Project - Malware Analaysis Report

Task 1

Simple Analysis

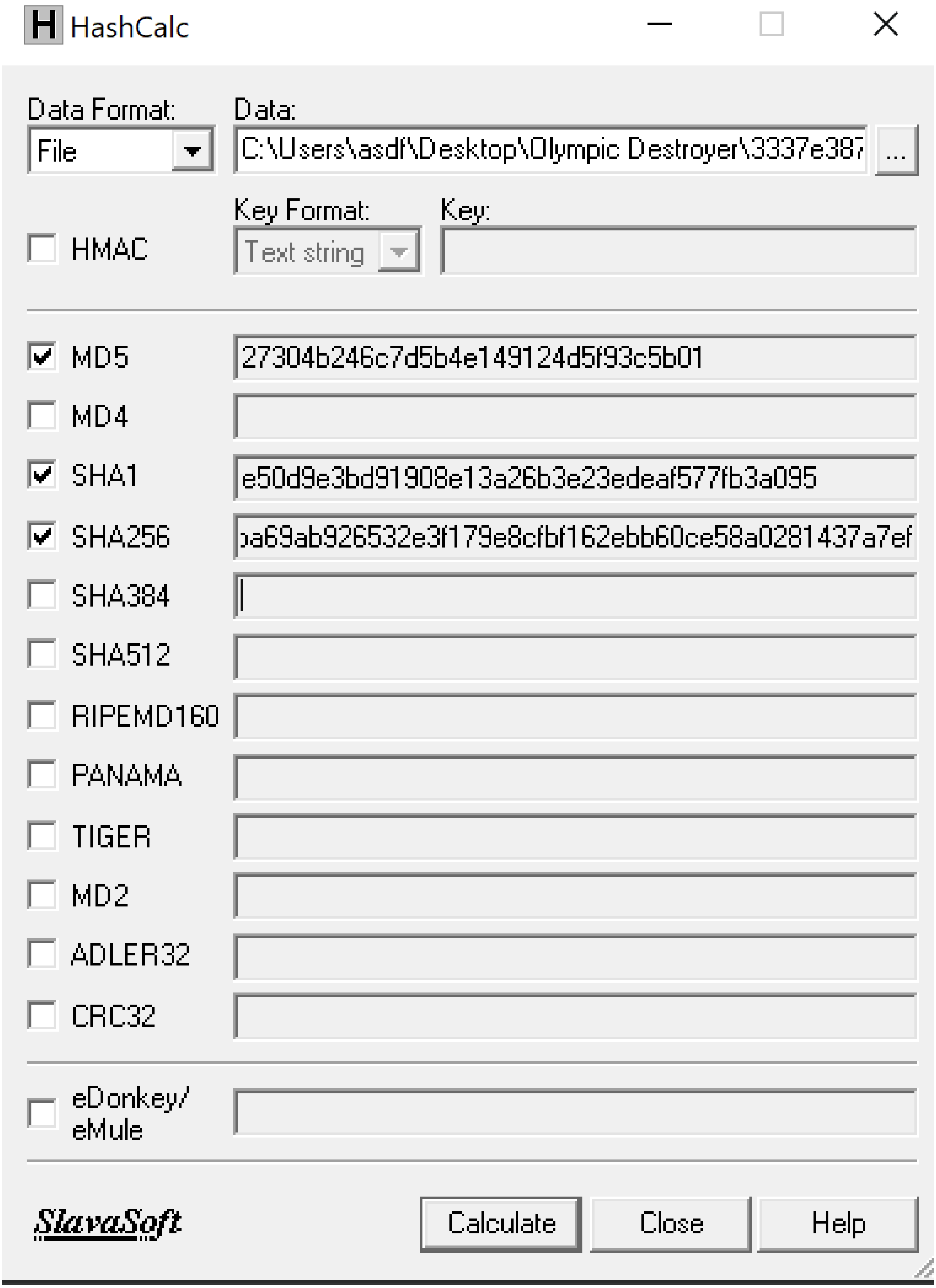
27304b246c7d5b4e149124d5f93c5b01.zip Olympic Destroyer

Basic Information about the sample

File name	3337e3875b05e0bfba69ab926532e3f179e8cfbf162ebb60ce58a0281437a7ef
File size	339,096 bytes
File type	Document
MD5	27304b246c7d5b4e149124d5f93c5b01
SHA1	e50d9e3bd91908e13a26b3e23edeaf577fb3a095
SHA256	3337e3875b05e0bfba69ab926532e3f179e8cfbf162ebb60ce58a0281437a7ef
Sample Origin	Downloaded from LumniNUS https://luminus.nus.edu.sg/modules/c0629e16-d7d2-40c0-8fc2-01e6d2e7184f/files/e3039acb-8e33-463a-a7ab-6903ab3ab9e4
Date of Analysis	19/11/2021 12:58
Type of Analysis	Basic Static and Dynamic Analysis
Packed	False
Compilation Date	28/06/2016
Executive Summary	The macro will run the executable file psexec.exe which is used to create a reverse shell.

Basic Static Analysis

Hashing - Malware Fingerprint



Data Format: File

Data: C:\Users\asdf\Desktop\Olympic Destroyer\3337e387

□ HMAC Key Format: Text string Key:

☑ MD5 27304b246c7d5b4e149124d5f93c5b01

□ MD4

☑ SHA1 e50d9e3bd91908e13a26b3e23edeaf577fb3a095

☑ SHA256 a69ab926532e3f179e8cfbf162ebb60ce58a0281437a7ef

□ SHA384

□ SHA512

□ RIPEMD160

□ PANAMA

□ TIGER

□ MD2

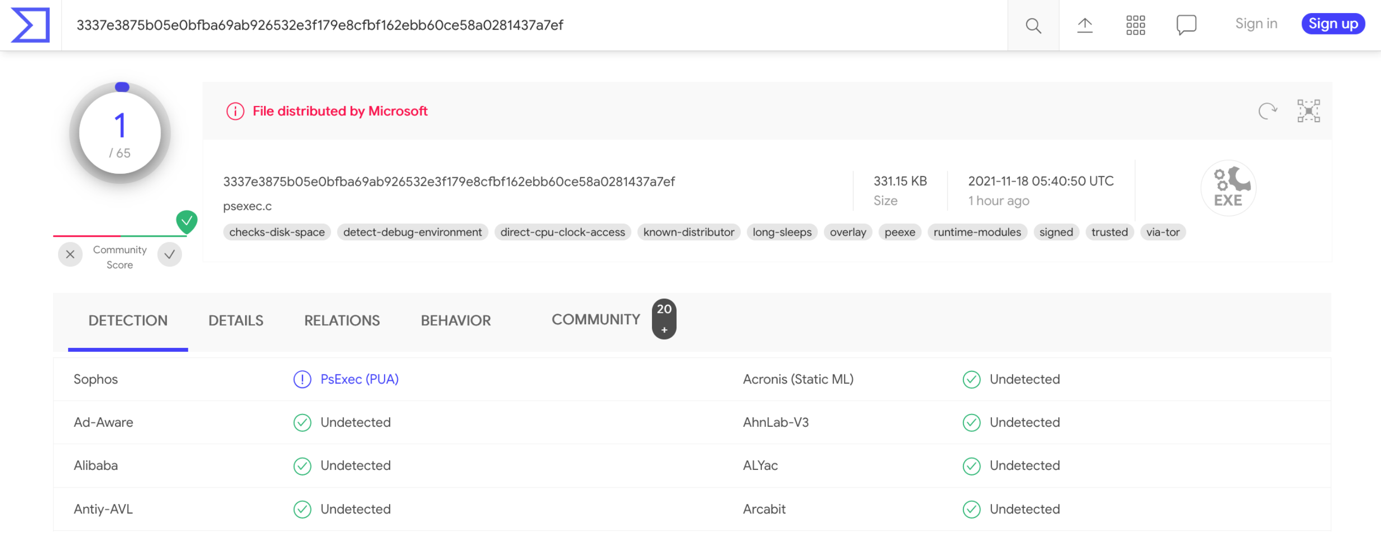
□ ADLER32

□ CRC32

□ eDonkey/ eMule

Virustotal

Matches 1/65 existing definition of antivirus. SOPHOS - PsExec (PUA)



3337e3875b05e0bfba69ab926532e3f179e8cfbf162ebb60ce58a0281437a7ef

Sign in Sign up

1 / 65

Community Score

File distributed by Microsoft

3337e3875b05e0bfba69ab926532e3f179e8cfbf162ebb60ce58a0281437a7ef
psexec.c

331.15 KB
Size

2021-11-18 05:40:50 UTC
1 hour ago

EXE

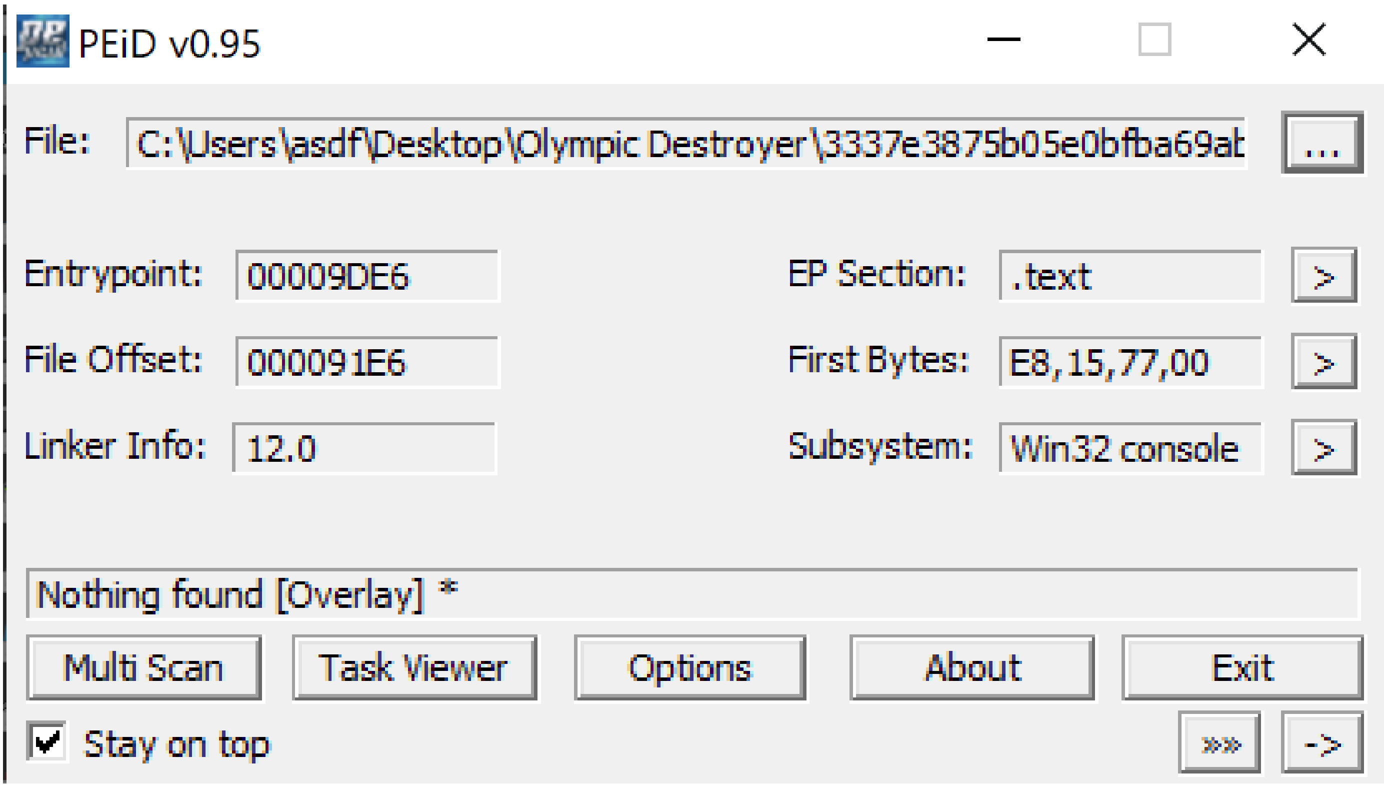
checks-disk-space detect-debug-environment direct-cpu-clock-access known-distributor long-sleeps overlay peexe runtime-modules signed trusted via-tor

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY 20+

Sophos	PsExec (PUA)	Acronis (Static ML)	Undetected
Ad-Aware	Undetected	AhnLab-V3	Undetected
Alibaba	Undetected	ALYac	Undetected
Antiy-AVL	Undetected	Arcabit	Undetected

Packing

The malware is not packed.



