Detect Remote Access via USB Hardware (TinyPilot, PiKVM), Detection Strategy DET0159

Archived: 2026-04-05 16:01:45 UTC

AN0446

Detection of USB-based remote access hardware (e.g., TinyPilot, PiKVM) attached to the host via drive or peripheral enumeration, triggering vendor identifiers or unusual EDID announcements.

Log Sources

Mutable Elements

Field	Description
VendorID	Device vendor strings may need tuning to include additional remote hardware sources.
SerialNumber	Serial numbers for known implants can vary per campaign and may need expansion.
TimeWindow	Adjust the detection window for peripheral enumeration based on environment and operating hours.

AN0447

Insertion of USB-based hardware proxies (e.g., PiKVM) which register under predictable names (e.g., tinypilot) or mount under known paths (e.g., /opt/tinypilot-privileged).

Log Sources

Data Component	Name	Channel
Drive Creation (DC0042)	auditd:SYSCALL	udev events or drive enumeration involving TinyPilot paths or device classes

Mutable Elements

Field	Description
FriendlyName	Different hardware may present differently; names like 'TinyPilot' may need expanding to cover custom implants.
MountPath	Path matching (e.g., /opt/tinypilot) is mutable based on distro, customization, and staging.

AN0448

Attachment of hardware-backed USB KVM devices (e.g., TinyPilot) that enumerate new HID or serial communication interfaces with identifiable metadata.

Log Sources

Data Component	Name	Channel
Drive Creation (DC0042)	macos:unifiedlog	Hardware enumeration events via IOKit or USBMuxd showing TinyPilot or unknown keyboard/mouse

Mutable Elements

Field	Description
DeviceClass	Input or HID devices may be benign or malicious depending on context; tune based on environment (e.g., BYOD/dev stations).
SerialCorrelationDepth	Correlating serials across multiple device insertions may reduce noise but requires tuning.
