Transfer Data to Cloud Account, Technique T1537 - Enterprise

Archived: 2026-04-05 18:42:19 UTC

Adversaries may exfiltrate data by transferring the data, including through sharing/syncing and creating backups of cloud environments, to another cloud account they control on the same service.

A defender who is monitoring for large transfers to outside the cloud environment through normal file transfers or over command and control channels may not be watching for data transfers to another account within the same cloud provider. Such transfers may utilize existing cloud provider APIs and the internal address space of the cloud provider to blend into normal traffic or avoid data transfers over external network interfaces.[1]

Adversaries may also use cloud-native mechanisms to share victim data with adversary-controlled cloud accounts, such as creating anonymous file sharing links or, in Azure, a shared access signature (SAS) URI.[2]

Incidents have been observed where adversaries have created backups of cloud instances and transferred them to separate accounts.[3]

Source: https://attack.mitre.org/techniques/T1537