# TTP Detail – T1535

## TTP Information

Name: Unused/Unsupported Cloud Regions

Description: Adversaries may create cloud instances in unused geographic service regions in order to evade detection. Access is usually obtained through compromising accounts used to manage cloud infrastructure.

Cloud service providers often provide infrastructure throughout the world in order to improve performance, provide redundancy, and allow customers to meet compliance requirements. Oftentimes, a customer will only use a subset of the available regions and may not actively monitor other regions. If an adversary creates resources in an unused region, they may be able to operate undetected.

A variation on this behavior takes advantage of differences in functionality across cloud regions. An adversary could utilize regions which do not support advanced detection services in order to avoid detection of their activity.

An example of adversary use of unused AWS regions is to mine cryptocurrency through [Resource Hijacking](https://attack.mitre.org/techniques/T1496), which can cost organizations substantial amounts of money over time depending on the processing power used.(Citation: CloudSploit - Unused AWS Regions)

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## Kill Chain Phases

**•** mitre-attack: defense-evasion