Malicious DLL

DLL's using Dependency Walker

DLLs (Dynamic Link Libraries) in the context of cybersecurity often refer to dynamic libraries that contain code and data used by multiple programs simultaneously. In cybersecurity, DLLs can be both a potential vulnerability and a tool for defense.

Here are some key points:

1. Defense:

- Code Signing: Authenticating DLLs using digital signatures helps ensure they haven't been tampered with.
- Integrity Monitoring: Monitoring DLLs for changes can help detect unauthorized modifications.
- Least Privilege: Limiting the permissions and access rights of DLLs and the processes that use them can reduce the potential impact of DLL-related attacks.
- Sandboxing: Running applications in isolated environments can mitigate the impact of DLL-based attacks by containing their effects.

2. Tools:

- Dependency Walker: A tool for analyzing dependencies and functions of DLLs.
- Process Monitor: Monitors DLL-related activities such as DLL loading, unloading, and injection.
- Dependency Checkers: Tools that help identify vulnerable or outdated DLLs in applications and systems.

Process Explorer and Import tab

1. Process Explorer:

- Real-time Process View: Process Explorer provides a real-time view of running processes and the DLLs they have loaded.
- Dynamic Exploration: It allows you to explore DLLs in use by specific processes at any given moment.
- Focus on Systemwide View*: Process Explorer gives an overview of all processes and their associated DLLs, offering insights into system-wide activity.

2. Import Tab in Dependency Walker:

- Static Analysis: The Import tab in Dependency Walker provides a static analysis of a specific executable or DLL file, showing the DLLs that the file imports functions from.
- Dependency Tree: It presents a hierarchical view of imported functions and the DLLs providing those functions, aiding in understanding the static dependencies before execution.
- Focus on Specific Files: Dependency Walker focuses on a specific executable or DLL file and its dependencies rather than the entire system's runtime behavior.

Comparison between Process Explorer and Import tab

- Real-time vs. Static: Process Explorer offers real-time insights into DLL usage during runtime, while the Import tab provides a static analysis of dependencies before execution.
- Dynamic Exploration vs. Fixed View: Process Explorer allows for dynamic exploration of DLL usage by running processes, whereas Dependency Walker's Import tab presents a fixed snapshot of dependencies based on a specific file.

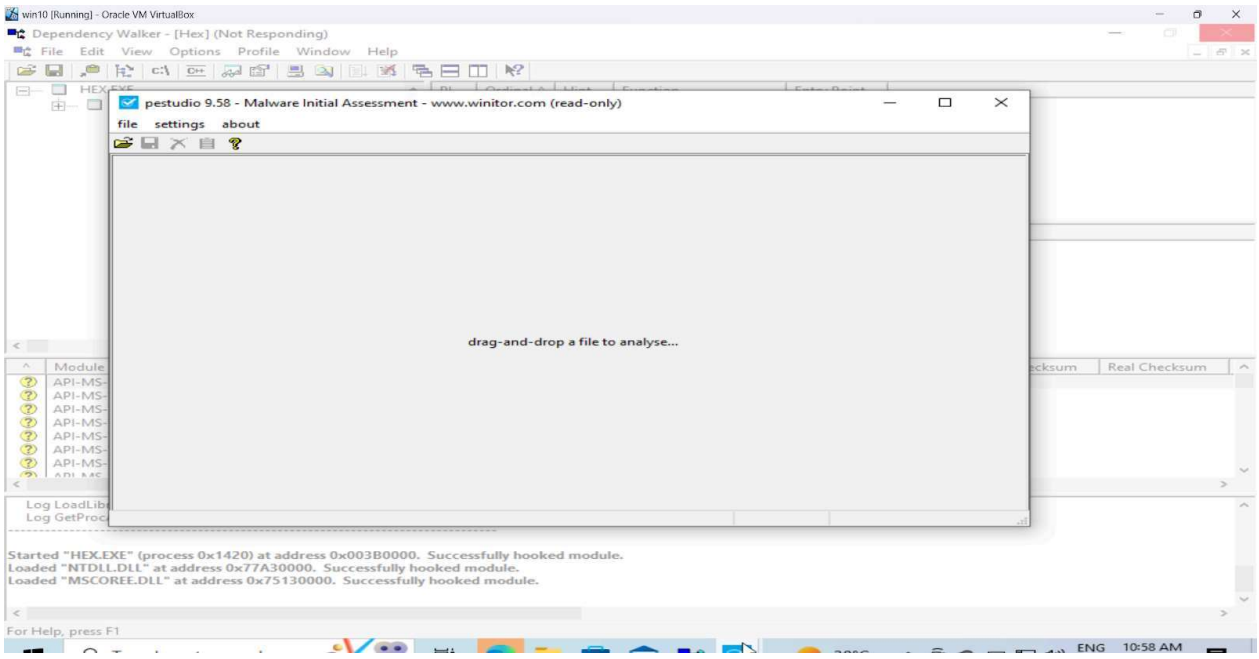
- Systemwide View vs. Specific File View: Process Explorer provides a system-wide view of DLL usage across all processes, while Dependency Walker focuses on analyzing dependencies for individual executable or DLL files.

