# TTP Detail – T1653

## TTP Information

Name: Power Settings

Description: Adversaries may impair a system's ability to hibernate, reboot, or shut down in order to extend access to infected machines. When a computer enters a dormant state, some or all software and hardware may cease to operate which can disrupt malicious activity.(Citation: Sleep, shut down, hibernate)

Adversaries may abuse system utilities and configuration settings to maintain access by preventing machines from entering a state, such as standby, that can terminate malicious activity.(Citation: Microsoft: Powercfg command-line options)(Citation: systemdsleep Linux)

For example, `powercfg` controls all configurable power system settings on a Windows system and can be abused to prevent an infected host from locking or shutting down.(Citation: Two New Monero Malware Attacks Target Windows and Android Users) Adversaries may also extend system lock screen timeout settings.(Citation: BATLOADER: The Evasive Downloader Malware) Other relevant settings, such as disk and hibernate timeout, can be similarly abused to keep the infected machine running even if no user is active.(Citation: CoinLoader: A Sophisticated Malware Loader Campaign)

Aware that some malware cannot survive system reboots, adversaries may entirely delete files used to invoke system shut down or reboot.(Citation: Condi-Botnet-binaries)

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Kill Chain Phases

**•** mitre-attack: persistence

## Malware

* Line Dancer
* Line Runner