

a.) Vizsgálja meg, hogy a neptunkod.exe milyen API hívásokat használ a kernel32.dll-ből (Win alrendszer DLL)!

Dependencies (x64)

File View Options Help

hzs05v

G:\EGYETEM\2021-22-2\OS\HZS05V09Gy
 C:\Windows\SysWOW64\kernel32.dll
 C:\Windows\SysWOW64\MSVCRT.dll

PI	Ordinal	Hint	Function	Module
		N/A	207 (0x00cf) DeleteCriticalSection	C:\Windows\SysWOW64\kernel32.dll
		N/A	236 (0x00ec) EnterCriticalSection	C:\Windows\SysWOW64\kernel32.dll
		N/A	279 (0x0117) ExitProcess	C:\Windows\SysWOW64\kernel32.dll
		N/A	510 (0x01fe) GetLastError	C:\Windows\SysWOW64\kernel32.dll
		N/A	529 (0x0211) GetModuleHandleA	C:\Windows\SysWOW64\kernel32.dll
		N/A	577 (0x0241) GetProcAddress	C:\Windows\SysWOW64\kernel32.dll
		N/A	734 (0x02de) InitializeCriticalSection	C:\Windows\SysWOW64\kernel32.dll
		N/A	814 (0x032e) LeaveCriticalSection	C:\Windows\SysWOW64\kernel32.dll
		N/A	1140 (0x0474) SetUnhandledExceptionFilter	C:\Windows\SysWOW64\kernel32.dll
		N/A	1173 (0x0495) TlsGetValue	C:\Windows\SysWOW64\kernel32.dll
		N/A	1213 (0x04bd) VirtualProtect	C:\Windows\SysWOW64\kernel32.dll
		N/A	1215 (0x04bf) VirtualQuery	C:\Windows\SysWOW64\kernel32.dll

E	Ordinal	Hint	Function	VirtualAddress	Demand
	1 (0x0001)		N/A BaseThreadInitThunk	0x0001fa10	None
	2 (0x0002)		N/A InterlockedPushListSList	NTDLL.RtlInterlockedPushListSList	None
	3 (0x0003)		N/A Wow64Transition	0x00082034	None
	4 (0x0004)		N/A AcquireSRWLockExclusive	NTDLL.RtlAcquireSRWLockExclusive	None
	5 (0x0005)		N/A AcquireSRWLockShared	NTDLL.RtlAcquireSRWLockShared	None
	6 (0x0006)		N/A ActivateActCtx	0x00020ac0	None
	7 (0x0007)		N/A ActivateActCtxWorker	0x00020400	None
	8 (0x0008)		N/A AddAtomA	0x000195a0	None
	9 (0x0009)		N/A AddAtomW	0x0001b8d0	None
	10 (0x000a)		N/A AddConsoleAliasA	0x00023c10	None
	11 (0x000b)		N/A AddConsoleAliasW	0x00023c20	None
	12 (0x000c)		N/A AddDllDirectory	api-ms-win-core-libraryloader-l1-	None
	13 (0x000d)		N/A AddIntegrityLabelToBoundaryDescri	0x00035fc0	None
	14 (0x000e)		N/A AddLocalAlternateComputerNameA	0x00052e00	None
	15 (0x000f)		N/A AddLocalAlternateComputerNameW	0x00052e60	None

b.) Keresse meg NTDLL.DLL-t! Mi ennek a szerepe? Vizsgálja meg az exportált függvényeket, milyen információkat kap az NT API-ról! „

Dependencies (x64)

File View Options Help

hzs05v

G:\EGYETEM\2021-22-2\OS\HZS05V0sGyak\...

