Acquire Infrastructure: Serverless, Sub-technique T1583.007 - Enterprise

Archived: 2026-04-05 15:50:38 UTC

Adversaries may purchase and configure 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 acquired, the serverless runtime environment can be leveraged to either respond directly to infected machines or to Proxy traffic to an adversary-owned command and control server.[1][2][3] 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.[4][1]

Source: https://attack.mitre.org/techniques/T1583/007