Detect Default File Association Hijack via Registry & Execution Correlation on Windows, Detection Strategy DET0061

Archived: 2026-04-05 14:21:03 UTC

AN0170

Detects modification of registry keys used for default file handlers, followed by anomalous process execution from user-initiated file opens. This includes tracking changes under HKCU and HKCR for file extension mappings, and correlating them with new or suspicious handler paths launching unusual child processes (e.g., PowerShell, cmd, wscript).

Log Sources

Mutable Elements

Field	Description
TimeWindow	Defines how long after the registry modification to correlate a suspicious process execution
UserContext	Tune to ignore known admin or installer behavior in specific user profiles
SuspiciousHandlerPathRegex	Pattern match for suspicious handler paths (e.g., powershell.exe, rundll32.exe)
