDeliverDataBlock"
77d46fea  "EtwEnumerateProcessRegGuids"
77d47006  "EtwEventActivityIdControl"
77d47020  "EtwEventEnabled"
77d47030  "EtwEventProviderEnabled"
77d47048  "EtwEventRegister"
77d47059  "EtwEventSetInformation"
77d47070  "EtwEventUnregister"
77d47083  "EtwEventWrite"
77d47091  "EtwEventWriteEndScenario"
77d470aa  "EtwEventWriteEx"
77d470ba  "EtwEventWriteFull"
77d470cc  "EtwEventWriteNoRegistration"
77d470e8  "EtwEventWriteStartScenario"
77d47103  "EtwEventWriteString"
77d47117  "EtwEventWriteTransfer"
77d4712d  "EtwGetTraceEnableFlags"
77d47144  "EtwGetTraceEnableLevel"
77d4715b  "EtwGetTraceLoggerHandle"
77d47173  "EtwLogTraceEvent"
77d47184  "EtwNotificationRegister"
77d4719c  "EtwNotificationUnregister"
77d471b6  "EtwProcessPrivateLoggerRequest"
77d471d5  "EtwRegisterSecurityProvider"
77d471f1  "EtwRegisterTraceGuidsA"
77d47208  "EtwRegisterTraceGuidsW"
77d4721f  "EtwReplyNotification"
77d47234  "EtwSendNotification"
77d47248  "EtwSetMark"
77d47253  "EtwTraceEventInstance"
77d47269  "EtwTraceMessage"
77d47279  "EtwTraceMessageVa"
77d4728b  "EtwUnregisterTraceGuids"
77d472a3  "EtwWriteUMSecurityEvent"
77d472bb  "EtwpCreateEtwThread"
77d472cf  "EtwpGetCpuSpeed"
77d472df  "EvtIntReportAuthzEventAndSourceA"
77d472ff  "sync"
77d47304  "EvtIntReportEventAndSourceAsync"
77d47324  "KiFastSystemCall"
77d47335  "KiFastSystemCallRet"
77d47349  "KiIntSystemCall"
77d47359  "KiRaiseUserExceptionDispatcher"
77d47378  "KiUserApcDispatcher"
```

```
77d4738c  "KiUserCallbackDispatcher"
77d473a5  "KiUserExceptionDispatcher"
77d473bf  "LdrAccessResource"
77d473d1  "LdrAddDllDirectory"
77d473e4  "LdrAddLoadAsDataTable"
77d473fa  "LdrAddRefDll"
77d47407  "LdrAppxHandleIntegrityFailure"
77d47425  "LdrCallEnclave"
77d47434  "LdrControlFlowGuardEnforced"
77d47450  "LdrCreateEnclave"
77d47461  "LdrDeleteEnclave"
77d47472  "LdrDisableThreadCalloutsForDll"
77d47491  "LdrEnumResources"
77d474a2  "LdrEnumerateLoadedModules"
77d474bc  "LdrFastFailInLoaderCallout"
77d474d7  "LdrFindEntryForAddress"
77d474ee  "LdrFindResourceDirectory_U"
77d47509  "LdrFindResourceEx_U"
77d4751d  "LdrFindResource_U"
77d4752f  "LdrFlushAlternateResourceModules"
77d4754f  ""
77d47550  "LdrGetDllDirectory"
77d47563  "LdrGetDllFullName"
77d47575  "LdrGetDllHandle"
77d47585  "LdrGetDllHandleByMapping"
77d4759e  "LdrGetDllHandleByName"
77d475b4  "LdrGetDllHandleEx"
77d475c6  "LdrGetDllPath"
77d475d4  "LdrGetFailureData"
77d475e6  "LdrGetFileNameFromLoadAsDataTabl"
77d47606  "e"
77d47608  "LdrGetProcedureAddress"
77d4761f  "LdrGetProcedureAddressEx"
77d47638  "LdrGetProcedureAddressForCaller"
77d47658  "LdrInitShimEngineDynamic"
77d47671  "LdrInitializeEnclave"
77d47686  "LdrInitializeThunk"
77d47699  "LdrLoadAlternateResourceModule"
77d476b8  "LdrLoadAlternateResourceModuleEx"
77d476d8  ""
77d476d9  "LdrLoadDll"
77d476e4  "LdrLoadEnclaveModule"
77d476f9  "LdrLockLoaderLock"
77d4770b  "LdrOpenImageFileOptionsKey"
77d47726  "LdrParentInterlockedPopEntrySLis"
77d47746  "t"
77d47748  "LdrParentRtlInitializeNtUserPfn"
77d47768  "LdrParentRtlResetNtUserPfn"
77d47783  "LdrParentRtlRetrieveNtUserPfn"
77d477a1  "LdrProcessRelocationBlock"
77d477bb  "LdrProcessRelocationBlockEx"
77d477d7  "LdrQueryImageFileExecutionOption"
77d477f7  "s"
77d477f9  "LdrQueryImageFileExecutionOption"
77d47819  "sEx"
77d4781d  "LdrQueryImageFileKeyOption"
77d47838  "LdrQueryModuleServiceTags"
```

