# TTP Detail – T1136.001

## TTP Information

Name: Local Account

Description: Adversaries may create a local account to maintain access to victim systems. Local accounts are those configured by an organization for use by users, remote support, services, or for administration on a single system or service.

For example, with a sufficient level of access, the Windows <code>net user /add</code> command can be used to create a local account. In Linux, the `useradd` command can be used, while on macOS systems, the <code>dscl -create</code> command can be used. Local accounts may also be added to network devices, often via common [Network Device CLI](https://attack.mitre.org/techniques/T1059/008) commands such as <code>username</code>, to ESXi servers via `esxcli system account add`, or to Kubernetes clusters using the `kubectl` utility.(Citation: cisco\_username\_cmd)(Citation: Kubernetes Service Accounts Security)

Such accounts may be used to establish secondary credentialed access that do not require persistent remote access tools to be deployed on the system.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Kill Chain Phases

**•** mitre-attack: persistence

## Malware

* Calisto
* Carbanak
* DarkGate
* Flame
* GoldenSpy
* HiddenWasp
* Hildegard
* Mis-Type
* S-Type
* SMOKEDHAM
* ServHelper
* ZxShell

## Tools

* Empire
* Net
* Pupy

## APTs (Intrusion Sets)

* APT3
* APT39
* APT41
* APT5
* Daggerfly
* Dragonfly
* FIN13
* Fox Kitten
* Indrik Spider
* Kimsuky
* Leafminer
* Magic Hound
* TeamTNT
* Wizard Spider