Detecting Junk Data in C2 Channels via Behavioral Analysis, Detection Strategy DET0011

Archived: 2026-04-05 12:47:16 UTC

AN0030

Processes generating large outbound connections with disproportionate send/receive ratios, often to uncommon ports or hosts, potentially inserting meaningless data into protocol payloads.

Log Sources

Mutable Elements

Field	Description
PayloadEntropyThreshold	Tunable threshold for Shannon entropy of network payloads.
TimeWindow	Duration of outbound data transfer to evaluate disproportionate upload size.
UserContext	Filter based on user accounts allowed to generate outbound traffic.

AN0031

Outbound traffic with anomalous payload sizes and patterns from non-networking processes, often observed via packet inspection or connection logs.

Log Sources

Mutable Elements

Field	Description
EntropyScore	Adjust based on expected entropy of typical outbound data.
ProcessWhitelist	Exclude known good binaries that generate high network output.
DataRatioThreshold	Minimum ratio of bytes_sent to bytes_received.

AN0032

Previously unseen applications generating outbound connections with atypical data flow characteristics, such as excessive data with no return response.

Log Sources

Mutable Elements

Field	Description
ParentProcessCheck	Allow filtering based on parent-child relationship for benign services.
HostWhitelist	Known legitimate C2-like patterns (e.g., Apple telemetry).

AN0033

Anomalous traffic from ESXi host management daemons (like hostd or vpxa) embedding non-standard payloads in management protocols (e.g., HTTPS) or beaconing behavior.

Log Sources

Mutable Elements

Field	Description
TLSFingerprintMismatch	Detects mismatched TLS client behavior vs expected for hostd/vpxa.
UnusualDestinationPorts	Highlight traffic from ESXi hosts to uncommon ports outside vCenter ranges.
