macOS Persistence Cheatsheet

v2.0 (20240420)

macOS 14 Sonoma · Apple Silicon (M1–M4) · Intel

Sections: Core Launch & Login Persistence · Authentication & Access Persistence · Shell & Scheduled Execution · Kernel, Extensions, Browser, Interpreter, and Handler Persistence · Persistence Adjacent & Legacy Mechanisms · Configuration Profiles & MDM

Legend: Common · Uncommon · Rare · Legacy · Deprecated · Requires root · Requires SIP off

Mechanisms

Sorted by frequency of observed persistence. Click any row for details.

Mechanism	Section	Requires root	Requires SIP off	Frequency
Launch Agents	Core Launch & Login Persistence	No	No	Common
Launch Daemons	Core Launch & Login Persistence	Yes	No	Common
Kernel extensions	Kernel, Extensions, Browser, Interpreter, and Handler Persistence	Yes	Yes	Rare
Login Items (legacy)	Core Launch & Login Persistence	No	No	Uncommon
Profile-delivered Wi-Fi	Configuration Profiles & MDM	Yes	No	Uncommon
Authorization plug-ins	Authentication & Access Persistence	Yes	Yes	Rare
Authorization DB rules	Authentication & Access Persistence	Yes	Yes	Rare
Login hooks	Shell & Scheduled Execution	Yes	No	Legacy
Startup hooks	Shell & Scheduled Execution	Yes	No	Legacy
Rc.local	Shell & Scheduled Execution	Yes	No	Legacy
Kernel boot-arg	Kernel, Extensions, Browser, Interpreter, and Handler Persistence	Yes	Yes	Legacy

Core Launch & Login Persistence

Mechanism	Requires root	Requires SIP off	Collection / Triage	Triage	What to review
Launch Agents	No	No	Artifacts: /Library/LaunchAgents ~/Library/LaunchAgents /Library/GroupContainers/*/Library/LaunchAgents Keywords: Program · ProgramArguments · RunAtLoad · KeepAlive · StartInterval · StartCalendarInterval · WatchPaths · QueueDirectories · MachServices · Sockets · LaunchEvents · ExitTimeOut · ThrottleInterval · EnvironmentVariables · UserName · GroupName · LimitLoadToSessionType · LimitLoadToHosts · LimitLoadToHardware · OnDemand · Disabled · ProcessType · Nice · StandardOutPath · StandardErrorPath · WorkingDirectory · Umask · SoftResourceLimits · HardResourceLimits · AssociatedBundleIdentifiers · ServiceIPC · EnablePressuredExit · EnableTransactions · LaunchOnlyOnce · MachRestartable · ProgramSearchPaths · ExecuteWithAsuid · SuidForDebugging · SessionCreate · LegacyTimers · AbandonProcessGroup · LowPriorityIO · LowPriorityBackgroundIO · MaterializeDatalessFiles · PreventSystemSleep · PreventDiskIdle · ExpectedRuntime · EnvironmentVariables.PATH · EnvironmentVariables.DYLD_* Commands: launchctl print gui/<uid>/<label> launchctl bootstrap gui/<uid> <plist> launchctl enable gui/<uid>/<label> launchctl kickstart -k gui/<uid>/<label> launchctl bootout gui/<uid> <plist> plutil -p <plist> codesign -dvvv --entitlements - <binary> spctl --assess --type execute --verbose=4 <binary> xattr -l <plist> find /Library/LaunchAgents ~/Library/LaunchAgents -name '*.plist' -mtime -7	Triage	
Launch Daemons	Yes	No	Artifacts: /Library/LaunchDaemons /Library/LaunchAgents /Library/PrivilegedHelperTools /Library/Preferences/com.apple.loginwindow.plist Keywords: Program · ProgramArguments · RunAtLoad · KeepAlive · StartInterval · StartCalendarInterval · WatchPaths · QueueDirectories · MachServices · Sockets · LaunchEvents · ExitTimeOut · ThrottleInterval · EnvironmentVariables · UserName · GroupName · LimitLoadToSessionType · LimitLoadToHosts · LimitLoadToHardware · OnDemand · Disabled · ProcessType · Nice · StandardOutPath · StandardErrorPath · WorkingDirectory · Umask · SoftResourceLimits · HardResourceLimits · AssociatedBundleIdentifiers · ServiceIPC · EnablePressuredExit · EnableTransactions · LaunchOnlyOnce · MachRestartable · ProgramSearchPaths · ExecuteWithAsuid · SuidForDebugging · SessionCreate · LegacyTimers · AbandonProcessGroup · LowPriorityIO · LowPriorityBackgroundIO · MaterializeDatalessFiles · PreventSystemSleep · PreventDiskIdle · ExpectedRuntime · EnvironmentVariables.PATH · EnvironmentVariables.DYLD_* Commands: launchctl print system/<label> launchctl bootstrap system <plist> launchctl enable system/<label> launchctl kickstart -k system/<label> launchctl bootout system <plist> plutil -p <plist> codesign -dvvv --entitlements - <binary> spctl --assess --type execute --verbose=4 <binary> xattr -l <plist> find /Library/LaunchDaemons -name '*.plist' -mtime -7	Triage	
Kernel extensions / Kext	Yes	Yes	Artifacts: /Library/Extensions /Library/Preferences/com.apple.kext.caches/Startup/KextPlist Keywords: BundleIdentifier · OSBundleRequired · IOKitPersonalities · IOPropertyMatch · IOProbeScore · IOClass · IOProviderClass · IOMatchCategory · IOUserClientClass · IOUserServerName · IOKitDebug · OSBundleLibraries · OSBundleCompatibleVersion · OSBundleMachOKernelVersion · NSPrincipalClass · CFBundleExecutable · CFBundleIdentifier · CFBundleVersion · CFBundleShortVersionString · CFBundleInfoDictionaryVersion · CFBundleSupportedPlatforms · DTPlatformName · DTSDKName · DTXcode · DTXcodeBuild · LSMinimumSystemVersion · LSMinimumSystemVersionByArchitecture · LSBundleLocalizations · CFBundleDevelopmentRegion · CFBundleSignature · CFBundleGetInfoString · CFBundleGetInfoHelpMap · CFBundleURLTypes · CFBundleURLSchemes · CFBundleURLIconFile · CFBundleURLName · CFBundleURLRole · CFBundleURLSchemeIsEditable · CFBundleURLSchemeIsHidden · CFBundleURLSchemeIsPrivate · CFBundleURLSchemeIsSecure · CFBundleURLSchemeIsSecureOnly · CFBundleURLSchemeIsSecureOnlyOnly · CFBundleURLSchemeIsSecureOnlyOnly · CFBundleURLSchemeIsSecureOnly

