Unused (Unsupported) Cloud Regions (version 1.0)

**Cloud Service Label: IaaS**

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. For example, AWS GuardDuty is not supported in every region. 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.

Examples

|  |  |
| --- | --- |
| **Name** | **Description** |
| CloudSploit | This blog post notes how they received an email about an ASW customer who had not deactivated unused regions and found there to be 50 EC2 instances running to mine Bitcoin 24/7. |

Mitigations

|  |  |
| --- | --- |
| **Mitigation** | **Description** |
| Software Configuration | Cloud service providers may allow customers to deactivate unused regions. |
| Monitor Unused Regions | Even if the region is unused, it should be set up to be monitored utilizing tools such as CloudTrail. |
| Deactivate Unused Region Endpoints | Disable user ability to generate STS credentials in unused regions. |
| Don’t Enable New Regions Unless Required | If a region is not enabled by default and when a malicious actor attempts to create new resource, they will be asked to first enabled the region. They will be unable to do so if they do not have administrator privileges or the correct IAM role. |

Detection

|  |  |
| --- | --- |
| **Detection** | **Description** |
| Enable CloudTrail across all regions in AWS | To enabled CloudTrail across all regions:   1. Sign into the AWS Management Console and open the CloudTrail console 2. Click on *Trails* 3. Set necessary Trails to All option in the I column 4. Click on a trail via the link *Name* column 5. Set *Logging* to *ON* 6. Set *Apply trail to all regions* to *Yes* |
| Configure log profile to capture activity logs for all regions in Azure | To set up activity logs for all regions:   1. Navigate to Azure console 2. Go to *Activity log* 3. Select *Export* 4. Select *Subscription* 5. Check *Select all* in *Regions* 6. Select *Save* |
| Monitoring for Regional Activity | Tools like Splunk or even CloudSploit have the ability to alert based on region and ingest CloudTrail logs. In CloudSploit, a plugin called EC2 Max Count can be configured to alert after a certain threshold of EC2 instances is met. Real-Time Events service is another feature of CloudSploit that allows alerts for activity in unused regions. |

References

1. https://blog.cloudsploit.com/the-danger-of-unused-aws-regions-af0bf1b878fc. Accessed July 1, 2020.