Serverless Execution, Technique T1648 - Enterprise

Archived: 2026-04-05 17:42:09 UTC

Adversaries may abuse serverless computing, integration, and automation services to execute arbitrary code in cloud environments. Many cloud providers offer a variety of serverless resources, including compute engines, application integration services, and web servers.

Adversaries may abuse these resources in various ways as a means of executing arbitrary commands. For example, adversaries may use serverless functions to execute malicious code, such as crypto-mining malware (i.e. Resource Hijacking).[1] Adversaries may also create functions that enable further compromise of the cloud environment. For example, an adversary may use the `IAM:PassRole` permission in AWS or the `iam.serviceAccounts.actAs` permission in Google Cloud to add Additional Cloud Roles to a serverless cloud function, which may then be able to perform actions the original user cannot.[2][3]

Serverless functions can also be invoked in response to cloud events (i.e. Event Triggered Execution), potentially enabling persistent execution over time. For example, in AWS environments, an adversary may create a Lambda function that automatically adds Additional Cloud Credentials to a user and a corresponding CloudWatch events rule that invokes that function whenever a new user is created.[4] This is also possible in many cloud-based office application suites. For example, in Microsoft 365 environments, an adversary may create a Power Automate workflow that forwards all emails a user receives or creates anonymous sharing links whenever a user is granted access to a document in SharePoint.[5][6] In Google Workspace environments, they may instead create an Apps Script that exfiltrates a user's data when they open a file.[7][8]

Source: https://attack.mitre.org/techniques/T1648