Detection of Application Window Enumeration via API or Scripting, Detection Strategy DET0097

Archived: 2026-04-05 15:52:44 UTC

AN0271

Processes using Win32 API calls (e.g., EnumWindows, GetForegroundWindow) or scripting tools (e.g., PowerShell, VBScript) to enumerate open windows. These often appear with reconnaissance or data collection TTPs.

Log Sources

Mutable Elements

Field	Description
AccessedFunction	Tune to focus on suspicious function calls (e.g., user32.dll!EnumWindows).
UserContext	Detect behavior from non-interactive or low-privileged users where enumeration is uncommon.
TimeWindow	Shorten detection scope to rapid successive window enumeration attempts.

AN0272

Scripted or binary usage of X11 utilities (e.g., xdotool, wmctrl) or direct /proc/*/window mappings to discover open GUI windows and active desktops.

Log Sources

Mutable Elements

Field	Description
ExecutableName	Common window management utilities can be tuned to reduce noise (e.g., xprop, xwininfo).
DisplayContext	Restrict detection to processes executing under graphical sessions (e.g., DISPLAY=:0).

AN0273

Processes that utilize AppleScript, `CGWindowListCopyWindowInfo`, or `NSRunningApplication` APIs to list active application windows and foreground processes.

Log Sources

Mutable Elements

Field	Description
AppleScriptTarget	Tunable to ignore benign scripting like automation by known apps.
ParentProcess	Useful to suppress expected automation processes.

Source: https://attack.mitre.org/detectionstrategies/DET0097