Operációs Rendszerek Bsc

3.gyak

2021.02.24

Készítette:

Veres Balázs Bsc

GÉIK

ZKY1YM

Sajóörös 2021

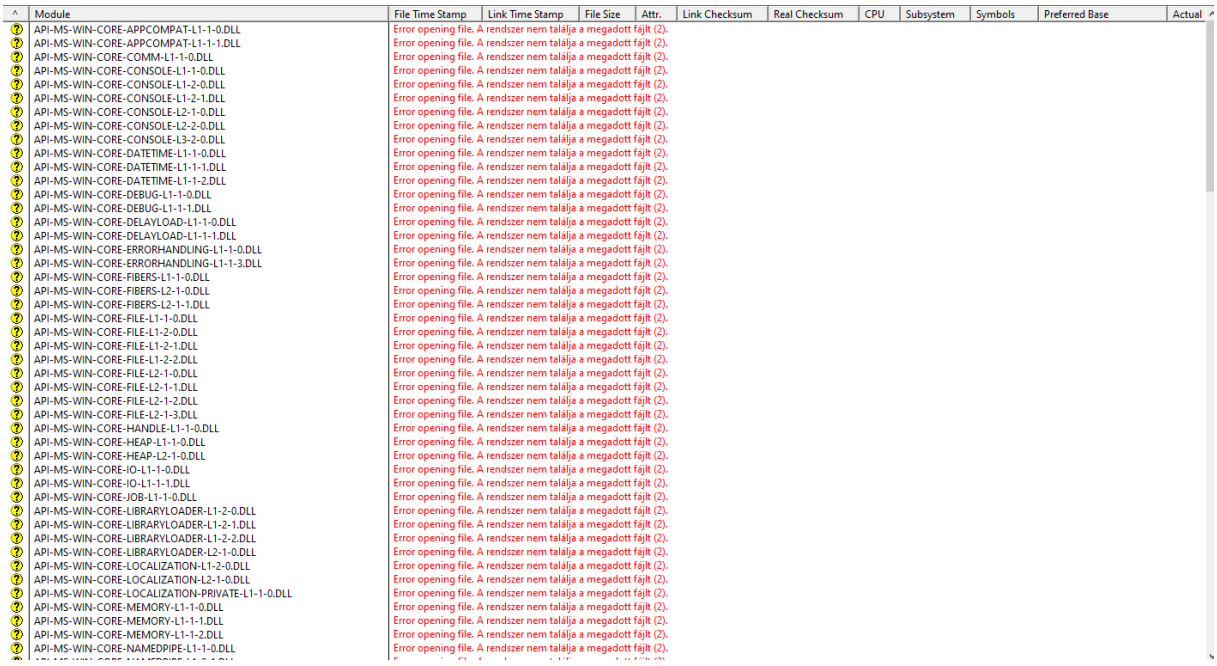
1.feladat : A Dependency Walker segítségével végezze el a következő feladatokat. Nyissa meg a neptunkod.exe fájlt!

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

PI	Ordinal ^	Hint	Function	Entry Point
C	N/A	269 (0x010D)	DeleteCriticalSection	Not Bound
C	N/A	305 (0x0131)	EnterCriticalSection	Not Bound
C	N/A	536 (0x0218)	GetCurrentProcess	Not Bound
C	N/A	537 (0x0219)	GetCurrentProcessId	Not Bound
C	N/A	541 (0x021D)	GetCurrentThreadId	Not Bound
C	N/A	610 (0x0262)	GetLastError	Not Bound
C	N/A	722 (0x02D2)	GetStartupInfoA	Not Bound
C	N/A	747 (0x02EB)	GetSystemTimeAsFileTime	Not Bound
C	N/A	775 (0x0307)	GetTickCount	Not Bound
C	N/A	864 (0x0360)	InitializeCriticalSection	Not Bound
C	N/A	952 (0x03B8)	LeaveCriticalSection	Not Bound
C	N/A	1094 (0x0446)	QueryPerformanceCounter	Not Bound
C	N/A	1180 (0x049C)	RtlAddFunctionTable	Not Bound
C	N/A	1181 (0x049D)	RtlCaptureContext	Not Bound
C	N/A	1188 (0x04A4)	RtlLookupFunctionEntry	Not Bound
C	N/A	1195 (0x04AB)	RtlVirtualUnwind	Not Bound
C	N/A	1347 (0x0543)	SetUnhandledExceptionFilter	Not Bound
C	N/A	1361 (0x0551)	Sleep	Not Bound
C	N/A	1376 (0x0560)	TerminateProcess	Not Bound
C	N/A	1396 (0x0574)	TlsGetValue	Not Bound
C	N/A	1410 (0x0582)	UnhandledExceptionFilter	Not Bound
C	N/A	1444 (0x05A4)	VirtualProtect	Not Bound
C	N/A	1446 (0x05A6)	VirtualQuery	Not Bound

b) Milyen függőségei vannak a kernel32.dll-nek!