PEiD v0.95

File: C:\Users\asdf\Desktop\Olympic Destroyer\3337e3875b05e0bfba69ab

Entrypoint: 00009DE6

EP Section: .text

File Offset: 000091E6

First Bytes: E8,15,77,00

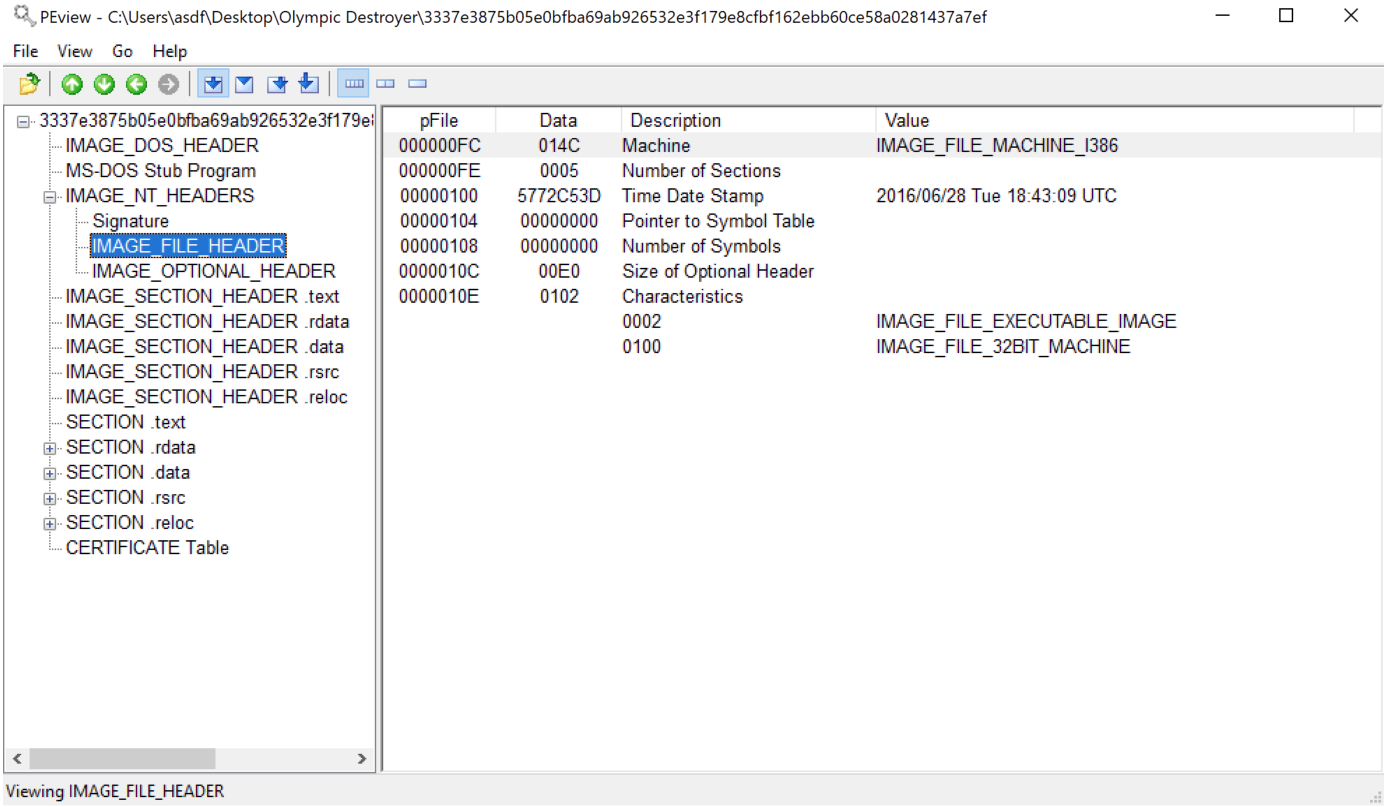
Linker Info: 12.0

Subsystem: Win32 console

Nothing found [Overlay] *

Compilation Date

The file was compiled on 2016/06/28 Tue 18:43:09 UTC



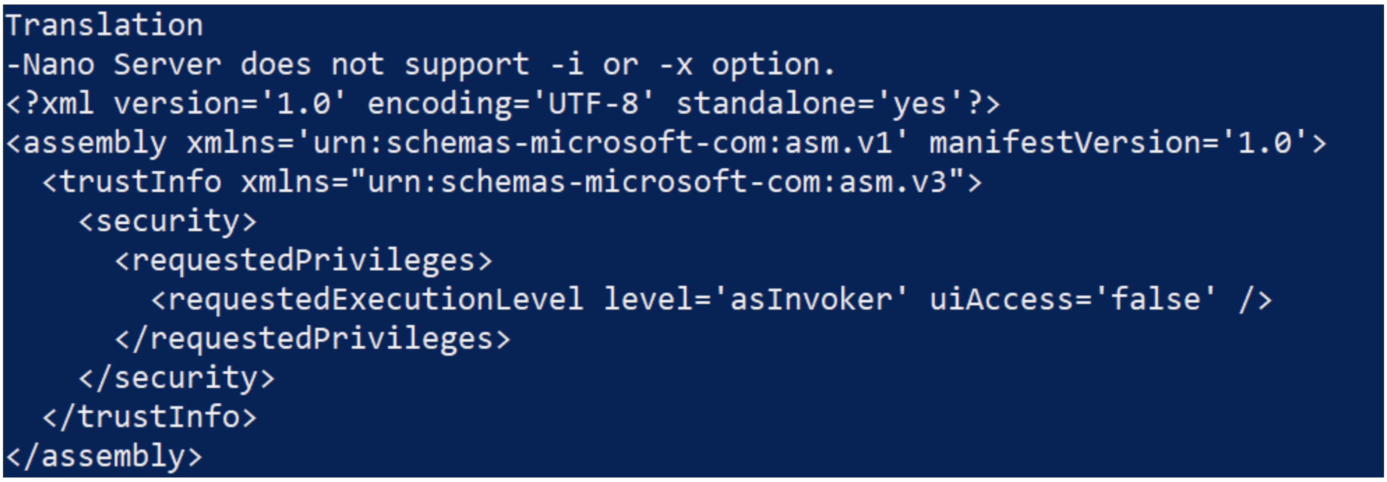
PEview - C:\Users\asdf\Desktop\Olympic Destroyer\3337e3875b05e0bfba69ab926532e3f179e8cfbf162ebb60ce58a0281437a7ef

```
3337e3875b05e0bfba69ab926532e3f179e8
  IMAGE_DOS_HEADER
  MS-DOS Stub Program
  IMAGE_NT_HEADERS
    Signature
    IMAGE_FILE_HEADER
    IMAGE_OPTIONAL_HEADER
  IMAGE_SECTION_HEADER .text
  IMAGE_SECTION_HEADER .rdata
  IMAGE_SECTION_HEADER .data
  IMAGE_SECTION_HEADER .rsrc
  IMAGE_SECTION_HEADER .reloc
  SECTION .text
  SECTION .rdata
  SECTION .data
  SECTION .rsrc
  SECTION .reloc
  CERTIFICATE Table
```

pFile	Data	Description	Value
000000FC	014C	Machine	IMAGE_FILE_MACHINE_I386
000000FE	0005	Number of Sections	
00000100	5772C53D	Time Date Stamp	2016/06/28 Tue 18:43:09 UTC
00000104	00000000	Pointer to Symbol Table	
00000108	00000000	Number of Symbols	
0000010C	00E0	Size of Optional Header	
0000010E	0102	Characteristics	
		0002	IMAGE_FILE_EXECUTABLE_IMAGE
		0100	IMAGE_FILE_32BIT_MACHINE

