macOS Persistence Cheatsheet

v1.1 (10/24/2026)

Filter: Root · Sudo · Auth · Cron · Login · Kext · Plist · Network · Config · Content · Exec · Sandbox · Signed · Unsigned · Apple · Third-Party

Legend: Root · Sudo · Auth · Signed · Unsigned · Apple · Third-Party

Mechanism

Click a card to jump to its section. Filters apply instantly. Use the chips above to narrow by tag, privilege, or keyword.

Core Launch & Login Persistence

launchd · Root · Sudo · Auth · Signed · Apple

Launch Agents — Root · Sudo · Plist

Per-user persistent daemons

Tags: user · persistent · session

Launch Daemons — Root · Sudo · Plist

Boot-time daemons

Tags: boot · persistent · system

launchd overrides / disabled agents — Root · Sudo · Persistence

Hidden persistence

Tags: persistence · hidden · system

BTM / SMAppService — Root · Sudo · Modern

macOS 13+ Background Task Management

Tags: modern · background · system

Login Items (legacy / classic) — Sudo · Auth · Persistence

Pre-Ventura login items

Tags: legacy · auth · persistence

Embedded Login Helpers — Sudo · Auth · Persistence

Supporting LaunchAgents or LSUIElement helpers

Tags: helper · nested · background · auth

Shell, Access, and Scheduled Execution

Shell init (zsh) — Root · Sudo · Persistence

Interactive or login zsh

Tags: login shell · interactive · shell · trigger

Shell init (bash) — Root · Sudo · Persistence

Interactive or login bash

Tags: login shell · interactive · shell · trigger

SSH authorized_keys — Sudo · Persistence

Remote access persistence

Tags: ssh · persistence · remote · access

Cron — Root · Sudo · Persistence

Legacy cron

Tags: legacy · persistence · scheduled

At / atrun — Root · Sudo · Persistence

Rarely used on modern systems, but still supported

Tags: legacy · persistence · scheduled

Periodic Jobs — Root · Sudo · Persistence

Scripted scheduled

Tags: legacy · scheduled · system

Emond — Root · Sudo · Persistence

Deprecated Network

Tags: legacy · deprecated · network

Extensions, Browser, Interpreter, and Handler Surfaces

System Extensions — Root · Sudo · Persistence

Signed system extensions

Tags: system · signed · kernel · network

Kext — Root · Sudo · Persistence

Legacy kernel extensions

Tags: legacy · kernel · signed · unsigned

XDATs — Root · Sudo · Persistence

Legacy Apple Extensions

Tags: legacy · signed · apple · extension

Python Startup Hooks — Root · Sudo · Persistence

Interpreter startup hooks

Tags: interpreter · startup · hook · persistence

LaunchServices URL / UTI Handlers — Root · Sudo · Persistence

Handler persistence

Tags: handler · persistence · system

Chromium Extensions — Sudo · Persistence

Browser plugins

Tags: browser · extension · persistence

Core Launch & Login Persistence

Mechanism	Required privilege	Scope of Trust	Plist	Collection / Triage	Trigger	What to review
Launch Agents launchd · Root · Sudo Sudo launchd	Root	Sudo	Plist	Artifacts / Data ~/Library/LaunchAgents/*.plist /Library/LaunchAgents/* /System/Library/LaunchAgents/* Relevance Plugins & Preferences(plist) Persistence Mechanism / Source of power Commands launchctl print gui/$(id -u) find ~/Library/LaunchAgents -name '*.plist' find /Library/LaunchAgents -maxdepth 1 -name '*.plist' plutil -p <plist> Tools launchctl print gui/$(id -u)/<label> launchctl bootout gui/$(id -u)/<label> plutil -p <plist>	User session	Review LaunchAgents Directory, Check Recent Modifications, Verify Ownership, Inspect Program Path, Check Arguments, Check Environment Variables, Review Persistence Mechanisms, Portfolio, Review, and Remediation Loop. Use `launchctl print gui/$(id -u)/<label>` to inspect a specific agent's runtime state. Any LaunchAgent plist dropped into `~/Library/LaunchAgents` or `/Library/LaunchAgents` runs at every login. Malware frequently uses this for persistence. Verify the ownership and permissions on the plist and the binary it points to. Unexpected agents in `~/Library/LaunchAgents` are a common persistence location. Cross-reference with Apple's default agents in `/System/Library/LaunchAgents` to spot anomalies.
Launch Daemons launchd · Root · Sudo Sudo launchd	Root	Sudo	Plist	Artifacts / Data /Library/LaunchDaemons/* /System/Library/LaunchDaemons/* Relevance Plugins & Preferences(plist) Persistence service endpoints and loaded binary path Commands find /Library/LaunchDaemons -maxdepth 1 -name '*.plist' plutil -p <plist> Tools launchctl print system/<label> launchctl bootout system/<label> plutil -p <plist>	Boot / pre-login	Review LaunchDaemons Directory, Check Recent Modifications, Verify Ownership, Inspect Program Path, Check Arguments, Check Environment Variables, Review Persistence Mechanisms, Portfolio, Review, and Remediation Loop. Use `launchctl print system/<label>` to inspect a specific daemon's runtime state. Any LaunchDaemon plist dropped into `/Library/LaunchDaemons` runs at boot with root privileges. Malware frequently uses this for persistence. Verify the ownership and permissions on the plist and the binary it points to. Unexpected daemons in `/Library/LaunchDaemons` are a common persistence location. Cross-reference with Apple's default daemons in `/System/Library/LaunchDaemons` to spot anomalies.
