Detection Strategy for T1547.010 – Port Monitor DLL Persistence via spoolsv.exe (Windows), Detection Strategy DET0204

Archived: 2026-04-02 10:58:05 UTC

Analytics

- Windows

AN0580

Detects suspicious registry modifications under `HKLM\SYSTEM\CurrentControlSet\Control\Print\Monitors\*\Driver`, DLL loads by `spoolsv.exe` of non-standard or unsigned modules, and abnormal usage of the `AddMonitor` API by non-installation processes. This pattern often indicates an attempt to persist a malicious DLL via the print monitor mechanism, particularly when correlated with creation of files in `C:\Windows\System32` not tied to known patches or installations.

Log Sources

Mutable Elements

Field	Description
TargetDLLDirectory	Expected directory path for legitimate monitor DLLs (e.g., C:\Windows\System32)
SignedImageValidation	Enable/disable signature validation on DLLs loaded by spoolsv.exe
UserContextScope	Define whether only SYSTEM/user installs are expected to make changes to the port monitor registry keys
TimeWindow	Timeframe between registry modification and subsequent spoolsv.exe DLL load
AddMonitorCallContext	Filter on calling process of AddMonitor API to detect anomalies outside installer/updater

---