Account Manipulation: Additional Cloud Roles, Sub-technique T1098.003 - Enterprise

Archived: 2026-04-02 10:51:10 UTC

An adversary may add additional roles or permissions to an adversary-controlled cloud account to maintain persistent access to a tenant. For example, adversaries may update IAM policies in cloud-based environments or add a new global administrator in Office 365 environments.[1][2][3][4] With sufficient permissions, a compromised account can gain almost unlimited access to data and settings (including the ability to reset the passwords of other admins).[5]
[4]

This account modification may immediately follow Create Account or other malicious account activity. Adversaries may also modify existing Valid Accounts that they have compromised. This could lead to privilege escalation, particularly if the roles added allow for lateral movement to additional accounts.

For example, in AWS environments, an adversary with appropriate permissions may be able to use the `CreatePolicyVersion` API to define a new version of an IAM policy or the `AttachUserPolicy` API to attach an IAM policy with additional or distinct permissions to a compromised user account.[6]

In some cases, adversaries may add roles to adversary-controlled accounts outside the victim cloud tenant. This allows these external accounts to perform actions inside the victim tenant without requiring the adversary to Create Account or modify a victim-owned account.[7]

Source: https://attack.mitre.org/techniques/T1098/003