Remote Services: Cloud Services, Sub-technique T1021.007 - Enterprise

Archived: 2026-04-05 16:57:20 UTC

Adversaries may log into accessible cloud services within a compromised environment using Valid Accounts that are synchronized with or federated to on-premises user identities. The adversary may then perform management actions or access cloud-hosted resources as the logged-on user.

Many enterprises federate centrally managed user identities to cloud services, allowing users to login with their domain credentials in order to access the cloud control plane. Similarly, adversaries may connect to available cloud services through the web console or through the cloud command line interface (CLI) (e.g., Cloud API), using commands such as `Connect-AZAccount` for Azure PowerShell, `Connect-MgGraph` for Microsoft Graph PowerShell, and `gcloud auth login` for the Google Cloud CLI.

In some cases, adversaries may be able to authenticate to these services via Application Access Token instead of a username and password.

Source: https://attack.mitre.org/techniques/T1021/007