# TTP Detail – T1580

## TTP Information

Name: Cloud Infrastructure Discovery

Description: An adversary may attempt to discover infrastructure and resources that are available within an infrastructure-as-a-service (IaaS) environment. This includes compute service resources such as instances, virtual machines, and snapshots as well as resources of other services including the storage and database services.

Cloud providers offer methods such as APIs and commands issued through CLIs to serve information about infrastructure. For example, AWS provides a <code>DescribeInstances</code> API within the Amazon EC2 API that can return information about one or more instances within an account, the <code>ListBuckets</code> API that returns a list of all buckets owned by the authenticated sender of the request, the <code>HeadBucket</code> API to determine a bucket’s existence along with access permissions of the request sender, or the <code>GetPublicAccessBlock</code> API to retrieve access block configuration for a bucket.(Citation: Amazon Describe Instance)(Citation: Amazon Describe Instances API)(Citation: AWS Get Public Access Block)(Citation: AWS Head Bucket) Similarly, GCP's Cloud SDK CLI provides the <code>gcloud compute instances list</code> command to list all Google Compute Engine instances in a project (Citation: Google Compute Instances), and Azure's CLI command <code>az vm list</code> lists details of virtual machines.(Citation: Microsoft AZ CLI) In addition to API commands, adversaries can utilize open source tools to discover cloud storage infrastructure through [Wordlist Scanning](https://attack.mitre.org/techniques/T1595/003).(Citation: Malwarebytes OSINT Leaky Buckets - Hioureas)

An adversary may enumerate resources using a compromised user's access keys to determine which are available to that user.(Citation: Expel IO Evil in AWS) The discovery of these available resources may help adversaries determine their next steps in the Cloud environment, such as establishing Persistence.(Citation: Mandiant M-Trends 2020)An adversary may also use this information to change the configuration to make the bucket publicly accessible, allowing data to be accessed without authentication. Adversaries have also may use infrastructure discovery APIs such as <code>DescribeDBInstances</code> to determine size, owner, permissions, and network ACLs of database resources. (Citation: AWS Describe DB Instances) Adversaries can use this information to determine the potential value of databases and discover the requirements to access them. Unlike in [Cloud Service Discovery](https://attack.mitre.org/techniques/T1526), this technique focuses on the discovery of components of the provided services rather than the services themselves.

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## Kill Chain Phases

**•** mitre-attack: discovery

## Tools

* Pacu

## APTs (Intrusion Sets)

* Scattered Spider