Gather Victim Host Information: Client Configurations, Sub-technique T1592.004 - Enterprise

Archived: 2026-04-05 15:12:33 UTC

Adversaries may gather information about the victim's client configurations that can be used during targeting. Information about client configurations may include a variety of details and settings, including operating system/version, virtualization, architecture (ex: 32 or 64 bit), language, and/or time zone.

Adversaries may gather this information in various ways, such as direct collection actions via Active Scanning (ex: listening ports, server banners, user agent strings) or Phishing for Information. Adversaries may also compromise sites then include malicious content designed to collect host information from visitors.[1] Information about the client configurations may also be exposed to adversaries via online or other accessible data sets (ex: job postings, network maps, assessment reports, resumes, or purchase invoices). Gathering this information may reveal opportunities for other forms of reconnaissance (ex: Search Open Websites/Domains or Search Open Technical Databases), establishing operational resources (ex: Develop Capabilities or Obtain Capabilities), and/or initial access (ex: Supply Chain Compromise or External Remote Services).

Source: https://attack.mitre.org/techniques/T1592/004