A képen látható függőségek nem az összes függőség. A hibák false positivek.



^	Module	File Time Stamp	Link Time Stamp	File Size	Attr.	Link Checksum	Real Checksum	CPU	Subsystem	Symbols	Preferred Base	Actual
	API-MS-WIN-CORE-APPCOMPAT-L1-1-0.DLL	Error opening file. A rendszer nem találja a megadott fájlt (2).										
	API-MS-WIN-CORE-APPCOMPAT-L1-1-1.DLL	Error opening file. A rendszer nem találja a megadott fájlt (2).										
	API-MS-WIN-CORE-COMM-L1-1-0.DLL	Error opening file. A rendszer nem találja a megadott fájlt (2).										
	API-MS-WIN-CORE-CONSOLE-L1-1-0.DLL	Error opening file. A rendszer nem találja a megadott fájlt (2).										
	API-MS-WIN-CORE-CONSOLE-L1-2-0.DLL	Error opening file. A rendszer nem találja a megadott fájlt (2).										
	API-MS-WIN-CORE-CONSOLE-L1-2-1.DLL	Error opening file. A rendszer nem találja a megadott fájlt (2).										
	API-MS-WIN-CORE-CONSOLE-L2-1-0.DLL	Error opening file. A rendszer nem találja a megadott fájlt (2).										
	API-MS-WIN-CORE-CONSOLE-L2-2-0.DLL	Error opening file. A rendszer nem találja a megadott fájlt (2).										
	API-MS-WIN-CORE-CONSOLE-L3-2-0.DLL	Error opening file. A rendszer nem találja a megadott fájlt (2).										
	API-MS-WIN-CORE-DATETIME-L1-1-0.DLL	Error opening file. A rendszer nem találja a megadott fájlt (2).										
	API-MS-WIN-CORE-DATETIME-L1-1-1.DLL	Error opening file. A rendszer nem találja a megadott fájlt (2).										
	API-MS-WIN-CORE-DATETIME-L1-1-2.DLL	Error opening file. A rendszer nem találja a megadott fájlt (2).										
	API-MS-WIN-CORE-DEBUG-L1-1-0.DLL	Error opening file. A rendszer nem találja a megadott fájlt (2).										
	API-MS-WIN-CORE-DEBUG-L1-1-1.DLL	Error opening file. A rendszer nem találja a megadott fájlt (2).										
	API-MS-WIN-CORE-DELAYLOAD-L1-1-0.DLL	Error opening file. A rendszer nem találja a megadott fájlt (2).										
	API-MS-WIN-CORE-DELAYLOAD-L1-1-1.DLL	Error opening file. A rendszer nem találja a megadott fájlt (2).										
	API-MS-WIN-CORE-ERRORHANDLING-L1-1-0.DLL	Error opening file. A rendszer nem találja a megadott fájlt (2).										
	API-MS-WIN-CORE-ERRORHANDLING-L1-1-3.DLL	Error opening file. A rendszer nem találja a megadott fájlt (2).										
	API-MS-WIN-CORE-FIBERS-L1-1-0.DLL	Error opening file. A rendszer nem találja a megadott fájlt (2).										
	API-MS-WIN-CORE-FIBERS-L2-1-0.DLL	Error opening file. A rendszer nem találja a megadott fájlt (2).										
	API-MS-WIN-CORE-FIBERS-L2-1-1.DLL	Error opening file. A rendszer nem találja a megadott fájlt (2).										
	API-MS-WIN-CORE-FILE-L1-1-0.DLL	Error opening file. A rendszer nem találja a megadott fájlt (2).										
	API-MS-WIN-CORE-FILE-L1-2-0.DLL	Error opening file. A rendszer nem találja a megadott fájlt (2).										
	API-MS-WIN-CORE-FILE-L1-2-1.DLL	Error opening file. A rendszer nem találja a megadott fájlt (2).										
	API-MS-WIN-CORE-FILE-L1-2-2.DLL	Error opening file. A rendszer nem találja a megadott fájlt (2).										
