# TTP Detail – T1574.001

## TTP Information

Name: DLL

Description: Adversaries may abuse dynamic-link library files (DLLs) in order to achieve persistence, escalate privileges, and evade defenses. DLLs are libraries that contain code and data that can be simultaneously utilized by multiple programs. While DLLs are not malicious by nature, they can be abused through mechanisms such as side-loading, hijacking search order, and phantom DLL hijacking.(Citation: unit 42)

Specific ways DLLs are abused by adversaries include:

### DLL Sideloading
Adversaries may execute their own malicious payloads by side-loading DLLs. Side-loading involves hijacking which DLL a program loads by planting and then invoking a legitimate application that executes their payload(s).

Side-loading positions both the victim application and malicious payload(s) alongside each other. Adversaries likely use side-loading as a means of masking actions they perform under a legitimate, trusted, and potentially elevated system or software process. Benign executables used to side-load payloads may not be flagged during delivery and/or execution. Adversary payloads may also be encrypted/packed or otherwise obfuscated until loaded into the memory of the trusted process.

Adversaries may also side-load other packages, such as BPLs (Borland Package Library).(Citation: kroll bpl)

### DLL Search Order Hijacking
Adversaries may execute their own malicious payloads by hijacking the search order that Windows uses to load DLLs. This search order is a sequence of special and standard search locations that a program checks when loading a DLL. An adversary can plant a trojan DLL in a directory that will be prioritized by the DLL search order over the location of a legitimate library. This will cause Windows to load the malicious DLL when it is called for by the victim program.(Citation: unit 42)

### DLL Redirection
Adversaries may directly modify the search order via DLL redirection, which after being enabled (in the Registry or via the creation of a redirection file) may cause a program to load a DLL from a different location.(Citation: Microsoft redirection)(Citation: Microsoft - manifests/assembly)

### Phantom DLL Hijacking
Adversaries may leverage phantom DLL hijacking by targeting references to non-existent DLL files. They may be able to load their own malicious DLL by planting it with the correct name in the location of the missing module.(Citation: Hexacorn DLL Hijacking)(Citation: Hijack DLLs CrowdStrike)

### DLL Substitution
Adversaries may target existing, valid DLL files and substitute them with their own malicious DLLs, planting them with the same name and in the same location as the valid DLL file.(Citation: Wietze Beukema DLL Hijacking)

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

Remote DLL hijacking can occur when a program sets its current directory to a remote location, such as a Web share, before loading a DLL.(Citation: dll pre load owasp)(Citation: microsoft remote preloading)

If a valid DLL 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.

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## Kill Chain Phases

**•** mitre-attack: persistence

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

**•** mitre-attack: defense-evasion

## Malware

* Astaroth
* BADNEWS
* BBSRAT
* BOOSTWRITE
* Chaes
* Chinoxy
* Clambling
* Crutch
* DarkGate
* Denis
* Downdelph
* Dridex
* Ecipekac
* Egregor
* FinFisher
* FoggyWeb
* Goopy
* HTTPBrowser
* HUI Loader
* Hikit
* HyperBro
* InvisiMole
* Javali
* Kerrdown
* LoFiSe
* LookBack
* Lumma Stealer
* Melcoz
* Metamorfo
* MirageFox
* Nebulae
* Ninja
* Pandora
* Pcexter
* PlugX
* PowGoop
* Prikormka
* QakBot
* RCSession
* RainyDay
* Ramsay
* Raspberry Robin
* RedLeaves
* Sakula
* StrelaStealer
* SysUpdate
* T9000
* WEBC2
* WastedLocker
* Waterbear
* Wingbird
* ZeroT
* gh0st RAT
* metaMain

## Tools

* Brute Ratel C4
* Empire
* PowerSploit

## APTs (Intrusion Sets)

* APT19
* APT3
* APT32
* APT41
* Aquatic Panda
* BRONZE BUTLER
* BackdoorDiplomacy
* BlackTech
* Chimera
* Cinnamon Tempest
* Daggerfly
* Earth Lusca
* Evilnum
* FIN13
* GALLIUM
* Higaisa
* Lazarus Group
* LuminousMoth
* MuddyWater
* Mustang Panda
* Naikon
* Patchwork
* RTM
* SideCopy
* Sidewinder
* Storm-1811
* Threat Group-3390
* Tonto Team
* Tropic Trooper
* Velvet Ant
* Whitefly
* menuPass