Gather Victim Network Information: Network Trust Dependencies, Sub-technique T1590.003 - Enterprise

Archived: 2026-04-05 14:40:34 UTC

Adversaries may gather information about the victim's network trust dependencies that can be used during targeting. Information about network trusts may include a variety of details, including second or third-party organizations/domains (ex: managed service providers, contractors, etc.) that have connected (and potentially elevated) network access.

Adversaries may gather this information in various ways, such as direct elicitation via Phishing for Information. Information about network trusts may also be exposed to adversaries via online or other accessible data sets (ex: Search Open Technical Databases).[1] Gathering this information may reveal opportunities for other forms of reconnaissance (ex: Active Scanning or Search Open Websites/Domains), establishing operational resources (ex: Acquire Infrastructure or Compromise Infrastructure), and/or initial access (ex: Trusted Relationship).

Source: https://attack.mitre.org/techniques/T1590/003