```
77d47852  "LdrQueryOptionalDelayLoadedAPI"
77d47871  "LdrQueryProcessModuleInformation"
77d47891  ""
77d47892  "LdrRegisterDllNotification"
77d478ad  "LdrRemoveDllDirectory"
77d478c3  "LdrRemoveLoadAsDataTable"
77d478dc  "LdrResFindResource"
77d478ef  "LdrResFindResourceDirectory"
77d4790b  "LdrResGetRCConfig"
77d4791d  "LdrResRelease"
77d4792b  "LdrResSearchResource"
77d47940  "LdrResolveDelayLoadedAPI"
77d47959  "LdrResolveDelayLoadsFromDll"
77d47975  "LdrRscIsTypeExist"
77d47987  "LdrSetAppCompatDllRedirectionCal"
77d479a7  "lback"
77d479ad  "LdrSetDefaultDllDirectories"
77d479c9  "LdrSetDllDirectory"
77d479dc  "LdrSetDllManifestProber"
77d479f4  "LdrSetImplicitPathOptions"
77d47a0e  "LdrSetMUICacheType"
77d47a21  "LdrShutdownProcess"
77d47a34  "LdrShutdownThread"
77d47a46  "LdrStandardizeSystemPath"
77d47a5f  "LdrSystemDllInitBlock"
77d47a75  "LdrUnloadAlternateResourceModule"
77d47a95  ""
77d47a96  "LdrUnloadAlternateResourceModule"
77d47ab6  "Ex"
77d47ab9  "LdrUnloadDll"
77d47ac6  "LdrUnlockLoaderLock"
77d47ada  "LdrUnregisterDllNotification"
77d47af7  "LdrUpdatePackageSearchPath"
77d47b12  "LdrVerifyImageMatchesChecksum"
77d47b30  "LdrVerifyImageMatchesChecksumEx"
77d47b50  "LdrpChildNtdll"
77d47b5f  "LdrpResGetMappingSize"
77d47b75  "LdrpResGetResourceDirectory"
77d47b91  "MD4Final"
77d47b9a  "MD4Init"
77d47ba2  "MD4Update"
77d47bac  "MD5Final"
77d47bb5  "MD5Init"
77d47bbd  "MD5Update"
77d47bc7  "NlsAnsiCodePage"
77d47bd7  "NlsMbCodePageTag"
77d47be8  "NlsMbOemCodePageTag"
77d47bfc  "NtAcceptConnectPort"
77d47c10  "NtAccessCheck"
77d47c1e  "NtAccessCheckAndAuditAlarm"
77d47c39  "NtAccessCheckByType"
77d47c4d  "NtAccessCheckByTypeAndAuditAlarm"
77d47c6d  ""
77d47c6e  "NtAccessCheckByTypeResultList"
77d47c8c  "NtAccessCheckByTypeResultListAnd"
77d47cac  "AuditAlarm"
77d47cb7  "NtAccessCheckByTypeResultListAnd"
```

