# Behavior-chain detection for T1132.002 Data Encoding: Non-Standard Encoding across Windows, Linux, macOS, ESXi, Detection Strategy DET0326

Archived: 2026-04-05 13:57:20 UTC

### AN0927

A process/script constructs or references a custom/alphabet translation table (e.g., 64/85/32+ arbitrary chars, XOR/base-N loops) or emits long high-entropy strings that do NOT validate as standard Base64/Hex → shortly after, the same process (or its child) generates outbound traffic with asymmetric bytes_out:bytes_in, fixed-size beacons, or protocol/header mismatches (e.g., Content-Type says JSON but body fails JSON parse / contains non-standard alphabet).

#### Log Sources

#### Mutable Elements

| Field | Description |
|---|---|
| EntropyThreshold | Minimum Shannon entropy for the suspected token/payload (e.g., >4.8). |
| TokenLengthThreshold | Minimum continuous token length to treat as potential non-standard payload (e.g., ≥120 chars). |
| BytesOutToInRatio | Out:In ratio considered suspicious (e.g., ≥4:1). |
| FixedPacketStdDevThreshold | Std. dev. threshold (size or interval) to mark packets as 'uniform' (beacon-like). |
| TimeWindow | Correlation window from encode routine to egress (default 10m). |
| KnownLegitEncoders | Legitimate in-house/custom encoders to suppress. |

### AN0928

Shell scripts or binaries implement custom mapping tables (tr/sed/awk/golang/rust/python encode loops), or emit long high-entropy tokens that fail Base64/Hex validation → correlated with egress showing asymmetric flow, protocol-mismatch payloads, or DNS/HTTP bodies containing low-diversity-but-long custom alphabets.

#### Log Sources

#### Mutable Elements

| Field | Description |
| --- | --- |
| EntropyThreshold | Payload entropy minimum. |
| TokenLengthThreshold | Length threshold for suspect tokens. |
| BytesOutToInRatio | Asymmetry cutoff for flows. |
| TimeWindow | Correlation join window. |
| KnownEncoders | Legitimate internal tools/agents. |

**AN0929**

EndpointSecurity/Unified Logs show processes generating custom alphabets or long high-entropy, non-standard tokens → network logs (PF/Zeek/EDR) show asymmetric beacons, protocol mismatches, or periodic fixed-size posts.

**Log Sources**

**Mutable Elements**

| Field | Description |
| --- | --- |
| EntropyThreshold | Payload entropy minimum. |
| TokenLengthThreshold | Minimum suspicious token length. |
| BytesOutToInRatio | Asymmetry threshold. |
| TimeWindow | Correlation window. |
| AllowedSignedBinaries | Signed binaries that legitimately implement custom encoders. |

**AN0930**

ESXi shell or scripts produce long, high-entropy tokens (non-standard alphabets) in shell.log/hostd, followed by outbound flows (NSX/Zeek) with asymmetric ratios or protocol mismatches to non-management endpoints.

**Log Sources**

**Mutable Elements**

| Field | Description |
| --- | --- |
| MgmtCIDRs | CIDRs allowed for normal ESXi mgmt/backup. |
| BytesOutToInRatio | Asymmetry cutoff (e.g., ≥3). |

| Field | Description |
| --- | --- |
| TokenLengthThreshold | Minimum token length. |
| TimeWindow | Correlation window. |

---

Source: https://attack.mitre.org/detectionstrategies/DET0326#AN0927