Detection Strategy for MFA Interception via Input Capture and Smart Card Proxying, Detection Strategy DET0246

Archived: 2026-04-05 16:25:41 UTC

AN0687

Behavior chain involving unexpected API calls to capture keyboard input, driver loads for keyloggers, or remote use of smart card authentication via logon sessions not initiated by local user interaction

Log Sources

Mutable Elements

Field	Description
AccessMask	Tunable based on what memory-level access the keylogger uses (e.g., 0x10 for read)
ProcessNameExclusions	Legitimate accessibility tools may use similar API calls (e.g., Magnifier.exe)
TimeWindow	Define how quickly access + registry mod + smart card use must co-occur

AN0688

Detection of unauthorized keylogger behavior through access to `/dev/input`, loading kernel modules (e.g., via insmod), or polling user input devices from non-user shells

Log Sources

Mutable Elements

Field	Description
PathTarget	Can tune based on device paths accessed for keyboard input (e.g., /dev/input/event0)
UserContext	Exclude root or admin-auth shell sessions if needed
ModuleWhitelist	Set a known list of allowed kernel modules

AN0689

Processes accessing TCC-protected input APIs or polling HID services without user interaction, or dynamically loaded keylogging frameworks using accessibility privileges

Log Sources

Mutable Elements

Field	Description
AccessibilityAPIUsage	Detection of programs requesting access to input monitoring (e.g., CGEventTap)
TCCBypassAttempt	Alert if TCC settings are altered or bypassed
SignedBinaryCheck	Tunable based on developer signing status (legitimate software vs unsigned)