In summary, while both tools provide insights into DLL usage, they serve different purposes: Process Explorer for dynamic, real-time monitoring of system-wide DLL usage, and Dependency Walker for static analysis of dependencies for specific files.

To Check Whether Malware Contains Malicious DLL:

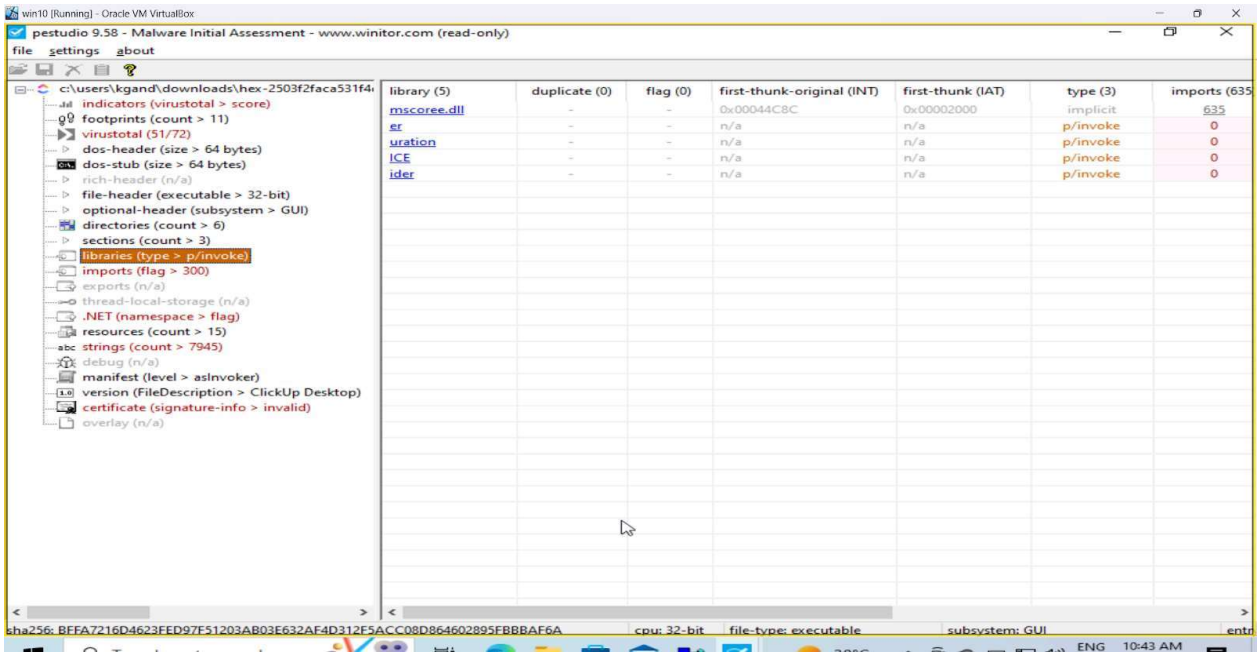
For Checking of the Malicious DLL in the Malware we have to use a tool called Dependency Walker. It will Check if the EXE contains any Malicious DLL's Present in the EXE. for Checking of the Malicious DLL You can follow the given steps:

Step 1: Open the file in PEstudio



Then click on the the library tab

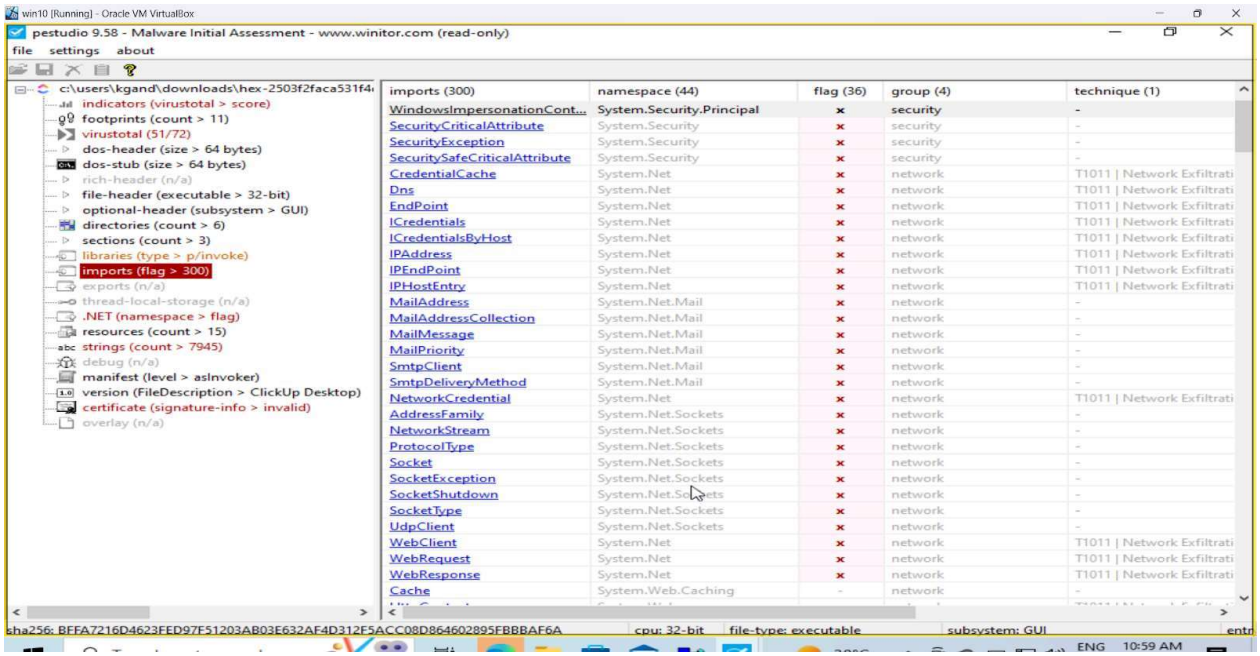
Here you can see how many DLL or library are used by the file.