```
77d47cd7  "AuditAlarmByHandle"
77d47cea  "NtAcquireProcessActivityReferenc"
77d47d0a  "e"
77d47d0c  "NtAddAtom"
77d47d16  "NtAddAtomEx"
77d47d22  "NtAddBootEntry"
77d47d31  "NtAddDriverEntry"
77d47d42  "NtAdjustGroupsToken"
77d47d56  "NtAdjustPrivilegesToken"
77d47d6e  "NtAdjustTokenClaimsAndDeviceGrou"
77d47d8e  "ps"
77d47d91  "NtAlertResumeThread"
77d47da5  "NtAlertThread"
77d47db3  "NtAlertThreadByThreadId"
77d47dcb  "NtAllocateLocallyUniqueId"
77d47de5  "NtAllocateReserveObject"
77d47dfd  "NtAllocateUserPhysicalPages"
77d47e19  "NtAllocateUuids"
77d47e29  "NtAllocateVirtualMemory"
77d47e41  "NtAllocateVirtualMemoryEx"
77d47e5b  "NtAlpcAcceptConnectPort"
77d47e73  "NtAlpcCancelMessage"
77d47e87  "NtAlpcConnectPort"
77d47e99  "NtAlpcConnectPortEx"
77d47ead  "NtAlpcCreatePort"
77d47ebe  "NtAlpcCreatePortSection"
77d47ed6  "NtAlpcCreateResourceReserve"
77d47ef2  "NtAlpcCreateSectionView"
77d47f0a  "NtAlpcCreateSecurityContext"
77d47f26  "NtAlpcDeletePortSection"
77d47f3e  "NtAlpcDeleteResourceReserve"
77d47f5a  "NtAlpcDeleteSectionView"
77d47f72  "NtAlpcDeleteSecurityContext"
77d47f8e  "NtAlpcDisconnectPort"
77d47fa3  "NtAlpcImpersonateClientContainer"
77d47fc3  "OfPort"
77d47fca  "NtAlpcImpersonateClientOfPort"
77d47fe8  "NtAlpcOpenSenderProcess"
77d48000  "NtAlpcOpenSenderThread"
77d48017  "NtAlpcQueryInformation"
77d4802e  "NtAlpcQueryInformationMessage"
77d4804c  "NtAlpcRevokeSecurityContext"
77d48068  "NtAlpcSendWaitReceivePort"
77d48082  "NtAlpcSetInformation"
77d48097  "NtApphelpCacheControl"
77d480ad  "NtAreMappedFilesTheSame"
77d480c5  "NtAssignProcessToJobObject"
77d480e0  "NtAssociateWaitCompletionPacket"
77d48100  "NtCallEnclave"
77d4810e  "NtCallbackReturn"
77d4811f  "NtCancelIoFile"
77d4812e  "NtCancelIoFileEx"
77d4813f  "NtCancelSynchronousIoFile"
77d48168  "NtCancelTimer"
77d48159  "NtCancelTimer2"
77d48176  "NtCancelWaitCompletionPacket"
77d48193  "NtClearEvent"
```

```
77d481a0  "NtClose"
77d481a8  "NtCloseObjectAuditAlarm"
77d481c0  "NtCommitComplete"
77d481d1  "NtCommitEnlistment"
77d481e4  "NtCommitRegistryTransaction"
```

There are a lot of functions that can be used for malicious intents. This does not mean that they are being used in that way. We will have to perform more analysis before making a definitive statement.

Kernel32.dll

```
0:000> dd 76110000+91020
761a1020  00000000 ae0a74bf 00000000 00094e96
761a1030  00000001 0000063b 0000063b 00091048
761a1040  00092934 00094220 00018460 00094ed0
761a1050  00081f64 00094f1a 00094f50 00017510
761a1060  0001e7d0 00043030 000430b0 00070260
761a1070  00070270 00094fd6 00018430 000447a0
761a1080  000446a0 00017530 0001e780 00017ee0
761a1090  00017260 00017f00 00011e40 0009510f
0:000> dd 76110000+00092934
761a2934  00094f02 00094f3b 00094f6e 00094f7d
761a2944  00094f92 00094f9b 00094fa4 00094fb5
761a2954  00094fc6 0009500b 00095031 00095050
761a2964  0009506f 0009507c 0009508f 000950a7
761a2974  000950c2 000950d7 000950f4 00095133
761a2984  00095174 00095187 00095194 000951ae
761a2994  000951cc 00095203 00095248 00095293
761a29a4  000952ee 00095343 00095396 000953eb
```

From here we get the function addresses.

Script:

r? @$t0 = ((int *) (0x761A2934))

.for (r @$t1 = 0; @$t1 < 100; r @$t1 = @$t1 + 1) {da KERNEL32+(@@c++(@$t0[@$t1]));}

We will output the functions here:

```
0:000> $$><C:\Users\Administrator\Desktop\lab3_dimitry\script.wds
761a4f02  "AcquireSRWLockExclusive"
761a4f3b  "AcquireSRWLockShared"
761a4f6e  "ActivateActCtx"
761a4f7d  "ActivateActCtxWorker"
761a4f92  "AddAtomA"
761a4f9b  "AddAtomW"
761a4fa4  "AddConsoleAliasA"
761a4fb5  "AddConsoleAliasW"
761a4fc6  "AddDllDirectory"
761a500b  "AddIntegrityLabelToBoundaryDescr"
761a502b  "iptor"
761a5031  "AddLocalAlternateComputerNameA"
761a5050  "AddLocalAlternateComputerNameW"
```

