# TTP Detail – T1136.002

## TTP Information

Name: Domain Account

Description: Adversaries may create a domain account to maintain access to victim systems. Domain accounts are those managed by Active Directory Domain Services where access and permissions are configured across systems and services that are part of that domain. Domain accounts can cover user, administrator, and service accounts. With a sufficient level of access, the <code>net user /add /domain</code> command can be used to create a domain account.(Citation: Savill 1999)

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

## Tools

* Empire
* Net
* PsExec
* Pupy

## APTs (Intrusion Sets)

* BlackByte
* GALLIUM
* HAFNIUM
* Wizard Spider