# TTP Detail – T1063

## TTP Information

Name: Security Software Discovery

Description: Adversaries may attempt to get a listing of security software, configurations, defensive tools, and sensors that are installed on the system. This may include things such as local firewall rules and anti-virus. Adversaries may use the information from [Security Software Discovery](https://attack.mitre.org/techniques/T1063) during automated discovery to shape follow-on behaviors, including whether or not the adversary fully infects the target and/or attempts specific actions.

### Windows

Example commands that can be used to obtain security software information are [netsh](https://attack.mitre.org/software/S0108), <code>reg query</code> with [Reg](https://attack.mitre.org/software/S0075), <code>dir</code> with [cmd](https://attack.mitre.org/software/S0106), and [Tasklist](https://attack.mitre.org/software/S0057), but other indicators of discovery behavior may be more specific to the type of software or security system the adversary is looking for.

### Mac

It's becoming more common to see macOS malware perform checks for LittleSnitch and KnockKnock software.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Kill Chain Phases

**•** mitre-attack: discovery