Gather Victim Org Information: Business Relationships, Sub-technique T1591.002 - Enterprise

Archived: 2026-04-05 16:43:41 UTC

Adversaries may gather information about the victim's business relationships that can be used during targeting. Information about an organization’s business relationships 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. This information may also reveal supply chains and shipment paths for the victim’s hardware and software resources.

Adversaries may gather this information in various ways, such as direct elicitation via Phishing for Information. Information about business relationships may also be exposed to adversaries via online or other accessible data sets (ex: Social Media or Search Victim-Owned Websites).[1] Gathering this information may reveal opportunities for other forms of reconnaissance (ex: Phishing for Information or Search Open Websites/Domains), establishing operational resources (ex: Establish Accounts or Compromise Accounts), and/or initial access (ex: Supply Chain Compromise, Drive-by Compromise, or Trusted Relationship).

Source: https://attack.mitre.org/techniques/T1591/002