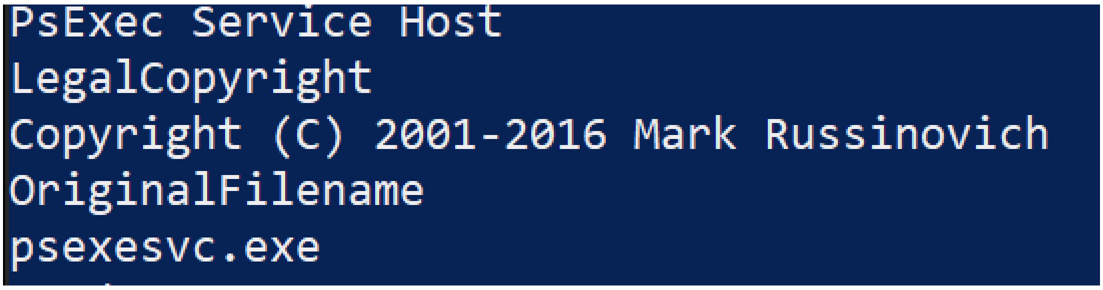
Viewing IMAGE_FILE_HEADER

Strings Analysis



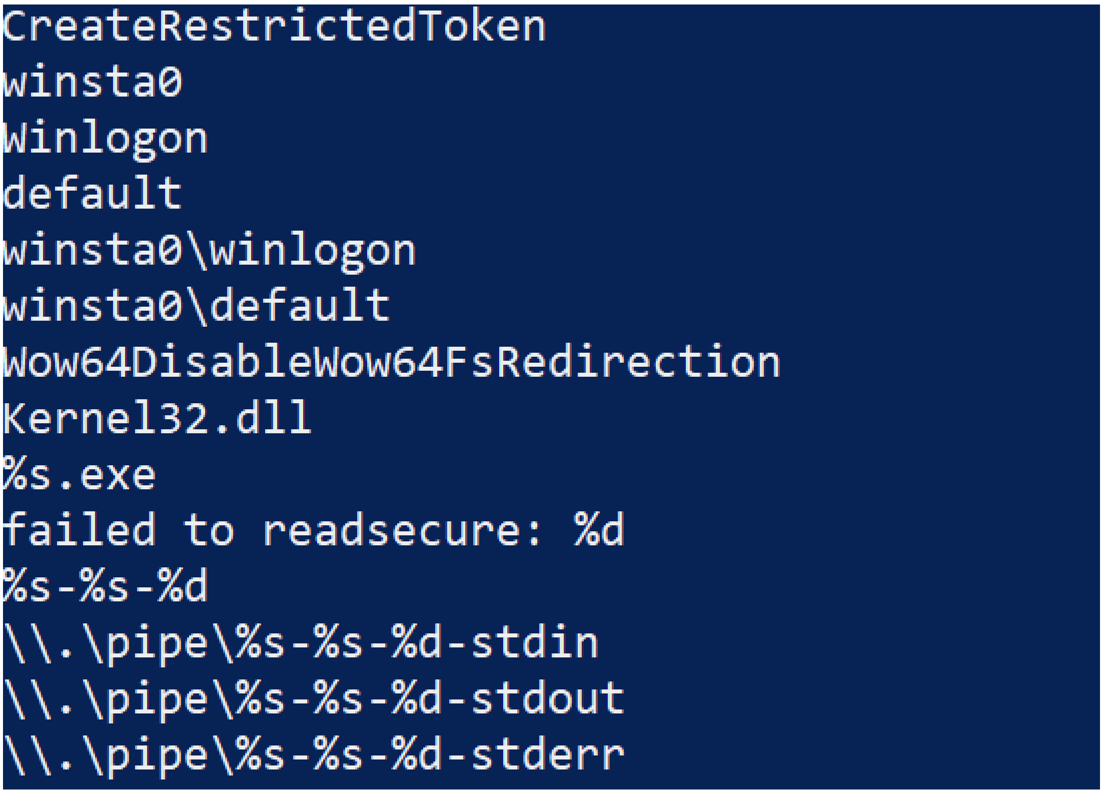
```
Translation
-Nano Server does not support -i or -x option.
<?xml version='1.0' encoding='UTF-8' standalone='yes'?>
<assembly xmlns='urn:schemas-microsoft-com:asm.v1' manifestVersion='1.0'>
  <trustInfo xmlns="urn:schemas-microsoft-com:asm.v3">
    <security>
      <requestedPrivileges>
        <requestedExecutionLevel level='asInvoker' uiAccess='false' />
      </requestedPrivileges>
    </security>
  </trustInfo>
</assembly>
```

Run as Invoker allows the malware to bypass administrator rights



```
PsExec Service Host
LegalCopyright
Copyright (C) 2001-2016 Mark Russinovich
OriginalFilename
psexesvc.exe
```

Runs the process psexesvc.exe

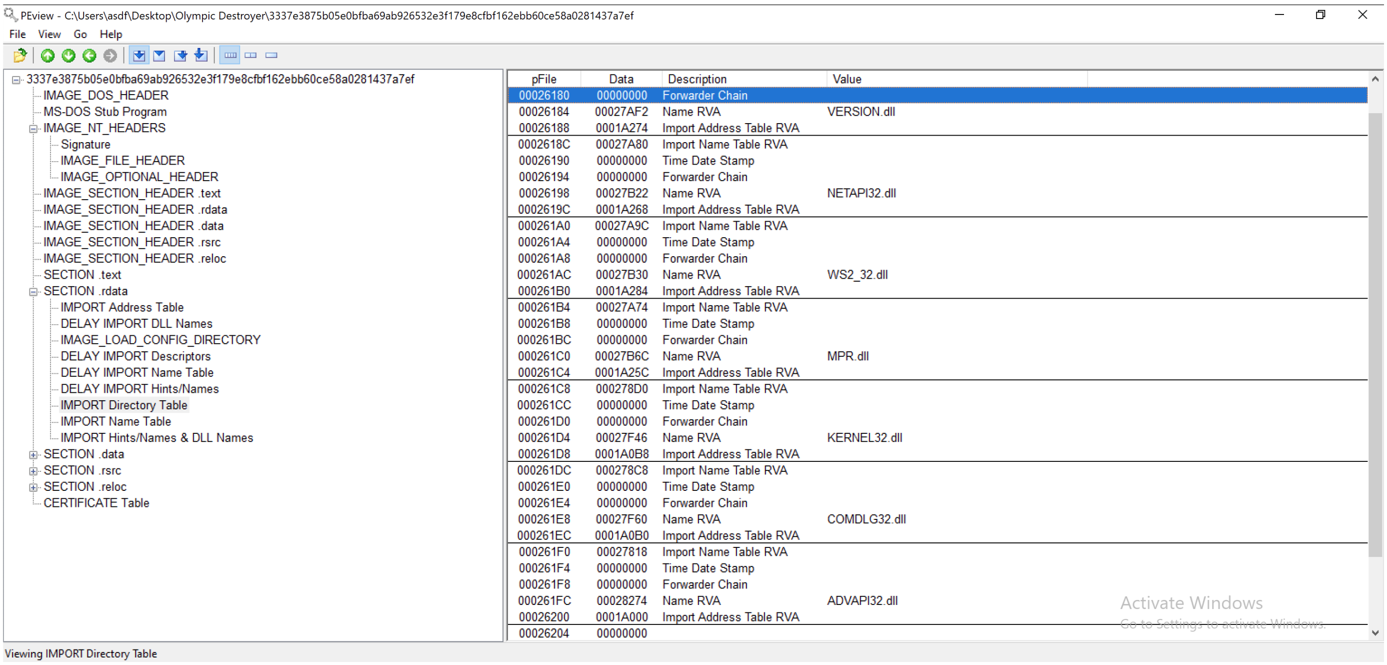


```
CreateRestrictedToken
winsta0
Winlogon
default
winsta0\winlogon
winsta0\default
Wow64DisableWow64FsRedirection
Kernel32.dll
%s.exe
failed to readsecure: %d
%s-%s-%d
\\.\pipe\%s-%s-%d-stdin
\\.\pipe\%s-%s-%d-stdout
\\.\pipe\%s-%s-%d-stderr
```

It probably creates pipe used to manipulate data coming in/out. read data from pipe. Malware has networking capability which allows a remote user to gain access to a shell. It seems to takes standard input from a remote servers and displays the output result to the remote server as well.

DLL Imports

It imports 7 DLL modules: VERSION.dll, NETAPI32.dll, WS2_32.dll, MPR.dll, KERNEL32.dll, COMDLG32.dll, ADVAPI32.dll



PEview - C:\Users\asdf\Desktop\Olympic Destroyer\3337e3875b05e0bfba69ab926532e3f179e8cfbf162ebb60ce58a0281437a7ef

```
3337e3875b05e0bfba69ab926532e3f179e8cfbf162ebb60ce58a0281437a7ef
    IMAGE_DOS_HEADER
    MS-DOS Stub Program
    IMAGE_NT_HEADERS
        Signature
        IMAGE_FILE_HEADER
        IMAGE_OPTIONAL_HEADER
    IMAGE_SECTION_HEADER .text
    IMAGE_SECTION_HEADER .rdata
    IMAGE_SECTION_HEADER .data
    IMAGE_SECTION_HEADER .rsrc
    IMAGE_SECTION_HEADER .reloc
    SECTION .text
    SECTION .rdata
        IMPORT Address Table
        DELAY IMPORT DLL Names
        IMAGE_LOAD_CONFIG_DIRECTORY
        DELAY IMPORT Descriptors
        DELAY IMPORT Name Table
        DELAY IMPORT Hints/Names
        IMPORT Directory Table
        IMPORT Name Table
        IMPORT Hints/Names & DLL Names
    SECTION .data
    SECTION .rsrc
    SECTION .reloc
    CERTIFICATE Table
```

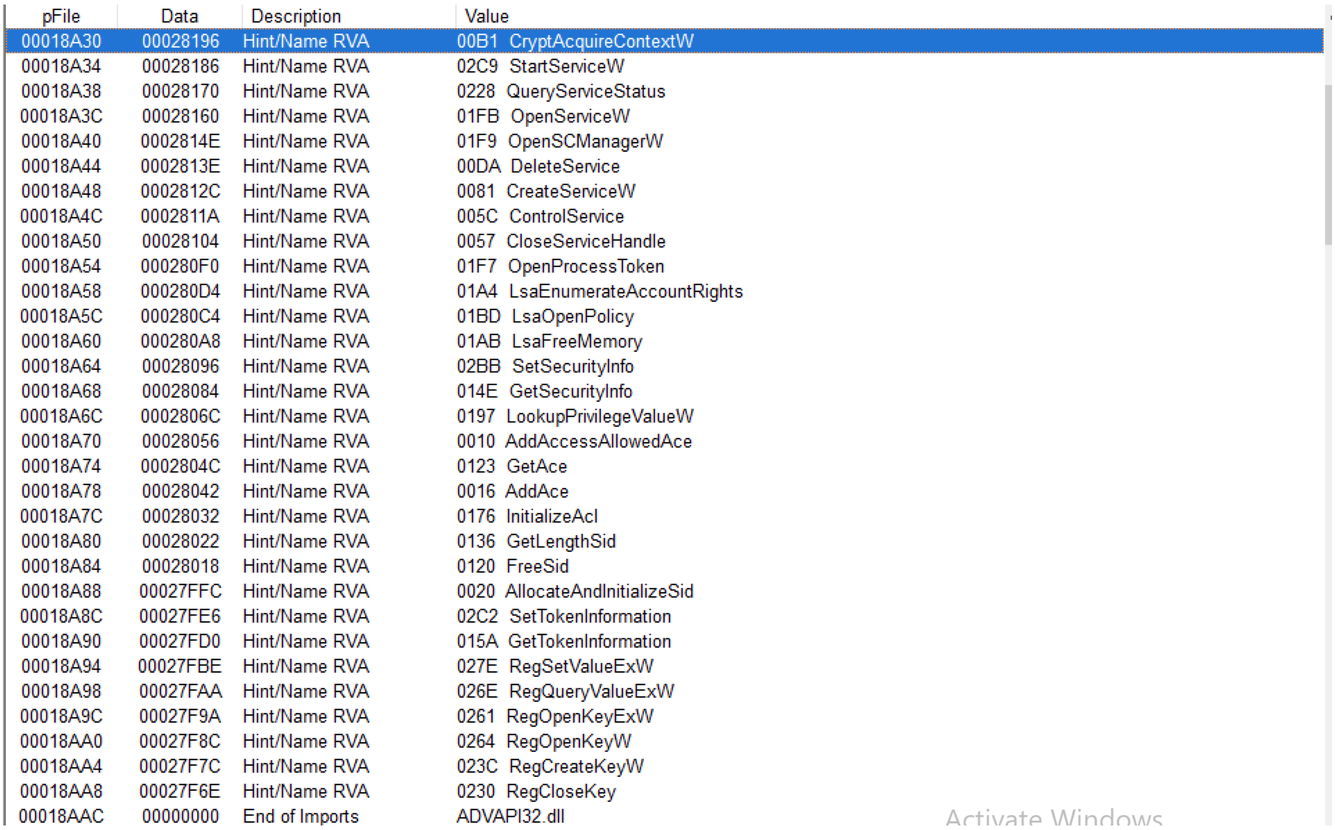
pFile	Data	Description	Value
00026180	00000000	Forwarder Chain	
00026184	00027AF2	Name RVA	VERSION.dll
00026188	0001A274	Import Address Table RVA	
0002618C	00027A80	Import Name Table RVA	
00026190	00000000	Time Date Stamp	
00026194	00000000	Forwarder Chain	
00026198	00027B22	Name RVA	NETAPI32.dll
0002619C	0001A268	Import Address Table RVA	
000261A0	00027A9C	Import Name Table RVA	
000261A4	00000000	Time Date Stamp	
000261A8	00000000	Forwarder Chain	
000261AC	00027B30	Name RVA	WS2_32.dll
000261B0	0001A284	Import Address Table RVA	
000261B4	00027A74	Import Name Table RVA	
000261B8	00000000	Time Date Stamp	
000261BC	00000000	Forwarder Chain	
000261C0	00027B6C	Name RVA	MPR.dll
000261C4	0001A25C	Import Address Table RVA	
000261C8	000278D0	Import Name Table RVA	
000261CC	00000000	Time Date Stamp	
000261D0	00000000	Forwarder Chain	
000261D4	00027F46	Name RVA	KERNEL32.dll
000261D8	0001A0B8	Import Address Table RVA	
000261DC	000278C8	Import Name Table RVA	
000261E0	00000000	Time Date Stamp	
000261E4	00000000	Forwarder Chain	
000261E8	00027F60	Name RVA	COMDLG32.dll
000261EC	0001A0B0	Import Address Table RVA	
000261F0	00027818	Import Name Table RVA	
000261F4	00000000	Time Date Stamp	
000261F8	00000000	Forwarder Chain	
000261FC	00028274	Name RVA	ADVAPI32.dll
00026200	0001A000	Import Address Table RVA	
00026204	00000000		