```
761a506f  "AddRefActCtx"
761a507c  "AddRefActCtxWorker"
761a508f  "AddResourceAttributeAce"
761a50a7  "AddSIDToBoundaryDescriptor"
761a50c2  "AddScopedPolicyIDAce"
761a50d7  "AddSecureMemoryCacheCallback"
761a50f4  "AddVectoredContinueHandler"
761a5133  "AddVectoredExceptionHandler"
761a5174  "AdjustCalendarDate"
761a5187  "AllocConsole"
761a5194  "AllocateUserPhysicalPages"
761a51ae  "AllocateUserPhysicalPagesNuma"
761a51cc  "AppPolicyGetClrCompat"
761a5203  "AppPolicyGetCreateFileAccess"
761a5248  "AppPolicyGetLifecycleManagement"
761a5293  "AppPolicyGetMediaFoundationCodec"
761a52b3  "Loading"
761a52ee  "AppPolicyGetProcessTerminationMe"
761a530e  "thod"
761a5343  "AppPolicyGetShowDeveloperDiagnos"
761a5363  "tic"
761a5396  "AppPolicyGetThreadInitialization"
761a53b6  "Type"
761a53eb  "AppPolicyGetWindowingModel"
761a542c  "AppXGetOSMaxVersionTested"
761a546b  "ApplicationRecoveryFinished"
761a5487  "ApplicationRecoveryInProgress"
761a54a5  "AreFileApisANSI"
761a54b5  "AssignProcessToJobObject"
761a54ce  "AttachConsole"
761a54dc  "BackupRead"
761a54e7  "BackupSeek"
761a54f2  "BackupWrite"
761a54fe  "BaseCheckAppcompatCache"
761a5516  "BaseCheckAppcompatCacheEx"
761a5530  "BaseCheckAppcompatCacheExWorker"
761a5550  "BaseCheckAppcompatCacheWorker"
761a556e  "BaseCheckElevation"
761a5581  "BaseCleanupAppcompatCacheSupport"
761a55a1  ""
761a55a2  "BaseCleanupAppcompatCacheSupport"
761a55c2  "Worker"
761a55c9  "BaseDestroyVDMEnvironment"
761a55e3  "BaseDllReadWriteIniFile"
761a55fb  "BaseDumpAppcompatCache"
761a5612  "BaseDumpAppcompatCacheWorker"
761a562f  "BaseElevationPostProcessing"
761a564b  "BaseFlushAppcompatCache"
761a5663  "BaseFlushAppcompatCacheWorker"
761a5681  "BaseFormatObjectAttributes"
761a569c  "BaseFormatTimeOut"
761a56ae  "BaseFreeAppCompatDataForProcessW"
761a56ce  "orker"
761a56d4  "BaseGenerateAppCompatData"
761a56ee  "BaseGetNamedObjectDirectory"
761a570a  "BaseInitAppcompatCacheSupport"
761a5728  "BaseInitAppcompatCacheSupportWor"
```