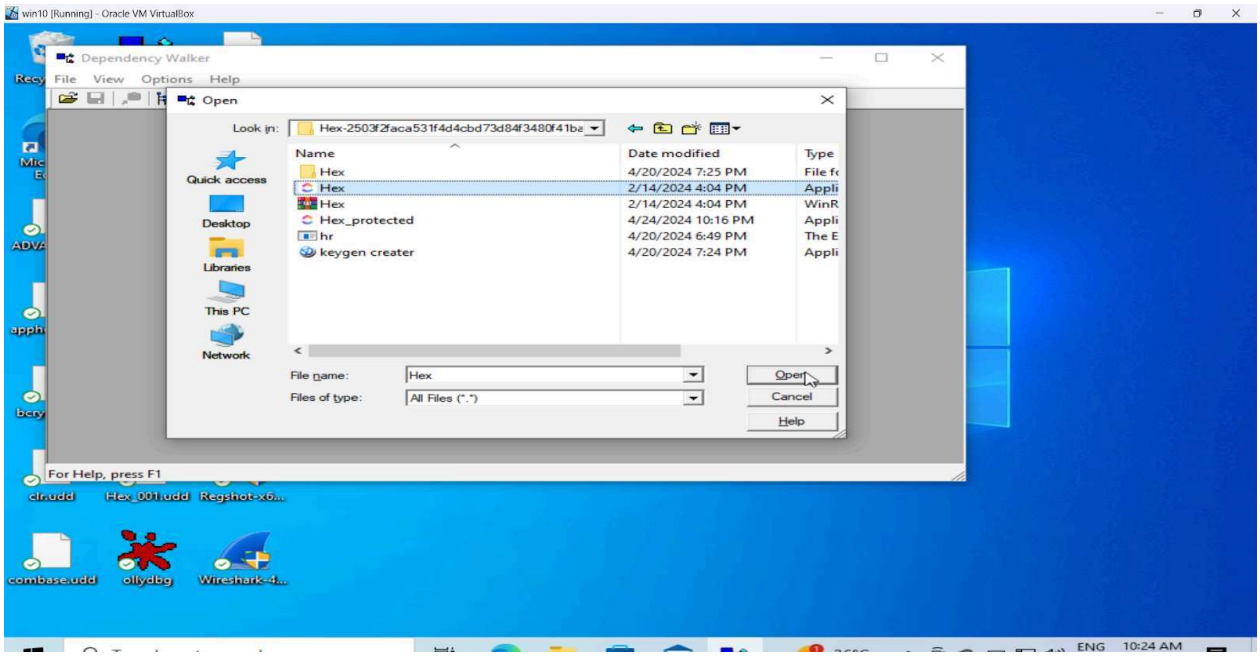
In this file use mscoree.dll

Now go in import you see the malicious import

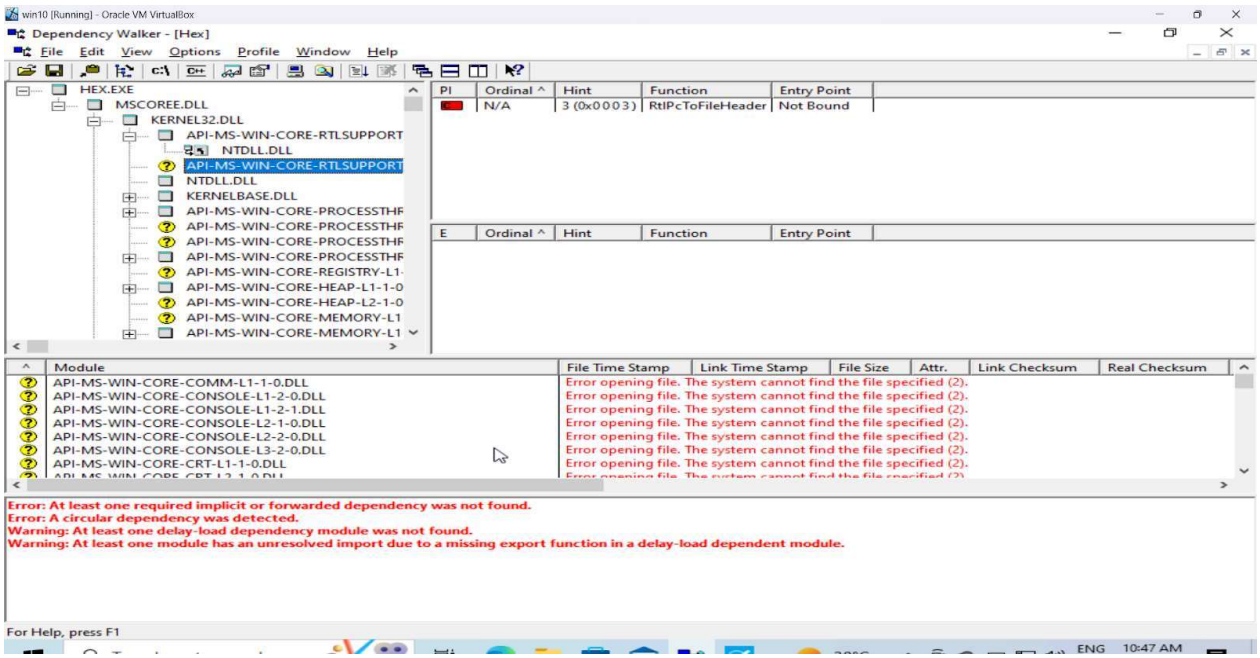
Which has the red flag



Now open Dependancy walker

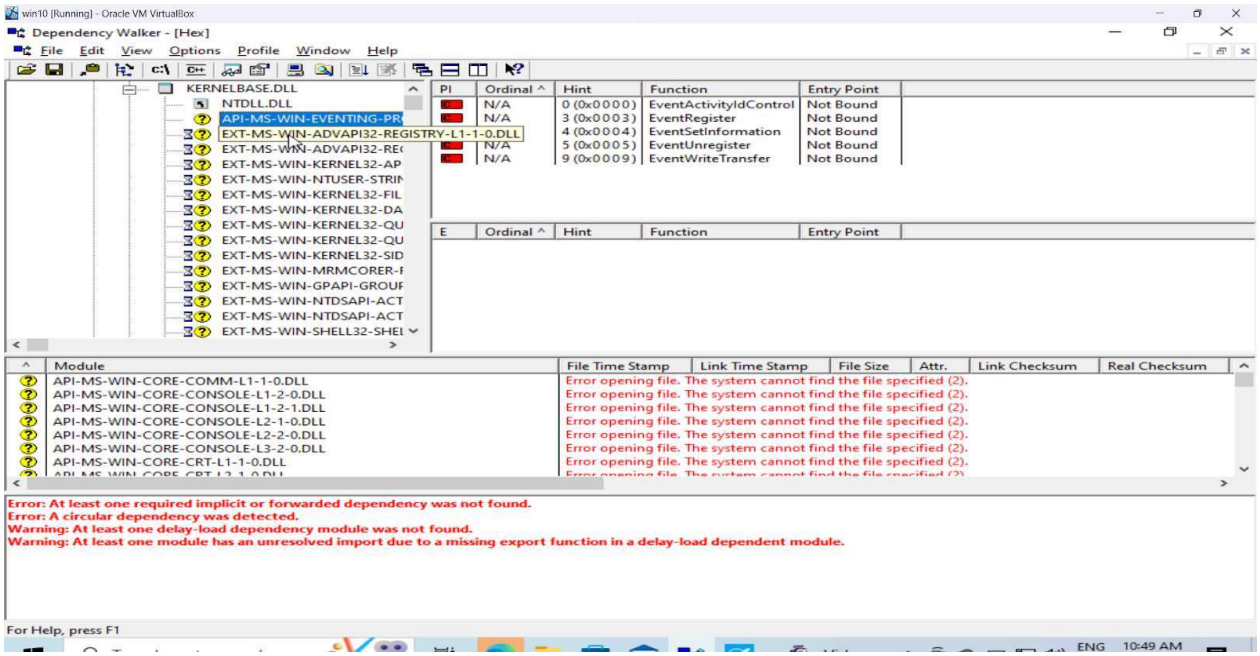


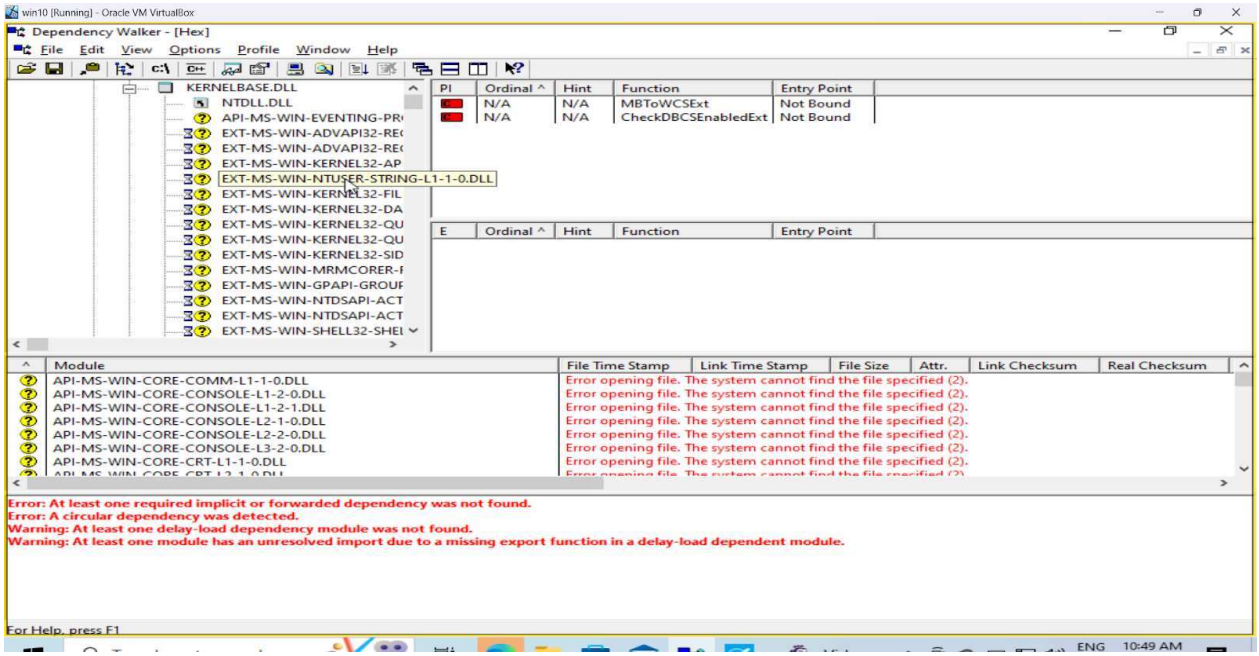
Select the file

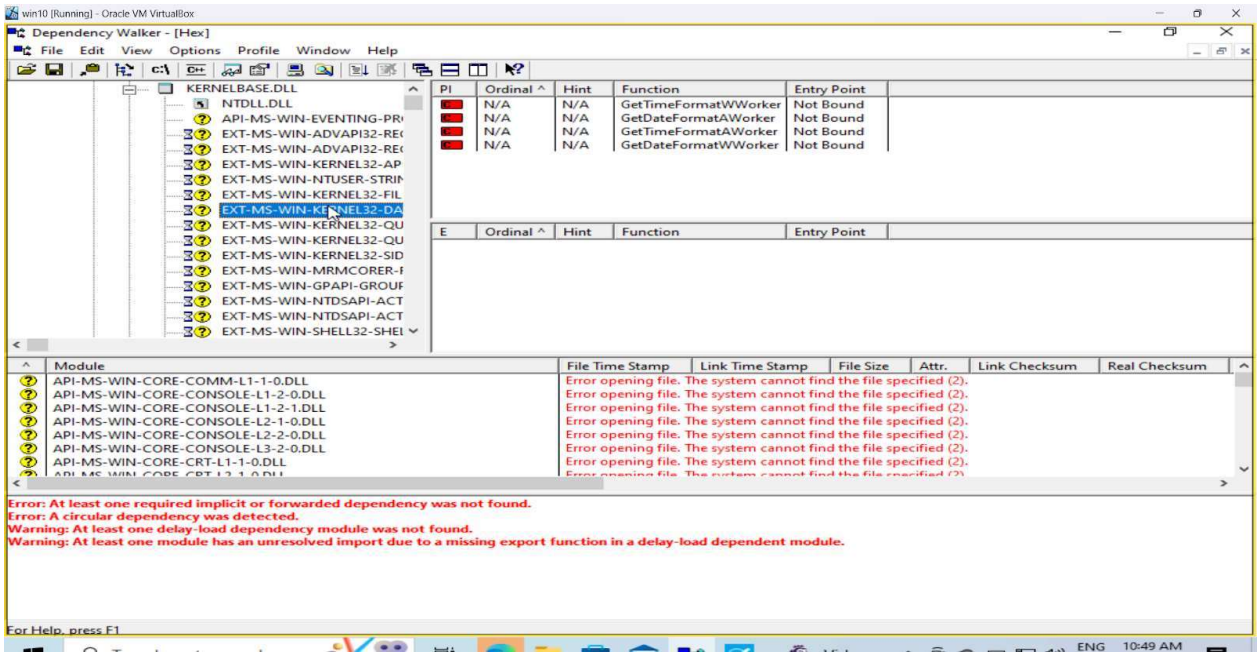


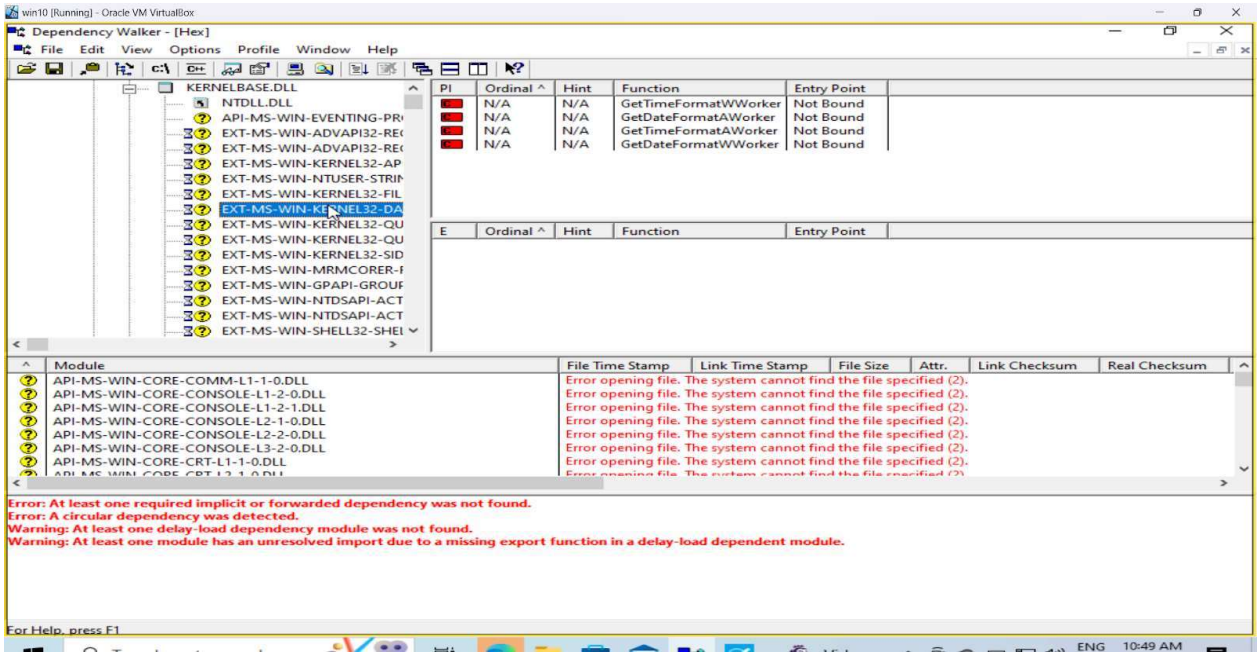
Here you can see the mscore.dll

Here you can see all the errors


win10 [Running] - Oracle VM VirtualBox
Dependency Walker - [Hex]
File Edit View Options Profile Window Help
KERNELBASE.DLL
NTDLL.DLL
API-MS-WIN-EVENTING-PR
EXT-MS-WIN-ADVAPI32-REGISTRY-L1-1-0.DLL
EXT-MS-WIN-ADVAPI32-RE
EXT-MS-WIN-KERNEL32-AP
EXT-MS-WIN-NTUSER-STRI