Viewing IMPORT Directory Table

ADVAPI32.dll is used to:

1. access service manager with import functions such as StartServiceW, CreateServiceW, ControlService etc...

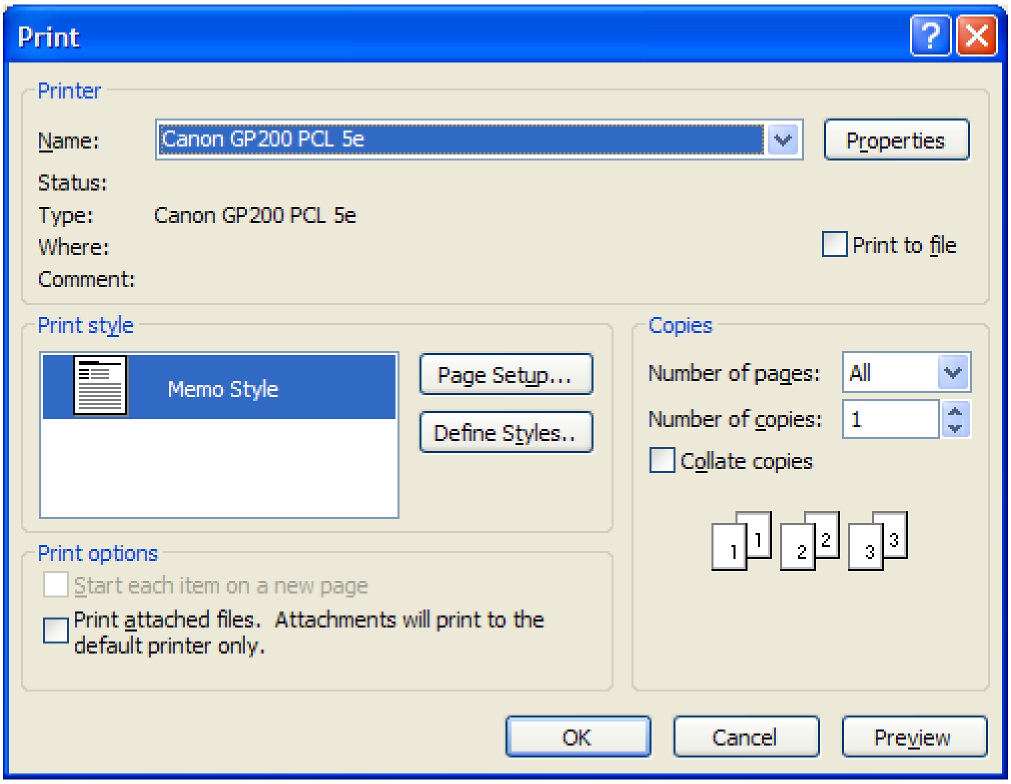
2. access registers with import functions such as RegSetValueExW, RegOpenKeyW, etc...



pFile	Data	Description	Value
00018A30	00028196	Hint/Name RVA	00B1 CryptAcquireContextW
00018A34	00028186	Hint/Name RVA	02C9 StartServiceW
00018A38	00028170	Hint/Name RVA	0228 QueryServiceStatus
00018A3C	00028160	Hint/Name RVA	01FB OpenServiceW
00018A40	0002814E	Hint/Name RVA	01F9 OpenSCManagerW
00018A44	0002813E	Hint/Name RVA	00DA DeleteService
00018A48	0002812C	Hint/Name RVA	0081 CreateServiceW
00018A4C	0002811A	Hint/Name RVA	005C ControlService
00018A50	00028104	Hint/Name RVA	0057 CloseServiceHandle
00018A54	000280F0	Hint/Name RVA	01F7 OpenProcessToken
00018A58	000280D4	Hint/Name RVA	01A4 LsaEnumerateAccountRights
00018A5C	000280C4	Hint/Name RVA	01BD LsaOpenPolicy
00018A60	000280A8	Hint/Name RVA	01AB LsaFreeMemory
00018A64	00028096	Hint/Name RVA	02BB SetSecurityInfo
00018A68	00028084	Hint/Name RVA	014E GetSecurityInfo
00018A6C	0002806C	Hint/Name RVA	0197 LookupPrivilegeValueW
00018A70	00028056	Hint/Name RVA	0010 AddAccessAllowedAce
00018A74	0002804C	Hint/Name RVA	0123 GetAce
00018A78	00028042	Hint/Name RVA	0016 AddAce
00018A7C	00028032	Hint/Name RVA	0176 InitializeAcl
00018A80	00028022	Hint/Name RVA	0136 GetLengthSid
00018A84	00028018	Hint/Name RVA	0120 FreeSid
00018A88	00027FFC	Hint/Name RVA	0020 AllocateAndInitializeSid
00018A8C	00027FE6	Hint/Name RVA	02C2 SetTokenInformation
00018A90	00027FD0	Hint/Name RVA	015A GetTokenInformation
00018A94	00027FBE	Hint/Name RVA	027E RegSetValueExW
00018A98	00027FAA	Hint/Name RVA	026E RegQueryValueExW
00018A9C	00027F9A	Hint/Name RVA	0261 RegOpenKeyExW
00018AA0	00027F8C	Hint/Name RVA	0264 RegOpenKeyW
00018AA4	00027F7C	Hint/Name RVA	023C RegCreateKeyW
00018AA8	00027F6E	Hint/Name RVA	0230 RegCloseKey
00018AAC	00000000	End of Imports	ADVAPI32.dll

COMDLG32.dll accesses one import function: PrintDlgW. Print Dialog Box is typically used to let the user select options for a particular print job.

For example:



Print

Printer

Name: Canon GP200 PCL 5e

Status:

Type: Canon GP200 PCL 5e

Where:

Comment:

□ Print to file

Print style

Memo Style

Copies

Number of pages: All

Number of copies: 1

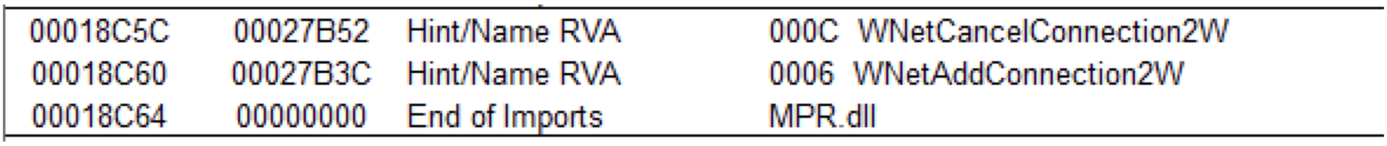
□ Collate copies

Print options

□ Start each item on a new page

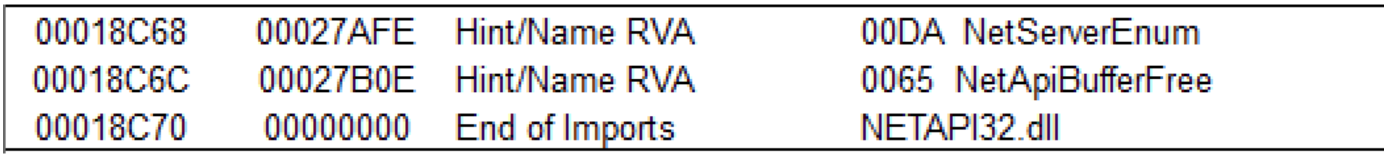
□ Print attached files. Attachments will print to the default printer only.

MPR.dll is used to handle the connection of the remote shell.



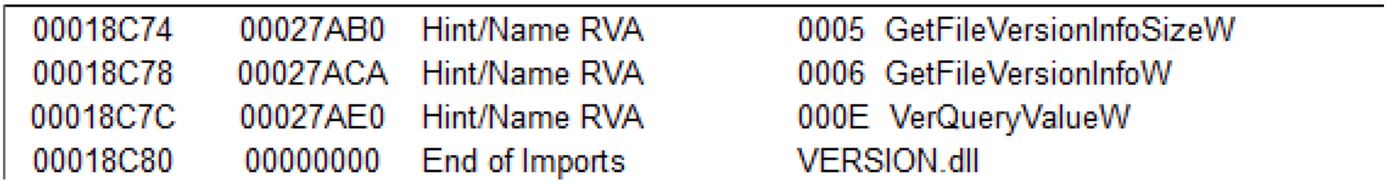
00018C5C	00027B52	Hint/Name RVA	000C WNetCancelConnection2W
00018C60	00027B3C	Hint/Name RVA	0006 WNetAddConnection2W
00018C64	00000000	End of Imports	MPR.dll

NETAPI32.dll is used to list all the servers that are visible to the domain. Possibly used to link to the remote attacker's machine.



