# TTP Detail – T1596.003

## TTP Information

Name: Digital Certificates

Description: Adversaries may search public digital certificate data for information about victims that can be used during targeting. Digital certificates are issued by a certificate authority (CA) in order to cryptographically verify the origin of signed content. These certificates, such as those used for encrypted web traffic (HTTPS SSL/TLS communications), contain information about the registered organization such as name and location.

Adversaries may search digital certificate data to gather actionable information. Threat actors can use online resources and lookup tools to harvest information about certificates.(Citation: SSLShopper Lookup) Digital certificate data may also be available from artifacts signed by the organization (ex: certificates used from encrypted web traffic are served with content).(Citation: Medium SSL Cert) Information from these sources may reveal opportunities for other forms of reconnaissance (ex: [Active Scanning](https://attack.mitre.org/techniques/T1595) or [Phishing for Information](https://attack.mitre.org/techniques/T1598)), establishing operational resources (ex: [Develop Capabilities](https://attack.mitre.org/techniques/T1587) or [Obtain Capabilities](https://attack.mitre.org/techniques/T1588)), and/or initial access (ex: [External Remote Services](https://attack.mitre.org/techniques/T1133) or [Trusted Relationship](https://attack.mitre.org/techniques/T1199)).

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## Kill Chain Phases

**•** mitre-attack: reconnaissance