# Detecting Code Injection via mavinject.exe (App-V Injector), Detection Strategy DET0433

Archived: 2026-04-05 17:24:14 UTC

TimeWindow Correlation interval (e.g., 5–10 minutes) linking mavinject start → ProcessAccess → module load/network from the target process. DLLPathRegex Patterns for suspicious DLL locations (e.g., %TEMP%, Downloads, UNC shares) to reduce noise from legitimate injections. TargetProcessAllowList Common legitimate targets for App-V (if used) to suppress; flag unusual targets like browsers, LSASS, Winlogon, EDR processes. MinGrantedAccessSet Set of access rights that imply injection (VM_WRITE, VM_OPERATION, CREATE_THREAD). Tune for your EDR/sysmon formatting. ParentProcessFilter Legitimate parents starting mavinject (e.g., App-V services) vs. suspicious parents (Office, script hosts, browsers). ExternalIPAllowlist Known enterprise update/CDN ranges to exclude when correlating post-injection network activity. SignedToUnsignedTransition Alerting when Microsoft-signed mavinject leads to loading unsigned DLLs in a target process.

---