Search Open Technical Databases: Digital Certificates, Sub-technique T1596.003 - Enterprise

Archived: 2026-04-05 17:22:22 UTC

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.[1] Digital certificate data may also be available from artifacts signed by the organization (ex: certificates used from encrypted web traffic are served with content).[2] Information from these sources may reveal opportunities for other forms of reconnaissance (ex: Active Scanning or Phishing for Information), establishing operational resources (ex: Develop Capabilities or Obtain Capabilities), and/or initial access (ex: External Remote Services or Trusted Relationship).

Source: https://attack.mitre.org/techniques/T1596/003