Cross-host C2 via Removable Media Relay, Detection Strategy DET0090

Archived: 2026-04-02 12:20:54 UTC

AN0247

Behavioral sequence where removable media is mounted, files are written/updated, and subsequently read/executed on a separate host, suggesting removable-media relay communication.

Log Sources

Mutable Elements

Field	Description
RemovableDriveLetter	Adjust drive letters used in detection (e.g., E:, F:, G:) depending on enterprise usage.
WriteToReadTimeWindow	Tunable window for file write on one host followed by file read or execution on another (e.g., within 10 minutes).
FileNamePattern	Common naming schemes for payload, tasking, or exfil files (e.g., task.txt, beacon.log, data.bin).

AN0248

Detection of file write-access to USB-mount directories (e.g., /media/, /run/media/) followed by same-file access or execution on another host.

Log Sources

Mutable Elements

Field	Description
MountPathPattern	Typical mount paths to monitor (e.g., /media/usb*, /run/media/username/*).
TimeWindowBetweenHosts	Tunable detection window to correlate read/write between different hosts within a short interval (e.g., <15m).

AN0249

Correlates removable volume mounts (disk arbitration) with file I/O events on that volume, followed by same file execution shortly after insert.

Log Sources

Mutable Elements

Field	Description
VolumeNameFilter	Known suspicious USB volume labels or types (e.g., NO NAME, SECUREDATA).
ProcessContext	Unusual processes accessing USB drives (e.g., bash, Python, unsigned binaries).
