Domain Fronting Behavior via Mismatched TLS SNI and HTTP Host Headers, Detection Strategy DET0196

Archived: 2026-04-05 17:57:22 UTC

AN0564

Suspicious outbound HTTPS connections where the TLS Server Name Indication (SNI) does not match the HTTP Host header, indicating potential use of domain fronting to mask C2 traffic via CDNs.

Log Sources

Mutable Elements

Field	Description
SNIHostMismatch	Define acceptable mismatch ratio between SNI and HTTP Host fields based on legitimate domain usage patterns.
CDNAllowList	Whitelist of known safe CDN front-end domains (e.g., `cdn.company.com`).
ProcessInitiator	Filter for suspicious initiators of domain fronting, e.g., scripting engines, lolbins, unknown binaries.

AN0565

Applications such as `curl`, `wget`, or custom binaries initiate HTTPS connections where the TLS SNI is mismatched or absent while HTTP Host targets CDN-available C2 endpoints.

Log Sources

Mutable Elements

Field	Description
SNIFieldAbsent	Detect TLS sessions where SNI is empty—'domainless' fronting.
AllowedTools	Environmental tuning for known binaries using alternate SNI for testing (e.g., API tests).
ProcessContext	Enrich command-line arguments or parent-child lineage to detect abuse.

AN0566

Unsigned or user-space apps initiate TLS connections with one hostname and HTTP headers requesting a different domain, commonly abused in CDN-resident domain fronting techniques.

Log Sources

Mutable Elements

Field	Description
UnsignedBinary	Helps tune detection when unsigned apps initiate fronted sessions.
HostHeaderMatch	Threshold to flag inconsistent domain targeting in encrypted sessions.
SOCKSPortAnomaly	Alert on unusual ports used in HTTPS+SOCKS activity patterns.

AN0567

Traffic originating from ESXi hosts or management interfaces displays SNI-to-Host mismatch behavior, particularly anomalous given typical infrastructure communication patterns.

Log Sources

Mutable Elements

Field	Description
AdminPortAccess	ESXi hosts should rarely initiate external HTTPS—threshold to alert.
TLSHandshakeOutliers	Define entropy or timing anomalies for TLS handshake.
DomainMismatchThreshold	SNI/Host mismatch occurrence tolerance.