	API-MS-WIN-CORE-FILE-L2-1-0.DLL	Error opening file. A rendszer nem találja a megadott fájlt (2).										
	API-MS-WIN-CORE-FILE-L2-1-1.DLL	Error opening file. A rendszer nem találja a megadott fájlt (2).										
	API-MS-WIN-CORE-FILE-L2-1-2.DLL	Error opening file. A rendszer nem találja a megadott fájlt (2).										
	API-MS-WIN-CORE-FILE-L2-1-3.DLL	Error opening file. A rendszer nem találja a megadott fájlt (2).										
	API-MS-WIN-CORE-HANDLE-L1-1-0.DLL	Error opening file. A rendszer nem találja a megadott fájlt (2).										
	API-MS-WIN-CORE-HEAP-L1-1-0.DLL	Error opening file. A rendszer nem találja a megadott fájlt (2).										
	API-MS-WIN-CORE-HEAP-L2-1-0.DLL	Error opening file. A rendszer nem találja a megadott fájlt (2).										
	API-MS-WIN-CORE-IO-L1-1-0.DLL	Error opening file. A rendszer nem találja a megadott fájlt (2).										
	API-MS-WIN-CORE-IO-L1-1-1.DLL	Error opening file. A rendszer nem találja a megadott fájlt (2).										
	API-MS-WIN-CORE-JOB-L1-1-0.DLL	Error opening file. A rendszer nem találja a megadott fájlt (2).										
	API-MS-WIN-CORE-LIBRARYLOADER-L1-2-0.DLL	Error opening file. A rendszer nem találja a megadott fájlt (2).										
	API-MS-WIN-CORE-LIBRARYLOADER-L1-2-1.DLL	Error opening file. A rendszer nem találja a megadott fájlt (2).										
	API-MS-WIN-CORE-LIBRARYLOADER-L1-2-2.DLL	Error opening file. A rendszer nem találja a megadott fájlt (2).										
	API-MS-WIN-CORE-LIBRARYLOADER-L2-1-0.DLL	Error opening file. A rendszer nem találja a megadott fájlt (2).										
	API-MS-WIN-CORE-LOCALIZATION-L1-2-0.DLL	Error opening file. A rendszer nem találja a megadott fájlt (2).										
	API-MS-WIN-CORE-LOCALIZATION-L2-1-0.DLL	Error opening file. A rendszer nem találja a megadott fájlt (2).										
	API-MS-WIN-CORE-LOCALIZATION-PRIVATE-L1-1-0.DLL	Error opening file. A rendszer nem találja a megadott fájlt (2).										
	API-MS-WIN-CORE-MEMORY-L1-1-0.DLL	Error opening file. A rendszer nem találja a megadott fájlt (2).										
	API-MS-WIN-CORE-MEMORY-L1-1-1.DLL	Error opening file. A rendszer nem találja a megadott fájlt (2).										
	API-MS-WIN-CORE-MEMORY-L1-1-2.DLL	Error opening file. A rendszer nem találja a megadott fájlt (2).										
	API-MS-WIN-CORE-NAMEDPIPE-L1-1-0.DLL	Error opening file. A rendszer nem találja a megadott fájlt (2).										

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

Az NTDLL NT kernel függvényeket tartalmaz. Ezen weboldal alapján:
https://www.geoffchappell.com/studies/windows/win32/ntdll/api/index.htm?tx=47,49

A programom a:

DeleteCriticalSection

EnterCriticalSection

GetCurrentProcess

GetTickCount

InitializeCriticalSection

LeaveCriticalSection

QueryPerformanceCounter

RtlAddFunctionTable

RtlCaptureContext

RtlLookupFunctionEntry

RtlVirtualUnwind

SetUnhandledExceptionFilter

TerminateProcess

UnhandledExceptionFilter

függvényeket használja.

Az NTDLL.DLL függvényei sok esetben újra exportálták, és megtalálhatóak a KERNEL32.DLL-ben is. (forrás: https://www.geoffchappell.com/studies/windows/win32/ntdll/index.htm?tx=4,47,49)