Shell & Scheduled Executor

Mechanism	Standard privilege	Source of truth	Enforcement/Usage	Trigger	What to review
Shell init (zsh) Global Shell · Zsh · Environment Defines an current exec(1)	Broad	Zsh	~/.zshenv, ~/.zprofile, ~/.zshrc, ~/.zlogin, ~/.zlogout Environment export PATH=/usr/local/bin:$PATH export EDITOR=vim export LANG=en_US.UTF-8 Aliases alias ll='ls -lFh --color=auto' alias grep='grep --color=auto' Functions mkcd() { mkdir -p "$1" && cd "$1" } Hooks precmd() { print -Pn "\e]2;%n@%m:%~\a" } Keybinds bindkey -e bindkey '^[[A' history-substring-search-up bindkey '^[[B' history-substring-search-down Completion autoload -Uz compinit compinit -d ~/.cache/zsh/zcompdump Plugins source ~/.zsh/plugins/zsh-autosuggestions/zsh-autosuggestions.zsh source ~/.zsh/plugins/zsh-syntax-highlighting/zsh-syntax-highlighting.zsh	Login shell Interactive shell shell-spawn	Aliases: Check for shadowing of common commands (ls, cd, rm, cat, grep, ssh, vim, etc.). Functions: Check for shadowing of common commands (ls, cd, rm, cat, grep, ssh, vim, etc.). Hooks: Check for expensive operations (slow prompt). Keybinds: Check for conflicts with vim-mode or custom widgets. Completion: Check for slow compinit (should use -C flag if cache is fresh). Plugins: Check for missing or broken plugin paths. Exec: Check for unexpected exec(1) calls (should be rare). Environment: Check for stale or incorrect PATH, EDITOR, LANG.
Shell init (bash) Global Shell · Bash · Environment Defines an current exec(1)	Broad	Bash	~/.bashrc, ~/.bash_profile, ~/.bash_login, ~/.profile, ~/.bash_logout Environment export PATH=/usr/local/bin:$PATH export EDITOR=vim export LANG=en_US.UTF-8 Aliases alias ll='ls -lFh --color=auto' alias grep='grep --color=auto' Functions mkcd() { mkdir -p "$1" && cd "$1" } Hooks PROMPT_COMMAND='printf "\033]2;%u@%h:%w\007"' Keybinds bind -m vi-insert '"\C-p": history-search-backward' bind -m vi-insert '"\C-n": history-search-forward' Completion source /usr/share/bash-completion/bash_completion Plugins source ~/.bash/plugins/bash-preexec.sh Exec exec /usr/local/bin/tmux -2 -u -f ~/.tmux.conf exec /usr/local/bin/fish -l -c 'tmux -CC attach -d -t main' Shell chsh -s /usr/local/bin/fish $USER Sudoers Defaults:%admin !tty_tickets Defaults:%admin timestamp_timeout=15	Login shell Interactive shell shell-spawn	Aliases: Check for shadowing of common commands (ls, cd, rm, cat, grep, ssh, vim, etc.). Functions: Check for shadowing of common commands (ls, cd, rm, cat, grep, ssh, vim, etc.). Hooks: Check for expensive operations (slow prompt). Keybinds: Check for conflicts with vim-mode or custom widgets. Completion: Check for missing bash-completion. Plugins: Check for missing or broken plugin paths. Exec: Check for unexpected exec(1) calls (should be rare). Environment: Check for stale or incorrect PATH, EDITOR, LANG. Sudoers: Check for overly broad %admin rules (should be limited to trusted users). Shell: Check for unexpected chsh changes (should be rare).
Cron Global Cron · Utility · All systems Runs tasks Runs tasks	Broad	Cron	/etc/crontab, /etc/cron.d/* Environment SHELL=/bin/sh PATH=/usr/local/bin:/usr/bin:/bin Variables MAILTO=root Tasks */5 * * * * root /usr/local/bin/health-check.sh --quiet 0 2 * * * root /usr/local/bin/backup.sh --incremental 0 3 * * 0 root /usr/local/bin/backup.sh --full Exec exec /usr/local/bin/health-check.sh --quiet exec /usr/local/bin/backup.sh --incremental Shell SHELL=/usr/local/bin/fish Sudoers Defaults:%admin !tty_tickets Defaults:%admin timestamp_timeout=15	Scheduled execution	Aliases: Check for shadowing of common commands (ls, cd, rm, cat, grep, ssh, vim, etc.). Variables: Check for stale or incorrect PATH, SHELL, MAILTO. Tasks: Check for missing or broken plugin paths. Exec: Check for unexpected exec(1) calls (should be rare). Shell: Check for unexpected chsh changes (should be rare). Sudoers: Check for overly broad %admin rules (should be limited to trusted users).
