Detection of Exfiltration Over Alternate Network Interfaces, Detection Strategy DET0077

Archived: 2026-04-02 10:39:13 UTC

AN0212

Execution of file transfer or network access activity through non-primary interfaces (e.g., WiFi, Bluetooth, cellular) by processes not typically associated with such behavior (e.g., rundll32, powershell, regsvr32).

Log Sources

Mutable Elements

Field	Description
InterfaceType	Filter for specific interface categories (e.g., WiFi, Bluetooth, 4G).
FileSizeThreshold	Tunable for environment-specific large file access events pre-transfer.
TimeWindow	Temporal correlation window for file read followed by network activity.

AN0213

Use of `rfkill`, `nmcli`, or low-level tools (e.g., `iw`, `hcitool`, `pppd`) to enable alternate interfaces followed by data transfer via non-primary NICs.

Log Sources

Mutable Elements

Field	Description
CommandPattern	Match known interface manipulation utilities or driver invocations.
NetworkDevice	Tunable to non-default or rarely used interfaces (e.g., wlan1, hci0).

AN0214

AppleScript or system calls to activate WiFi/Bluetooth interfaces (`networksetup`, `blueutil`), followed by exfiltration via AirDrop, cloud sync, or network socket.

Log Sources

Mutable Elements

Field	Description
Protocol	Protocol used for exfil (e.g., AirDrop, mDNS, Apple File Service).
InterfaceActivityWindow	Time period between interface activation and transfer.

Source: https://attack.mitre.org/detectionstrategies/DET0077#AN0212