# TTP Detail – T1529

## TTP Information

Name: System Shutdown/Reboot

Description: Adversaries may shutdown/reboot systems to interrupt access to, or aid in the destruction of, those systems. Operating systems may contain commands to initiate a shutdown/reboot of a machine or network device. In some cases, these commands may also be used to initiate a shutdown/reboot of a remote computer or network device via [Network Device CLI](https://attack.mitre.org/techniques/T1059/008) (e.g. <code>reload</code>).(Citation: Microsoft Shutdown Oct 2017)(Citation: alert\_TA18\_106A) They may also include shutdown/reboot of a virtual machine via hypervisor / cloud consoles or command line tools.

Shutting down or rebooting systems may disrupt access to computer resources for legitimate users while also impeding incident response/recovery.

Adversaries may attempt to shutdown/reboot a system after impacting it in other ways, such as [Disk Structure Wipe](https://attack.mitre.org/techniques/T1561/002) or [Inhibit System Recovery](https://attack.mitre.org/techniques/T1490), to hasten the intended effects on system availability.(Citation: Talos Nyetya June 2017)(Citation: Talos Olympic Destroyer 2018)

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## Kill Chain Phases

**•** mitre-attack: impact

## Malware

* AcidPour
* AcidRain
* Apostle
* AvosLocker
* BFG Agonizer
* Black Basta
* CHIMNEYSWEEP
* DCSrv
* DarkGate
* HermeticWiper
* KillDisk
* Latrodectus
* LockerGoga
* LookBack
* Maze
* MultiLayer Wiper
* NotPetya
* Olympic Destroyer
* Shamoon
* ShrinkLocker
* WhisperGate
* XLoader

## APTs (Intrusion Sets)

* APT37
* APT38
* Lazarus Group