Operációs rendszerek BSc

2. konzultáció gyakorlat

2020.02.26.

Készítette:

Hegedűs Attila László BSc
Mérnök-informatikus
levelező
D2OVJ9

Miskolc, 2021

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

A kernel32.dll-ből hívott API-k:

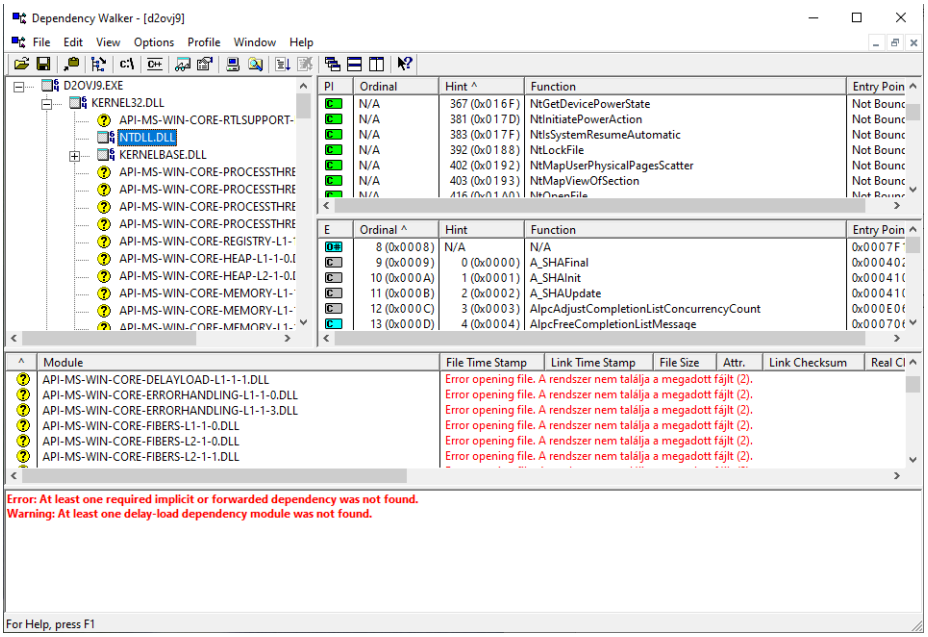
- NTDLL.DLL
- KERNELBASE.DLL
- RPCRT4.DLL

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

- NTDLL.DLL
- KERNELBASE.DLL
- RPCRT4.DLL

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

Az ntdll.dll a Windows Native API-t exportálja. A Native API az interfész, melyet az operációs rendszer user-mode komponensei használnak, és melynek képesnek kell lennie futni Win32 vagy más API alrendszerek támogatása nélkül. Legtöbb exportált függvénye Nt kezdetű, például NtClose stb. A Dependency Walker ablakában bal oldalon láthatjuk, hogy a D2OVJ9.EXE-került futtatásra, és fa szerűen ábrázolja a függőségeket. A jobb oldali felső szekcióban találhatjuk az exportált függvényeket, melyek meghívásra kerültek a ntdll.dll-ből a program futása során, a jobb oldal alsó szekciójában a .dll fájl összes függvényét láthatjuk. Látható, hogy egy egyszerűnek tűnő program futása során is több száz függvény kerül meghívásra a Windows API-n keresztül.



Források:
https://en.wikipedia.org/wiki/Microsoft_Windows_library_files#NTDLL.DLL