JS/Lua Global Shell · Unsupported · All systems Runs user-space daemons, can run as root Runs user-space daemons, can run as root	Broad	Node	~/.pm2/dump.pm2 Environment export NODE_ENV=production Exec exec /usr/local/bin/pm2 start ecosystem.config.js --no-daemon Shell SHELL=/usr/local/bin/fish Sudoers Defaults:%admin !tty_tickets Defaults:%admin timestamp_timeout=15	Shell spawn Interactive shell Scheduled execution	Aliases: Check for shadowing of common commands (ls, cd, rm, cat, grep, ssh, vim, etc.). Variables: Check for stale or incorrect PATH, SHELL, MAILTO. Tasks: Check for missing or broken plugin paths. Exec: Check for unexpected exec(1) calls (should be rare). Shell: Check for unexpected chsh changes (should be rare). Sudoers: Check for overly broad %admin rules (should be limited to trusted users).
Periodic Jobs Global System · Utility · All systems System scheduler	Broad	Mac	/Library/LaunchDaemons/com.company.backup.plist /Library/LaunchDaemons/com.company.cleanup.plist /Library/LaunchDaemons/com.company.monitor.plist /Library/LaunchAgents/com.company.sync.plist /Library/Scripts/backup.sh /Library/Scripts/cleanup.sh /Library/Scripts/monitor.sh /Library/Scripts/sync.sh /Library/Logs/com.company.backup.log /Library/Logs/com.company.cleanup.log /Library/Logs/com.company.monitor.log /Library/Logs/com.company.sync.log /var/log/system.log /var/log/kernel.log /var/log/install.log /var/log/wifi.log /var/log/secure.log /var/log/daily.out /var/log/weekly.out /var/log/monthly.out /var/log/cron.log /var/db/com.apple.xpc.launchd/disabled.501.plist /var/db/com.apple.xpc.launchd/disabled.plist Kernel extensions /Library/Extensions /System/Library/Extensions Kernel extensions (macOS 11+) /Library/SystemExtensions /var/db/SystemExtensions Profiles /Library/Managed Preferences /var/db/ConfigurationProfiles Auth plugins /Library/Security/SecurityAgentPlugins Authorization rights /var/db/auth.db Spotlight importers /Library/Spotlight /System/Library/Spotlight Quick Look generators /Library/QuickLook /System/Library/QuickLook Audio plug-ins /Library/Audio/Plug-Ins /System/Library/Audio/Plug-Ins Login items ~/Library/LaunchAgents/com.company.login.plist Shell SHELL=/usr/local/bin/fish Sudoers Defaults:%admin !tty_tickets Defaults:%admin timestamp_timeout=15	Daily / weekly / monthly / maintenance	Aliases: Check for shadowing of common commands (ls, cd, rm, cat, grep, ssh, vim, etc.). Variables: Check for stale or incorrect PATH, SHELL, MAILTO. Tasks: Check for missing or broken plugin paths. Exec: Check for unexpected exec(1) calls (should be rare). Shell: Check for unexpected chsh changes (should be rare). Sudoers: Check for overly broad %admin rules (should be limited to trusted users).
Calendar Alerts/Events Global Cron · Utility · All systems Calendar event alerts executed	Broad	Cron	/Library/Calendars/* /Library/Calendars/Calendar.sqlite /Library/Preferences/com.apple.ical.plist Exec exec /usr/local/bin/notify-calendar --lookahead 15m Shell SHELL=/usr/local/bin/fish Sudoers Defaults:%admin !tty_tickets Defaults:%admin timestamp_timeout=15	Event alerts / reminders	Aliases: Check for shadowing of common commands (ls, cd, rm, cat, grep, ssh, vim, etc.). Variables: Check for stale or incorrect PATH, SHELL, MAILTO. Tasks: Check for missing or broken plugin paths. Exec: Check for unexpected exec(1) calls (should be rare). Shell: Check for unexpected chsh changes (should be rare). Sudoers: Check for overly broad %admin rules (should be limited to trusted users).
Emacs Global Editor · Utility · Lib: emacsclient, lib Persistent Emacs	Broad	Emacs	~/.emacs.d/init.el ~/.emacs.d/early-init.el ~/.emacs.d/custom.el ~/.emacs.d/elpa/ ~/.emacs.d/lisp/ ~/.emacs.d/themes/ ~/.emacs.d/snippets/ ~/.emacs.d/eln-cache/ ~/.emacs.d/server/ ~/.emacs.d/auto-save-list/ ~/.emacs.d/backup/ ~/.emacs.d/bookmarks ~/.emacs.d/recentf ~/.emacs.d/savehist ~/.emacs.d/tramp ~/.emacs.d/transient/ ~/.emacs.d/eln-cache/*-*-*-*/*.eln Shell SHELL=/usr/local/bin/fish Sudoers Defaults:%admin !tty_tickets Defaults:%admin timestamp_timeout=15	Emacs startup Emacs shutdown Emacs idle Emacs frame focus Emacs buffer save Emacs buffer kill Emacs mode change Emacs idle timer Emacs daemon Emacs client Emacs package update Emacs package install Emacs package delete Emacs theme change Emacs server Emacs client Emacs process Emacs buffer Emacs frame Emacs window Emacs mode Emacs hook Emacs timer Emacs idle timer Emacs process filter Emacs process sentinel Emacs process output Emacs process input Emacs process exit Emacs process signal Emacs process status Emacs process buffer Emacs process mark