```
761a5748  "ker"
761a574c  "BaseIsAppcompatInfrastructureDis"
761a576c  "abled"
761a5772  "BaseIsAppcompatInfrastructureDis"
761a5792  "abledWorker"
761a579e  "BaseIsDosApplication"
761a57b3  "BaseQueryModuleData"
761a57c7  "BaseReadAppCompatDataForProcessW"
761a57e7  "orker"
761a57ed  "BaseSetLastNTError"
761a4ea3  "BaseThreadInitThunk"
761a5800  "BaseUpdateAppcompatCache"
761a5819  "BaseUpdateAppcompatCacheWorker"
761a5838  "BaseUpdateVDMEntry"
761a584b  "BaseVerifyUnicodeString"
761a5863  "BaseWriteErrorElevationRequiredE"
761a5883  "vent"
761a5888  "Basep8BitStringToDynamicUnicodeS"
761a58a8  "tring"
761a58ae  "BasepAllocateActivationContextAc"
761a58ce  "tivationBlock"
761a58dc  "BasepAnsiStringToDynamicUnicodeS"
761a58fc  "tring"
761a5902  "BasepAppContainerEnvironmentExte"
761a5922  "nsion"
761a5928  "BasepAppXExtension"
761a593b  "BasepCheckAppCompat"
761a594f  "BasepCheckWebBladeHashes"
761a5968  "BasepCheckWinSaferRestrictions"
761a5987  "BasepConstructSxsCreateProcessMe"
761a59a7  "ssage"
761a59ad  "BasepCopyEncryption"
761a59c1  "BasepFreeActivationContextActiva"
761a59e1  "tionBlock"
761a59eb  "BasepFreeAppCompatData"
761a5a02  "BasepGetAppCompatData"
761a5a18  "BasepGetComputerNameFromNtPath"
761a5a37  "BasepGetExeArchType"
761a5a4b  "BasepInitAppCompatData"
761a5a62  "BasepIsProcessAllowed"
761a5a78  "BasepMapModuleHandle"
761a5a8d  "BasepNotifyLoadStringResource"
761a5aab  "BasepPostSuccessAppXExtension"
761a5ac9  "BasepProcessInvalidImage"
761a5ae2  "BasepQueryAppCompat"
761a5af6  "BasepQueryModuleChpeSettings"
761a5b13  "BasepReleaseAppXContext"
761a5b2b  "BasepReleaseSxsCreateProcessUtil"
761a5b4b  "ityStruct"
761a5b55  "BasepReportFault"
761a5b66  "BasepSetFileEncryptionCompressio"
761a5b86  "n"
761a5b88  "Beep"
761a5b8d  "BeginUpdateResourceA"
761a5ba2  "BeginUpdateResourceW"
761a5bb7  "BindIoCompletionCallback"
761a5bd0  "BuildCommDCBA"
```

```
761a5bde  "BuildCommDCBAndTimeoutsA"
761a5bf7  "BuildCommDCBAndTimeoutsW"
761a5c10  "BuildCommDCBW"
761a5c1e  "CallNamedPipeA"
761a5c2d  "CallNamedPipeW"
761a5c3c  "CallbackMayRunLong"
761a5c4f  "CancelDeviceWakeupRequest"
761a5c69  "CancelIo"
761a5c72  "CancelIoEx"
761a5c7d  "CancelSynchronousIo"
761a5c91  "CancelThreadpoolIo"
761a5cc3  "CancelTimerQueueTimer"
761a5cd9  "CancelWaitableTimer"
761a5ced  "CeipIsOptedIn"
761a5d14  "ChangeTimerQueueTimer"
761a5d2a  "CheckAllowDecryptedRemoteDestina"
761a5d4a  "tionPolicy"
761a5d55  "CheckElevation"
761a5d64  "CheckElevationEnabled"
761a5d7a  "CheckForReadOnlyResource"
761a5d93  "CheckForReadOnlyResourceFilter"
761a5db2  "CheckNameLegalDOS8Dot3A"
761a5dca  "CheckNameLegalDOS8Dot3W"
761a5de2  "CheckRemoteDebuggerPresent"
761a5dfd  "CheckTokenCapability"
761a5e12  "CheckTokenMembershipEx"
761a5e29  "ClearCommBreak"
761a5e38  "ClearCommError"
761a5e47  "CloseConsoleHandle"
761a5e5a  "CloseHandle"
761a5e66  "ClosePackageInfo"
761a5e93  "ClosePrivateNamespace"
761a5ea9  "CloseProfileUserMapping"
761a5ec1  "CloseState"
761a5ee2  "CloseThreadpool"
761a5f06  "CloseThreadpoolCleanupGroup"
761a5f3e  "CloseThreadpoolCleanupGroupMembe"
761a5f5e  "rs"
761a5f84  "CloseThreadpoolIo"
761a5fb2  "CloseThreadpoolTimer"
761a5fdc  "CloseThreadpoolWait"
761a6004  "CloseThreadpoolWork"
761a602c  "CmdBatNotification"
761a603f  "CommConfigDialogA"
761a6051  "CommConfigDialogW"
761a6063  "CompareCalendarDates"
761a6078  "CompareFileTime"
761a6088  "CompareStringA"
761a6097  "CompareStringEx"
761a60a7  "CompareStringOrdinal"
761a60bc  "CompareStringW"
761a60cb  "ConnectNamedPipe"
761a60dc  "ConsoleMenuControl"
761a60ef  "ContinueDebugEvent"
761a6102  "ConvertCalDateTimeToSystemTime"
761a6121  "ConvertDefaultLocale"
761a6136  "ConvertFiberToThread"
```

