# TTP Detail – T1526

## TTP Information

Name: Cloud Service Discovery

Description: An adversary may attempt to enumerate the cloud services running on a system after gaining access. These methods can differ from platform-as-a-service (PaaS), to infrastructure-as-a-service (IaaS), or software-as-a-service (SaaS). Many services exist throughout the various cloud providers and can include Continuous Integration and Continuous Delivery (CI/CD), Lambda Functions, Entra ID, etc. They may also include security services, such as AWS GuardDuty and Microsoft Defender for Cloud, and logging services, such as AWS CloudTrail and Google Cloud Audit Logs.

Adversaries may attempt to discover information about the services enabled throughout the environment. Azure tools and APIs, such as the Microsoft Graph API and Azure Resource Manager API, can enumerate resources and services, including applications, management groups, resources and policy definitions, and their relationships that are accessible by an identity.(Citation: Azure - Resource Manager API)(Citation: Azure AD Graph API)

For example, Stormspotter is an open source tool for enumerating and constructing a graph for Azure resources and services, and Pacu is an open source AWS exploitation framework that supports several methods for discovering cloud services.(Citation: Azure - Stormspotter)(Citation: GitHub Pacu)

Adversaries may use the information gained to shape follow-on behaviors, such as targeting data or credentials from enumerated services or evading identified defenses through [Disable or Modify Tools](https://attack.mitre.org/techniques/T1562/001) or [Disable or Modify Cloud Logs](https://attack.mitre.org/techniques/T1562/008).

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## Kill Chain Phases

**•** mitre-attack: discovery

## Tools

* AADInternals
* Pacu
* ROADTools