Application / daemon plug-ins

Allow Auth 30 minutes

Identity-aware plug-ins.

Application / daemon plug-ins

Allow Auth 30 minutes

Identity-aware plug-ins.

Application / daemon plug-ins

Allow Auth 30 minutes

Identity-aware plug-ins.

Application Support helpers

Deny Auth 30 minutes

Background helpers in user app support.

Application Support helpers

Deny Auth 30 minutes

Background helpers in user app support.

Application Support helpers

Deny Auth 30 minutes

Background helpers in user app support.

Application startup scripts

Allow Auth 30 minutes

Launch-at-login scripts.

Application startup scripts

Allow Auth 30 minutes

Launch-at-login scripts.

Application startup scripts

Allow Auth 30 minutes

Launch-at-login scripts.

App preference triggers

Deny Auth 30 minutes

Apps / formats preference rules.

App preference triggers

Deny Auth 30 minutes

Apps / formats preference rules.

App preference triggers

Deny Auth 30 minutes

Apps / formats preference rules.

Python Startup Hooks

Allow Auth 30 minutes

Site hooks.

Python Startup Hooks

Allow Auth 30 minutes

Site hooks.

Python Startup Hooks

Allow Auth 30 minutes

Site hooks.

LaunchServices URL Handlers

Allow Auth 30 minutes

Scheme ownership.

LaunchServices URL Handlers

Allow Auth 30 minutes

Scheme ownership.

LaunchServices URL Handlers

Allow Auth 30 minutes

Scheme ownership.

Input Methods / Input Sources

Allow Auth 30 minutes

Keyboard input sources.

Input Methods / Input Sources

Allow Auth 30 minutes

Keyboard input sources.

Input Methods / Input Sources

Allow Auth 30 minutes

Keyboard input sources.

Screen Saver bundles

Allow Auth 30 minutes

Legacy .saver bundles and Screen Saver extension modules.

Screen Saver bundles

Allow Auth 30 minutes

Legacy .saver bundles and Screen Saver extension modules.

Screen Saver bundles

Allow Auth 30 minutes

Legacy .saver bundles and Screen Saver extension modules.

Persistence Adjacent & Legacy Mechanisms

These may sit in a small review lane. Many of these are not persistence-adjacent mechanisms in the same sense as launchd, XPC, login items, or shell startup.

