# TTP Detail – T1586.003

## TTP Information

Name: Cloud Accounts

Description: Adversaries may compromise cloud accounts that can be used during targeting. Adversaries can use compromised cloud accounts to further their operations, including leveraging cloud storage services such as Dropbox, Microsoft OneDrive, or AWS S3 buckets for [Exfiltration to Cloud Storage](https://attack.mitre.org/techniques/T1567/002) or to [Upload Tool](https://attack.mitre.org/techniques/T1608/002)s. Cloud accounts can also be used in the acquisition of infrastructure, such as [Virtual Private Server](https://attack.mitre.org/techniques/T1583/003)s or [Serverless](https://attack.mitre.org/techniques/T1583/007) infrastructure. Additionally, cloud-based messaging services such as Twilio, SendGrid, AWS End User Messaging, AWS SNS (Simple Notification Service), or AWS SES (Simple Email Service) may be leveraged for spam or [Phishing](https://attack.mitre.org/techniques/T1566).(Citation: Palo Alto Unit 42 Compromised Cloud Compute Credentials 2022)(Citation: Netcraft SendGrid 2024) Compromising cloud accounts may allow adversaries to develop sophisticated capabilities without managing their own servers.(Citation: Awake Security C2 Cloud)

A variety of methods exist for compromising cloud accounts, such as gathering credentials via [Phishing for Information](https://attack.mitre.org/techniques/T1598), purchasing credentials from third-party sites, conducting [Password Spraying](https://attack.mitre.org/techniques/T1110/003) attacks, or attempting to [Steal Application Access Token](https://attack.mitre.org/techniques/T1528)s.(Citation: MSTIC Nobelium Oct 2021) Prior to compromising cloud accounts, adversaries may conduct Reconnaissance to inform decisions about which accounts to compromise to further their operation. In some cases, adversaries may target privileged service provider accounts with the intent of leveraging a [Trusted Relationship](https://attack.mitre.org/techniques/T1199) between service providers and their customers.(Citation: MSTIC Nobelium Oct 2021)

## Threat-Mapped Scoring

Score: 3.0

Priority: P2 - Serious (High)

## Kill Chain Phases

**•** mitre-attack: resource-development

## APTs (Intrusion Sets)

* APT29