C:\Windows\SysWOW64\kernel32.dll

api-ms-win-core-rtlsupport-l1-1-0.dll

api-ms-win-core-rtlsupport-l1-2-0.dll

C:\Windows\SysWOW64\ntdll.dll

C:\Windows\SysWOW64\kernelbase.dll

api-ms-win-core-processthreads-l1-1-0.dll

api-ms-win-core-processthreads-l1-2-0.dll

api-ms-win-core-registry-l1-1-0.dll

api-ms-win-core-heap-l1-1-0.dll

api-ms-win-core-heap-l2-1-0.dll

api-ms-win-core-memory-l1-1-1.dll

api-ms-win-core-memory-l1-1-0.dll

api-ms-win-core-memory-l1-1-2.dll

api-ms-win-core-handle-l1-1-0.dll

api-ms-win-core-synch-l1-1-0.dll

api-ms-win-core-synch-l1-2-1.dll

api-ms-win-core-synch-l1-2-0.dll

api-ms-win-core-file-l1-1-0.dll

api-ms-win-core-file-l1-2-0.dll

api-ms-win-core-file-l1-2-1.dll

api-ms-win-core-delayload-l1-1-0.dll

api-ms-win-core-io-l1-1-0.dll

api-ms-win-core-io-l1-1-1.dll

api-ms-win-core-job-l1-1-0.dll

api-ms-win-core-threadpool-legacy-l1-1-0.dll

api-ms-win-core-threadpool-private-l1-1-0.dll

api-ms-win-core-libraryloader-l1-1-0.dll

api-ms-win-core-libraryloader-l1-2-0.dll

api-ms-win-core-libraryloader-l1-2-1.dll

api-ms-win-core-namedpipe-l1-1-0.dll

api-ms-win-core-namedpipe-l1-2-0.dll

api-ms-win-core-datetime-l1-1-0.dll

api-ms-win-core-datetime-l1-1-1.dll

api-ms-win-core-datetime-l1-1-2.dll

api-ms-win-core-sysinfo-l1-2-0.dll

Ordinal	Hint	Function	Module
206 (0x00ce)		N/A NtMmOemCodePageTag	C:\Windows\SysWOW64\ntdll.dll
207 (0x00cf)		N/A NtAcceptConnectPort	C:\Windows\SysWOW64\ntdll.dll
208 (0x00d0)		N/A NtAccessCheck	C:\Windows\SysWOW64\ntdll.dll
209 (0x00d1)		N/A NtAccessCheckAndAuditAlarm	C:\Windows\SysWOW64\ntdll.dll
210 (0x00d2)		N/A NtAccessCheckByType	C:\Windows\SysWOW64\ntdll.dll
211 (0x00d3)		N/A NtAccessCheckByTypeAndAuditAlarm	C:\Windows\SysWOW64\ntdll.dll
212 (0x00d4)		N/A NtAccessCheckByTypeAndPolicyCheck	C:\Windows\SysWOW64\ntdll.dll
213 (0x00d5)		N/A NtAccessCheckByTypePolicyCheck	C:\Windows\SysWOW64\ntdll.dll
214 (0x00d6)		N/A NtAccessCheckByTypeResult	C:\Windows\SysWOW64\ntdll.dll
215 (0x00d7)		N/A NtAcquireCrossVmMutant	C:\Windows\SysWOW64\ntdll.dll
216 (0x00d8)		N/A NtAcquireProcessAct	C:\Windows\SysWOW64\ntdll.dll
217 (0x00d9)		N/A NtAddAtom	C:\Windows\SysWOW64\ntdll.dll
218 (0x00da)		N/A NtAddAtomEx	C:\Windows\SysWOW64\ntdll.dll
219 (0x00db)		N/A NtAddBootEntry	C:\Windows\SysWOW64\ntdll.dll
220 (0x00dc)		N/A NtAddDriverEntry	C:\Windows\SysWOW64\ntdll.dll
221 (0x00dd)		N/A NtAdjustGroupsToken	C:\Windows\SysWOW64\ntdll.dll
222 (0x00de)		N/A NtAdjustPrivilegesToken	C:\Windows\SysWOW64\ntdll.dll
223 (0x00df)		N/A NtAdjustTokenClaims	C:\Windows\SysWOW64\ntdll.dll
224 (0x00e0)		N/A NtAlertResumeThread	C:\Windows\SysWOW64\ntdll.dll
225 (0x00e1)		N/A NtAlertThread	C:\Windows\SysWOW64\ntdll.dll
226 (0x00e2)		N/A NtAlertThreadByThreadId	C:\Windows\SysWOW64\ntdll.dll
227 (0x00e3)		N/A NtAllocateLocallyUniqueId	C:\Windows\SysWOW64\ntdll.dll
228 (0x00e4)		N/A NtAllocateReserveObject	C:\Windows\SysWOW64\ntdll.dll
229 (0x00e5)		N/A NtAllocateUserPhysicalPages	C:\Windows\SysWOW64\ntdll.dll
230 (0x00e6)		N/A NtAllocateUserPhysicalPagesEx	C:\Windows\SysWOW64\ntdll.dll
231 (0x00e7)		N/A NtAllocateUuids	C:\Windows\SysWOW64\ntdll.dll
232 (0x00e8)		N/A NtAllocateVirtualMemory	C:\Windows\SysWOW64\ntdll.dll
233 (0x00e9)		N/A NtAllocateVirtualMemoryEx	C:\Windows\SysWOW64\ntdll.dll
234 (0x00ea)		N/A NtAlpcAcceptConnectPort	C:\Windows\SysWOW64\ntdll.dll
235 (0x00eb)		N/A NtAlpcCancelMessage	C:\Windows\SysWOW64\ntdll.dll
236 (0x00ec)		N/A NtAlpcConnectPort	C:\Windows\SysWOW64\ntdll.dll

