# TTP Detail – T1649

## TTP Information

Name: Steal or Forge Authentication Certificates

Description: Adversaries may steal or forge certificates used for authentication to access remote systems or resources. Digital certificates are often used to sign and encrypt messages and/or files. Certificates are also used as authentication material. For example, Entra ID device certificates and Active Directory Certificate Services (AD CS) certificates bind to an identity and can be used as credentials for domain accounts.(Citation: O365 Blog Azure AD Device IDs)(Citation: Microsoft AD CS Overview)

Authentication certificates can be both stolen and forged. For example, AD CS certificates can be stolen from encrypted storage (in the Registry or files)(Citation: APT29 Deep Look at Credential Roaming), misplaced certificate files (i.e. [Unsecured Credentials](https://attack.mitre.org/techniques/T1552)), or directly from the Windows certificate store via various crypto APIs.(Citation: SpecterOps Certified Pre Owned)(Citation: GitHub CertStealer)(Citation: GitHub GhostPack Certificates) With appropriate enrollment rights, users and/or machines within a domain can also request and/or manually renew certificates from enterprise certificate authorities (CA). This enrollment process defines various settings and permissions associated with the certificate. Of note, the certificate’s extended key usage (EKU) values define signing, encryption, and authentication use cases, while the certificate’s subject alternative name (SAN) values define the certificate owner’s alternate names.(Citation: Medium Certified Pre Owned)

Abusing certificates for authentication credentials may enable other behaviors such as [Lateral Movement](https://attack.mitre.org/tactics/TA0008). Certificate-related misconfigurations may also enable opportunities for [Privilege Escalation](https://attack.mitre.org/tactics/TA0004), by way of allowing users to impersonate or assume privileged accounts or permissions via the identities (SANs) associated with a certificate. These abuses may also enable [Persistence](https://attack.mitre.org/tactics/TA0003) via stealing or forging certificates that can be used as [Valid Accounts](https://attack.mitre.org/techniques/T1078) for the duration of the certificate's validity, despite user password resets. Authentication certificates can also be stolen and forged for machine accounts.

Adversaries who have access to root (or subordinate) CA certificate private keys (or mechanisms protecting/managing these keys) may also establish [Persistence](https://attack.mitre.org/tactics/TA0003) by forging arbitrary authentication certificates for the victim domain (known as “golden” certificates).(Citation: Medium Certified Pre Owned) Adversaries may also target certificates and related services in order to access other forms of credentials, such as [Golden Ticket](https://attack.mitre.org/techniques/T1558/001) ticket-granting tickets (TGT) or NTLM plaintext.(Citation: Medium Certified Pre Owned)

## Threat-Mapped Scoring

Score: 3.25

Priority: P2 - Serious (High)

## Kill Chain Phases

**•** mitre-attack: credential-access

## Tools

* AADInternals
* Mimikatz

## APTs (Intrusion Sets)

* APT29