Encrypted Channel: SSL Pinning, Sub-technique T1521.003 - Mobile

Archived: 2026-04-05 13:32:16 UTC

Adversaries may use SSL Pinning to protect the C2 traffic from being intercepted and analyzed.

SSL Pinning is a technique commonly utilized by legitimate websites to ensure that encrypted communications are only allowed with a pre-defined certificate. If another certificate is presented, it could indicate device compromise, traffic interception, or another upstream issue. While benign usages are common, it is also possible for adversaries to abuse this technology to protect malicious C2 traffic.

In normal, not pinned SSL validation, when a client connects to a server using HTTPS, it typically checks whether the server's SSL/TLS certificate is signed by a trusted Certificate Authority (CA) in the device's trust store. If the certificate is valid and signed by a trusted CA, the connection is established. However, with SSL Pinning , the client is configured to trust a specific SSL/TLS certificate or public key, rather than relying on the device's trust store. This means that even if the server's certificate is signed by a trusted CA, the client will only establish the connection of the certificate or key is pinned.

There are two types of SSL Pinning :

1. Certificate Pinning: The client stores a copy of the server's certificate and compares it with the certificate received during the SSL handshake. If the certificates match, then the client proceeds with the connection. This approach also works with self-signed certificates.

2. Public Key Pinning: Instead of pinning the entire certificate, the client pins just the public key extracted from the certificate. This is often more flexible, as it allows the server to renew its certificate without having to update the pinned certificate or breaking the SSL connection.

Source: https://attack.mitre.org/techniques/T1521/003