VirtualAddress: 0x00126918

C:\Windows\SysWOW64\ntdll.dll Properties

General Exports Load config

File

NT Layer DLL

(Verified) Microsoft Windows

Version: 10.0.19041.1466

Target machine: i386

Time stamp: 08:08:06 06/08/2046

Image base: 0x4b2800000123000

Checksum: 0x1a5edf (correct)

Subsystem: Windows CUI

Subsystem version: 10.0

Characteristics: Executable, DLL, Dynamic base, NX compatible

Sections:

Name	VA	Size
.text	0x1000	0x11f800
PAGE	0x121000	0x600
RT	0x122000	0x200
.data	0x123000	0xe00
.mdata	0x129000	0x2400
.00cfg	0x12c000	0x200
.rsrc	0x12d000	0x70000
.reloc	0x19d000	0x5200

Module	Machine	Type	File Size	Image Base	Virtual Size	Entry point	Subsystem	Subsystem version
C:\Windows\SysWOW64\kernel32.dll	i386	Dll; Executable	0x0009c730	0x6b800000	0x000f0000	0x0001f640	0x00000003	10.0
C:\Windows\SysWOW64\MSVCRT.dll	i386	Dll; Executable	0x000bd458	0x10100000	0x000bf000	0x00035ac0	0x00000002	10.0
api-ms-win-core-rtlsupport-l1-1-0.dll ->	i386	Dll; Executable	0x0019e5f0	0x4b280000	0x001a3000	0x00000000	0x00000003	10.0
api-ms-win-core-rtlsupport-l1-2-0.dll ->	i386	Dll; Executable	0x0019e5f0	0x4b280000	0x001a3000	0x00000000	0x00000003	10.0
C:\Windows\SysWOW64\ntdll.dll	i386	Dll; Executable	0x0019e5f0	0x4b280000	0x001a3000	0x00000000	0x00000003	10.0

Az NTDLL.DLL a Windows Native API-t exportálja, és ezzel nagyon sok függvényt képes használni. A natív API az operációs rendszer felhasználói módú összetevői által használt interfész, amelynek a Win32 vagy más API-alrendszerek támogatása nélkül kell futnia. Ennek az API-nak a nagy része az NTDLL.DLL-ban van implementálva, és ezekben a könyvtárakban az exportáltak többsége Nt előtaggal rendelkezik, például az NtDisplayString. A natív API-kat a KERNEL32.DLL által exportált „kernel API” vagy „alap API” megvalósítására is használják. A Windows-alkalmazások nagy többsége nem hívja meg közvetlenül az NTDLL.DLL-t