Price Hiller
Cody Ledbetter
Roman Rendon
Sean Nicosia
Project Group 10

AWS & Terraform: Proving Provenance of Emails via DKIM

Overview

The purpose of this project is to create a simple DKIM record tracker using Amazon Web Services (AWS) resources orchestrated through Terraform.

Tracking DKIM records is of increasing importance in modern business environments due to the prevalence of man-in-the-middle attacks in email. Proving the provenance of an email allows for an aggrieved party to show, beyond a reasonable doubt, a breach of a business partner's emails before a court. Maintaining historical DKIM records is tantamount to proving historical email provenance.

For instance, take business partners agreeing to a wire transfer in which an attacker has access to one of the partner's emails. The attacker could then send an email from the breached partner, appearing as them, with the attacker's bank info to fraudulently attain funds. If the partner lost their funds to the attacker, they would now have a cause of action to recover their lost funds from their business partner due to that partner's cybersecurity negligence.

Goals

1. Understand the basics of various AWS resources such as (but not limited to):
   - Lambda
   - Route53
   - DynamoDB
   - EventBridge Scheduler
2. Learn to provision resources in a public cloud with Hashicorp Terraform
3. Understand how to execute idempotent, coordinated DNS record lookups from AWS
4. Demonstrate knowledge of modern CI/CD practices, leveraging pipelines to test, build, and deploy services from Github using Github Actions
5. Understand secure secret management & lifecycles in AWS
   - AWS Key Management Service
   - AWS Identity Access Management

Testbed & Software Tools

1. AWS
   - Lambda
   - Route53
   - DynamoDB
   - EventBridge Scheduler
   - AWS Key Management Service
   - AWS Identity Access Management
2. Python 3.13
3. Terraform
4. Github & Github Actions