# TTP Detail – T1569.002

## TTP Information

Name: Service Execution

Description: Adversaries may abuse the Windows service control manager to execute malicious commands or payloads. The Windows service control manager (<code>services.exe</code>) is an interface to manage and manipulate services.(Citation: Microsoft Service Control Manager) The service control manager is accessible to users via GUI components as well as system utilities such as <code>sc.exe</code> and [Net](https://attack.mitre.org/software/S0039).

[PsExec](https://attack.mitre.org/software/S0029) can also be used to execute commands or payloads via a temporary Windows service created through the service control manager API.(Citation: Russinovich Sysinternals) Tools such as [PsExec](https://attack.mitre.org/software/S0029) and <code>sc.exe</code> can accept remote servers as arguments and may be used to conduct remote execution.

Adversaries may leverage these mechanisms to execute malicious content. This can be done by either executing a new or modified service. This technique is the execution used in conjunction with [Windows Service](https://attack.mitre.org/techniques/T1543/003) during service persistence or privilege escalation.

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## Kill Chain Phases

**•** mitre-attack: execution

## Malware

* Anchor
* Attor
* BBSRAT
* Bad Rabbit
* BlackByte 2.0 Ransomware
* Clambling
* Cobalt Strike
* DEADWOOD
* DarkGate
* HOPLIGHT
* HermeticWiper
* HermeticWizard
* Hydraq
* HyperBro
* IPsec Helper
* InvisiMole
* LockBit 3.0
* LoudMiner
* Mafalda
* Net Crawler
* Netwalker
* NotPetya
* Okrum
* Olympic Destroyer
* Pandora
* Proxysvc
* Pysa
* Ragnar Locker
* RemoteCMD
* SLOTHFULMEDIA
* Shamoon
* StrongPity
* SysUpdate
* TinyTurla
* WastedLocker
* WhisperGate
* Wingbird
* Winnti for Windows
* ZxShell
* gh0st RAT

## Tools

* Brute Ratel C4
* Empire
* Impacket
* Koadic
* Net
* PoshC2
* PsExec
* Pupy
* Winexe
* xCmd

## APTs (Intrusion Sets)

* APT32
* APT38
* APT39
* APT41
* BlackByte
* Blue Mockingbird
* Chimera
* FIN6
* INC Ransom
* Ke3chang
* Moonstone Sleet
* Silence
* Velvet Ant
* Wizard Spider