Detection of Persistence Artifact Removal Across Host Platforms, Detection Strategy DET0040

Archived: 2026-04-05 12:46:43 UTC

AN0113

Detects adversary activity that removes persistence artifacts such as services, registry keys, scheduled tasks, user accounts, and binaries through commands like `sc delete`, `schtasks /delete`, or `reg delete`.

Log Sources

Mutable Elements

Field	Description
TargetRegistryPathRegex	Filters known persistence keys like Run/RunOnce, Image File Execution Options
DeletedScheduledTaskName	Monitors known or suspicious task names deleted post-persistence
DeletedAccountGroupScope	Focuses on highly privileged or recently created accounts

AN0114

Detects removal of persistence artifacts such as crontab entries, systemd service units, and malicious user accounts through commands like `crontab -r`, `rm /etc/systemd/system/*.service`, or `userdel`.

Log Sources

Mutable Elements

Field	Description
ServicePathMatch	Targets suspicious or orphaned unit files in /etc/systemd/system/
CronUserScope	Focus on crontab activity from root or uncommon users
UserDeletionActivity	Looks for userdel or passwd deletion

AN0115

Detects deletion of launch agents (~/Library/LaunchAgents/) and launch daemons (/Library/LaunchDaemons/), especially after suspicious process execution or when tied to known persistence methods.

Log Sources

Mutable Elements

Field	Description
LaunchDaemonPath	Common plist file paths for persistence: ~/Library/LaunchAgents/*.plist
CorrelatedProcessImage	Ties deletion to parent process (e.g., suspicious AppleScript runner)

AN0116

Detects adversary removal of persistence implants (e.g., rc.local entries or crontab injections) via CLI (`rm` , `sed` , `crontab -r`) and deletion of startup or management scripts.

Log Sources

Mutable Elements

Field	Description
ScriptRemovalPath	e.g., /etc/rc.local, /etc/init.d/custom.sh
StartupEntryClearance	Wipe or truncate of persistence locations

---

Source: https://attack.mitre.org/detectionstrategies/DET0040#AN0114