Data Obfuscation: Protocol or Service Impersonation, Sub-technique T1001.003 - Enterprise

Archived: 2026-04-05 18:11:31 UTC

Adversaries may impersonate legitimate protocols or web service traffic to disguise command and control activity and thwart analysis efforts. By impersonating legitimate protocols or web services, adversaries can make their command and control traffic blend in with legitimate network traffic.

Adversaries may impersonate a fake SSL/TLS handshake to make it look like subsequent traffic is SSL/TLS encrypted, potentially interfering with some security tooling, or to make the traffic look like it is related with a trusted entity.

Adversaries may also leverage legitimate protocols to impersonate expected web traffic or trusted services. For example, adversaries may manipulate HTTP headers, URI endpoints, SSL certificates, and transmitted data to disguise C2 communications or mimic legitimate services such as Gmail, Google Drive, and Yahoo Messenger.[1] [2]

Source: https://attack.mitre.org/techniques/T1001/003