Detect User Activity Based Sandbox Evasion via Input & Artifact Probing, Detection Strategy DET0420

Archived: 2026-04-05 12:58:22 UTC

AN1182

Process execution that probes user activity artifacts (e.g., desktop files, registry history) following recent user login/unlock events.

Log Sources

Mutable Elements

Field	Description
TimeWindow	Window between user unlock and access to user history
UserContext	Focus on non-system accounts doing user activity probing

AN1183

Access to shell history or GUI input state (xdotool, xinput) for presence validation prior to payload execution.

Log Sources

Mutable Elements

Field	Description
ArtifactCountThreshold	Number of distinct user files accessed before trigger
KnownToolSignatures	Suppress expected automation tools

AN1184

API usage or filesystem access revealing user state or browser artifacts (e.g., Safari bookmarks, CGEventState).

Log Sources

Data Component	Name	Channel
OS API Execution (DC0021)	macos:unifiedlog	Execution of input detection APIs (e.g., CGEventSourceKeyState)
File Access (DC0055)	macos:unifiedlog	Access to ~/Library/Safari/Bookmarks.plist or recent files

Mutable Elements

Field	Description
TimeWindow	Temporal correlation between login and file access
UserContext	Exclude expected UI activity from login agents

Source: https://attack.mitre.org/detectionstrategies/DET0420#AN1182