launchd overrides / disabled agents launchd · Root · Sudo Persistence	Root	Sudo	Persistence	Artifacts / Data /private/var/db/com.apple.xpcd/com.apple.xpcd.plist Relevance Persistence disabled / execution evade Commands find /var/db/com.apple.xpcd/ -name '*.plist' plutil -p /var/db/com.apple.xpcd/com.apple.xpcd.plist Tools launchctl print disabled system launchctl print disabled gui/$(id -u) Commands launchctl print system/<label> launchctl print gui/$(id -u)/<label> plutil -p <plist>	Persistence under service evade	Review Disabled Services, Check Recent Modifications, Verify Ownership, Inspect Program Path, Check Arguments, Check Environment Variables, Review Persistence Mechanisms, Portfolio, Review, and Remediation Loop. Use `launchctl print system/<label>` to inspect a specific service's runtime state. Entries in the disabled services database can persist long after the service has been removed and stay.
BTM / SMAppService macOS · Root · Sudo Modern · Background Task Management	Root	Sudo	Modern	Artifacts / Data /private/var/db/com.apple.backgroundtaskmanagement/BackgroundItems.btm /var/db/lsds/lsdsdb.sqlite Relevance Persistence / Persistence via Background Task Management Commands sqlite3 -header -column /private/var/db/com.apple.backgroundtaskmanagement/BackgroundItems.btm "select * from items;" Tools sqlite3 -header -column /private/var/db/com.apple.backgroundtaskmanagement/BackgroundItems.btm "select * from items;" Commands sqlite3 -header -column /private/var/db/lsds/lsdsdb.sqlite "select * from lsdbtable;" Tools sqlite3 -header -column /private/var/db/lsds/lsdsdb.sqlite "select * from lsdbtable;"	Modern	Review Background Items Database, Check Recent Modifications, Verify Ownership, Inspect Program Path, Check Arguments, Check Environment Variables, Review Persistence Mechanisms, Portfolio, Review, and Remediation Loop. Use `sqlite3 -header -column /private/var/db/com.apple.backgroundtaskmanagement/BackgroundItems.btm "select * from items;"` to inspect the BTM database. Entries in the BTM database can persist long after the service has stopped. Malware frequently uses this for persistence. Verify the ownership and permissions on the database. Unexpected entries in `/private/var/db/com.apple.backgroundtaskmanagement/BackgroundItems.btm` are a common persistence location. Cross-reference with Apple's default entries in `/private/var/db/lsds/lsdsdb.sqlite` to spot anomalies.
Login Items (legacy / classic) Sudo · Auth · Persistence Pre-Ventura login items	Sudo	Auth	Persistence	Commands sqlite3 -header -column ~/Library/Application\ Support/com.apple.TCC/TCC.db "select * from access where service='kTCCServiceAppleEvents';" Tools sqlite3 -header -column ~/Library/Application\ Support/com.apple.TCC/TCC.db "select * from access where service='kTCCServiceAppleEvents';" Commands osascript -e 'tell application "System Events" to get properties of login item "<name>"' plutil -p ~/Library/Logs/com.crowd.Macs.plist Tools osascript -e 'tell application "System Events" to get properties of login item "<name>"' plutil -p ~/Library/Logs/com.crowd.Macs.plist	Legacy auth	Review Legacy Login Items, Check Recent Modifications, Verify Ownership, Inspect Program Path, Check Arguments, Check Environment Variables, Review Persistence Mechanisms, Portfolio, Review, and Remediation Loop. Use `osascript -e 'tell application "System Events" to get properties of login item "<name>"'` to inspect a specific login item's runtime state. Legacy login items are stored in `~/Library/Application Support/com.apple.TCC/TCC.db` and persist across reboots. Malware frequently uses this for persistence. Review the TCC database for unexpected entries. Cross-reference with Apple's default entries to spot anomalies.
Embedded Login Helpers Sudo · Auth · Persistence Supporting LaunchAgents or LSUIElement helpers	Sudo	Auth	Persistence	Commands /bin/ls -R /Applications/*.app/Contents/Library/LoginItems/* Tools /bin/ls -R /Applications/*.app/Contents/Library/LoginItems/* Commands /usr/bin/find /Applications -name "*.app" -exec ls -d {}/Contents/Library/LoginItems/* \; Tools /usr/bin/find /Applications -name "*.app" -exec ls -d {}/Contents/Library/LoginItems/* \;	Legacy auth · nested · background	Review Embedded Login Helpers, Check Recent Modifications, Verify Ownership, Inspect Program Path, Check Arguments, Check Environment Variables, Review Persistence Mechanisms, Portfolio, Review, and Remediation Loop. Use `/usr/bin/find /Applications -name "*.app" -exec ls -d {}/Contents/Library/LoginItems/* \;` to inspect embedded login helpers. Embedded helpers can persist independently of their parent app. Malware frequently uses this for persistence. Review the contents of each app's `Contents/Library/LoginItems` directory. Cross-reference with Apple's default helpers to spot anomalies.