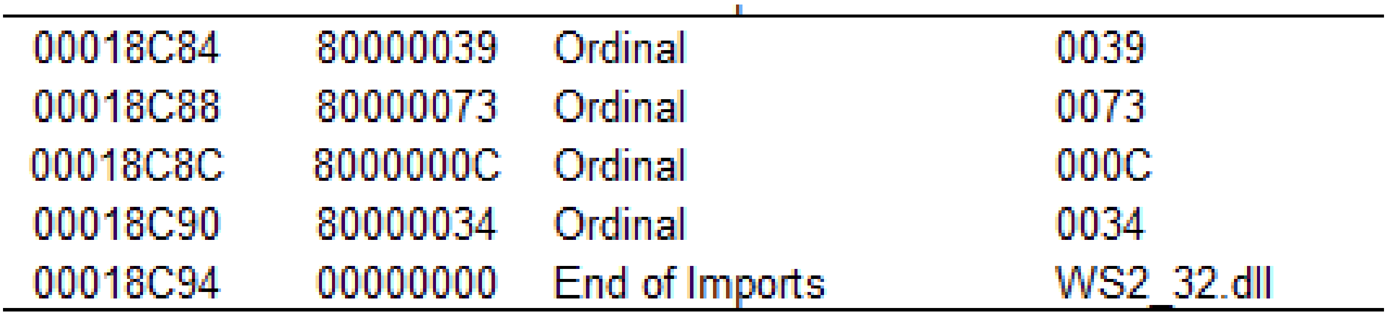
```
00018C68    00027AFE    Hint/Name RVA        00DA  NetServerEnum
00018C6C    00027B0E    Hint/Name RVA        0065  NetApiBufferFree
00018C70    00000000    End of Imports       NETAPI32.dll
```

VERSION.DLL is used to calibrate the correct version of the malicious file.



```
00018C74    00027AB0    Hint/Name RVA        0005  GetFileVersionInfoSizeW
00018C78    00027ACA    Hint/Name RVA        0006  GetFileVersionInfoW
00018C7C    00027AE0    Hint/Name RVA        000E  VerQueryValueW
00018C80    00000000    End of Imports       VERSION.dll
```

WS2_32.dll is the Windows Socket Library file used for application to work with the network. The malware uses this to create the pipe for the reverse shell.

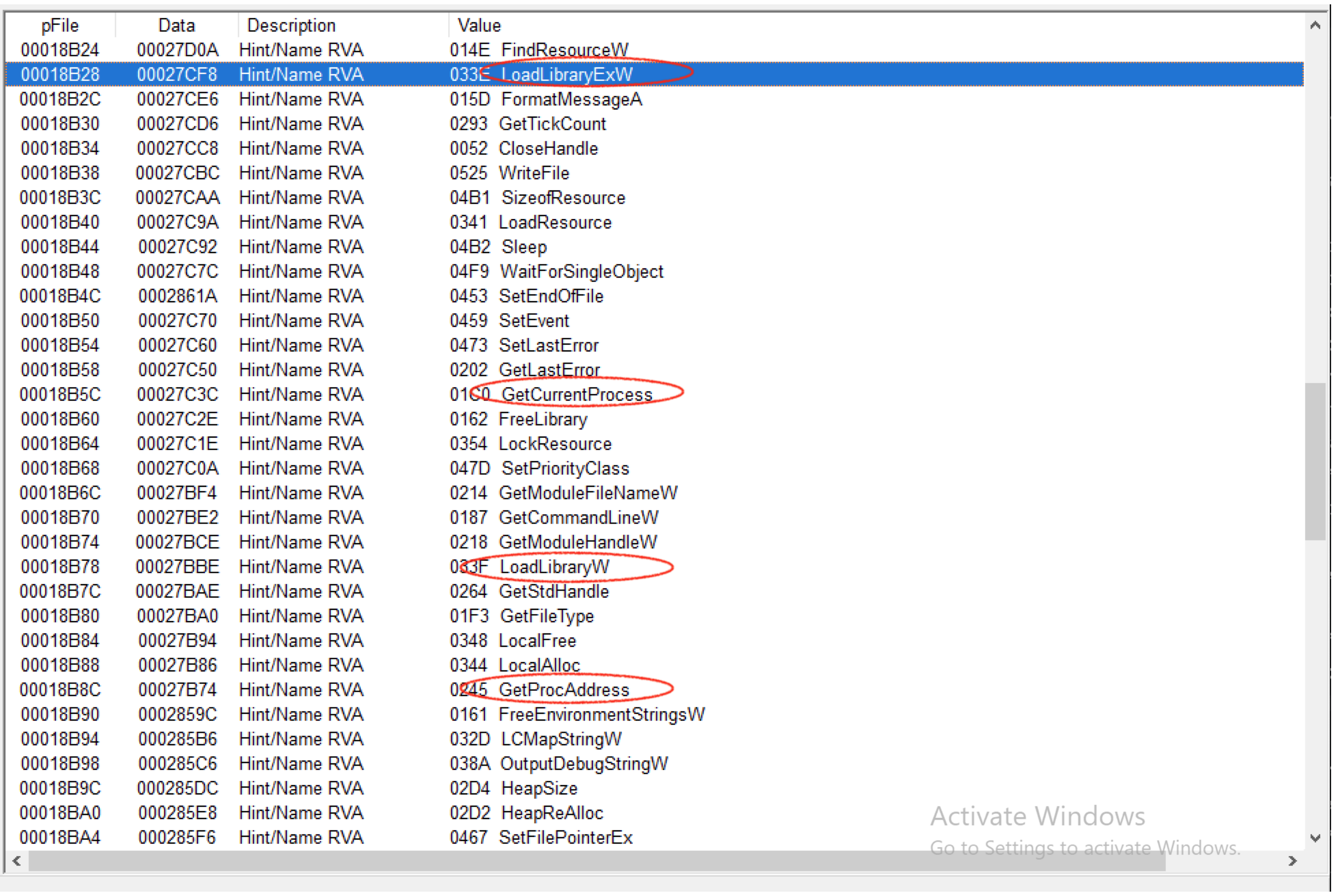


```
00018C84    80000039    Ordinal              0039
00018C88    80000073    Ordinal              0073
00018C8C    8000000C    Ordinal              000C
00018C90    80000034    Ordinal              0034
00018C94    00000000    End of Imports       WS2_32.dll
```

MOST IMPORTATNT: **KERNEL32.dll** is used to manipulate memory, file, and hardware.
Here the import functions shows some signs fo covert malware launching via DLL injection.

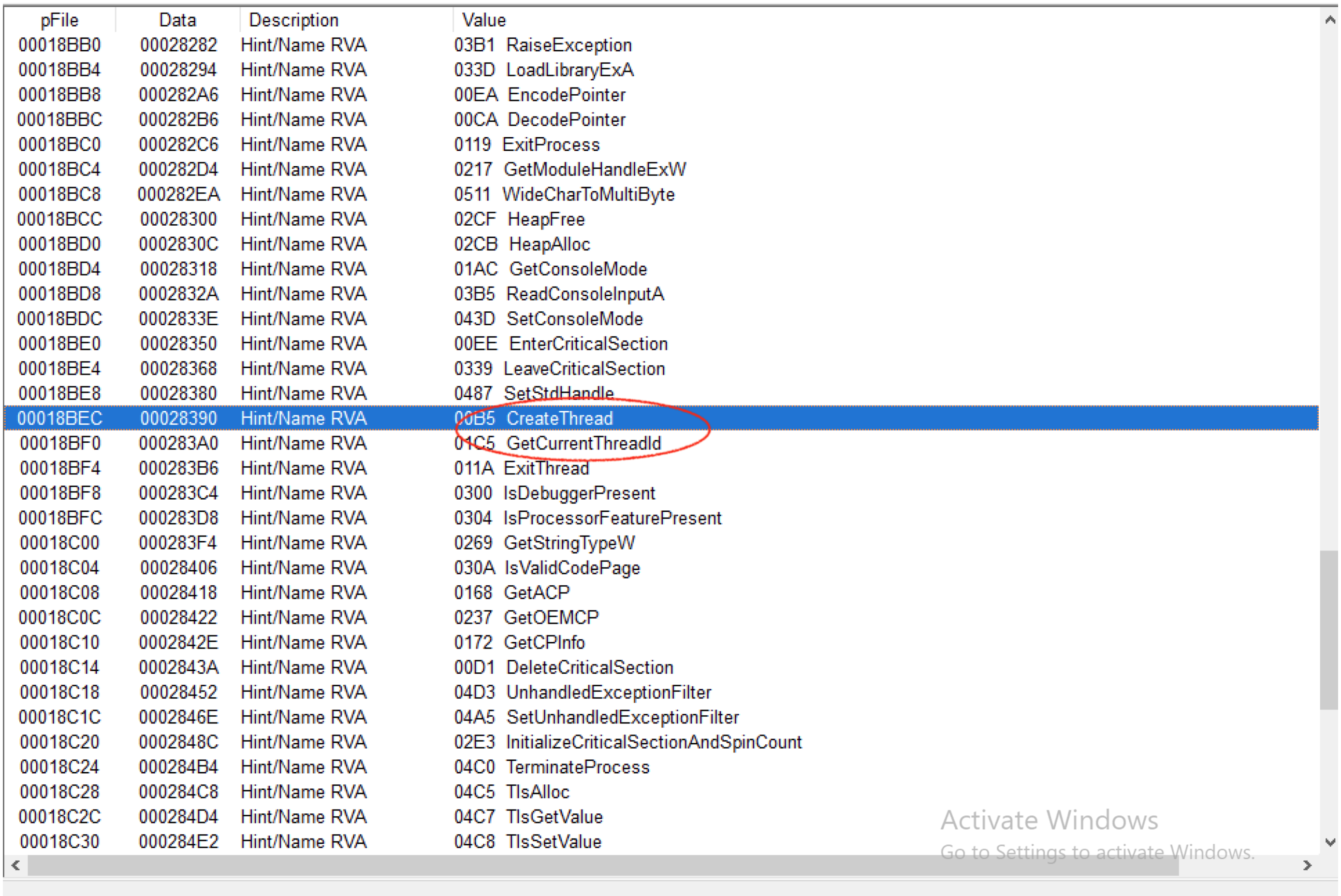
From the functions imported here we understand that this malware attempts to create a multithreaded reverse shell with sockets.
WindowAPI used:

1. Injecting code into a remote process
    1. **LoadLibrary**
2. obtain a handle to the victim process (search the process list for the injection target)
    1. **GetCurrentProcess**
    2. **GetProcAddress**



