Obtain Capabilities: Digital Certificates, Sub-technique T1588.004 - Enterprise

Archived: 2026-04-02 10:44:08 UTC

Adversaries may buy and/or steal SSL/TLS certificates that can be used during targeting. SSL/TLS certificates are designed to instill trust. They include information about the key, information about its owner's identity, and the digital signature of an entity that has verified the certificate's contents are correct. If the signature is valid, and the person examining the certificate trusts the signer, then they know they can use that key to communicate with its owner.

Adversaries may purchase or steal SSL/TLS certificates to further their operations, such as encrypting C2 traffic (ex: Asymmetric Cryptography with Web Protocols) or even enabling Adversary-in-the-Middle if the certificate is trusted or otherwise added to the root of trust (i.e. Install Root Certificate). The purchase of digital certificates may be done using a front organization or using information stolen from a previously compromised entity that allows the adversary to validate to a certificate provider as that entity. Adversaries may also steal certificate materials directly from a compromised third-party, including from certificate authorities.[1] Adversaries may register or hijack domains that they will later purchase an SSL/TLS certificate for.

Certificate authorities exist that allow adversaries to acquire SSL/TLS certificates, such as domain validation certificates, for free.[2]

After obtaining a digital certificate, an adversary may then install that certificate (see Install Digital Certificate) on infrastructure under their control.

Source: https://attack.mitre.org/techniques/T1588/004