Mechanism	Scanned paths	Extension / Image	Trigger	What to review
Installer Packages Installer Allow Auth 30 minutes Package scripts.	/private/var/db/receipts/*.plist /private/var/db/receipts/*.bom /private/var/db/receipts/*.plist /private/var/db/receipts/*.bom	.pkg	Package installation	Installer packages can run preinstall and postinstall scripts as root. Receipts persist after the package is removed. Review recently installed packages, unsigned packages, and packages that add LaunchDaemons, helpers, or system-wide preferences.
Kernel Extensions / Activations / Quick Actions Kernel Allow Auth 30 minutes Legacy kernel extensions and Finder Quick Actions. Kernel extensions and Finder Quick Actions.	/Library/Extensions /System/Library/Extensions ~/Library/Services /Library/Services /System/Library/Services	.kext .workflow	Kernel loading, Finder Quick Actions invoked by user	Kernel extensions load into the kernel and can change system behavior. Review unsigned, third-party, or recently added kexts. Quick Actions run workflows from Finder menus.
Unix exec Rules (/opt/sbin/rpf-exec) Kernel Deny Auth 30 minutes Kernel-enforced exec allowlist. Kernel-enforced exec allowlist.	/opt/sbin/rpf-exec/rules.conf	Kernel exec allowlist	Every exec()	Kernel-enforced allowlist of binaries that may exec. Rules are matched against the exec path, SHA-256, and optional parent path. Review rules that allow broad directories or unsigned binaries.
TCC / Accessibility Grants Kernel Allow Auth 30 minutes Privacy grants that enable persistence. Privacy grants that enable persistence.	/Library/Application Support/com.apple.TCC/TCC.db ~/Library/Application Support/com.apple.TCC/TCC.db	Accessibility, Full Disk Access, Screen Recording, Input Monitoring, and related grants that enable persistence and telemetry.	Accessibility, Full Disk Access, Screen Recording, Input Monitoring, and related grants that enable persistence and telemetry.	Accessibility and Full Disk Access grants let apps control other apps and read protected data. Review recently granted, unexpected, or broad grants. Revoke stale grants for apps you no longer use.
DYLD_*/dylder/ / LaunchDaemon Kernel Allow Auth 30 minutes Dynamic library environment hacks.	/Library/LaunchDaemons /System/Library/LaunchDaemons /Library/Preferences/com.apple.dyld /Library/Caches/com.apple.dyld /Library/Dyld/dylder.conf	.plist .dylib .conf	Dynamic library loading, LaunchDaemon startup	Dylder configs and LaunchDaemons can inject libraries into processes. Review unexpected dylibs, broad dylder configs, and recently added LaunchDaemons.
Application / binary modifications Kernel Allow Auth 30 minutes Tamper and replacement.	/Applications /Library/Application Support /Library/Caches /Library/Preferences /Library/Logs /Library/Frameworks /Library/Extensions /Library/Services /Library/Dyld /Library/Caches/com.apple.dyld /Library/Preferences/com.apple.dyld /Library/Dyld/dylder.conf	.app .dylib .kext .plist .conf	Tamper and replacement	Tamper and replacement of system and third-party binaries, frameworks, and dylder configs. Review unexpected changes, broad writes, and recently modified system binaries.
LC_LOAD_DYLIB Addition Kernel Allow Auth 30 minutes Binary edit.	/Applications /Library/Application Support /Library/Caches /Library/Preferences /Library/Logs /Library/Frameworks /Library/Extensions /Library/Services /Library/Dyld /Library/Caches/com.apple.dyld /Library/Preferences/com.apple.dyld /Library/Dyld/dylder.conf	.app .dylib .kext .plist .conf	Tamper and replacement	Adding a new dylib load command to a Mach-O binary. Review unexpected changes, broad writes, and recently modified system binaries.

Apple Support helpers

Deny Auth 30 minutes

Background helpers in user app support.

Application startup scripts

Allow Auth 30 minutes

Launch-at-login scripts.

App preference triggers

Deny Auth 30 minutes

Apps / formats preference rules.

Python Startup Hooks

Allow Auth 30 minutes

Site hooks.

LaunchServices URL Handlers

Allow Auth 30 minutes

Scheme ownership.

Input Methods / Input Sources

Allow Auth 30 minutes

Keyboard input sources.

Screen Saver bundles

Allow Auth 30 minutes

Legacy .saver bundles and Screen Saver extension modules.

Kernel Extensions / Activations / Quick Actions

Allow Auth 30 minutes

Legacy kernel extensions and Finder Quick Actions.

Unix exec Rules (/opt/sbin/rpf-exec)

Deny Auth 30 minutes

Kernel-enforced exec allowlist.

TCC / Accessibility Grants

Allow Auth 30 minutes

Privacy grants that enable persistence.

DYLD_*/dylder/ / LaunchDaemon

Allow Auth 30 minutes

Dynamic library environment hacks.

Application / binary modifications

Allow Auth 30 minutes

Tamper and replacement.

LC_LOAD_DYLIB Addition

Allow Auth 30 minutes

Binary edit.

