Credentials from Password Stores: Cloud Secrets Management Stores, Sub-technique T1555.006 - Enterprise

Archived: 2026-04-05 15:46:45 UTC

Adversaries may acquire credentials from cloud-native secret management solutions such as AWS Secrets Manager, GCP Secret Manager, Azure Key Vault, and Terraform Vault.

Secrets managers support the secure centralized management of passwords, API keys, and other credential material. Where secrets managers are in use, cloud services can dynamically acquire credentials via API requests rather than accessing secrets insecurely stored in plain text files or environment variables.

If an adversary is able to gain sufficient privileges in a cloud environment – for example, by obtaining the credentials of high-privileged Cloud Accounts or compromising a service that has permission to retrieve secrets – they may be able to request secrets from the secrets manager. This can be accomplished via commands such as `get-secret-value` in AWS, `gcloud secrets describe` in GCP, and `az key vault secret show` in Azure.[1][2][3][4][5]

Note: this technique is distinct from Cloud Instance Metadata API in that the credentials are being directly requested from the cloud secrets manager, rather than through the medium of the instance metadata API.

Source: https://attack.mitre.org/techniques/T1555/006