# TTP Detail – T1596

## TTP Information

Name: Search Open Technical Databases

Description: Adversaries may search freely available technical databases for information about victims that can be used during targeting. Information about victims may be available in online databases and repositories, such as registrations of domains/certificates as well as public collections of network data/artifacts gathered from traffic and/or scans.(Citation: WHOIS)(Citation: DNS Dumpster)(Citation: Circl Passive DNS)(Citation: Medium SSL Cert)(Citation: SSLShopper Lookup)(Citation: DigitalShadows CDN)(Citation: Shodan)

Adversaries may search in different open databases depending on what information they seek to gather. Information from these sources may reveal opportunities for other forms of reconnaissance (ex: [Phishing for Information](https://attack.mitre.org/techniques/T1598) or [Search Open Websites/Domains](https://attack.mitre.org/techniques/T1593)), establishing operational resources (ex: [Acquire Infrastructure](https://attack.mitre.org/techniques/T1583) or [Compromise Infrastructure](https://attack.mitre.org/techniques/T1584)), 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

## APTs (Intrusion Sets)

* APT28
* Kimsuky