# TTP Detail – T1518

## TTP Information

Name: Software Discovery

Description: Adversaries may attempt to get a listing of software and software versions that are installed on a system or in a cloud environment. Adversaries may use the information from [Software Discovery](https://attack.mitre.org/techniques/T1518) during automated discovery to shape follow-on behaviors, including whether or not the adversary fully infects the target and/or attempts specific actions.

Such software may be deployed widely across the environment for configuration management or security reasons, such as [Software Deployment Tools](https://attack.mitre.org/techniques/T1072), and may allow adversaries broad access to infect devices or move laterally.

Adversaries may attempt to enumerate software for a variety of reasons, such as figuring out what security measures are present or if the compromised system has a version of software that is vulnerable to [Exploitation for Privilege Escalation](https://attack.mitre.org/techniques/T1068).

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## Kill Chain Phases

**•** mitre-attack: discovery

## Malware

* Bazar
* Bundlore
* CharmPower
* Cobalt Strike
* ComRAT
* Cuckoo Stealer
* Dridex
* DustySky
* Dyre
* HotCroissant
* InvisiMole
* KGH\_SPY
* LightSpy
* LunarWeb
* MarkiRAT
* Metamorfo
* Orz
* P.A.S. Webshell
* QakBot
* RTM
* Raccoon Stealer
* SUGARDUMP
* SVCReady
* Samurai
* Siloscape
* SocGholish
* SpicyOmelette
* StrelaStealer
* TajMahal
* Woody RAT
* XCSSET
* down\_new

## Tools

* ShimRatReporter

## APTs (Intrusion Sets)

* BRONZE BUTLER
* HEXANE
* Inception
* MuddyWater
* Mustang Panda
* SideCopy
* Sidewinder
* Tropic Trooper
* Volt Typhoon
* Windigo
* Windshift
* Wizard Spider