# TTP Detail – T1574.009

## TTP Information

Name: Path Interception by Unquoted Path

Description: Adversaries may execute their own malicious payloads by hijacking vulnerable file path references. Adversaries can take advantage of paths that lack surrounding quotations by placing an executable in a higher level directory within the path, so that Windows will choose the adversary's executable to launch.

Service paths (Citation: Microsoft CurrentControlSet Services) and shortcut paths may also be vulnerable to path interception if the path has one or more spaces and is not surrounded by quotation marks (e.g., <code>C:\unsafe path with space\program.exe</code> vs. <code>"C:\safe path with space\program.exe"</code>). (Citation: Help eliminate unquoted path) (stored in Windows Registry keys) An adversary can place an executable in a higher level directory of the path, and Windows will resolve that executable instead of the intended executable. For example, if the path in a shortcut is <code>C:\program files\myapp.exe</code>, an adversary may create a program at <code>C:\program.exe</code> that will be run instead of the intended program. (Citation: Windows Unquoted Services) (Citation: Windows Privilege Escalation Guide)

This technique can be used for persistence if executables are called on a regular basis, as well as privilege escalation if intercepted executables are started by a higher privileged process.

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## Kill Chain Phases

**•** mitre-attack: persistence

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

**•** mitre-attack: defense-evasion

## Tools

* Empire
* PowerSploit