# TTP Detail – T1648

## TTP Information

Name: Serverless Execution

Description: 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](https://attack.mitre.org/techniques/T1496)).(Citation: Cado Security Denonia) 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](https://attack.mitre.org/techniques/T1098/003) to a serverless cloud function, which may then be able to perform actions the original user cannot.(Citation: Rhino Security Labs AWS Privilege Escalation)(Citation: Rhingo Security Labs GCP Privilege Escalation)  
  
Serverless functions can also be invoked in response to cloud events (i.e. [Event Triggered Execution](https://attack.mitre.org/techniques/T1546)), potentially enabling persistent execution over time. For example, in AWS environments, an adversary may create a Lambda function that automatically adds [Additional Cloud Credentials](https://attack.mitre.org/techniques/T1098/001) to a user and a corresponding CloudWatch events rule that invokes that function whenever a new user is created.(Citation: Backdooring an AWS account) 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.(Citation: Varonis Power Automate Data Exfiltration)(Citation: Microsoft DART Case Report 001) In Google Workspace environments, they may instead create an Apps Script that exfiltrates a user's data when they open a file.(Citation: Cloud Hack Tricks GWS Apps Script)(Citation: OWN-CERT Google App Script 2024)

## Threat-Mapped Scoring

Score: 1.9

Priority: P3 - Important (Medium)

## Kill Chain Phases

**•** mitre-attack: execution

## Tools

* Pacu