EXT-MS-WIN-KERNEL32-FIL
EXT-MS-WIN-KERNEL32-DA
EXT-MS-WIN-KERNEL32-QU
EXT-MS-WIN-KERNEL32-QU
EXT-MS-WIN-KERNEL32-SID
EXT-MS-WIN-MRMCORER-I
EXT-MS-WIN-GPAPI-GROUI
EXT-MS-WIN-NTDSAPI-ACT
EXT-MS-WIN-NTDSAPI-ACT
EXT-MS-WIN-SHELL32-SHEI
PI Ordinal ^ Hint Function Entry Point
N/A 0 (0x0000) EventActivityIdControl Not Bound
N/A 3 (0x0003) EventRegister Not Bound
4 (0x0004) EventSetInformation Not Bound
N/A 5 (0x0005) EventUnregister Not Bound
N/A 9 (0x0009) EventWriteTransfer Not Bound
E Ordinal ^ Hint Function Entry Point
Module File Time Stamp Link Time Stamp File Size Attr. Link Checksum Real Checksum
API-MS-WIN-CORE-COMM-L1-1-0.DLL
API-MS-WIN-CORE-CONSOLE-L1-2-0.DLL
API-MS-WIN-CORE-CONSOLE-L1-2-1.DLL
API-MS-WIN-CORE-CONSOLE-L2-1-0.DLL
