Detection Strategy for System Binary Proxy Execution: Regsvr32, Detection Strategy DET0282

Archived: 2026-04-05 16:38:04 UTC

AN0785

Detection focuses on identifying anomalous regsvr32.exe executions that deviate from normal administrative or system use. Defenders may observe regsvr32.exe loading scriptlets or DLLs from unusual paths (especially temporary directories or remote URLs), command-line arguments invoking /i or /u with suspicious file references, network connections initiated by regsvr32.exe, and unsigned or untrusted DLLs being loaded shortly after regsvr32.exe invocation. Correlated sequences include regsvr32.exe process creation, module load of DLL/scriptlet, and optional outbound network traffic.

Log Sources

Mutable Elements

Field	Description
AllowedDLLPaths	Directories where DLL loading via regsvr32.exe is expected (e.g., C:\Windows\System32).
ScriptletExtensions	File extensions considered suspicious when executed by regsvr32.exe (e.g., .sct, .ocx).
TimeWindow	Timeframe to correlate regsvr32.exe process creation with subsequent module loads and network connections.
ParentProcessWhitelist	Parent processes from which regsvr32.exe is expected (e.g., explorer.exe during legitimate COM object registration).