# TTP Detail – T1059.009

## TTP Information

Name: Cloud API

Description: Adversaries may abuse cloud APIs to execute malicious commands. APIs available in cloud environments provide various functionalities and are a feature-rich method for programmatic access to nearly all aspects of a tenant. These APIs may be utilized through various methods such as command line interpreters (CLIs), in-browser Cloud Shells, [PowerShell](https://attack.mitre.org/techniques/T1059/001) modules like Azure for PowerShell(Citation: Microsoft - Azure PowerShell), or software developer kits (SDKs) available for languages such as [Python](https://attack.mitre.org/techniques/T1059/006).

Cloud API functionality may allow for administrative access across all major services in a tenant such as compute, storage, identity and access management (IAM), networking, and security policies.

With proper permissions (often via use of credentials such as [Application Access Token](https://attack.mitre.org/techniques/T1550/001) and [Web Session Cookie](https://attack.mitre.org/techniques/T1550/004)), adversaries may abuse cloud APIs to invoke various functions that execute malicious actions. For example, CLI and PowerShell functionality may be accessed through binaries installed on cloud-hosted or on-premises hosts or accessed through a browser-based cloud shell offered by many cloud platforms (such as AWS, Azure, and GCP). These cloud shells are often a packaged unified environment to use CLI and/or scripting modules hosted as a container in the cloud environment.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Kill Chain Phases

**•** mitre-attack: execution

## Tools

* Pacu

## APTs (Intrusion Sets)

* APT29
* TeamTNT