CANARY TOKENS

New token Manage this token

What is this and why should I care? Documentation

Your AWS key token is active!

Copy this credential pair to your clipboard to use as desired:

```
aws_access_key_id = AKIAYVP4CIPPB4J6MWVQ
aws_secret_access_key =
eUBLmk4g56gcHMDOn7bGzvozHPCkSJ9000w5VLoJ
output = json
region = us-east-2
```

Download your AWS Creds

This canarytoken is triggered when someone uses this credential pair to access AWS programmatically (through the API).

The key is unique. i.e. There is no chance of somebody guessing these credentials.

If this token fires, it is a clear indication that this set of keys has "leaked".

Ideas for use:

- These credentials are often stored in a file called ~/.aws/credentials on linux/OSX systems. Generate a fake credential pair for your senior developers and sysadmins and keep it on their machines. If someone tries to access AWS with the pair you generated for Bob, chances are that Bob's been compromised.
- Place the credentials in private code repositories. If the token is triggered, it means that someone is accessing that repo without permission

Brought to you by Thinkst Canary, our insanely easy-to-use honeypot solution that deploys in just 3 minutes. **Know. When it matters.**