# TTP Detail – T1496.004

## TTP Information

Name: Cloud Service Hijacking

Description: Adversaries may leverage compromised software-as-a-service (SaaS) applications to complete resource-intensive tasks, which may impact hosted service availability.

For example, adversaries may leverage email and messaging services, such as AWS Simple Email Service (SES), AWS Simple Notification Service (SNS), SendGrid, and Twilio, in order to send large quantities of spam / [Phishing](https://attack.mitre.org/techniques/T1566) emails and SMS messages.(Citation: Invictus IR DangerDev 2024)(Citation: Permiso SES Abuse 2023)(Citation: SentinelLabs SNS Sender 2024) Alternatively, they may engage in LLMJacking by leveraging reverse proxies to hijack the power of cloud-hosted AI models.(Citation: Sysdig LLMJacking 2024)(Citation: Lacework LLMJacking 2024)

In some cases, adversaries may leverage services that the victim is already using. In others, particularly when the service is part of a larger cloud platform, they may first enable the service.(Citation: Sysdig LLMJacking 2024) Leveraging SaaS applications may cause the victim to incur significant financial costs, use up service quotas, and otherwise impact availability.

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## Kill Chain Phases

**•** mitre-attack: impact