Gather Victim Host Information: Firmware, Sub-technique T1592.003 - Enterprise

Archived: 2026-04-05 18:03:30 UTC

Adversaries may gather information about the victim's host firmware that can be used during targeting. Information about host firmware may include a variety of details such as type and versions on specific hosts, which may be used to infer more information about hosts in the environment (ex: configuration, purpose, age/patch level, etc.).

Adversaries may gather this information in various ways, such as direct elicitation via Phishing for Information. Information about host firmware may only be exposed to adversaries via online or other accessible data sets (ex: job postings, network maps, assessment reports, resumes, or purchase invoices).[1] 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 Exploit Public-Facing Application).

Source: https://attack.mitre.org/techniques/T1592/003