# TTP Detail – T1547.010

## TTP Information

Name: Port Monitors

Description: Adversaries may use port monitors to run an adversary supplied DLL during system boot for persistence or privilege escalation. A port monitor can be set through the <code>AddMonitor</code> API call to set a DLL to be loaded at startup.(Citation: AddMonitor) This DLL can be located in <code>C:\Windows\System32</code> and will be loaded and run by the print spooler service, `spoolsv.exe`, under SYSTEM level permissions on boot.(Citation: Bloxham)

Alternatively, an arbitrary DLL can be loaded if permissions allow writing a fully-qualified pathname for that DLL to the `Driver` value of an existing or new arbitrarily named subkey of <code>HKLM\SYSTEM\CurrentControlSet\Control\Print\Monitors</code>. The Registry key contains entries for the following:

\* Local Port
\* Standard TCP/IP Port
\* USB Monitor
\* WSD Port

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## Kill Chain Phases

**•** mitre-attack: persistence

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