Indirect Command Execution – Windows utility abuse behavior chain, Detection Strategy DET0200

Archived: 2026-04-05 16:01:17 UTC

AN0576

Cause→effect chain: (1) A user or service launches an indirection utility (e.g., forfiles.exe, pcalua.exe, wsl.exe, scriptrunner.exe, ssh.exe with -o ProxyCommand/LocalCommand). (2) That utility spawns a secondary program/command (PowerShell, cmd, msiexec, regsvr32, curl, arbitrary EXE) and/or opens outbound network connections. (3) Optional precursor modification of SSH config to persist LocalCommand/ProxyCommand. Correlate process creation, command/script content, file access to %USERPROFILE%.ssh\config, and network connections from the utility or its child.

Log Sources

Mutable Elements

Field	Description
TimeWindow	Correlation window between indirect launcher and spawned child/network activity (e.g., 10–30 minutes).
AllowedUtilities	Utilities permitted on admin/Jumphosts (forfiles, wsl, ssh) to reduce noise.
HighRiskChildren	Child images that indicate abuse (powershell.exe, cmd.exe, rundll32.exe, regsvr32.exe, mshta.exe, msiexec.exe, curl.exe, bitsadmin.exe).
UserContext	Raise severity when the actor is a standard/interactive user on a workstation rather than a server or CI agent.
DestCIDRs	Known-good egress networks for SSH/WSL activity to suppress expected admin automations.