Detection Strategy for Exclusive Control, Detection Strategy DET0015

Archived: 2026-04-05 15:54:01 UTC

AN0045

Detects unusual command executions and service modifications that indicate self-patching or disabling of vulnerable services post-compromise. Defenders should monitor for service stop commands, suspicious process termination, and execution of binaries or scripts aligned with known patching or service management tools outside of expected admin contexts.

Log Sources

Mutable Elements

Field	Description
ServiceList	Tunable list of critical or vulnerable services that defenders want to monitor for unexpected disabling.
TimeWindow	Defines correlation window (e.g., 5–15 minutes) between suspicious command execution and subsequent process termination.

AN0046

Detects adversary attempts to monopolize control of compromised systems by issuing service stop commands, unloading vulnerable modules, or forcefully killing competing processes. Defenders should monitor audit logs and syslog for administrative utilities (systemctl, service, kill) being invoked outside of normal change management.

Log Sources

Mutable Elements

Field	Description
CriticalProcessList	Defines specific Linux daemons and processes that should not be terminated outside maintenance windows.
AdminUserContext	Defines expected accounts permitted to execute service stop commands; deviations may be suspicious.

AN0047

Detects unauthorized termination of system daemons or commands issued through launchctl or kill to stop competing services or malware processes. Defenders should monitor unified logs and EDR telemetry for unusual service modifications or terminations.

Log Sources

Data Component	Name	Channel
Command Execution (DC0064)	macos:unifiedlog	launchctl unload, kill, or pkill commands affecting daemons or background services
Process Termination (DC0033)	macos:osquery	process_termination: Unexpected termination of processes tied to vulnerable or high-value services

Mutable Elements

Field	Description
ProtectedServiceList	Defines macOS services (e.g., securityd, keychain-related daemons) that should never be disabled.
