

Cybersecurity Incident Report

Date: March 29, 2025

Prepared by: Dennis Gilbert

Affected Account: AWS Account ID: 916147069515

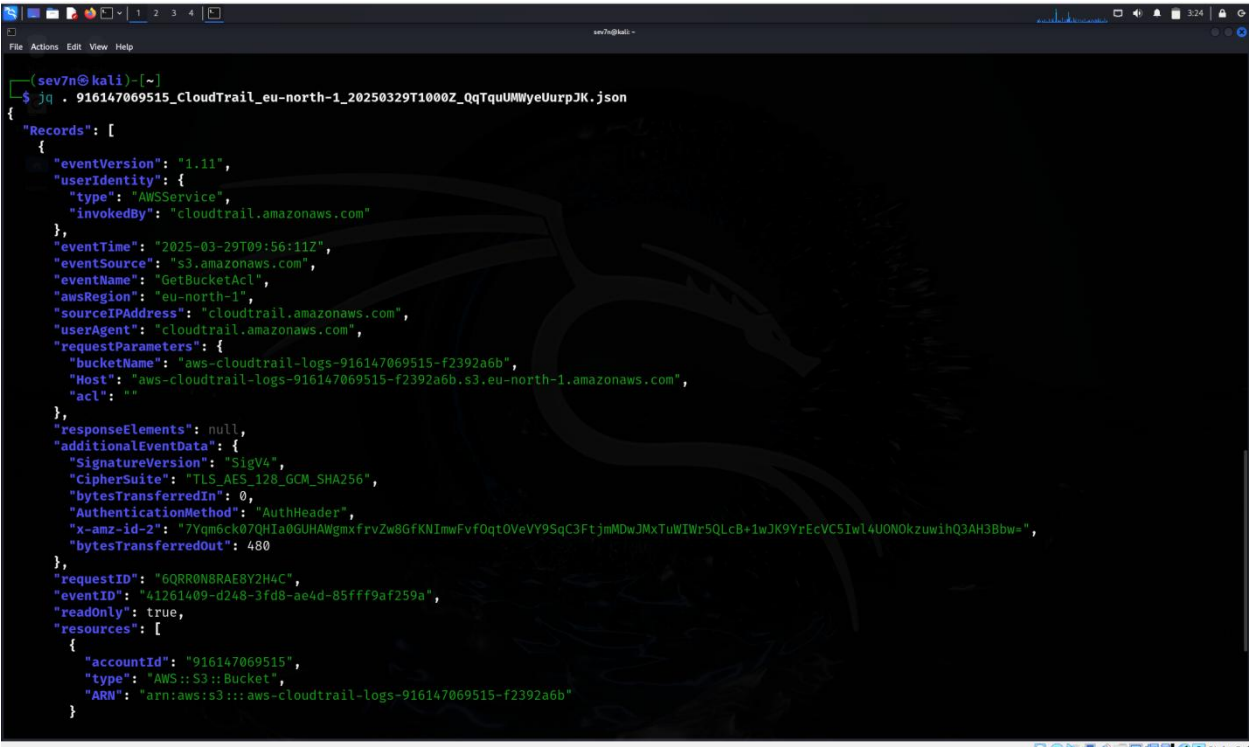
Incident Summary

This report details an unusual activity recorded in AWS CloudTrail logs involving an unauthorized attempt to access the Access Control List (ACL) of an Amazon S3 bucket. The event, originating from AWS CloudTrail, indicates an API call to GetBucketAcl on the S3 bucket aws-cloudtrail-logs-916147069515-f2392a6b. The request was made by cloudtrail.amazonaws.com on March 29, 2025, at 09:56:11 UTC. While the source IP address was identified as a legitimate AWS service, it is critical to assess whether this action was authorized and expected.