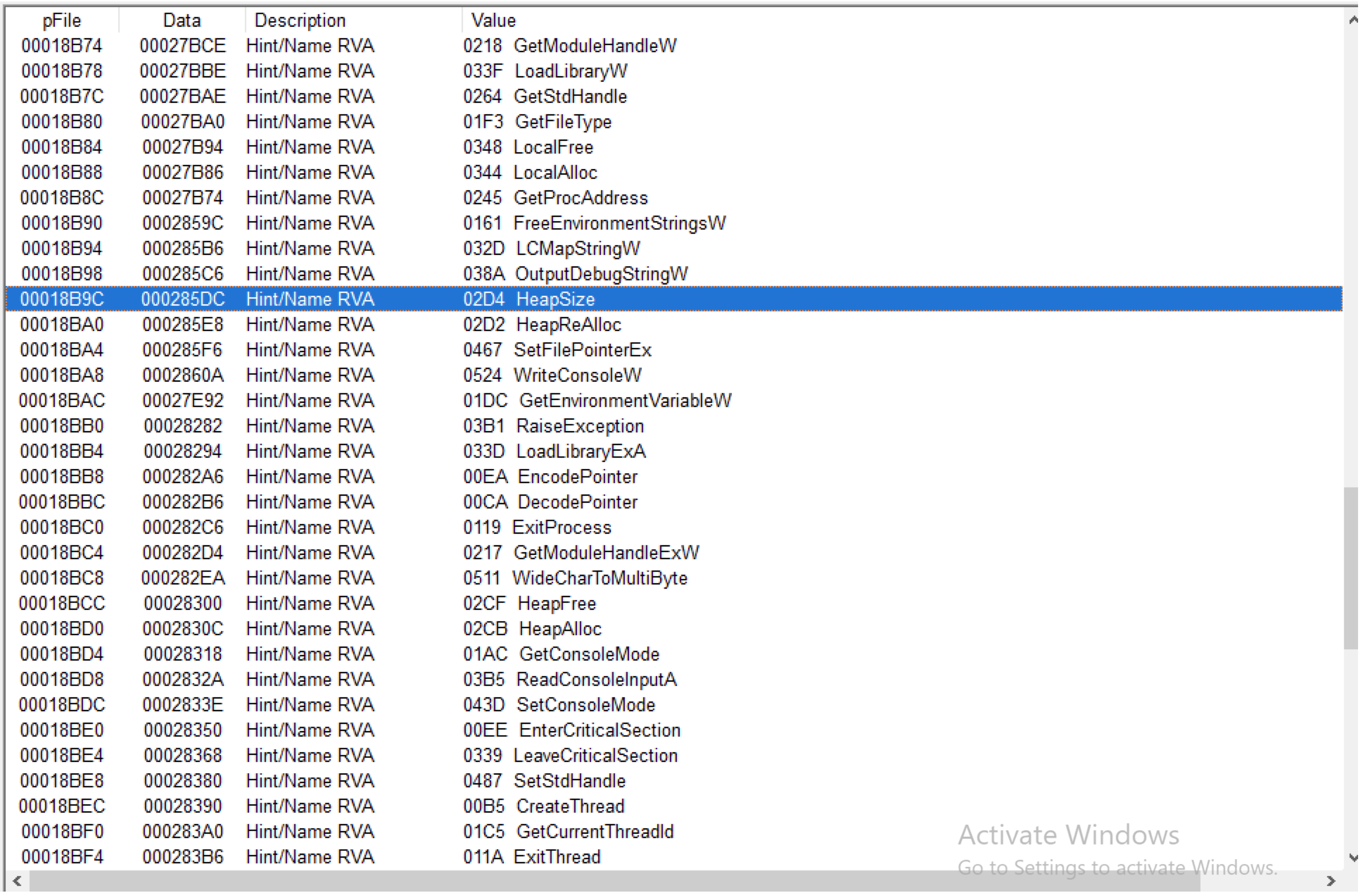
pFile	Data	Description	Value
00018B24	00027D0A	Hint/Name RVA	014E FindResourceW
00018B28	00027CF8	Hint/Name RVA	033E LoadLibraryExW
00018B2C	00027CE6	Hint/Name RVA	015D FormatMessageA
00018B30	00027CD6	Hint/Name RVA	0293 GetTickCount
00018B34	00027CC8	Hint/Name RVA	0052 CloseHandle
00018B38	00027CBC	Hint/Name RVA	0525 WriteFile
00018B3C	00027CAA	Hint/Name RVA	04B1 SizeofResource
00018B40	00027C9A	Hint/Name RVA	0341 LoadResource
00018B44	00027C92	Hint/Name RVA	04B2 Sleep
00018B48	00027C7C	Hint/Name RVA	04F9 WaitForSingleObject
00018B4C	0002861A	Hint/Name RVA	0453 SetEndOfFile
00018B50	00027C70	Hint/Name RVA	0459 SetEvent
00018B54	00027C60	Hint/Name RVA	0473 SetLastError
00018B58	00027C50	Hint/Name RVA	0202 GetLastError
00018B5C	00027C3C	Hint/Name RVA	01C0 GetCurrentProcess
00018B60	00027C2E	Hint/Name RVA	0162 FreeLibrary
00018B64	00027C1E	Hint/Name RVA	0354 LockResource
00018B68	00027C0A	Hint/Name RVA	047D SetPriorityClass
00018B6C	00027BF4	Hint/Name RVA	0214 GetModuleFileNameW
00018B70	00027BE2	Hint/Name RVA	0187 GetCommandLineW
00018B74	00027BCE	Hint/Name RVA	0218 GetModuleHandleW
00018B78	00027BBE	Hint/Name RVA	033F LoadLibraryW
00018B7C	00027BAE	Hint/Name RVA	0264 GetStdHandle
00018B80	00027BA0	Hint/Name RVA	01F3 GetFileType
00018B84	00027B94	Hint/Name RVA	0348 LocalFree
00018B88	00027B86	Hint/Name RVA	0344 LocalAlloc
00018B8C	00027B74	Hint/Name RVA	0245 GetProcAddress
00018B90	0002859C	Hint/Name RVA	0161 FreeEnvironmentStringsW
00018B94	000285B6	Hint/Name RVA	032D LCMapStringW
00018B98	000285C6	Hint/Name RVA	038A OutputDebugStringW
00018B9C	000285DC	Hint/Name RVA	02D4 HeapSize
00018BA0	000285E8	Hint/Name RVA	02D2 HeapReAlloc
00018BA4	000285F6	Hint/Name RVA	0467 SetFilePointerEx

4. launcher malware to create and execute a new thread in a process to create a pipe as indicated by analysis of strings.
    1. **CreateThread**
    2. **GetCurrentThreadId**



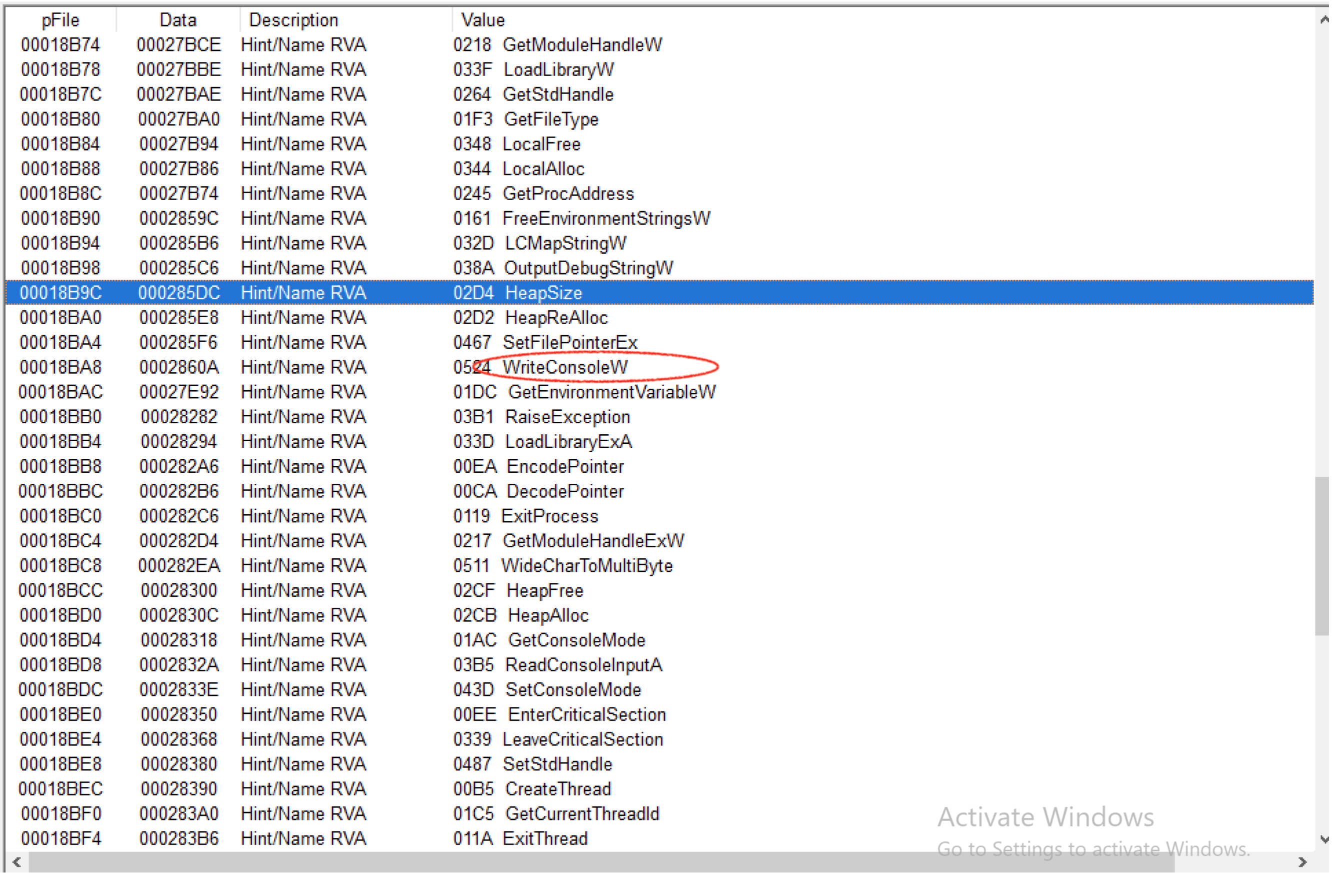
pFile	Data	Description	Value
00018BB0	00028282	Hint/Name RVA	03B1 RaiseException
00018BB4	00028294	Hint/Name RVA	033D LoadLibraryExA
00018BB8	000282A6	Hint/Name RVA	00EA EncodePointer
00018BBC	000282B6	Hint/Name RVA	00CA DecodePointer
00018BC0	000282C6	Hint/Name RVA	0119 ExitProcess
00018BC4	000282D4	Hint/Name RVA	0217 GetModuleHandleExW
00018BC8	000282EA	Hint/Name RVA	0511 WideCharToMultiByte
00018BCC	00028300	Hint/Name RVA	02CF HeapFree
00018BD0	0002830C	Hint/Name RVA	02CB HeapAlloc
00018BD4	00028318	Hint/Name RVA	01AC GetConsoleMode
00018BD8	0002832A	Hint/Name RVA	03B5 ReadConsoleInputA
00018BDC	0002833E	Hint/Name RVA	043D SetConsoleMode
00018BE0	00028350	Hint/Name RVA	00EE EnterCriticalSection
00018BE4	00028368	Hint/Name RVA	0339 LeaveCriticalSection
00018BE8	00028380	Hint/Name RVA	0487 SetStdHandle
00018BEC	00028390	Hint/Name RVA	00B5 CreateThread
00018BF0	000283A0	Hint/Name RVA	01C5 GetCurrentThreadId
00018BF4	000283B6	Hint/Name RVA	011A ExitThread
00018BF8	000283C4	Hint/Name RVA	0300 IsDebuggerPresent
00018BFC	000283D8	Hint/Name RVA	0304 IsProcessorFeaturePresent
00018C00	000283F4	Hint/Name RVA	0269 GetStringTypeW
00018C04	00028406	Hint/Name RVA	030A IsValidCodePage
00018C08	00028418	Hint/Name RVA	0168 GetACP
00018C0C	00028422	Hint/Name RVA	0237 GetOEMCP
00018C10	0002842E	Hint/Name RVA	0172 GetCPInfo
00018C14	0002843A	Hint/Name RVA	00D1 DeleteCriticalSection
00018C18	00028452	Hint/Name RVA	04D3 UnhandledExceptionFilter
00018C1C	0002846E	Hint/Name RVA	04A5 SetUnhandledExceptionFilter
00018C20	0002848C	Hint/Name RVA	02E3 InitializeCriticalSectionAndSpinCount
00018C24	000284B4	Hint/Name RVA	04C0 TerminateProcess
00018C28	000284C8	Hint/Name RVA	04C5 TlsAlloc
00018C2C	000284D4	Hint/Name RVA	04C7 TlsGetValue
00018C30	000284E2	Hint/Name RVA	04C8 TlsSetValue

