Behavioral Detection of Windows Command Shell Execution, Detection Strategy DET0202

Archived: 2026-04-05 13:43:52 UTC

AN0578

Detects interactive or scripted abuse of cmd.exe, batch files, or shell invocation chains. Focuses on parent-child relationships (e.g., cmd.exe launched from unusual parents), anomalous command-line parameters, and chaining with discovery, credential access, or lateral movement behaviors.

Log Sources

Mutable Elements

Field	Description
ParentProcessName	Cmd.exe launched from uncommon parents (e.g., msedge.exe, winword.exe) may indicate abuse.
TimeWindow	Cmd or .bat execution during non-working hours may indicate automation or C2 activity.
CommandLinePattern	Flags suspicious switches (e.g., /c ping, /k whoami) or command chaining (&&, ^).
ScriptStoragePath	Batch file execution from %TEMP%, C:\Users\Public, or external drives.
UserContext	Flags admin-level users executing cmd outside expected baselines.

Source: https://attack.mitre.org/detectionstrategies/DET0202#AN0578