# Behavior-chain, platform-aware detection strategy for T1125 Video Capture, Detection Strategy DET0197

Archived: 2026-04-05 16:52:39 UTC

### AN0568

A non-standard process (or script-hosted process) loads camera/video-capture libraries (e.g., avicap32.dll, mf.dll, ksproxy.ax), opens the Camera Frame Server/device, writes video/image artifacts (e.g., .mp4/.avi/.yuv) to unusual locations, and optionally initiates outbound transfer shortly after.

#### Log Sources

#### Mutable Elements

| Field | Description |
|---|---|
| TimeWindow | Correlation window (e.g., 0–20 minutes) between device access, file creation, and egress. |
| AllowedProcesses | Known legitimate camera consumers (e.g., Teams.exe, zoom.exe, obs64.exe) to suppress. |
| VideoExtensions | List of extensions to flag (.mp4, .avi, .mov, .yuv, .mkv, .h264) – tune for your estate. |
| RarePathRegex | Regex for unusual storage locations (e.g., %TEMP%*, C:\Windows\Tasks*, user profile hidden dirs). |
| MinFileSizeMB | Minimum size to reduce FP from thumbnails/snapshots. |
| ParentProcessAllowList | Service/agent parents permitted to broker camera access. |

### AN0569

A process opens/reads /dev/video* (V4L2), performs ioctl/read loops, writes large/continuous video artifacts to disk, and/or quickly establishes outbound connections for exfiltration.

#### Log Sources

#### Mutable Elements

| Field | Description |
| --- | --- |
| SyscallSet | Which syscalls to audit (openat, read, ioctl) – performance sensitive. |
| AllowedCallers | Legitimate processes (e.g., motion, Zoom, Chrome) that access /dev/video*. |
| VideoExtensions | List of file extensions to flag (.mp4/.avi/.mov/.mkv/.yuv/.h264). |
| MinContinuousReadCount | Minimum read/ioctl count to infer continuous capture. |
| TimeWindow | Correlate device open → file write → network exfil (e.g., 30m). |

**AN0570**

A non-whitelisted process receives TCC camera entitlement (kTCCServiceCamera), opens AppleCamera/AVFoundation device handles, writes .mov/.mp4 artifacts to unusual locations, and/or beacons/exfiltrates soon after.

**Log Sources**

| Data Component | Name | Channel |
| --- | --- | --- |
| OS API Execution (DC0021) | macos:unifiedlog | Access decisions to kTCCServiceCamera for unexpected binaries |
| File Access (DC0055) | macos:endpointsecurity | open: Process opens AppleCamera/IOUSB device nodes or AVFoundation frameworks |
| Process Creation (DC0032) | macos:endpointsecurity | exec: Exec of ffmpeg, avfoundation-based binaries, or custom signed apps accessing camera |
| File Creation (DC0039) | macos:unifiedlog | Process wrote large .mov/.mp4 in user temp/hidden dirs |

**Mutable Elements**

| Field | Description |
| --- | --- |
| TCCAllowList | Legitimate apps (Zoom, Teams, FaceTime) that are permitted to camera. |
| VideoExtensions | Mov/mp4/mkv/yuv etc., tuned to environment workloads. |
| TimeWindow | Correlation between TCC grant → file write → network egress. |
| MinFileSizeMB | Reduce FP from thumbnails/snapshots. |
| LaunchAgentPaths | Allowed persistence paths to reduce false positives when correlating with persistence. |

Source: https://attack.mitre.org/detectionstrategies/DET0197#AN0569