Dylib Hijacking / Proxying

Mac · Dylib

Detection: Monitor for unsigned or modified dylibs in DYLD_LIBRARY_PATH and DYLD_INSERT_LIBRARIES paths.

```
# Check for DYLD_INSERT_LIBRARIES in environment
launchctl getenv DYLD_INSERT_LIBRARIES

# Check for DYLD_LIBRARY_PATH
echo $DYLD_LIBRARY_PATH

# Find dylibs in suspicious locations
find /tmp /var/tmp /Users/Shared -name "*.dylib" -mtime -7

# Check for unsigned dylibs
for f in $(find /tmp -name "*.dylib"); do
  codesign -v "$f" 2>/dev/null || echo "$f: unsigned"
done

# Check loaded dylibs for unexpected paths
lsof -p <pid> | grac -E "\.dylib$"

# Monitor dylib loads via dtrace
dtrace -n 'pid$target:::dlopen { printf("%s", copyinstr(arg0)); }' -p <pid>
```

Login Hooks

Mac · Dylib

```
# Check current login hook
defaults read com.apple.loginwindow LoginHook

# Check logout hook
defaults read com.apple.loginwindow LogoutHook

# Check all loginwindow preferences
defaults read com.apple.loginwindow

# Check system-level login hooks
sudo defaults read /Library/Preferences/com.apple.loginwindow LoginHook

# Check user-level login hooks
defaults read ~/Library/Preferences/com.apple.loginwindow LoginHook

# Check if hooks are enabled
defaults read com.apple.loginwindow DoNotRunLoginHook

# Remove a login hook
defaults delete com.apple.loginwindow LoginHook

# Remove system-level hook
sudo defaults delete /Library/Preferences/com.apple.loginwindow LoginHook

# Check launchd agents that may be related
ls -la ~/Library/LaunchAgents/com.apple.loginwindow.plist

# Check for suspicious entries in loginwindow.plist
plutil -convert xml1 -o - ~/Library/Preferences/com.apple.loginwindow.plist | grep -A 2 LoginHook

# Check recent modifications to login hook files
find ~/Library/Preferences/com.apple.loginwindow.plist -mtime -7 -ls

# Check if loginwindow is running
ps aux | grep loginwindow

# Kill loginwindow to force reload
killall loginwindow

# Check for other persistence mechanisms that may be related
ls -la ~/Library/LaunchAgents/ | grep -i login
```

Startup Items

Mac · Rule

```
# Check /Library/StartupItems
ls -la /Library/StartupItems/

# Check /Library/Preferences/com.apple.loginwindow.plist
defaults read /Library/Preferences/com.apple.loginwindow

# Check StartupItems.plist
find /Library/StartupItems -name StartupItems.plist

# Check for executable files in StartupItems
find /Library/StartupItems -type f -perm -+x

# Check recent changes to StartupItems
find /Library/StartupItems -mtime -7 -ls

# Check if StartupItems are being processed
log show --predicate 'process == "SystemStarter"' --last 1d

# Check for suspicious StartupItems
for d in /Library/StartupItems/*; do
  [ -f "$d/StartupItems.plist" ] && echo "$d"
done
```

MC Scripts

Mac · Rule

```
# Check for MC scripts
ls -la ~/.zshrc ~/.zprofile ~/.zshenv ~/.zlogin ~/.zlogout

# Check for suspicious patterns
grep -E "(curl|wget|nc|ncat|bash -i|/dev/tcp|base64 -d|eval|exec)" ~/.zshrc ~/.zprofile ~/.zshenv ~/.zlogin ~/.zlogout

# Check recent modifications
find ~/ -name ".zshrc" -mtime -7 -ls

# Check for hidden files in home directory
find ~/ -name ".*" -mtime -7 -type f -ls

# Check for base64 encoded commands
grep -E "[A-Za-z0-9+/]{40}" ~/.zshrc ~/.zprofile ~/.zshenv ~/.zlogin ~/.zlogout

# Check for curl/wget to IP addresses
grep -E "(curl|wget).*[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}" ~/.zshrc ~/.zprofile ~/.zshenv ~/.zlogin ~/.zlogout

# Check for /dev/tcp usage
grep -E "/dev/tcp/" ~/.zshrc ~/.zprofile ~/.zshenv ~/.zlogin ~/.zlogout

# Check for eval/exec with variables
grep -E "(eval|exec).*\$" ~/.zshrc ~/.zprofile ~/.zshenv ~/.zlogin ~/.zlogout

# Check for nc/ncat usage
grep -E "(nc|ncat)" ~/.zshrc ~/.zprofile ~/.zshenv ~/.zlogin ~/.zlogout

# Check for python/perl/ruby one-liners
grep -E "(python|perl|ruby).*-[ce]" ~/.zshrc ~/.zprofile ~/.zshenv ~/.zlogin ~/.zlogout

# Check for mkfifo/mknod (reverse shell)
grep -E "(mkfifo|mknod)" ~/.zshrc ~/.zprofile ~/.zshenv ~/.zlogin ~/.zlogout

# Check for socat usage
grep -E "socat" ~/.zshrc ~/.zprofile ~/.zshenv ~/.zlogin ~/.zlogout

# Check for telnet usage
grep -E "telnet" ~/.zshrc ~/.zprofile ~/.zshenv ~/.zlogin ~/.zlogout

# Check for openssl s_client
grep -E "openssl s_client" ~/.zshrc ~/.zprofile ~/.zshenv ~/.zlogin ~/.zlogout

# Check for suspicious aliases
grep -E "^alias" ~/.zshrc ~/.zprofile ~/.zshenv ~/.zlogin ~/.zlogout | grep -E "(curl|wget|nc|bash|eval|exec|/dev/tcp|base64)"

# Check for suspicious functions
grep -E "^[a-zA-Z_]+\(\)" ~/.zshrc ~/.zprofile ~/.zshenv ~/.zlogin ~/.zlogout

# Check for suspicious PATH modifications
grep -E "^(export PATH|PATH=)" ~/.zshrc ~/.zprofile ~/.zshenv ~/.zlogin ~/.zlogout

# Check for suspicious environment variables
grep -E "^(export [A-Z_]+|[A-Z_]+=)" ~/.zshrc ~/.zprofile ~/.zshenv ~/.zlogin ~/.zlogout

# Check for suspicious sourcing
grep -E "^(source|\.) " ~/.zshrc ~/.zprofile ~/.zshenv ~/.zlogin ~/.zlogout

# Check for suspicious history manipulation
grep -E "(HISTFILE|HISTSIZE|HISTFILESIZE|HISTCONTROL|HISTIGNORE|HISTFORMAT|HISTTIMEFORMAT
```

