Boot or Logon Autostart Execution: Print Processors, Sub-technique T1547.012 - Enterprise

Archived: 2026-04-05 14:48:30 UTC

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.[1]

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 `AddPrintProcessor` API call with an account that has `SeLoadDriverPrivilege` enabled. Alternatively, a print processor can be registered to the print spooler service by adding the `HKLM\SYSTEM\[CurrentControlSet or ControlSet001]\Control\Print\Environments\[Windows architecture: e.g., Windows x64]\Print Processors\[user defined]\Driver` 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 `GetPrintProcessorDirectory` API call, or referenced via a relative path from this directory.[2] After the print processors are installed, the print spooler service, which starts during boot, must be restarted in order for them to run.[3]

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

Source: https://attack.mitre.org/techniques/T1547/012