Detection Strategy for T1218.011 Rundll32 Abuse, Detection Strategy DET0475

Archived: 2026-04-02 12:08:44 UTC

AN1308

Detects rundll32.exe invoked with atypical arguments (.dll, .cpl, javascript:, mshtml). DLLs not normally loaded by rundll32 are mapped into memory. Control_RunDLL or RunHTMLApplication invoked. Suspicious DLLs or scripts accessed from disk or network. Rundll32 reaches out to external domains (e.g., fetching .sct or .hta).

Log Sources

Mutable Elements

Field	Description
TimeWindow	Correlating rundll32 invocation with DLL load or network activity within X seconds.
ParentProcessFilter	Limit detection to suspicious parent processes (e.g., explorer.exe, office apps) vs. trusted installers.
AllowedDLLs	Baseline list of legitimate DLLs frequently executed by rundll32 in the environment.
ExternalIPRange	Scope of external IP ranges considered anomalous for rundll32 network connections.
