Behavioral Detection of Keylogging Activity Across Platforms, Detection Strategy DET0089

Archived: 2026-04-05 18:15:41 UTC

AN0243

Monitors suspicious usage of Windows API calls like SetWindowsHookEx, GetKeyState, or polling functions within non-UI service processes, combined with Registry or driver modifications.

Log Sources

Mutable Elements

Field	Description
TargetImage	Scope to sensitive GUI/session processes like winlogon.exe or osk.exe
AccessMask	Can be tuned to 0x1fffff for full-access injection detection
TimeWindow	Tunable for sustained polling or multiple registry edits in short succession

AN0244

Detects non-system processes accessing /dev/input/* or issuing ptrace/evdev syscalls used for reading keystroke buffers directly.

Log Sources

Mutable Elements

Field	Description
ProcessName	Exclude known good applications (e.g. Xorg, GNOME Shell)
DevicePath	Typically /dev/input/event*, but tunable to match custom input buses

AN0245

Detects unauthorized TCC access or use of Quartz Event Services (CGEventTapCreate) or IOHID for event tap installation within unexpected processes.

Log Sources

Mutable Elements

Field	Description
Service	com.apple.inputmonitoring, com.apple.accessibility, etc.
ExecutablePath	Tunable to exclude trusted endpoint monitoring tools

AN0246

Keylogging on legacy network devices via unauthorized system image modification or remote capture of console keystrokes (telnet, SSH) through altered firmware or man-in-the-middle key sniffing.

Log Sources

Mutable Elements

Field	Description
FirmwareVersion	Baseline hash or expected version for config/image integrity
Protocol	Scope to plaintext channels or low-assurance SSH versions

---