Behavioral Detection Strategy for T1123 Audio Capture Across Windows, Linux, macOS, Detection Strategy DET0221

Archived: 2026-04-05 18:06:52 UTC

AN0619

Unusual or unauthorized processes accessing microphone APIs (e.g., winmm.dll, avrt.dll) followed by audio file writes to user-accessible or temp directories.

Log Sources

Mutable Elements

Field	Description
TimeWindow	Time span in which the process accesses audio APIs and writes files, to reduce false positives.
TargetProcess	Set of approved processes known to legitimately use microphone (e.g., Zoom, Teams).
WriteDirectory	Allowlist of paths where legitimate apps store audio (e.g., user media folders).

AN0620

Processes accessing ALSA/PulseAudio devices or executing audio capture binaries like 'arecord', followed by file creation or suspicious child process spawning.

Log Sources

Mutable Elements

Field	Description
ExecutableName	Capture binaries like arecord, parecord, or ffmpeg.
DevicePath	Log attempts to access /dev/snd/*, /dev/dsp, /proc/asound/*.
UserContext	Whether the user has audio access rights or is running under elevated privileges.

AN0621

Processes invoking AVFoundation or CoreAudio frameworks, accessing input devices via TCC logs or Unified Logs, followed by writing AIFF/WAV/MP3 files to disk.

Log Sources

Mutable Elements

Field	Description
FrameworkCall	CoreAudio vs. AVFoundation vs. lower-level device access APIs.
TargetDirectory	Suspicious file drops (e.g., ~/Library/Caches/, /tmp/, nonstandard user folders).
AnomalousParent	Unexpected parent-child relationship between non-media apps and AV capture.