```
761a614b  "ConvertNLSDayOfWeekToWin32DayOfW"
761a616b  "eek"
761a616f  "ConvertSystemTimeToCalDateTime"
761a618e  "ConvertThreadToFiber"
761a61a3  "ConvertThreadToFiberEx"
761a61ba  "CopyContext"
761a61c6  "CopyFile2"
761a61d0  "CopyFileA"
761a61da  "CopyFileExA"
761a61e6  "CopyFileExW"
761a61f2  "CopyFileTransactedA"
761a6206  "CopyFileTransactedW"
761a621a  "CopyFileW"
761a6224  "CopyLZFile"
761a622f  "CreateActCtxA"
761a623d  "CreateActCtxW"
761a624b  "CreateActCtxWWorker"
761a625f  "CreateBoundaryDescriptorA"
761a6279  "CreateBoundaryDescriptorW"
761a6293  "CreateConsoleScreenBuffer"
761a62ad  "CreateDirectoryA"
761a62be  "CreateDirectoryExA"
761a62d1  "CreateDirectoryExW"
761a62e4  "CreateDirectoryTransactedA"
761a62ff  "CreateDirectoryTransactedW"
761a631a  "CreateDirectoryW"
761a632b  "CreateEnclave"
761a6366  "CreateEventA"
761a6373  "CreateEventExA"
761a6382  "CreateEventExW"
761a6391  "CreateEventW"
761a639e  "CreateFiber"
761a63aa  "CreateFiberEx"
761a63b8  "CreateFile2"
761a63c4  "CreateFileA"
761a63d0  "CreateFileMappingA"
761a63e3  "CreateFileMappingFromApp"
761a6433  "CreateFileMappingNumaA"
761a644a  "CreateFileMappingNumaW"
761a6461  "CreateFileMappingW"
761a6474  "CreateFileTransactedA"
761a648a  "CreateFileTransactedW"
761a64a0  "CreateFileW"
761a64ac  "CreateHardLinkA"
761a64bc  "CreateHardLinkTransactedA"
761a64d6  "CreateHardLinkTransactedW"
761a64f0  "CreateHardLinkW"
761a6500  "CreateIoCompletionPort"
761a6517  "CreateJobObjectA"
761a6528  "CreateJobObjectW"
761a6539  "CreateJobSet"
761a6546  "CreateMailslotA"
761a6556  "CreateMailslotW"
761a6566  "CreateMemoryResourceNotification"
761a6586  ""
761a6587  "CreateMutexA"
761a6594  "CreateMutexExA"
```

```
761a65a3  "CreateMutexExW"
761a65b2  "CreateMutexW"
761a65bf  "CreateNamedPipeA"
761a65d0  "CreateNamedPipeW"
761a65e1  "CreatePipe"
761a65ec  "CreatePrivateNamespaceA"
761a6604  "CreatePrivateNamespaceW"
761a661c  "CreateProcessA"
761a662b  "CreateProcessAsUserA"
761a6640  "CreateProcessAsUserW"
761a6655  "CreateProcessInternalA"
761a666c  "CreateProcessInternalW"
761a6683  "CreateProcessW"
761a6692  "CreateRemoteThread"
761a66a5  "CreateRemoteThreadEx"
761a66f5  "CreateSemaphoreA"
761a6706  "CreateSemaphoreExA"
761a6719  "CreateSemaphoreExW"
761a672c  "CreateSemaphoreW"
761a673d  "CreateSocketHandle"
761a6750  "CreateSymbolicLinkA"
761a6764  "CreateSymbolicLinkTransactedA"
761a6782  "CreateSymbolicLinkTransactedW"
761a67a0  "CreateSymbolicLinkW"
761a67b4  "CreateTapePartition"
761a67c8  "CreateThread"
761a67d5  "CreateThreadpool"
761a67e6  "CreateThreadpoolCleanupGroup"
761a6803  "CreateThreadpoolIo"
761a6816  "CreateThreadpoolTimer"
761a682c  "CreateThreadpoolWait"
761a6841  "CreateThreadpoolWork"
761a6856  "CreateTimerQueue"
761a6867  "CreateTimerQueueTimer"
761a687d  "CreateToolhelp32Snapshot"
761a6896  "CreateWaitableTimerA"
761a68ab  "CreateWaitableTimerExA"
761a68c2  "CreateWaitableTimerExW"
761a68d9  "CreateWaitableTimerW"
761a68ee  "CtrlRoutine"
```

The kernel DLL provides a lot of functions that can be used to create/modify files, check for elevation etc.