# TTP Detail – T1531

## TTP Information

Name: Account Access Removal

Description: Adversaries may interrupt availability of system and network resources by inhibiting access to accounts utilized by legitimate users. Accounts may be deleted, locked, or manipulated (ex: changed credentials) to remove access to accounts. Adversaries may also subsequently log off and/or perform a [System Shutdown/Reboot](https://attack.mitre.org/techniques/T1529) to set malicious changes into place.(Citation: CarbonBlack LockerGoga 2019)(Citation: Unit42 LockerGoga 2019)

In Windows, [Net](https://attack.mitre.org/software/S0039) utility, <code>Set-LocalUser</code> and <code>Set-ADAccountPassword</code> [PowerShell](https://attack.mitre.org/techniques/T1059/001) cmdlets may be used by adversaries to modify user accounts. Accounts could also be disabled by Group Policy. In Linux, the <code>passwd</code> utility may be used to change passwords. On ESXi servers, accounts can be removed or modified via esxcli (`system account set`, `system account remove`).

Adversaries who use ransomware or similar attacks may first perform this and other Impact behaviors, such as [Data Destruction](https://attack.mitre.org/techniques/T1485) and [Defacement](https://attack.mitre.org/techniques/T1491), in order to impede incident response/recovery before completing the [Data Encrypted for Impact](https://attack.mitre.org/techniques/T1486) objective.

## Threat-Mapped Scoring

Score: 3.25

Priority: P2 - Serious (High)

## Kill Chain Phases

**•** mitre-attack: impact

## Malware

* DEADWOOD
* LockerGoga
* MegaCortex
* Meteor

## APTs (Intrusion Sets)

* Akira
* LAPSUS$