# TTP Detail – T1038

## TTP Information

Name: DLL Search Order Hijacking

Description: Windows systems use a common method to look for required DLLs to load into a program. (Citation: Microsoft DLL Search) Adversaries may take advantage of the Windows DLL search order and programs that ambiguously specify DLLs to gain privilege escalation and persistence.

Adversaries may perform DLL preloading, also called binary planting attacks, (Citation: OWASP Binary Planting) by placing a malicious DLL with the same name as an ambiguously specified DLL in a location that Windows searches before the legitimate DLL. Often this location is the current working directory of the program. Remote DLL preloading attacks occur when a program sets its current directory to a remote location such as a Web share before loading a DLL. (Citation: Microsoft 2269637) Adversaries may use this behavior to cause the program to load a malicious DLL.

Adversaries may also directly modify the way a program loads DLLs by replacing an existing DLL or modifying a .manifest or .local redirection file, directory, or junction to cause the program to load a different DLL to maintain persistence or privilege escalation. (Citation: Microsoft DLL Redirection) (Citation: Microsoft Manifests) (Citation: Mandiant Search Order)

If a search order-vulnerable program is configured to run at a higher privilege level, then the adversary-controlled DLL that is loaded will also be executed at the higher level. In this case, the technique could be used for privilege escalation from user to administrator or SYSTEM or from administrator to SYSTEM, depending on the program.

Programs that fall victim to path hijacking may appear to behave normally because malicious DLLs may be configured to also load the legitimate DLLs they were meant to replace.

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## Kill Chain Phases

**•** mitre-attack: persistence

**•** mitre-attack: privilege-escalation

**•** mitre-attack: defense-evasion