

# Detection of Windows Service Creation or Modification, Detection Strategy DET0552

Archived: 2026-04-05 18:45:12 UTC

## AN1527

Detects creation or modification of Windows Services through command-line tools (e.g., `sc.exe`, `powershell.exe`), Registry key changes under `HKLM\System\CurrentControlSet\Services`, and service execution under SYSTEM with unsigned or anomalous binary paths. Detects privilege escalation via driver installation or `CreateServiceW` usage. Correlates parent-child lineage, startup behavior, and rare service names.

### Log Sources

### Mutable Elements

Field	Description
ServiceNamePattern	Regex for suspicious or uncommon service names (e.g., <code>`svhstx`</code> , <code>`winhelp`</code> , etc.)
ImagePathFilter	Flag services whose image path resides in uncommon directories (e.g., <code>`C:\Users\`</code> , <code>`C:\Temp\`</code> )
DriverExtensionList	Watch for <code>`sys`</code> files loaded by <code>`sc`</code> , Registry, or <code>`ZwLoadDriver`</code> APIs
StartupTypeChangeWindow	Temporal window to correlate Registry <code>`Start`</code> key changes with service creation
UnsignedBinaryAlert	Raise alerts for unsigned binaries registered as services

---

Source: <https://attack.mitre.org/detectionstrategies/DET0552>