Modify Cloud Resource Hierarchy, Technique T1666 - Enterprise

Archived: 2026-04-05 17:20:44 UTC

Adversaries may attempt to modify hierarchical structures in infrastructure-as-a-service (IaaS) environments in order to evade defenses.

IaaS environments often group resources into a hierarchy, enabling improved resource management and application of policies to relevant groups. Hierarchical structures differ among cloud providers. For example, in AWS environments, multiple accounts can be grouped under a single organization, while in Azure environments, multiple subscriptions can be grouped under a single management group.[1][2]

Adversaries may add, delete, or otherwise modify resource groups within an IaaS hierarchy. For example, in Azure environments, an adversary who has gained access to a Global Administrator account may create new subscriptions in which to deploy resources. They may also engage in subscription hijacking by transferring an existing pay-as-you-go subscription from a victim tenant to an adversary-controlled tenant. This will allow the adversary to use the victim's compute resources without generating logs on the victim tenant.[3][4]

In AWS environments, adversaries with appropriate permissions in a given account may call the `LeaveOrganization` API, causing the account to be severed from the AWS Organization to which it was tied and removing any Service Control Policies, guardrails, or restrictions imposed upon it by its former Organization. Alternatively, adversaries may call the `CreateAccount` API in order to create a new account within an AWS Organization. This account will use the same payment methods registered to the payment account but may not be subject to existing detections or Service Control Policies.[5]

Source: https://attack.mitre.org/techniques/T1666