# TTP Detail – T1518.001

## 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 a system or in a cloud environment. This may include things such as cloud monitoring agents and anti-virus. Adversaries may use the information from [Security Software Discovery](https://attack.mitre.org/techniques/T1518/001) during automated discovery to shape follow-on behaviors, including whether or not the adversary fully infects the target and/or attempts specific actions.

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

Adversaries may also utilize the [Cloud API](https://attack.mitre.org/techniques/T1059/009) to discover cloud-native security software installed on compute infrastructure, such as the AWS CloudWatch agent, Azure VM Agent, and Google Cloud Monitor agent. These agents may collect metrics and logs from the VM, which may be centrally aggregated in a cloud-based monitoring platform.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Kill Chain Phases

**•** mitre-attack: discovery

## Malware

* ABK
* Action RAT
* Amadey
* Astaroth
* AuTo Stealer
* Avenger
* BLUELIGHT
* BadPatch
* Bazar
* BlackByte Ransomware
* Bumblebee
* CHIMNEYSWEEP
* CHOPSTICK
* Carberp
* Clop
* Comnie
* CookieMiner
* CozyCar
* Crimson
* DUSTTRAP
* DarkGate
* DarkTortilla
* DarkWatchman
* DustySky
* EVILNUM
* Epic
* EvilBunny
* Exbyte
* FELIXROOT
* Felismus
* Ferocious
* FinFisher
* Flame
* FlawedAmmyy
* FunnyDream
* Gelsemium
* Gold Dragon
* Grandoreiro
* IcedID
* InvisiMole
* JPIN
* Kasidet
* Latrodectus
* LiteDuke
* LitePower
* Lizar
* Lumma Stealer
* LunarWeb
* Mafalda
* MarkiRAT
* Metamorfo
* Meteor
* Micropsia
* Mispadu
* MoleNet
* More\_eggs
* Mosquito
* Netwalker
* NotPetya
* POWERSTATS
* POWRUNER
* PUNCHBUGGY
* PipeMon
* Prikormka
* QakBot
* RTM
* Raspberry Robin
* Remsec
* RogueRobin
* SUNBURST
* Skidmap
* SpicyOmelette
* StoneDrill
* StreamEx
* StrongPity
* Stuxnet
* T9000
* TAMECAT
* TajMahal
* ThiefQuest
* VERMIN
* Valak
* Waterbear
* WhisperGate
* Wingbird
* Woody RAT
* XCSSET
* YAHOYAH
* Zeus Panda
* ZxxZ
* build\_downer
* down\_new
* jRAT
* xCaon

## Tools

* Brute Ratel C4
* Empire
* Pacu
* SILENTTRINITY
* Tasklist
* netsh

## APTs (Intrusion Sets)

* APT38
* APT42
* Aquatic Panda
* BlackByte
* Cobalt Group
* Darkhotel
* FIN8
* Kimsuky
* Malteiro
* MuddyWater
* Naikon
* Patchwork
* Play
* Rocke
* SideCopy
* Sidewinder
* TA2541
* TeamTNT
* The White Company
* ToddyCat
* Tropic Trooper
* Turla
* Windshift
* Wizard Spider