# Search Open Technical Databases: WHOIS, Sub-technique T1596.002 - Enterprise

Archived: 2026-04-05 17:22:41 UTC

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.[1]

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 or Phishing for Information), establishing operational resources (ex: Acquire Infrastructure or Compromise Infrastructure), and/or initial access (ex: External Remote Services or Trusted Relationship).

---