# TTP Detail – T1490

## TTP Information

Name: Inhibit System Recovery

Description: Adversaries may delete or remove built-in data and turn off services designed to aid in the recovery of a corrupted system to prevent recovery.(Citation: Talos Olympic Destroyer 2018)(Citation: FireEye WannaCry 2017) This may deny access to available backups and recovery options.  
  
Operating systems may contain features that can help fix corrupted systems, such as a backup catalog, volume shadow copies, and automatic repair features. Adversaries may disable or delete system recovery features to augment the effects of [Data Destruction](https://attack.mitre.org/techniques/T1485) and [Data Encrypted for Impact](https://attack.mitre.org/techniques/T1486).(Citation: Talos Olympic Destroyer 2018)(Citation: FireEye WannaCry 2017) Furthermore, adversaries may disable recovery notifications, then corrupt backups.(Citation: disable\_notif\_synology\_ransom)  
  
A number of native Windows utilities have been used by adversaries to disable or delete system recovery features:  
  
\* <code>vssadmin.exe</code> can be used to delete all volume shadow copies on a system - <code>vssadmin.exe delete shadows /all /quiet</code>  
\* [Windows Management Instrumentation](https://attack.mitre.org/techniques/T1047) can be used to delete volume shadow copies - <code>wmic shadowcopy delete</code>  
\* <code>wbadmin.exe</code> can be used to delete the Windows Backup Catalog - <code>wbadmin.exe delete catalog -quiet</code>  
\* <code>bcdedit.exe</code> can be used to disable automatic Windows recovery features by modifying boot configuration data - <code>bcdedit.exe /set {default} bootstatuspolicy ignoreallfailures & bcdedit /set {default} recoveryenabled no</code>  
\* <code>REAgentC.exe</code> can be used to disable Windows Recovery Environment (WinRE) repair/recovery options of an infected system  
\* <code>diskshadow.exe</code> can be used to delete all volume shadow copies on a system - <code>diskshadow delete shadows all</code> (Citation: Diskshadow) (Citation: Crytox Ransomware)  
  
On network devices, adversaries may leverage [Disk Wipe](https://attack.mitre.org/techniques/T1561) to delete backup firmware images and reformat the file system, then [System Shutdown/Reboot](https://attack.mitre.org/techniques/T1529) to reload the device. Together this activity may leave network devices completely inoperable and inhibit recovery operations.  
  
On ESXi servers, adversaries may delete or encrypt snapshots of virtual machines to support [Data Encrypted for Impact](https://attack.mitre.org/techniques/T1486), preventing them from being leveraged as backups (e.g., via ` vim-cmd vmsvc/snapshot.removeall`).(Citation: Cybereason)  
  
Adversaries may also delete “online” backups that are connected to their network – whether via network storage media or through folders that sync to cloud services.(Citation: ZDNet Ransomware Backups 2020) In cloud environments, adversaries may disable versioning and backup policies and delete snapshots, database backups, machine images, and prior versions of objects designed to be used in disaster recovery scenarios.(Citation: Dark Reading Code Spaces Cyber Attack)(Citation: Rhino Security Labs AWS S3 Ransomware)

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Kill Chain Phases

**•** mitre-attack: impact

## Malware

* Akira
* Avaddon
* BFG Agonizer
* Babuk
* BitPaymer
* Black Basta
* BlackByte 2.0 Ransomware
* BlackByte Ransomware
* BlackCat
* Clop
* Conficker
* Conti
* DEATHRANSOM
* DarkGate
* DarkWatchman
* Diavol
* EKANS
* FIVEHANDS
* H1N1
* HELLOKITTY
* HermeticWiper
* INC Ransomware
* InvisiMole
* JCry
* LockBit 2.0
* LockBit 3.0
* Maze
* MegaCortex
* Meteor
* MultiLayer Wiper
* Netwalker
* Olympic Destroyer
* Playcrypt
* Prestige
* ProLock
* Pysa
* REvil
* ROADSWEEP
* Ragnar Locker
* RansomHub
* RobbinHood
* Royal
* Ryuk
* WannaCry
* WastedLocker

## APTs (Intrusion Sets)

* BlackByte
* Sandworm Team
* Wizard Spider