# TTP Detail – T1546.007

## TTP Information

Name: Netsh Helper DLL

Description: Adversaries may establish persistence by executing malicious content triggered by Netsh Helper DLLs. Netsh.exe (also referred to as Netshell) is a command-line scripting utility used to interact with the network configuration of a system. It contains functionality to add helper DLLs for extending functionality of the utility.(Citation: TechNet Netsh) The paths to registered netsh.exe helper DLLs are entered into the Windows Registry at <code>HKLM\SOFTWARE\Microsoft\Netsh</code>.

Adversaries can use netsh.exe helper DLLs to trigger execution of arbitrary code in a persistent manner. This execution would take place anytime netsh.exe is executed, which could happen automatically, with another persistence technique, or if other software (ex: VPN) is present on the system that executes netsh.exe as part of its normal functionality.(Citation: Github Netsh Helper CS Beacon)(Citation: Demaske Netsh Persistence)

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Kill Chain Phases

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

**•** mitre-attack: persistence

## Tools

* netsh