Source
attack.mitre.org
Mechanisms
Emond
ATT&CK coverage for emond rules, queues, and event-driven actions on macOS.

Reviewed 2026-04

Source
attack.mitre.org
Mechanisms
Chromium Extensions
Firefox Extensions
ATT&CK coverage for browser extension persistence, including Chromium and Firefox profile or policy abuse.

Reviewed 2026-04

Source
attack.mitre.org
Mechanisms
Installer Packages
ATT&CK coverage for preinstall and postinstall execution paths that can drop or enable persistence.

Reviewed 2026-04

Source
attack.mitre.org
Mechanisms
Application / binary modification
ATT&CK technique for trojanized or modified host binaries that re-execute on normal app launch.

Reviewed 2026-04

Source
attack.mitre.org
Mechanisms
LC_LOAD_DYLIB Addition
ATT&CK mapping for malicious Mach-O load commands that force dylib execution on launch.

[S37]
Boot or Logon Initialization Scripts: Login Hook
MITRE ATT&CK · Reviewed 2026-04
Source
attack.mitre.org
Mechanisms
Login Hooks
ATT&CK coverage for loginwindow hook persistence and its privileged system-wide variant.

[S38]
Boot or Logon Initialization Scripts: Startup Items
MITRE ATT&CK · Reviewed 2026-04
Source
attack.mitre.org
Mechanisms
Startup Items
ATT&CK coverage for legacy StartupItems directories and their executable ordering model.

[S39]
Boot or Logon Initialization Scripts: RC Scripts
MITRE ATT&CK · Reviewed 2026-04
Source
attack.mitre.org
Mechanisms
RC Scripts
ATT&CK coverage for historical rc.local and rc.common execution paths on macOS.

[S40a]
Event Triggered Execution
MITRE ATT&CK · Reviewed 2026-04
Source
attack.mitre.org
Mechanisms
Mail.app Rules (AppleScript actions)
ATT&CK umbrella technique for event-triggered execution; Mail rules with AppleScript actions fit the pattern even though no dedicated sub-technique exists for Mail-rule abuse.

Community Research
2 sources

[S28d]
Folder Actions for Persistence on macOS
Community Research · Reviewed 2026-04
Source
specterops.io
Mechanisms
Folder Actions / Automator / Quick Actions
Defender-relevant research on Folder Actions as event-triggered persistence and the FolderActionsDispatcher preference state.

[S31]
Click File, App Opens
Community Research · Reviewed 2026-04
Source
objective-see.org
Mechanisms
LaunchServices / URL Handlers
Reverse-engineering write-up on Launch Services document-handler abuse for stealthy macOS persistence.

MDN Documentation
1 source

[S21d]
Native manifests
MDN Documentation · Reviewed 2026-04
Source
developer.mozilla.org
Mechanisms
Firefox Extensions
Adjacent pivot for Firefox extensions that use native messaging, managed storage, or PKCS#11 manifests on macOS.

Mozilla Documentation
1 source

[S21b]
Policy Templates for Firefox
Mozilla Documentation · Reviewed 2026-04
Source
mozilla.github.io
Mechanisms
Firefox Extensions
Official Firefox enterprise policy reference, including policies.json and ExtensionSettings. On macOS, policies.json is placed in Firefox.app/Contents/Resources/distribution.

Mozilla Support
2 sources

[S21a]
Deploy Firefox with extensions
Mozilla Support · Reviewed 2026-04
Source
support.mozilla.org
Mechanisms
Firefox Extensions
Official Mozilla enterprise deployment guidance for pre-installing extensions through the Firefox distribution/extensions directory.

