# TTP Detail – T1007

## TTP Information

Name: System Service Discovery

Description: Adversaries may try to gather information about registered local system services. Adversaries may obtain information about services using tools as well as OS utility commands such as <code>sc query</code>, <code>tasklist /svc</code>, <code>systemctl --type=service</code>, and <code>net start</code>.

Adversaries may use the information from [System Service Discovery](https://attack.mitre.org/techniques/T1007) during automated discovery to shape follow-on behaviors, including whether or not the adversary fully infects the target and/or attempts specific actions.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Kill Chain Phases

**•** mitre-attack: discovery

## Malware

* BBSRAT
* Babuk
* BitPaymer
* Black Basta
* Caterpillar WebShell
* Cobalt Strike
* Comnie
* Cuba
* DarkTortilla
* Dyre
* Elise
* Emissary
* Epic
* GeminiDuke
* GravityRAT
* GreyEnergy
* Heyoka Backdoor
* HotCroissant
* Hydraq
* HyperBro
* InvisiMole
* Ixeshe
* JPIN
* Kwampirs
* LookBack
* RATANKBA
* REvil
* RainyDay
* S-Type
* SLOTHFULMEDIA
* SUNBURST
* Sardonic
* SombRAT
* Sykipot
* SynAck
* SysUpdate
* TrickBot
* Ursnif
* Volgmer
* WINERACK
* ZLib
* ZxShell
* jRAT

## Tools

* Net
* PoshC2
* SILENTTRINITY
* Tasklist

## APTs (Intrusion Sets)

* APT1
* Aquatic Panda
* BRONZE BUTLER
* Chimera
* Earth Lusca
* Indrik Spider
* Ke3chang
* Kimsuky
* OilRig
* Poseidon Group
* TeamTNT
* Turla
* Volt Typhoon
* admin@338