Behavioral Detection of Fallback or Alternate C2 Channels, Detection Strategy DET0499

Archived: 2026-04-05 18:07:02 UTC

AN1376

Establishing network connections on uncommon ports or protocols following C2 disruption or blocking. Often executed by processes that typically exhibit no network activity.

Log Sources

Mutable Elements

Field	Description
DestinationPort	Can be tuned to include unexpected or high-entropy ports not typically associated with the process.
ProcessName	Useful to filter benign applications vs suspicious fallback attempts.
DataVolumeRatio	Tunable ratio of sent/received bytes to indicate potential C2 beaconing or exfiltration.
TimeWindow	Adjust temporal window to match likely fallback C2 retries after primary channel fails.

AN1377

Creation of outbound connections on alternate ports or using covert transport (e.g., ICMP, DNS) from non-network-intensive processes, following known disruption or blocked traffic.

Log Sources

Mutable Elements

Field	Description
ProtocolType	Can filter for rare fallback channel types (e.g., ICMP, DNS over HTTP).
UserContext	Tuning by user (e.g., root vs. service account) helps suppress noise.

AN1378

Outbound fallback traffic from low-profile or background launch agents using unusual protocols or destinations after primary channel inactivity.

Log Sources

Mutable Elements

Field	Description
LaunchAgentContext	Used to suppress known legitimate agents.
PayloadEntropy	Can help isolate covert or encrypted fallback traffic.

AN1379

Outbound traffic from host management services or guest-to-host interactions over unusual interfaces (e.g., backdoor API endpoints or external VPN tunnels).

Log Sources

Mutable Elements

Field	Description
InterfaceName	May vary based on ESXi build and should be filtered to suppress known interfaces.
FallbackIPRanges	Environment-specific ranges to ignore (e.g., DR tunnels or out-of-band mgmt).
