# TTP Detail – T1078.003

## TTP Information

Name: Local Accounts

Description: Adversaries may obtain and abuse credentials of a local account as a means of gaining Initial Access, Persistence, Privilege Escalation, or Defense Evasion. Local accounts are those configured by an organization for use by users, remote support, services, or for administration on a single system or service.

Local Accounts may also be abused to elevate privileges and harvest credentials through [OS Credential Dumping](https://attack.mitre.org/techniques/T1003). Password reuse may allow the abuse of local accounts across a set of machines on a network for the purposes of Privilege Escalation and Lateral Movement.

## Threat-Mapped Scoring

Score: 3.25

Priority: P2 - Serious (High)

## Kill Chain Phases

**•** mitre-attack: defense-evasion

**•** mitre-attack: persistence

**•** mitre-attack: privilege-escalation

**•** mitre-attack: initial-access

## Malware

* Cobalt Strike
* Emotet
* LockBit 3.0
* NotPetya
* Umbreon

## APTs (Intrusion Sets)

* APT29
* APT32
* FIN10
* FIN7
* HAFNIUM
* Kimsuky
* PROMETHIUM
* Play
* Sea Turtle
* Tropic Trooper
* Turla
* Velvet Ant