# TTP Detail – T1615

## TTP Information

Name: Group Policy Discovery

Description: Adversaries may gather information on Group Policy settings to identify paths for privilege escalation, security measures applied within a domain, and to discover patterns in domain objects that can be manipulated or used to blend in the environment. Group Policy allows for centralized management of user and computer settings in Active Directory (AD). Group policy objects (GPOs) are containers for group policy settings made up of files stored within a predictable network path `\<DOMAIN>\SYSVOL\<DOMAIN>\Policies\`.(Citation: TechNet Group Policy Basics)(Citation: ADSecurity GPO Persistence 2016)

Adversaries may use commands such as <code>gpresult</code> or various publicly available PowerShell functions, such as <code>Get-DomainGPO</code> and <code>Get-DomainGPOLocalGroup</code>, to gather information on Group Policy settings.(Citation: Microsoft gpresult)(Citation: Github PowerShell Empire) Adversaries may use this information to shape follow-on behaviors, including determining potential attack paths within the target network as well as opportunities to manipulate Group Policy settings (i.e. [Domain or Tenant Policy Modification](https://attack.mitre.org/techniques/T1484)) for their benefit.

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## Kill Chain Phases

**•** mitre-attack: discovery

## Malware

* DUSTTRAP
* Emissary
* LunarWeb

## Tools

* BloodHound
* Empire

## APTs (Intrusion Sets)

* Turla