Gather Victim Network Information: DNS, Sub-technique T1590.002 - Enterprise

Archived: 2026-04-02 11:07:50 UTC

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.[1]

Adversaries may gather this information in various ways, such as querying or otherwise collecting details via DNS/Passive DNS. DNS information may also be exposed to adversaries via online or other accessible data sets (ex: Search Open Technical Databases).[2][3] Gathering this information may reveal opportunities for other forms of reconnaissance (ex: Search Open Technical Databases, Search Open Websites/Domains, or Active Scanning), establishing operational resources (ex: Acquire Infrastructure or Compromise Infrastructure), and/or initial access (ex: External Remote Services).

Adversaries may also use DNS zone transfer (DNS query type AXFR) to collect all records from a misconfigured DNS server.[4][5][6]

Source: https://attack.mitre.org/techniques/T1590/002