5. create space for the malicious library name string
    1. **HeapSize**
    2. **HeapReAlloc**



pFile	Data	Description	Value
00018B74	00027BCE	Hint/Name RVA	0218 GetModuleHandleW
00018B78	00027BBE	Hint/Name RVA	033F LoadLibraryW
00018B7C	00027BAE	Hint/Name RVA	0264 GetStdHandle
00018B80	00027BA0	Hint/Name RVA	01F3 GetFileType
00018B84	00027B94	Hint/Name RVA	0348 LocalFree
00018B88	00027B86	Hint/Name RVA	0344 LocalAlloc
00018B8C	00027B74	Hint/Name RVA	0245 GetProcAddress
00018B90	0002859C	Hint/Name RVA	0161 FreeEnvironmentStringsW
00018B94	000285B6	Hint/Name RVA	032D LCMapStringW
00018B98	000285C6	Hint/Name RVA	038A OutputDebugStringW
00018B9C	000285DC	Hint/Name RVA	02D4 HeapSize
00018BA0	000285E8	Hint/Name RVA	02D2 HeapReAlloc
00018BA4	000285F6	Hint/Name RVA	0467 SetFilePointerEx
00018BA8	0002860A	Hint/Name RVA	0524 WriteConsoleW
00018BAC	00027E92	Hint/Name RVA	01DC GetEnvironmentVariableW
00018BB0	00028282	Hint/Name RVA	03B1 RaiseException
00018BB4	00028294	Hint/Name RVA	033D LoadLibraryExA
00018BB8	000282A6	Hint/Name RVA	00EA EncodePointer
00018BBC	000282B6	Hint/Name RVA	00CA DecodePointer
00018BC0	000282C6	Hint/Name RVA	0119 ExitProcess
00018BC4	000282D4	Hint/Name RVA	0217 GetModuleHandleExW
00018BC8	000282EA	Hint/Name RVA	0511 WideCharToMultiByte
00018BCC	00028300	Hint/Name RVA	02CF HeapFree
00018BD0	0002830C	Hint/Name RVA	02CB HeapAlloc
00018BD4	00028318	Hint/Name RVA	01AC GetConsoleMode
00018BD8	0002832A	Hint/Name RVA	03B5 ReadConsoleInputA
00018BDC	0002833E	Hint/Name RVA	043D SetConsoleMode
00018BE0	00028350	Hint/Name RVA	00EE EnterCriticalSection
00018BE4	00028368	Hint/Name RVA	0339 LeaveCriticalSection
00018BE8	00028380	Hint/Name RVA	0487 SetStdHandle
00018BEC	00028390	Hint/Name RVA	00B5 CreateThread
00018BF0	000283A0	Hint/Name RVA	01C5 GetCurrentThreadId
00018BF4	000283B6	Hint/Name RVA	011A ExitThread

6. Writes to a console and accomplishes reverse shell.

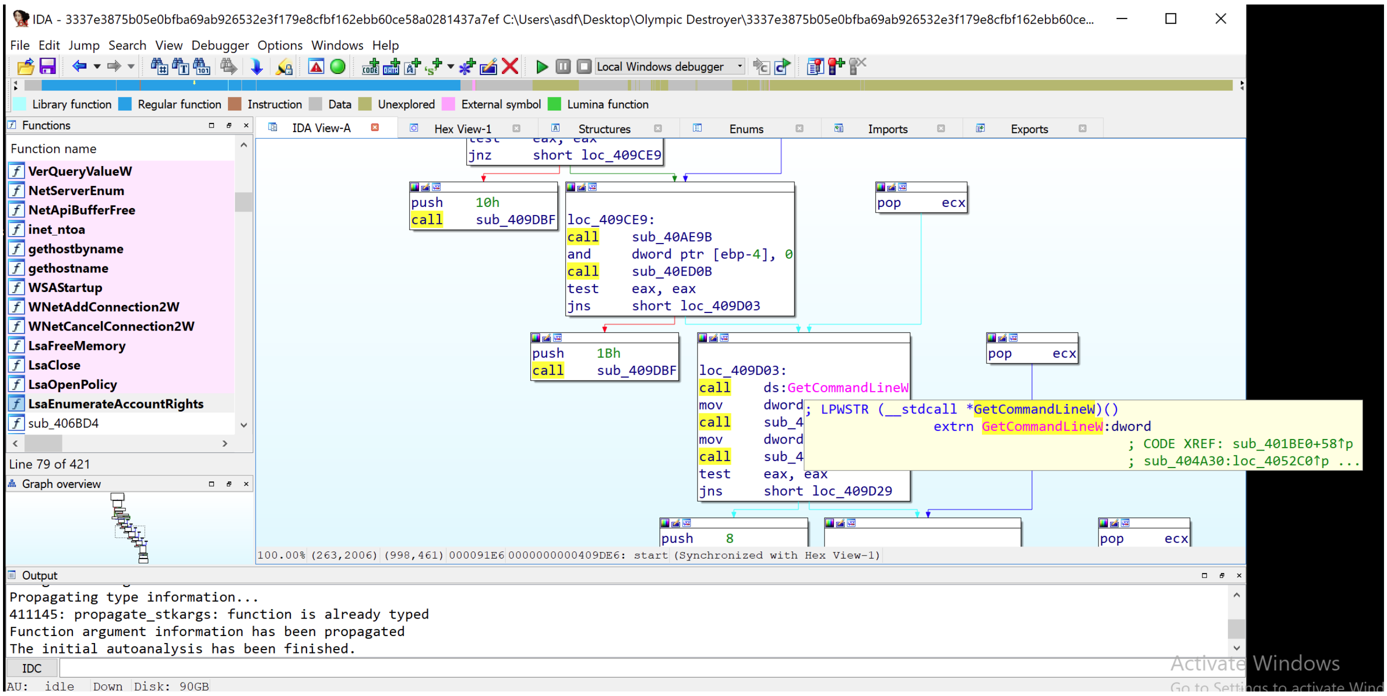


pFile	Data	Description	Value
00018B74	00027BCE	Hint/Name RVA	0218 GetModuleHandleW
00018B78	00027BBE	Hint/Name RVA	033F LoadLibraryW
00018B7C	00027BAE	Hint/Name RVA	0264 GetStdHandle
00018B80	00027BA0	Hint/Name RVA	01F3 GetFileType
00018B84	00027B94	Hint/Name RVA	0348 LocalFree
00018B88	00027B86	Hint/Name RVA	0344 LocalAlloc
00018B8C	00027B74	Hint/Name RVA	0245 GetProcAddress
00018B90	0002859C	Hint/Name RVA	0161 FreeEnvironmentStringsW
00018B94	000285B6	Hint/Name RVA	032D LCMapStringW
00018B98	000285C6	Hint/Name RVA	038A OutputDebugStringW
00018B9C	000285DC	Hint/Name RVA	02D4 HeapSize
00018BA0	000285E8	Hint/Name RVA	02D2 HeapReAlloc
00018BA4	000285F6	Hint/Name RVA	0467 SetFilePointerEx
00018BA8	0002860A	Hint/Name RVA	0524 WriteConsoleW
00018BAC	00027E92	Hint/Name RVA	01DC GetEnvironmentVariableW
00018BB0	00028282	Hint/Name RVA	03B1 RaiseException
00018BB4	00028294	Hint/Name RVA	033D LoadLibraryExA
00018BB8	000282A6	Hint/Name RVA	00EA EncodePointer
00018BBC	000282B6	Hint/Name RVA	00CA DecodePointer
00018BC0	000282C6	Hint/Name RVA	0119 ExitProcess
00018BC4	000282D4	Hint/Name RVA	0217 GetModuleHandleExW
00018BC8	000282EA	Hint/Name RVA	0511 WideCharToMultiByte
00018BCC	00028300	Hint/Name RVA	02CF HeapFree
00018BD0	0002830C	Hint/Name RVA	02CB HeapAlloc
00018BD4	00028318	Hint/Name RVA	01AC GetConsoleMode
00018BD8	0002832A	Hint/Name RVA	03B5 ReadConsoleInputA
00018BDC	0002833E	Hint/Name RVA	043D SetConsoleMode
00018BE0	00028350	Hint/Name RVA	00EE EnterCriticalSection
00018BE4	00028368	Hint/Name RVA	0339 LeaveCriticalSection
00018BE8	00028380	Hint/Name RVA	0487 SetStdHandle
00018BEC	00028390	Hint/Name RVA	00B5 CreateThread
00018BF0	000283A0	Hint/Name RVA	01C5 GetCurrentThreadId
00018BF4	000283B6	Hint/Name RVA	011A ExitThread

Activate Windows
Go to Settings to activate Windows.

IDA Pro

Calls GetCommandLineWindow, therefore confirms that it creates a reverse shell.



IDA - 3337e3875b05e0bfba69ab926532e3f179e8cfbf162ebb60ce58a0281437a7ef C:\Users\asdf\Desktop\Olympic Destroyer\3337e3875b05e0bfba69ab926532e3f179e8cfbf162ebb60ce...

VerQueryValueW
NetServerEnum
NetApiBufferFree
inet_ntoa
gethostbyname
gethostname
WSAStartup
WNetAddConnection2W
WNetCancelConnection2W
LsaFreeMemory
LsaClose
LsaOpenPolicy
LsaEnumerateAccountRights
sub_406BD4

Line 79 of 421

```
test    eax, eax
jnz     short loc_409CE9

push    10h
call    sub_409DBF

loc_409CE9:
call    sub_40AE9B
and     dword ptr [ebp-4], 0
call    sub_40ED0B
test    eax, eax
jns     short loc_409D03

pop     ecx

push    1Bh
call    sub_409DBF

loc_409D03:
call    ds:GetCommandLineW
mov     dword
call    sub_4
mov     dword
call    sub_4
test    eax, eax
jns     short loc_409D29

pop     ecx

push    8

pop     ecx
```

```
; LPWSTR (__stdcall *GetCommandLineW)()
                extrn GetCommandLineW:dword
                                        ; CODE XREF: sub_401BE0+58↑p
                                        ; sub_404A30:loc_4052C0↑p ...
```

