THE BRIDGE

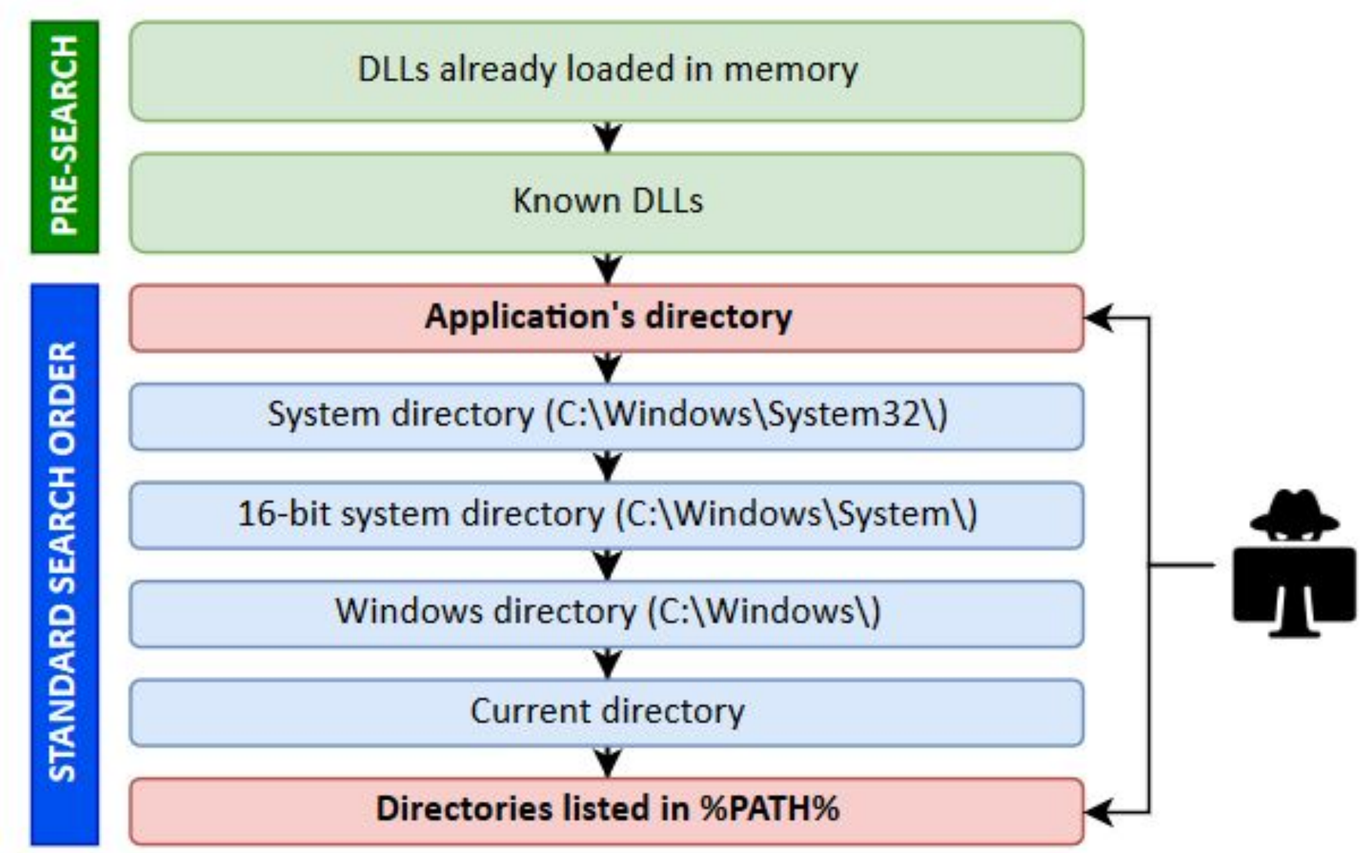
CYBER SECURITY

Escalada de Privilegios Windows I

Hijack Execution Flow: DLL Search Order Hijacking: Fom DLL Replacement to Phantom DLL

T1574	Hijack Execution Flow	Adversaries may execute their own malicious payloads by hijacking the way operating systems run programs. Hijacking execution flow can be for the purposes of persistence, since this hijacked execution may reoccur over time. Adversaries may also use these mechanisms to elevate privileges or evade defenses, such as application control or other restrictions on execution.

.001	DLL Search Order Hijacking	Adversaries may execute their own malicious payloads by hijacking the search order used to load DLLs. Windows systems use a common method to look for required DLLs to load into a program. Hijacking DLL loads may be for the purpose of establishing persistence as well as elevating privileges and/or evading restrictions on file execution.


PRE-SEARCH
DLLs already loaded in memory
Known DLLs
STANDARD SEARCH ORDER
Application's directory
System directory (C:\Windows\System32\)
16-bit system directory (C:\Windows\System\)
Windows directory (C:\Windows\)
Current directory
Directories listed in %PATH%

- (F) Full Control
- (M) Modify
- (W) Write

- The user we are currently logged in as (%USERNAME%)
- Authenticated Users
- Everyone
- BUILTIN\Users
- NT AUTHORITY\INTERACTIVE


THE
BRIDGE