Shell, Access, and Scheduled Execution

Mechanism	Required privilege	Scope of Trust	Plist	Collection / Triage	Trigger	What to review
Shell init (zsh) macOS · Current default Default on current macOS	Root	Sudo	Persistence	Artifacts / Data /etc/zshenv /etc/zprofile /etc/zshrc /etc/zlogin ~/.zshenv ~/.zprofile ~/.zshrc ~/.zlogin Relevance Commands executed in the interactive shell PROTOCOL\ENVIRONMENT\Shell Extensions / Interaction Commands /usr/bin/grep -E '^[^#]*(|;|&&|||`|\$\(|||

Safari App Extensions

macOS · Safari 15.4+

Modern, App-distributed Safari extension

Artifact	Path	Notes
Extension manifest	`<App>.app/Contents/Resources/manifest.plist`	
Extension binary	`<App>.app/Contents/MacOS/<app_name>`	
Extension bundle	`~/Library/Safari/Extensions/<app_name>.safariextz`	

Persistence

```
defaults read <app_name>
defaults read com.<vendor>.<app_name>
ls -la ~/Library/Safari/Extensions/
```

Detection

```
pgrep -f "<app_name>"
pgrep -f "<app_name>.app/Contents/MacOS"
ls -la ~/Library/Safari/Extensions/
```

Impact

```
<app_name>.app: <app_name>
~/Library/Safari/Extensions/<app_name>.safariextz
com.<vendor>.<app_name>
```

Remediation

```
open -a <app_name> && pkill -9 -f "<app_name>"
rm -rf <app_name>.app
rm ~/Library/Safari/Extensions/<app_name>.safariextz
defaults delete com.<vendor>.<app_name>
```

Verify

```
pgrep -f "<app_name>"
ls -la ~/Library/Safari/Extensions/
```

Safari Web Extensions

macOS · Safari 15.4+

Cross-browser WebExtension

Artifact	Path	Notes
Extension manifest	`<App>.app/Contents/Resources/manifest.plist`	
Extension binary	`<App>.app/Contents/MacOS/<app_name>`	
Extension bundle	`~/Library/Safari/Extensions/<app_name>.safariextz`	

