# TTP Detail – T1584.007

## TTP Information

Name: Serverless

Description: Adversaries may compromise serverless cloud infrastructure, such as Cloudflare Workers, AWS Lambda functions, or Google Apps Scripts, that can be used during targeting. By utilizing serverless infrastructure, adversaries can make it more difficult to attribute infrastructure used during operations back to them.

Once compromised, the serverless runtime environment can be leveraged to either respond directly to infected machines or to [Proxy](https://attack.mitre.org/techniques/T1090) traffic to an adversary-owned command and control server.(Citation: BlackWater Malware Cloudflare Workers)(Citation: AWS Lambda Redirector)(Citation: GWS Apps Script Abuse 2021) As traffic generated by these functions will appear to come from subdomains of common cloud providers, it may be difficult to distinguish from ordinary traffic to these providers - making it easier to [Hide Infrastructure](https://attack.mitre.org/techniques/T1665).(Citation: Detecting Command & Control in the Cloud)(Citation: BlackWater Malware Cloudflare Workers)

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Kill Chain Phases

**•** mitre-attack: resource-development