# TTP Detail – T1489

## TTP Information

Name: Service Stop

Description: Adversaries may stop or disable services on a system to render those services unavailable to legitimate users. Stopping critical services or processes can inhibit or stop response to an incident or aid in the adversary's overall objectives to cause damage to the environment.(Citation: Talos Olympic Destroyer 2018)(Citation: Novetta Blockbuster)

Adversaries may accomplish this by disabling individual services of high importance to an organization, such as <code>MSExchangeIS</code>, which will make Exchange content inaccessible.(Citation: Novetta Blockbuster) In some cases, adversaries may stop or disable many or all services to render systems unusable.(Citation: Talos Olympic Destroyer 2018) Services or processes may not allow for modification of their data stores while running. Adversaries may stop services or processes in order to conduct [Data Destruction](https://attack.mitre.org/techniques/T1485) or [Data Encrypted for Impact](https://attack.mitre.org/techniques/T1486) on the data stores of services like Exchange and SQL Server, or on virtual machines hosted on ESXi infrastructure.(Citation: SecureWorks WannaCry Analysis)(Citation: Crowdstrike Hypervisor Jackpotting Pt 2 2021)

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Kill Chain Phases

**•** mitre-attack: impact

## Malware

* Akira \_v2
* Avaddon
* AvosLocker
* Babuk
* BlackByte 2.0 Ransomware
* BlackCat
* Cheerscrypt
* Clop
* Conti
* Cuba
* Diavol
* EKANS
* Hannotog
* HermeticWiper
* HotCroissant
* INC Ransomware
* Industroyer
* KillDisk
* LockBit 2.0
* LockBit 3.0
* LookBack
* Maze
* MegaCortex
* Megazord
* Meteor
* Netwalker
* Olympic Destroyer
* Pay2Key
* Prestige
* Pysa
* REvil
* ROADSWEEP
* Ragnar Locker
* RansomHub
* RobbinHood
* Royal
* Ryuk
* SLOTHFULMEDIA
* WannaCry

## APTs (Intrusion Sets)

* Indrik Spider
* LAPSUS$
* Lazarus Group
* Sandworm Team
* Wizard Spider