Persistence

```
defaults read <app_name>
defaults read com.<vendor>.<app_name>
ls -la ~/Library/Safari/Extensions/
```

Detection

```
pgrep -f "<app_name>"
pgrep -f "<app_name>.app/Contents/MacOS"
ls -la ~/Library/Safari/Extensions/
```

Impact

```
<app_name>.app: <app_name>
~/Library/Safari/Extensions/<app_name>.safariextz
com.<vendor>.<app_name>
```

Remediation

```
open -a <app_name> && pkill -9 -f "<app_name>"
rm -rf <app_name>.app
rm ~/Library/Safari/Extensions/<app_name>.safariextz
defaults delete com.<vendor>.<app_name>
```

Verify

```
pgrep -f "<app_name>"
ls -la ~/Library/Safari/Extensions/
```

Application / document plug-ins

Windows · Mac · Linux

Browsers, office suites, media plug-ins

Artifact	Path	Notes
Plug-in binary	`%ProgramFiles%\Mozilla\plugins\<name>.dll`	
Plug-in binary	`%ProgramFiles(x86)%\Mozilla\plugins\<name>.dll`	
Plug-in binary	`%ProgramFiles%\Common Files\Microsoft Shared\Office<NN>\plugins\<name>.dll`	
Plug-in binary	`%ProgramFiles(x86)%\Common Files\Microsoft Shared\Office<NN>\plugins\<name>.dll`	
Plug-in binary	`%ProgramFiles%\Microsoft Office\Office<NN>\Bin\<name>.dll`	
Plug-in binary	`%ProgramFiles(x86)%\Microsoft Office\Office<NN>\Bin\<name>.dll`	
Plug-in binary	`%ProgramFiles%\Microsoft Office\Office<NN>\Bin\Addins\<name>.dll`	
Plug-in binary	`%ProgramFiles(x86)%\Microsoft Office\Office<NN>\Bin\Addins\<name>.dll`	
Plug-in binary	`%ProgramFiles%\Microsoft Office\Office<NN>\Bin\Extensibility\<name>.dll`	
Plug-in binary	`%ProgramFiles(x86)%\Microsoft Office\Office<NN>\Bin\Extensibility\<name>.dll`	
Plug-in binary	`%ProgramFiles%\Microsoft Office\Office<NN>\Bin\Office Shared Add-Ins\<name>.dll`	
Plug-in binary	`%ProgramFiles(x86)%\Microsoft Office\Office<NN>\Bin\Office Shared Add-Ins\<name>.dll`	
Plug-in binary	`%ProgramFiles%\Microsoft Office\Office<NN>\Bin\Office Shared Add-Ins\Extensibility\<name>.dll`	
Plug-in binary	`%ProgramFiles(x86)%\Microsoft Office\Office<NN>\Bin\Office Shared Add-Ins\Extensibility\<name>.dll`	
Plug-in binary	`%ProgramFiles%\Microsoft Office\Office<NN>\Bin\Office Shared Add-Ins\Extensibility\Microsoft Shared\<name>.dll`	
Plug-in binary	`%ProgramFiles(x86)%\Microsoft Office\Office<NN>\Bin\Office Shared Add-Ins\Extensibility\Microsoft Shared\<name>.dll`	
Plug-in binary	`%ProgramFiles%\Microsoft Office\Office<NN>\Bin\Office Shared Add-Ins\Extensibility\Microsoft Shared\Office Shared Add-Ins\<name>.dll`	
