# TTP Detail – T1069.002

## TTP Information

Name: Domain Groups

Description: Adversaries may attempt to find domain-level groups and permission settings. The knowledge of domain-level permission groups can help adversaries determine which groups exist and which users belong to a particular group. Adversaries may use this information to determine which users have elevated permissions, such as domain administrators.

Commands such as <code>net group /domain</code> of the [Net](https://attack.mitre.org/software/S0039) utility, <code>dscacheutil -q group</code> on macOS, and <code>ldapsearch</code> on Linux can list domain-level groups.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Kill Chain Phases

**•** mitre-attack: discovery

## Malware

* BADHATCH
* BlackCat
* Cobalt Strike
* Egregor
* GRIFFON
* Gootloader
* Helminth
* Kwampirs
* Latrodectus
* OSInfo
* POWRUNER
* REvil
* SoreFang
* WellMess

## Tools

* AdFind
* BloodHound
* Brute Ratel C4
* CrackMapExec
* Net
* SILENTTRINITY
* dsquery

## APTs (Intrusion Sets)

* Dragonfly
* FIN7
* INC Ransom
* Inception
* Ke3chang
* LAPSUS$
* OilRig
* ToddyCat
* Turla
* Volt Typhoon