# TTP Detail – T1596.002

## TTP Information

Name: WHOIS

Description: Adversaries may search public WHOIS data for information about victims that can be used during targeting. WHOIS data is stored by regional Internet registries (RIR) responsible for allocating and assigning Internet resources such as domain names. Anyone can query WHOIS servers for information about a registered domain, such as assigned IP blocks, contact information, and DNS nameservers.(Citation: WHOIS)

Adversaries may search WHOIS data to gather actionable information. Threat actors can use online resources or command-line utilities to pillage through WHOIS data for information about potential victims. 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: [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