# TTP Detail – T1592.003

## TTP Information

Name: Firmware

Description: 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](https://attack.mitre.org/techniques/T1598). 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).(Citation: ArsTechnica Intel) Gathering this information may reveal opportunities for other forms of reconnaissance (ex: [Search Open Websites/Domains](https://attack.mitre.org/techniques/T1593) or [Search Open Technical Databases](https://attack.mitre.org/techniques/T1596)), establishing operational resources (ex: [Develop Capabilities](https://attack.mitre.org/techniques/T1587) or [Obtain Capabilities](https://attack.mitre.org/techniques/T1588)), and/or initial access (ex: [Supply Chain Compromise](https://attack.mitre.org/techniques/T1195) or [Exploit Public-Facing Application](https://attack.mitre.org/techniques/T1190)).

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## Kill Chain Phases

**•** mitre-attack: reconnaissance