Playing with DLLs for Fun & Profit

Understanding DLL Hijacking and DLL Sideloading
for Persistence & Privilege Escalation

# whoami (@shahrukhiqbal24)

- Wannabe Hacker, Red Teamer, Penetration Tester
- Seasonal Bug Bounty Hunter
- CTF Player
- Advocate for “Hacking Is NOT A Crime”
- Seasonal Blogger

Agenda

- Understanding Statically vs. Dynamically Compiled Applications
- Introduction to DLLs and their need and importance
- Introduction to Post-Exploitation: Persistence and Privilege Escalation
- DLL Hijacking
- DLL Sideloading
- Looking for DLL Misconfigurations

Let’s Get Started!

Statically vs. Dynamically Compiled Applications

- Statically Compiled Windows Applications
  - Portable stand-alone executable files
  - No prerequisites
  - All the libraries and functions are present in the application code itself
  - Shipped as a complete package
- Dynamically Compiled Windows Applications
  - Contains undefined functions and variables
  - Compiled at run-time
  - Require some prerequisites to compile and install
  - Usually shipped as a bundle with a lot of files or as an installer

Dynamic Linked Libraries (DLLs)

- Microsoft’s implementation of Dynamic Linking or Shared Libraries
- When a program is run on Windows operating systems, much of the functionality of the program may be provided by DLLs
- Helps promote code reuse, efficient memory usage, and reduced disk space
- Makes the application run faster
- Advantages of using DLLs:
    - Uses fewer resources
    - Promotes modular architecture
    - Easy installation and deployment

Introduction to Post-Exploitation

- Second-last phase of the Ethical Hacking Lifecycle
- Also called Action-on-Objectives
- Includes (but not limited to):
  - Lateral movement
  - Privilege Escalation
  - Persistence
  - Credential Dumping
  - Data Exfiltration

Persistence

- Also called Maintaining Access
- Techniques includes (but not limited to):
  - Creating Users
  - Creating Scheduled Tasks
  - Modifying Registry

Privilege Escalation

- Elevating current user privileges
- Types: (i) Vertical and (ii) Horizontal
- Vertical
  - Elevating current privileges in terms of User Access Control (UAC)
  - Getting Admin from a Standard User or SYSTEM from Admin User
- Horizontal
  - Elevating current privileges in order to access additional resources within the computer or network

Let The Fun Begin!

DLL Hijacking

- Overview:
  - Also called DLL Search Order Hijacking
  - Listed in the MITRE ATT&CK Framework as an Enterprise Technique within Hijack Execution Flow
  - Technique ID T1574.001
  - Can be used for Persistence, Defense Evasion and Privilege Escalation
- Details:
  - Windows loads DLLs when a process or application is started
  - Windows looks for DLLs in directories following the below order:
    - Application’s directory
    - System and System32 directory
    - Windows directory
    - Current working directory
    - Directories in %PATH%
  - In case of a missing DLL, the application becomes vulnerable to DLL Hijacking.

DLL Hijacking

- How to exploit:
  - Place a maliciously crafted DLL within the Search Order Path of the application
  - Restart the application
  - DLL gets executed
- Prerequisites of a successful attack:
  - The Search Order Path must be writable
  - Malicious DLL should export the same functions (or entry points) as the original DLL

DLL Sideloading

- Slightly different from DLL Hijacking
- Applications’ manifest contains references to DLLs which are to be loaded
- Looks for weak references in the manifest file
- Places a malicious DLL within the executable’s directory and attempts to load the malicious version of the DLL
- Two variants:
    a. Drop a signed executable with a malicious DLL named as the legitimate DLL the executable loads
    b. Move an executable from System directory into a writable directory and place a malicious DLL along-side it

Implications of Hijacking & Sideloading DLLs

1. Initial Access
2. Persistence
3. Privilege Escalation

How to Find DLL Misconfigurations

References

- https://docs.microsoft.com/en-us/troubleshoot/windows-client/deployment/dynamic-link-library
- https://attack.mitre.org/techniques/T1574/001/
- https://attack.mitre.org/techniques/T1574/002/
- https://itm4n.github.io/windows-dll-hijacking-clarified/
- https://www.youtube.com/watch?v=3eROsG_WNpE&t=17s
- https://www.mandiant.com/sites/default/files/2021-09/rpt-dll-sideloading.pdf
- https://maniakarisk.com/dll-side-loading-attack-takes-advantage/

Thank You!

Connect with me:
LinkedIn / Twitter: @shahrukhiqbal24