Windows Detection Strategy for T1547.012 - Print Processor DLL Persistence, Detection Strategy DET0026

Archived: 2026-04-05 13:18:09 UTC

Analytics

- Windows

AN0074

Correlated registry modifications under Print Processors path, followed by DLL file creation within the system print processor directory, and DLL load by spoolsv.exe. Malicious execution often occurs during service restart or system boot, with SYSTEM-level privileges.

Log Sources

Mutable Elements

Field	Description
TimeWindow	Correlate Registry + DLL Write + Module Load within a short boot or spooler restart window (e.g., 5 minutes).
PrintProcessorDirectory	System-specific path derived from GetPrintProcessorDirectory API call; may differ across Windows versions or configurations.
DLLNamePattern	Some environments may use custom or non-standard DLL naming conventions for print processors. Allowlist known values.
SignedImageValidation	Check Authenticode signature and issuer chain for loaded DLLs to reduce false positives.
ServiceRestartTrigger	Monitor for spoolsv.exe restart events that trigger malicious print processor loading.