Plug-in binary	`%ProgramFiles(x86)%\Microsoft Office\Office<NN>\Bin\Office Shared Add-Ins\Extensibility\Microsoft Shared\Office Shared Add-Ins\<name>.dll`	
Plug-in binary	`%ProgramFiles%\Microsoft Office\Office<NN>\Bin\Office Shared Add-Ins\Extensibility\Microsoft Shared\Office Shared Add-Ins\Microsoft Shared\<name>.dll`	
Plug-in binary	`%ProgramFiles(x86)%\Microsoft Office\Office<NN>\Bin\Office Shared Add-Ins\Extensibility\Microsoft Shared\Office Shared Add-Ins\Microsoft Shared\<name>.dll`	
Plug-in binary	`%ProgramFiles%\Microsoft Office\Office<NN>\Bin\Office Shared Add-Ins\Extensibility\Microsoft Shared\Office Shared Add-Ins\Microsoft Shared\Office<NN>\<name>.dll`	
Plug-in binary	`%ProgramFiles(x86)%\Microsoft Office\Office<NN>\Bin\Office Shared Add-Ins\Extensibility\Microsoft Shared\Office Shared Add-Ins\Microsoft Shared\Office<NN>\<name>.dll`	
Plug-in binary	`%ProgramFiles%\Microsoft Office\Office<NN>\Bin\Office Shared Add-Ins\Extensibility\Microsoft Shared\Office Shared Add-Ins\Microsoft Shared\Office<NN>\Addins\<name>.dll`	
Plug-in binary	`%ProgramFiles(x86)%\Microsoft Office\Office<NN>\Bin\Office Shared Add-Ins\Extensibility\Microsoft Shared\Office Shared Add-Ins\Microsoft Shared\Office<NN>\Addins\<name>.dll`	
Plug-in binary	`%ProgramFiles%\Microsoft Office\Office<NN>\Bin\Office Shared Add-Ins\Extensibility\Microsoft Shared\Office Shared Add-Ins\Microsoft Shared\Office<NN>\Extensibility\<name>.dll`	
Plug-in binary	`%ProgramFiles(x86)%\Microsoft Office\Office<NN>\Bin\Office Shared Add-Ins\Extensibility\Microsoft Shared\Office Shared Add-Ins\Microsoft Shared\Office<NN>\Extensibility\<name>.dll`	
Plug-in binary	`%ProgramFiles%\Microsoft Office\Office<NN>\Bin\Office Shared Add-Ins\Extensibility\Microsoft Shared\Office Shared Add-Ins\Microsoft Shared\Office<NN>\Extensibility\Microsoft Shared\<name>.dll`	
Plug-in binary	`%ProgramFiles(x86)%\Microsoft Office\Office<NN>\Bin\Office Shared Add-Ins\Extensibility\Microsoft Shared\Office Shared Add-Ins\Microsoft Shared\Office<NN>\Extensibility\Microsoft Shared\<name>.dll`	
Plug-in binary	`%ProgramFiles%\Microsoft Office\Office<NN>\Bin\Office Shared Add-Ins\Extensibility\Microsoft Shared\Office Shared Add-Ins\Microsoft Shared\Office<NN>\Extensibility\Microsoft Shared\Office<NN>\<name>.dll`	
Plug-in binary	`%ProgramFiles(x86)%\Microsoft Office\Office<NN>\Bin\Office Shared Add-Ins\Extensibility\Microsoft Shared\Office Shared Add-Ins\Microsoft Shared\Office<NN>\Extensibility\Microsoft Shared\Office<NN>\<name>.dll`	

