Exploitation for Client Execution – cross-platform behavior chain (browser/Office/3rd-party apps), Detection Strategy DET0287

Archived: 2026-04-05 13:10:01 UTC

AN0797

Cause→effect chain: (1) A client app (browser, Office, PDF/Flash/reader) experiences a crash/abnormal exit or loads from an unusual location, then (2) drops or modifies a file in user-writable paths, and/or (3) spawns an unexpected child (e.g., powershell/cmd/mshta/rundll32/wscript/installer), and (4) establishes outbound C2-like connections shortly after. Correlate application logs, file writes, process lineage, and network egress within a short window.

Log Sources

Mutable Elements

Field	Description
TimeWindow	Correlation window (e.g., 15m) between crash/write/child/network.
HighRiskChildren	List of child processes that should rarely spawn from Office/browsers (powershell.exe, cmd.exe, wscript.exe, mshta.exe, rundll32.exe, regsvr32.exe, msiexec.exe, curl.exe).
UserPaths	Writable paths to watch (Downloads, %TEMP%, %APPDATA%, OneDrive, Office startup folders).
AllowedPlugins	Known add-ins/extensions and updater binaries to reduce noise.
EgressAllowlist	Known update/CDN domains and proxy egress CIDRs for suppression.

AN0798

Cause→effect chain: (1) Browser/Office/reader process logs crash/segfault or abnormal sandbox message, (2) new executable/script/write occurs in $HOME (Downloads, ~/.cache, /tmp), (3) unexpected child like curl/wget/bash/python opens network connections soon after.

Log Sources

Mutable Elements

Field	Description
TimeWindow	5–20m correlation window.
UserPaths	HOME write targets: ~/Downloads, ~/.config/autostart, ~/.local/share, /tmp.
HighRiskChildren	bash, sh, python, perl, node, curl, wget, socat, openssl, xxd.
PackageUpdaters	Allow-list common updaters (snap, flatpak, packagekit) to reduce FP.

AN0799

Cause → effect chain: (1) App crash/abnormal termination in unified logs for Safari/Chrome/Office/Preview, (2) new files/scripts in ~/Library, ~/Downloads, /private/var/folders/*, (3) unexpected child (osascript, zsh, bash, curl) spawned by those apps, (4) new outbound connections.

Log Sources

Mutable Elements

Field	Description
TimeWindow	10–30m correlation window.
HighRiskChildren	osascript, bash, zsh, curl, python, pbpaste/pbcopy, open -a Terminal.
UserPaths	~/Library/LaunchAgents, ~/Library/Containers/*/Data, /private/var/folders/*.
QuarantineBypass	Flag files with missing com.apple.quarantine extended attribute when sourced from internet.
