Encrypted Channel, Technique T1573 - Enterprise

Archived: 2026-04-05 15:08:48 UTC

ID	Name	Analytic ID	Analytic Description
DET0273	Detection Strategy for Encrypted Channel across OS Platforms	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.
		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.
		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.
		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.
		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.

Source: https://attack.mitre.org/techniques/T1573