# TTP Detail – T1036.010

## TTP Information

Name: Masquerade Account Name

Description: Adversaries may match or approximate the names of legitimate accounts to make newly created ones appear benign. This will typically occur during [Create Account](https://attack.mitre.org/techniques/T1136), although accounts may also be renamed at a later date. This may also coincide with [Account Access Removal](https://attack.mitre.org/techniques/T1531) if the actor first deletes an account before re-creating one with the same name.(Citation: Huntress MOVEit 2023)

Often, adversaries will attempt to masquerade as service accounts, such as those associated with legitimate software, data backups, or container cluster management.(Citation: Elastic CUBA Ransomware 2022)(Citation: Aquasec Kubernetes Attack 2023) They may also give accounts generic, trustworthy names, such as “admin”, “help”, or “root.”(Citation: Invictus IR Cloud Ransomware 2024) Sometimes adversaries may model account names off of those already existing in the system, as a follow-on behavior to [Account Discovery](https://attack.mitre.org/techniques/T1087).

Note that this is distinct from [Impersonation](https://attack.mitre.org/techniques/T1656), which describes impersonating specific trusted individuals or organizations, rather than user or service account names.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Kill Chain Phases

**•** mitre-attack: defense-evasion

## Malware

* Flame
* ServHelper

## APTs (Intrusion Sets)

* APT3
* Dragonfly
* Magic Hound
* Storm-1811