# TTP Detail – T1547.012

## TTP Information

Name: Print Processors

Description: Adversaries may abuse print processors to run malicious DLLs during system boot for persistence and/or privilege escalation. Print processors are DLLs that are loaded by the print spooler service, `spoolsv.exe`, during boot.(Citation: Microsoft Intro Print Processors)

Adversaries may abuse the print spooler service by adding print processors that load malicious DLLs at startup. A print processor can be installed through the <code>AddPrintProcessor</code> API call with an account that has <code>SeLoadDriverPrivilege</code> enabled. Alternatively, a print processor can be registered to the print spooler service by adding the <code>HKLM\SYSTEM\\[CurrentControlSet or ControlSet001]\Control\Print\Environments\\[Windows architecture: e.g., Windows x64]\Print Processors\\[user defined]\Driver</code> Registry key that points to the DLL.

For the malicious print processor to be correctly installed, the payload must be located in the dedicated system print-processor directory, that can be found with the <code>GetPrintProcessorDirectory</code> API call, or referenced via a relative path from this directory.(Citation: Microsoft AddPrintProcessor May 2018) After the print processors are installed, the print spooler service, which starts during boot, must be restarted in order for them to run.(Citation: ESET PipeMon May 2020)

The print spooler service runs under SYSTEM level permissions, therefore print processors installed by an adversary may run under elevated privileges.

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## Kill Chain Phases

**•** mitre-attack: persistence

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

## Malware

* Gelsemium
* PipeMon

## APTs (Intrusion Sets)

* Earth Lusca