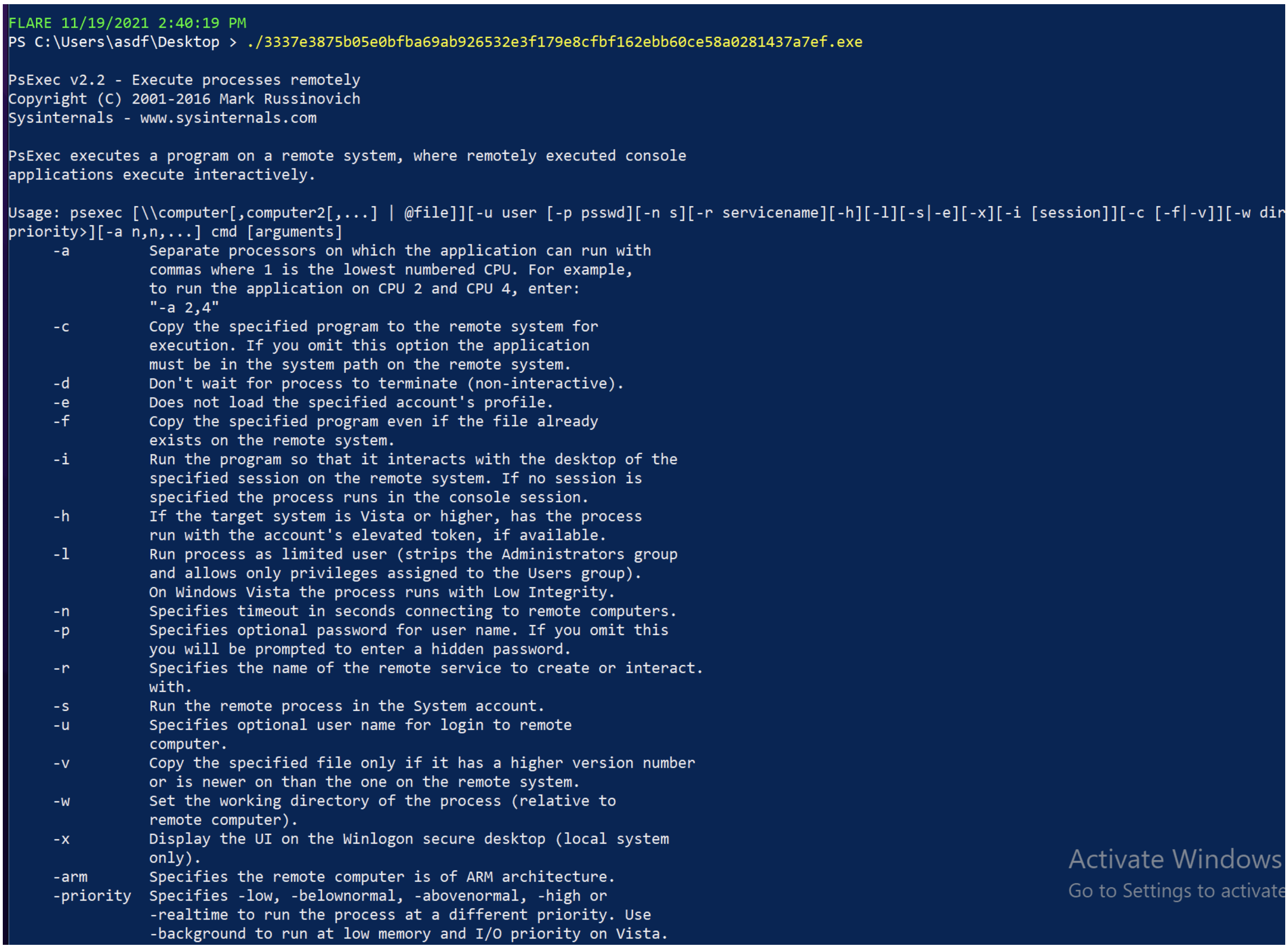
```
100.00% (263,2006) (998,461) 000091E6 0000000000409DE6: start (Synchronized with Hex View-1)
```

```
Propagating type information...
411145: propagate_stkargs: function is already typed
Function argument information has been propagated
The initial autoanalysis has been finished.
```

```
AU:  idle   Down  Disk: 90GB
```

Activate Windows
Go to Settings to activate Wind

Interesting Screenshot from running the executable file

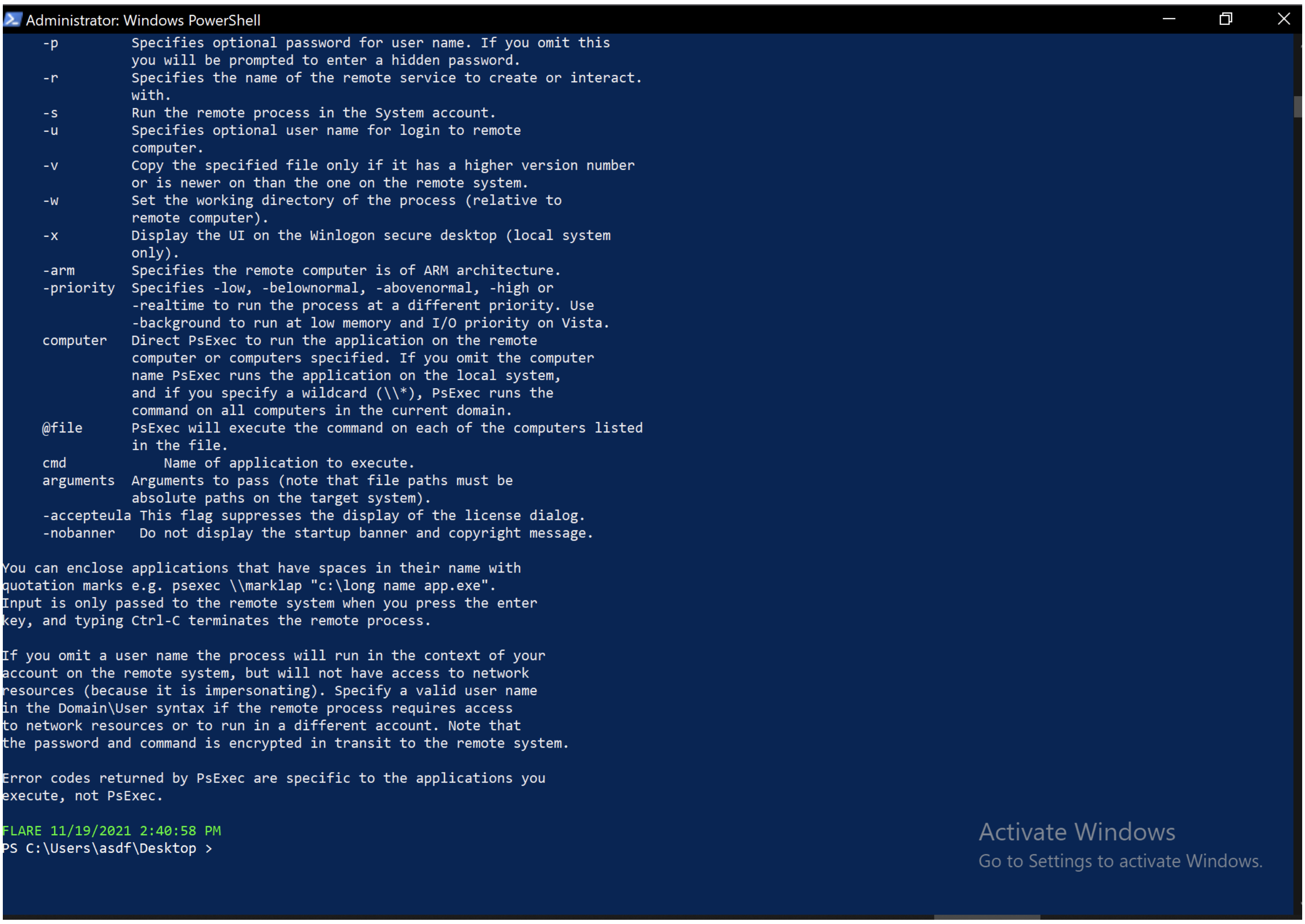


```
FLARE 11/19/2021 2:40:19 PM
PS C:\Users\asdf\Desktop > ./3337e3875b05e0bfba69ab926532e3f179e8cfbf162ebb60ce58a0281437a7ef.exe

PsExec v2.2 - Execute processes remotely
Copyright (C) 2001-2016 Mark Russinovich
Sysinternals - www.sysinternals.com

PsExec executes a program on a remote system, where remotely executed console
applications execute interactively.

Usage: psexec [\\computer[,computer2[,...] | @file]][-u user [-p psswd][-n s][-r servicename][-h][-l][-s|-e][-x][-i [session]][-c [-f|-v]][-w dir
priority>][-a n,n,...] cmd [arguments]
     -a         Separate processors on which the application can run with
                commas where 1 is the lowest numbered CPU. For example,
                to run the application on CPU 2 and CPU 4, enter:
                "-a 2,4"
     -c         Copy the specified program to the remote system for
                execution. If you omit this option the application
                must be in the system path on the remote system.
     -d         Don't wait for process to terminate (non-interactive).
     -e         Does not load the specified account's profile.
     -f         Copy the specified program even if the file already
                exists on the remote system.
     -i         Run the program so that it interacts with the desktop of the
                specified session on the remote system. If no session is
                specified the process runs in the console session.
     -h         If the target system is Vista or higher, has the process
                run with the account's elevated token, if available.
     -l         Run process as limited user (strips the Administrators group
                and allows only privileges assigned to the Users group).
                On Windows Vista the process runs with Low Integrity.
     -n         Specifies timeout in seconds connecting to remote computers.
     -p         Specifies optional password for user name. If you omit this
                you will be prompted to enter a hidden password.
     -r         Specifies the name of the remote service to create or interact.
                with.
     -s         Run the remote process in the System account.
     -u         Specifies optional user name for login to remote
                computer.
     -v         Copy the specified file only if it has a higher version number
                or is newer on than the one on the remote system.
     -w         Set the working directory of the process (relative to
                remote computer).
     -x         Display the UI on the Winlogon secure desktop (local system
                only).
     -arm       Specifies the remote computer is of ARM architecture.
     -priority  Specifies -low, -belownormal, -abovenormal, -high or
                -realtime to run the process at a different priority. Use
                -background to run at low memory and I/O priority on Vista.
```



```
     -p         Specifies optional password for user name. If you omit this
                you will be prompted to enter a hidden password.
     -r         Specifies the name of the remote service to create or interact.
                with.
     -s         Run the remote process in the System account.
     -u         Specifies optional user name for login to remote
                computer.
     -v         Copy the specified file only if it has a higher version number
                or is newer on than the one on the remote system.
     -w         Set the working directory of the process (relative to
                remote computer).
     -x         Display the UI on the Winlogon secure desktop (local system
                only).
     -arm       Specifies the remote computer is of ARM architecture.
     -priority  Specifies -low, -belownormal, -abovenormal, -high or
                -realtime to run the process at a different priority. Use
                -background to run at low memory and I/O priority on Vista.
     computer   Direct PsExec to run the application on the remote
                computer or computers specified. If you omit the computer
                name PsExec runs the application on the local system,
                and if you specify a wildcard (\\*), PsExec runs the
                command on all computers in the current domain.
     @file      PsExec will execute the command on each of the computers listed
                in the file.
     cmd            Name of application to execute.
     arguments  Arguments to pass (note that file paths must be
                absolute paths on the target system).
     -accepteula This flag suppresses the display of the license dialog.
     -nobanner   Do not display the startup banner and copyright message.

You can enclose applications that have spaces in their name with
quotation marks e.g. psexec \\marklap "c:\long name app.exe".
Input is only passed to the remote system when you press the enter
key, and typing Ctrl-C terminates the remote process.

If you omit a user name the process will run in the context of your
account on the remote system, but will not have access to network
resources (because it is impersonating). Specify a valid user name
in the Domain\User syntax if the remote process requires access
to network resources or to run in a different account. Note that
the password and command is encrypted in transit to the remote system.

Error codes returned by PsExec are specific to the applications you
execute, not PsExec.

FLARE 11/19/2021 2:40:58 PM
PS C:\Users\asdf\Desktop >
```

It seems like it is a program that helps execute processes remotely as suspected. There is instructions on how to use the psexec file.