Search Open Websites/Domains: Search Engines, Sub-technique T1593.002 - Enterprise

Archived: 2026-04-05 18:41:34 UTC

Adversaries may use search engines to collect information about victims that can be used during targeting. Search engine services typical crawl online sites to index context and may provide users with specialized syntax to search for specific keywords or specific types of content (i.e. filetypes).[1][2]

Adversaries may craft various search engine queries depending on what information they seek to gather. Threat actors may use search engines to harvest general information about victims, as well as use specialized queries to look for spillages/leaks of sensitive information such as network details or credentials. Information from these sources may reveal opportunities for other forms of reconnaissance (ex: Phishing for Information or Search Open Technical Databases), establishing operational resources (ex: Establish Accounts or Compromise Accounts), and/or initial access (ex: Valid Accounts or Phishing).

Source: https://attack.mitre.org/techniques/T1593/002