# TTP Detail – T1078.002

## TTP Information

Name: Domain Accounts

Description: Adversaries may obtain and abuse credentials of a domain account as a means of gaining Initial Access, Persistence, Privilege Escalation, or Defense Evasion.(Citation: TechNet Credential Theft) 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 users, administrators, and services.(Citation: Microsoft AD Accounts)

Adversaries may compromise domain accounts, some with a high level of privileges, through various means such as [OS Credential Dumping](https://attack.mitre.org/techniques/T1003) or password reuse, allowing access to privileged resources of the domain.

## 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
* CreepySnail
* Ryuk
* Shamoon
* Stuxnet

## APTs (Intrusion Sets)

* APT3
* APT5
* Agrius
* Aquatic Panda
* BlackByte
* Chimera
* Cinnamon Tempest
* Indrik Spider
* Magic Hound
* Naikon
* OilRig
* Play
* Sandworm Team
* TA505
* Threat Group-1314
* ToddyCat
* Volt Typhoon
* Wizard Spider