User Execution – multi-surface behavior chain (documents/links → helper/unpacker → LOLBIN/child → egress), Detection Strategy DET0478

Archived: 2026-04-05 13:21:02 UTC

AN1314

Cause→effect chain: (1) User-facing app (Office/PDF/archiver/browser) records an open/click or abnormal event, then (2) a downloaded file is created in a user-writable path and/or decompressed, (3) the parent user app spawns a living-off-the-land binary (e.g., powershell/cmd/mshta/rundll32/msiexec/wscript/expand/zip) or installer, and (4) immediate outbound HTTP(S)/DNS/SMB from the same lineage.

Log Sources

Mutable Elements

Field	Description
TimeWindow	Correlation window (e.g., 15 minutes) from document open to child/egress.
HighRiskParents	Apps that should rarely spawn OS utilities (winword.exe, excel.exe, powerpnt.exe, acrord32.exe, chrome/msedge/firefox, 7zFM.exe, winrar.exe, explorer.exe).
HighRiskChildren	LOLBIN list: powershell.exe, cmd.exe, wscript.exe, cscript.exe, mshta.exe, rundll32.exe, regsvr32.exe, msiexec.exe, curl.exe, bitsadmin.exe, pcalua.exe, expand.exe, tar.exe.
UserPaths	Writable paths to watch: %USERPROFILE%\Downloads, %TEMP%, %APPDATA%*, OneDrive/Teams cache, Office startup folders.
EgressAllowList	Corporate update/CDN domains and proxy egress CIDRs to suppress benign updater traffic.

AN1315

Cause→effect chain: (1) User app/browser/archiver logs an open/click or abnormal exit, (2) new executable/script/archive extracted into $HOME/Downloads, /tmp, or ~/.cache, (3) parent app spawns shell/interpreter (bash/sh/python/node/curl/wget) or desktop file, and (4) new outbound connection(s) from the child lineage.

Log Sources

Mutable Elements

Field	Description
TimeWindow	5–20 minute correlation window.
UserPaths	$HOME/Downloads, /tmp, ~/.cache, ~/.config/autostart, ~/.local/share.
HighRiskChildren	bash, sh, zsh, python*, perl, node, curl, wget, xdg-open, kde-open, gio open, unzip/tar extraction leading to exec.
PkgUpdaters	Allow-list snap/flatpak/packagekit/apt workers to reduce false positives.

AN1316

Cause→effect chain: (1) unified logs show application open/click or crash for Safari/Chrome/Office/Preview/archiver, (2) file write/extraction into ~/Downloads, /private/var/folders/* or ~/Library, (3) parent app spawns osascript/bash/zsh/curl/python or opens a quarantined app with Gatekeeper prompts, (4) network egress from child.

Log Sources

Mutable Elements

Field	Description
TimeWindow	10–30 minute correlation window.
HighRiskChildren	osascript, bash, zsh, curl, python, open -a Terminal, installer, tccutil misuse.
QuarantineSignals	Flag new apps lacking com.apple.quarantine or with quarantine='0081' (downloaded then auto-opened).

AN1317

Cause→effect chain in CI/dev desktops: (1) user triggers container run/pull after opening a doc/link/script, (2) newly created image/container uses unexpected external registry or entrypoint, (3) container starts and immediately egresses to suspicious destinations.

Log Sources

Mutable Elements

Field	Description
TrustedRegistries	Approved registries/namespaces.

Field	Description
AllowedEntrypoints	Expected CMD/ENTRYPOINT for known images.
TimeWindow	Correlate user action → docker/podman run within 10 minutes.

AN1318

Cause→effect chain in cloud consoles: (1) user clicks link then invokes instance/image creation via API, (2) instance/image originates from external AMI or unknown image, (3) instance immediately egresses or retrieves payloads.

Log Sources

Mutable Elements

Field	Description
ApprovedImages	AMI/image allow-list with owners.
UserContext	High-risk identities (federated, external IdP).
TimeWindow	5–30 minutes from console/API action to network egress.
