Detection Strategy for Encrypted Channel across OS Platforms, Detection Strategy DET0273

Archived: 2026-04-05 17:36:05 UTC

AN0759

Processes that normally do not initiate network connections establishing outbound encrypted TLS/SSL sessions, especially with asymmetric traffic volumes (client sending more than receiving) or non-standard certificate chains. Defender observations correlate process creation with unexpected network encryption libraries being loaded.

Log Sources

Mutable Elements

Field	Description
AllowedEncryptedProcesses	Whitelist processes expected to use TLS (e.g., browsers, mail clients).
EntropyThreshold	Payload randomness threshold to distinguish C2 encryption from legitimate traffic.
TimeWindow	Correlation window between process creation, module load, and encrypted connection.

AN0760

Processes like curl, wget, python, socat, or custom binaries initiating TLS/SSL sessions to non-standard destinations. Defender sees abnormal syscalls for connect(), loading of libssl libraries, and persistent outbound encrypted traffic from daemons not normally communicating externally.

Log Sources

Mutable Elements

Field	Description
WhitelistedDaemons	Legitimate system services expected to use TLS (e.g., package updates).
CertificateAuthorities	Trusted CAs; flag self-signed or unrecognized certs.

AN0761

Applications or launchd jobs initiating encrypted TLS traffic to rare external hosts. Defender observes unified logs showing ssl/TLS API calls by processes not baseline-approved, and payload entropy suggesting encrypted C2 sessions.

Log Sources

Mutable Elements

Field	Description
DoHResolvers	Known legitimate DoH endpoints to reduce false positives.
PayloadEntropyThreshold	High-entropy traffic deviations used to detect concealed channels.

AN0762

VMware management daemons or guest processes initiating encrypted connections outside expected vCenter, update servers, or internal comms. Defender identifies hostd or vpxa initiating outbound TLS flows with uncommon destinations.

Log Sources

Mutable Elements

Field	Description
AllowedMgmtHosts	Baseline approved endpoints for vCenter or update services.

AN0763

Unusual TLS tunnels through ports not normally encrypted (e.g., TLS on port 8080, 53). Defender sees NetFlow/IPFIX or packet inspection indicating high-entropy traffic volumes and asymmetric client/server exchange ratios.

Log Sources

Mutable Elements

Field	Description
PortProfiles	Define expected TLS port usage to flag anomalies.
TrafficAsymmetryRatio	Sent/received byte thresholds to catch hidden C2.

Source: https://attack.mitre.org/detectionstrategies/DET0273#AN0763