API-MS-WIN-CORE-CONSOLE-L2-2-0.DLL
API-MS-WIN-CORE-CONSOLE-L3-2-0.DLL
API-MS-WIN-CORE-CRT-L1-1-0.DLL
Error opening file. The system cannot find the file specified (2).
Error: At least one required implicit or forwarded dependency was not found.
Error: A circular dependency was detected.
Warning: At least one delay-load dependency module was not found.
Warning: At least one module has an unresolved import due to a missing export function in a delay-load dependent module.
For Help, press F1
ENG 10:49 AM


win10 [Running] - Oracle VM VirtualBox
Dependency Walker - [Hex]
File Edit View Options Profile Window Help
KERNELBASE.DLL
NTDLL.DLL
API-MS-WIN-EVENTING-PR
EXT-MS-WIN-ADVAPI32-RE
EXT-MS-WIN-ADVAPI32-RE
EXT-MS-WIN-KERNEL32-AP
EXT-MS-WIN-NTUSER-STRING-L1-1-0.DLL
EXT-MS-WIN-KERNEL32-FIL
EXT-MS-WIN-KERNEL32-DA
EXT-MS-WIN-KERNEL32-QU
EXT-MS-WIN-KERNEL32-QU
EXT-MS-WIN-KERNEL32-SID
EXT-MS-WIN-MRMCORER-I
EXT-MS-WIN-GPAPI-GROUI
EXT-MS-WIN-NTDSAPI-ACT
EXT-MS-WIN-NTDSAPI-ACT
EXT-MS-WIN-SHELL32-SHEI
PI Ordinal ^ Hint Function Entry Point
N/A N/A MBToWCSExt Not Bound
N/A N/A CheckDBCSEnabledExt Not Bound
E Ordinal ^ Hint Function Entry Point
Module File Time Stamp Link Time Stamp File Size Attr. Link Checksum Real Checksum
API-MS-WIN-CORE-COMM-L1-1-0.DLL
API-MS-WIN-CORE-CONSOLE-L1-2-0.DLL
API-MS-WIN-CORE-CONSOLE-L1-2-1.DLL
API-MS-WIN-CORE-CONSOLE-L2-1-0.DLL
API-MS-WIN-CORE-CONSOLE-L2-2-0.DLL
API-MS-WIN-CORE-CONSOLE-L3-2-0.DLL
API-MS-WIN-CORE-CRT-L1-1-0.DLL
Error opening file. The system cannot find the file specified (2).
Error: At least one required implicit or forwarded dependency was not found.
Error: A circular dependency was detected.
Warning: At least one delay-load dependency module was not found.
Warning: At least one module has an unresolved import due to a missing export function in a delay-load dependent module.
For Help, press F1
ENG 10:49 AM





By analysis all this stuff we can conclude

that ntdll from kernelbase.dll is malicious

Conclusion :

Understanding how DLLs work and implementing proper security measures can help mitigate risks associated with them in cybersecurity contexts. By the use of dependency walker we have found the above details on malicious DLLs.