[S21c]
Manage policies on macOS desktops
Mozilla Support · Reviewed 2026-04
Source
support.mozilla.org
Mechanisms
Firefox Extensions
macOS-specific Firefox policy support, including org.mozilla.firefox preference payloads and Firefox 64 / ESR 60.4 policy support.

Tool Documentation
4 sources

[S25]
KnockKnock
Tool Documentation · Reviewed 2026-04
Source
objective-see.org
Mechanisms
Application Support helpers
Defender-oriented catalogue of macOS persistence locations that is useful for user-space helper staging sweeps.

[S26]
KnockKnock
Tool Documentation · Reviewed 2026-04
Source
objective-see.org
Mechanisms
Application startup scripts
Useful operational reference when startup logic is hidden in app resources or user-scoped helper scripts.

[S27]
KnockKnock
Tool Documentation · Reviewed 2026-04
Source
objective-see.org
Mechanisms
App preference triggers
Helpful defender reference for preference-backed execution surfaces that are easy to miss in broad triage.

[S36a]
Dylib Hijack Scanner
Tool Documentation · Reviewed 2026-04
Source
objective-see.org
Mechanisms
Dylib Hijacking / Proxying
Practical defender reference for @rpath abuse, weak imports, and proxy dylib detection on macOS.

Vendor Documentation
11 sources

[S12b]
Use secure token, bootstrap token, and volume ownership in deployments
Vendor Documentation · Reviewed 2026-04
Source
support.apple.com
Mechanisms
Local accounts / hidden users / Remote Login
Apple deployment guidance for SecureToken, bootstrap token, and volume ownership context that helps DFIR assess durable account control and FileVault-adjacent access implications.

[S21e]
Native messaging
Vendor Documentation · Reviewed 2026-04
Source
developer.chrome.com
Mechanisms
Chromium Extensions
Official Chrome native messaging host reference. On macOS, host manifests live in fixed browser-specific system or user locations; the manifest maps a host name to an absolute native binary path, uses stdio transport, and restricts callers through allowed_origins.

[S21f]
Native messaging
Vendor Documentation · Reviewed 2026-04
Source
learn.microsoft.com
Mechanisms
Chromium Extensions
Microsoft Edge native messaging reference. Useful for Chromium-family DFIR because Edge uses its own macOS NativeMessagingHosts locations and the same host-manifest concepts: native binary path, stdio transport, and allowed extension origins.

[S30]
site - Site-specific configuration hook
Vendor Documentation · Reviewed 2026-04
Source
docs.python.org
Mechanisms
Python Startup Hooks
Official Python documentation for .pth files, sitecustomize.py, and usercustomize.py execution at interpreter start.

[S43]
Privacy Preferences Policy Control device management payload settings for Apple devices
Vendor Documentation · Reviewed 2026-04
Source
support.apple.com
Mechanisms
High-impact MDM payloads
Apple deployment reference for the com.apple.TCC.configuration-profile-policy payload, including service-specific allow or deny behavior and PPPC interpretation boundaries.

[S44]
Managed Login Items device management payload settings for Apple devices
Vendor Documentation · Reviewed 2026-04
Source
support.apple.com
Mechanisms
High-impact MDM payloads
Defines com.apple.servicemanagement managed login item rules and the matching keys used to auto-approve items.

[S45]
Manage login items and background tasks on Mac
Vendor Documentation · Reviewed 2026-04
Source
support.apple.com
Mechanisms
High-impact MDM payloads
Declarative Device Management / Managed background tasks
Operational guidance for background task management, rule matching, notifications, and sfltool or log-based validation on managed Macs.

[S46]
Certificates device management payload settings for Apple devices
Vendor Documentation · Reviewed 2026-04
Source
support.apple.com
Mechanisms
High-impact MDM payloads
Documents certificate payload identifiers that install roots, intermediates, or identities onto managed devices.

[S47]
Intro to certificate management for Apple devices
Vendor Documentation · Reviewed 2026-04
Source
support.apple.com
Mechanisms
High-impact MDM payloads
Explains certificate trust anchors, identities, and enterprise trust deployment through configuration profiles.

[S48]
Background task management declarative configuration for Apple devices
Vendor Documentation · Reviewed 2026-04
Source
support.apple.com
Mechanisms
Declarative Device Management / Managed background tasks
Apple deployment reference for macOS 15+ Declarative Device Management background task configuration, including MDM-delivered executables, scripts, and launchd configurations in managed service workflows.

[S48a]
Use declarative device management to manage Apple devices
Vendor Documentation · Reviewed 2026-04
Source
support.apple.com
Mechanisms
Declarative Device Management / Managed background tasks
Apple deployment overview for declarative device management, declarations, status reporting, and managed configuration context used to distinguish legitimate management state from suspicious policy-plane persistence.

macOS Automation
1 source

[S28c]
Automator Quick Actions
macOS Automation · Reviewed 2026-04
Source
macosxautomation.com
Mechanisms
Folder Actions / Automator / Quick Actions
Operational reference for Automator Quick Actions / Services workflows and their user-library Services integration.