# TTP Detail – T1590.002

## TTP Information

Name: DNS

Description: Adversaries may gather information about the victim's DNS that can be used during targeting. DNS information may include a variety of details, including registered name servers as well as records that outline addressing for a target’s subdomains, mail servers, and other hosts. DNS MX, TXT, and SPF records may also reveal the use of third party cloud and SaaS providers, such as Office 365, G Suite, Salesforce, or Zendesk.(Citation: Sean Metcalf Twitter DNS Records)

Adversaries may gather this information in various ways, such as querying or otherwise collecting details via [DNS/Passive DNS](https://attack.mitre.org/techniques/T1596/001). DNS information may also be exposed to adversaries via online or other accessible data sets (ex: [Search Open Technical Databases](https://attack.mitre.org/techniques/T1596)).(Citation: DNS Dumpster)(Citation: Circl Passive DNS) Gathering this information may reveal opportunities for other forms of reconnaissance (ex: [Search Open Technical Databases](https://attack.mitre.org/techniques/T1596), [Search Open Websites/Domains](https://attack.mitre.org/techniques/T1593), or [Active Scanning](https://attack.mitre.org/techniques/T1595)), 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)).

Adversaries may also use DNS zone transfer (DNS query type AXFR) to collect all records from a misconfigured DNS server.(Citation: Trails-DNS)(Citation: DNS-CISA)(Citation: Alexa-dns)

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## Kill Chain Phases

**•** mitre-attack: reconnaissance