Persistence

```
dir /s /b "%ProgramFiles%\Mozilla\plugins\*.dll"
dir /s /b "%ProgramFiles(x86)%\Mozilla\plugins\*.dll"
dir /s /b "%ProgramFiles%\Common Files\Microsoft Shared\Office<NN>\plugins\*.dll"
dir /s /b "%ProgramFiles(x86)%\Common Files\Microsoft Shared\Office<NN>\plugins\*.dll"
dir /s /b "%ProgramFiles%\Microsoft Office\Office<NN>\Bin\*.dll"
dir /s /b "%ProgramFiles(x86)%\Microsoft Office\Office<NN>\Bin\*.dll"
dir /s /b "%ProgramFiles%\Microsoft Office\Office<NN>\Bin\Addins\*.dll"
dir /s /b "%ProgramFiles(x86)%\Microsoft Office\Office<NN>\Bin\Addins\*.dll"
dir /s /b "%ProgramFiles%\Microsoft Office\Office<NN>\Bin\Extensibility\*.dll"
dir /s /b "%ProgramFiles(x86)%\Microsoft Office\Office<NN>\Bin\Extensibility\*.dll"
dir /s /b "%ProgramFiles%\Microsoft Office\Office<NN>\Bin\Office Shared Add-Ins\*.dll"
dir /s /b "%ProgramFiles(x86)%\Microsoft Office\Office<NN>\Bin\Office Shared Add-Ins\*.dll"
dir /s /b "%ProgramFiles%\Microsoft Office\Office<NN>\Bin\Office Shared Add-Ins\Extensibility\*.dll"
dir /s /b "%ProgramFiles(x86)%\Microsoft Office\Office<NN>\Bin\Office Shared Add-Ins\Extensibility\*.dll"
dir /s /b "%ProgramFiles%\Microsoft Office\Office<NN>\Bin\Office Shared Add-Ins\Extensibility\Microsoft Shared\*.dll"
dir /s /b "%ProgramFiles(x86)%\Microsoft Office\Office<NN>\Bin\Office Shared Add-Ins\Extensibility\Microsoft Shared\*.dll"
dir /s /b "%ProgramFiles%\Microsoft Office\Office<NN>\Bin\Office Shared Add-Ins\Extensibility\Microsoft Shared\Office Shared Add-Ins\*.dll"
dir /s /b "%ProgramFiles(x86)%\Microsoft Office\Office<NN>\Bin\Office Shared Add-Ins\Extensibility\Microsoft Shared\Office Shared Add-Ins\*.dll"
dir /s /b "%ProgramFiles%\Microsoft Office\Office<NN>\Bin\Office Shared Add-Ins\Extensibility\Microsoft Shared\Office Shared Add-Ins\Microsoft Shared\Office<NN>\*.dll"
dir /s /b "%ProgramFiles(x86)%\Microsoft Office\Office<NN>\Bin\Office Shared Add-Ins\Extensibility\Microsoft Shared\Office Shared Add-Ins\Microsoft Shared\Office<NN>\*.dll"
dir /s /b "%ProgramFiles%\Microsoft Office\Office<NN>\Bin\Office Shared Add-Ins\Extensibility\Microsoft Shared\Office Shared Add-Ins\Microsoft Shared\Office<NN>\Addins\*.dll"
dir /s /b "%ProgramFiles(x86)%\Microsoft Office\Office<NN>\Bin\Office Shared Add-Ins\Extensibility\Microsoft Shared\Office Shared Add-Ins\Microsoft Shared\Office<NN>\Addins\*.dll"
dir /s /b "%ProgramFiles%\Microsoft Office\Office<NN>\Bin\Office Shared Add-Ins\Extensibility\Microsoft Shared\Office Shared Add-Ins\Microsoft Shared\Office<NN>\Extensibility\*.dll"
dir /s /b "%ProgramFiles(x86)%\Microsoft Office\Office<NN>\Bin\Office Shared Add-Ins\Extensibility\Microsoft Shared\Office Shared Add-Ins\Microsoft Shared\Office<NN>\Extensibility\*.dll"
```

Detection

```
pgrep -f "<name>.dll"
```

Impact

```
<name>.dll
```

Remediation

```
pkill -9 -f "<name>.dll"
rm -rf <name>.dll
```

Verify

```
pgrep -f "<name>.dll"
```

Python Startup Hooks

CPU · Windows · Mac · Linux

Mac, Windows

Artifact	Path	Notes
Python startup hook	`<python_prefix>/lib/python<version>/sitecustomize.pyc`	
Python startup hook	`<python_prefix>/lib/python<version>/sitecustomize.pyo`	

01 Unified Logs for launch activity, especially suspicious launchd labels, repeated failures, and unexpected restarts.

02 backgroundtaskmanagementagent and related BTM records when Login Items or helpers look inconsistent with the installed app set.

03 sysextd, systemextensionsctl output, and approval-related records when a system extension or driver stack is in scope.

04 install.log and package provenance when preinstall / postinstall or helper deployment appears to have introduced persistence.

05 sshd logs plus auth context for unexpected authorized_keys changes, custom AuthorizedKeysFile usage, or unusual remote access timing.

06 Signer, Team ID, notarization, quarantine xattrs, mtime / birthtime, and first-seen telemetry to validate whether the artifact matches its claimed parent app or install flow.