Detection of Exfiltration Over Asymmetric Encrypted Non-C2 Protocol, Detection Strategy DET0512

Archived: 2026-04-05 17:18:27 UTC

AN1413

Detects non-browser processes that establish encrypted outbound connections (e.g., TLS/SSL) to unfamiliar or atypical destinations for the host/user, following a data staging or compression event.

Log Sources

Mutable Elements

Field	Description
TimeWindow	Correlates file access, encryption, and network transmission within a timeframe (e.g., 5 minutes).
CertificateIssuerDenylist	Blocks or flags untrusted certificate authorities in SSL/TLS handshakes.
BinaryAllowlist	Whitelist for known-good applications allowed to use encrypted outbound traffic.

AN1414

Detects staged file access (e.g., archive or obfuscation), followed by an encrypted outbound connection (TLS/HTTPS) from unusual processes such as curl/wget, Python scripts, or custom binaries.

Log Sources

Mutable Elements

Field	Description
ConnectionDestinationScope	Restrict outbound connections to non-corporate domains or IPs.
FileAccessExtensionList	List of extensions considered sensitive or exfil-worthy (e.g., .zip, .db, .xlsx).
SSLClientProcessBaseline	Define normal encrypted-traffic-capable binaries.

AN1415

Detects abnormal encrypted network connections (via TLS/HTTPS) initiated by non-browser binaries, particularly after sensitive file access or compression events.

Log Sources

Mutable Elements

Field	Description
OutboundTrafficVolumeThreshold	Trigger detection for large amounts of outbound encrypted data.
FileSensitivityContext	Tagging and prioritizing high-value directories/files in detection logic.

AN1416

Detects unexpected encrypted outbound connections from management components or guest VMs using TLS, particularly after data volume spikes or script-based orchestration from within guest environments.

Log Sources

Mutable Elements

Field	Description
VMToEgressPathWatchlist	Expected traffic routes for monitored VMs.
TLSClientAppIdentifier	Applications allowed to initiate TLS sessions from hypervisor level.
