# TTP Detail – T1069

## TTP Information

Name: Permission Groups Discovery

Description: Adversaries may attempt to discover group and permission settings. This information can help adversaries determine which user accounts and groups are available, the membership of users in particular groups, and which users and groups have elevated permissions.

Adversaries may attempt to discover group permission settings in many different ways. This data may provide the adversary with information about the compromised environment that can be used in follow-on activity and targeting.(Citation: CrowdStrike BloodHound April 2018)

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Kill Chain Phases

**•** mitre-attack: discovery

## Malware

* Carbon
* IcedID
* MURKYTOP
* Siloscape
* TrickBot

## Tools

* ShimRatReporter

## APTs (Intrusion Sets)

* APT3
* APT41
* FIN13
* TA505
* Volt Typhoon