Detection Strategy for Data Encoding in C2 Channels, Detection Strategy DET0108

Archived: 2026-04-05 14:24:23 UTC

AN0302

Atypical processes (e.g., powershell.exe, regsvr32.exe) encode large outbound traffic using Base64 or other character encodings; this traffic is sent over uncommon ports or embedded in protocol fields (e.g., HTTP cookies or headers).

Log Sources

Mutable Elements

Field	Description
PayloadEntropyThreshold	Adjust to accommodate legitimate compression or encryption patterns in normal web traffic
ProcessAllowlist	Define expected processes initiating outbound traffic to reduce false positives
AnomalyScoreThreshold	Set threshold for how far traffic deviates from baseline protocol structure or size

AN0303

Custom scripts or processes encode outbound traffic using gzip, Base64, or hex prior to exfiltration via curl, wget, or custom sockets. Encoding typically occurs before or during outbound connections from non-network daemons.

Log Sources

Mutable Elements

Field	Description
TimeWindow	Tune duration of multi-stage encoding + transfer operations to account for script variability
UserContext	Apply user allow/block list depending on which users normally perform CLI encoding

AN0304

Processes use built-in encoding utilities (e.g., `base64`, `xxd`, or `plutil`) to encode file contents followed by HTTP/HTTPS transfer via curl or custom applications.

Log Sources

Mutable Elements

Field	Description
EncodedCommandLengthThreshold	Minimum byte size of encoded strings to treat as suspicious
SuspiciousProcessChainDepth	Number of chained processes within a short window to treat as a correlated behavior

AN0305

ESXi daemons (e.g., hostd, vpxa) are wrapped or impersonated to send large outbound traffic using gzip/Base64 encoding over SSH or HTTP. These actions follow suspicious logins or shell access.

Log Sources

Mutable Elements

Field	Description
AuthSourceTrustLevel	Use to scope encoded traffic suspicion to accounts that should not initiate transfers
ExfilBurstThreshold	Threshold for bursty outbound traffic size deviation from baseline

---