Detection Strategy for Encrypted Channel via Symmetric Cryptography across OS Platforms, Detection Strategy DET0143

Archived: 2026-04-05 18:24:46 UTC

AN0400

Processes that typically do not perform cryptographic operations loading symmetric encryption libraries (e.g., bcryptprimitives.dll, aes.dll), then initiating outbound connections with high-entropy payloads. Defender correlates process creation, DLL load, and anomalous encrypted traffic patterns.

Log Sources

Mutable Elements

Field	Description
AllowedCryptoProcesses	Processes normally expected to use symmetric crypto (e.g., disk encryption, secure messaging).
EntropyThreshold	Minimum payload entropy score for flagging unusual encrypted sessions.
TimeWindow	Correlation window between module load and encrypted connection creation.

AN0401

Unexpected processes (e.g., bash, python, custom binaries) dynamically loading libcrypto or performing AES/RC4 encryption operations, then initiating outbound sessions with abnormal byte entropy or asymmetric traffic patterns.

Log Sources

Mutable Elements

Field	Description
TrustedCryptoLibs	Baseline expected crypto libraries to suppress false positives.
TrafficAsymmetryRatio	Ratio of sent/received bytes indicating possible hidden C2.

AN0402

Launchd jobs or user processes invoking symmetric crypto APIs from the Security framework and generating outbound connections carrying randomized payloads inconsistent with normal TLS patterns.

Log Sources

Mutable Elements

Field	Description
DoHResolvers	Legitimate DNS-over-HTTPS endpoints to avoid FP.
PayloadEntropyThreshold	Define entropy level at which traffic should be flagged.

AN0403

ESXi daemons (hostd, vpxa) unexpectedly using symmetric encryption routines for external connections. Defender identifies logs of service traffic with encrypted payloads inconsistent with VMware management baselines.

Log Sources

Mutable Elements

Field	Description
AllowedMgmtHosts	Baseline list of approved vCenter and update endpoints.

AN0404

Flows showing encrypted payloads with high entropy not matching TLS handshake patterns, particularly when occurring on non-standard ports. Defender observes NetFlow/IPFIX byte distribution anomalies or IDS/IPS detecting symmetric encryption patterns without associated key exchange.

Log Sources

Mutable Elements

Field	Description
PortProfiles	Baseline expected encryption by port/protocol.
TrafficVolumeThreshold	Volume thresholds for distinguishing benign VPN traffic from hidden C2.
