Data Encoding: Non-Standard Encoding, Sub-technique T1132.002 - Enterprise

Archived: 2026-04-05 13:13:26 UTC

ID	Name	Analytic ID	Analytic Description
DET0326	Behavior-chain detection for T1132.002 Data Encoding: Non-Standard Encoding across Windows, Linux, macOS, ESXi	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).
		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.
		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.
		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.