YEDİTEPE
UNIVERSITY

CYB 363

Operating Systems Security

Table of Contents

What are DLLs ?..... 2

What's DLL Search Order Hijacking Attack ?..... 3

Simulation..... 4

How to Prevent.....4

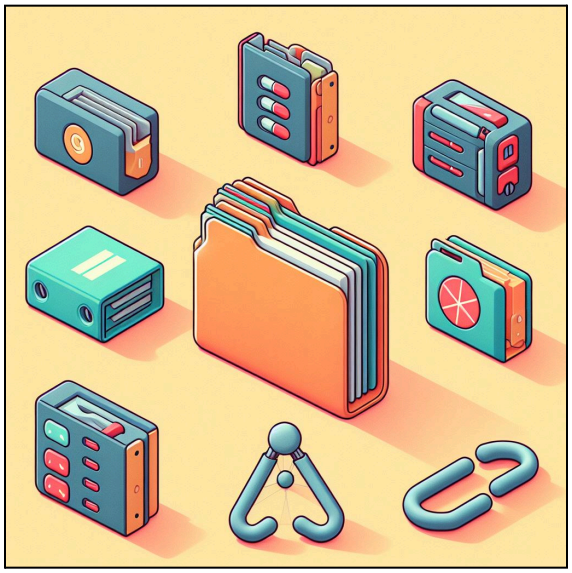
Student Information.....5

What are DLLs ?

DLLs are like shared code **libraries** that computer programs use. They contain instructions for doing common tasks. Many programs can use the same DLL, saving space and making things run smoother.

For instance, let's say you have two programs: a **word processor(**`word.exe`**)** and a **spreadsheet application(**`spreadsheet.exe`**)**. Both of these programs might need to perform common tasks like displaying fonts, handling print operations, or compressing/decompressing files. Instead of having the code for these tasks duplicated in both programs, the necessary code can be separated into DLLs like `fontdll.dll`, `printdll.dll`, and `zipdll.dll`.

Both the word processor and the spreadsheet application can then dynamically link to and use these shared DLL files at runtime, without having to include the complete code within their own executable files.

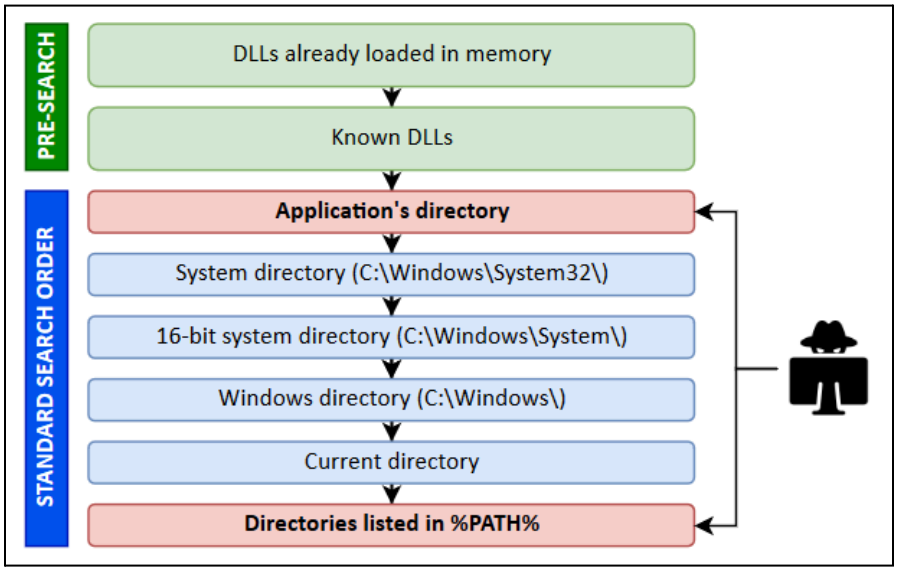


What's DLL Search Order Hijacking Attack ?

When an executable tries to load a DLL on Windows, OS helps executable to find the DLL by searching it in several locations like:

- **`C:\Windows\System32`**
- **`C:\Windows\System`**
- **`Current Directory …`**

DLL Search Order Hijacking occurs when a program loads a DLL from an insecure location before legitimate locations. In other words, if there is a location where the attacker has write access, then the attacker can place his own dll with the same name of the dll executable searching for and potentially import the attacker's dll instead of the legitimate one, which leads to running the attacker's custom code.



Simulation

[Click Here to Go to the Simulation Video]

How to Prevent

This attack worked because the Downloads directory is not a safe directory to execute programs. Windows provides some default directories for that use called:

1. **`Program Files`**
2. **`Program Files (x86)`**

If you look at the permission of these directories you can see that attackers are not allowed to create files without administrator privilege.

Another solution would be making proper permission adjustments for the directories you'll execute programs.

And lastly if you'll use a program that is developed by you or your organization, you can add your dll names to the **`KnownDLLs`** registry. When you add your dlls in this registry they cannot be hijacked as Windows looks for these DLLs directly from **`C:\Windows\System32`** which is a directory that attackers cannot create files without administrator permissions.

Student Information

- **Name:** Eren
- **Surname:** Burulday
- **Student Number:** 20201319002
- **Date:** 19.04.2024
- **Course:** CYB370
- **Section:** 1