Detection Strategy for Event Triggered Execution via Trap (T1546.005), Detection Strategy DET0369

Archived: 2026-04-05 16:08:01 UTC

AN1038

Correlate file modifications in shell startup scripts (e.g., .bashrc, .profile) with embedded `trap` commands and observe if those changes are followed by the unexpected execution of child processes when terminal signals (e.g., SIGINT) are triggered. Use contextual linking with user session activity to detect privilege misuse.

Log Sources

Mutable Elements

Field	Description
TargetShellFilePath	The path to user profile scripts (e.g., ~/.bashrc, ~/.zshrc); may differ by distro or shell type.
SignalTrapName	Trap signal (e.g., INT, HUP, TERM) can be environment-specific or attacker-tuned to evade.
TimeWindow	Temporal threshold to correlate trap insertion and process execution (e.g., 10s-5min)

AN1039

Detect unauthorized `trap` command registrations in shell startup files (e.g., .zprofile, .bash_profile, .zshrc) followed by execution chains during user terminal interaction. Use Unified Logs and EDR telemetry to correlate shell command parsing and process tree anomalies.

Log Sources

Mutable Elements

Field	Description
LoginShellConfigPaths	Startup files vary by shell (.bash_profile, .zshrc, etc.)
TrapCommandLengthThreshold	Short benign traps may differ from longer/multi-command malicious traps

Field	Description
ParentProcessAnomalyThreshold	Score or detect if new child process deviates from shell’s typical behavior

---

Source: https://attack.mitre.org/detectionstrategies/DET0369