Findings

1. Unauthorized API Call Attempt:

- Event Name: GetBucketAcl
- Event Source: s3.amazonaws.com
- Timestamp: 2025-03-29T09:56:11Z
- Region: eu-north-1
- Source IP Address: cloudtrail.amazonaws.com
- User Agent: cloudtrail.amazonaws.com
- Event ID: 41261409-d248-3fd8-ae4d-85fff9af259a
- Event Type: AwsApiCall
- Management Event: true
- Read-Only: true



```
(sev7n@kali) ~  
$ jq . 916147069515_cloudTrail_eu-north-1_20250329T1000Z_QqTquUMMyeUurpJK.json  
{  
  "Records": [  
    {  
      "eventVersion": "1.11",  
      "userIdentity": {  
        "type": "AWSService",  
        "invokedBy": "cloudtrail.amazonaws.com"  
      },  
      "eventTime": "2025-03-29T09:56:11Z",  
      "eventSource": "s3.amazonaws.com",  
      "eventName": "GetBucketAcl",  
      "awsRegion": "eu-north-1",  
      "sourceIPAddress": "cloudtrail.amazonaws.com",  
      "userAgent": "cloudtrail.amazonaws.com",  
      "requestParameters": {  
        "bucketName": "aws-cloudtrail-logs-916147069515-f2392a6b",  
        "Host": "aws-cloudtrail-logs-916147069515-f2392a6b.s3.eu-north-1.amazonaws.com",  
        "acl": ""  
      },  
      "responseElements": null,  
      "additionalEventData": {  
        "SignatureVersion": "SigV4",  
        "CipherSuite": "TLS_AES_128_GCM_SHA256",  
        "bytesTransferredIn": 0,  
        "AuthenticationMethod": "AuthHeader",  
        "x-amz-id-2": "7Yqm6ck07QHia0GUHAWgmxfvZw8GfKNImwFv0qtOveVY9SqC3FtjmMDwJmXtUWIwR5QLcB+1wJK9YrEcVC5IwL4UONOkzuwihQ3AH3Bbw=",  
        "bytesTransferredOut": 480  
      },  
      "requestID": "6QRRON8RAE8Y2H4C",  
      "eventID": "41261409-d248-3fd8-ae4d-85fff9af259a",  
      "readOnly": true,  
      "resources": [  
        {  
          "accountId": "916147069515",  
          "type": "AWS::S3::Bucket",  
          "ARN": "arn:aws:s3:::aws-cloudtrail-logs-916147069515-f2392a6b"  
        }  
      ]  
    }  
  ]  
}
```

2. Request Parameters:

- Target Bucket: aws-cloudtrail-logs-916147069515-f2392a6b
- Host: aws-cloudtrail-logs-916147069515-f2392a6b.s3.eu-north-1.amazonaws.com

- ACL Requested: Empty (potential enumeration attempt)

3. Security Configuration Weaknesses:

- Lack of explicit verification if this request was expected.
- Potential risk if unauthorized access is granted.
- CloudTrail logging confirms the event but does not explicitly deny access.

Risk Assessment

Threat Level: Medium

Potential Impact: Unauthorized retrieval of bucket ACL information, which may lead to further privilege escalation attempts.

Recommendations

1. Immediate Actions:

- **Verify Access Controls:** Ensure that only authorized IAM users or roles can query bucket ACLs.
- **Review IAM Policies:** Restrict GetBucketAcl permissions to necessary roles.
- **Enable S3 Bucket Policies:** Implement deny rules for unauthorized API calls.
- **Audit CloudTrail Logs:** Investigate additional unauthorized activities within the same timeframe.

2. Long-Term Security Measures:

- **Enable Multi-Factor Authentication (MFA):** Enforce MFA on all privileged accounts.
- **Monitor CloudTrail Events:** Set up alerts for sensitive API calls like GetBucketAcl.
- **Rotate Access Keys:** Ensure regular rotation of IAM access keys to reduce exposure risks..

Conclusion

The recorded `GetBucketAcl` API call by `cloudtrail.amazonaws.com` suggests an attempt to retrieve S3 bucket permissions. While the request originated from a recognized AWS service, further investigation is needed to confirm its legitimacy and prevent potential security risks. Immediate remediation steps, including access control verification, policy enforcement, and continuous monitoring, are recommended.

Action Required: Implement the recommended security measures and continuously monitor for suspicious activities.