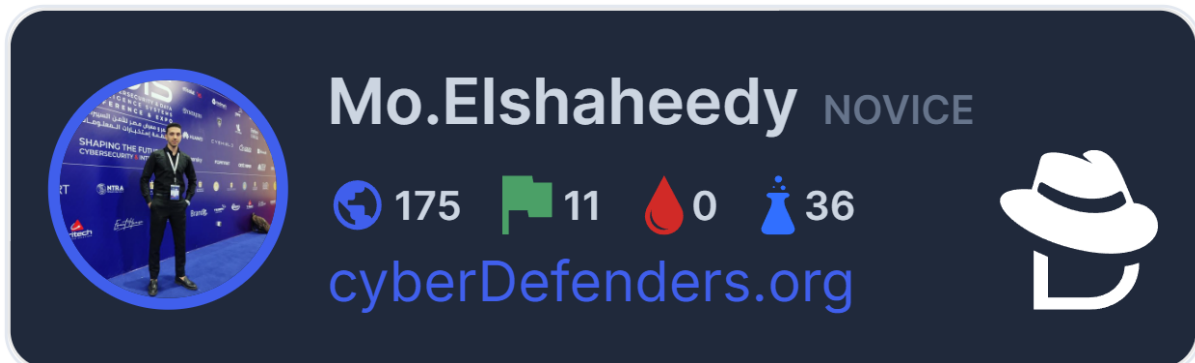


AWS RAID Challenge



<https://www.linkedin.com/in/elshaheedy/>

Topic: **Cloud Forensics**

LabLink: <https://cyberdefenders.org/blueteam-ctf-challenges/awraid/>

Scenario:

Your organization uses AWS for hosting critical data and applications. An incident has been reported involving unauthorized data access and potential exfiltration. The organization's security team has detected unusual activities and needs to investigate the incident to understand the scope, identify the attacker, and prevent further data breaches.

Tools:

- Splunk

Q1

Knowing which user account was compromised is essential for understanding the attacker's initial entry point into the environment. What is the username of the compromised user?

Query

```
index="aws_cloudtrail" eventSource="signin.amazonaws.com"  
responseElements.ConsoleLogin="Failure"
```

you will notice many failure authentication attempts

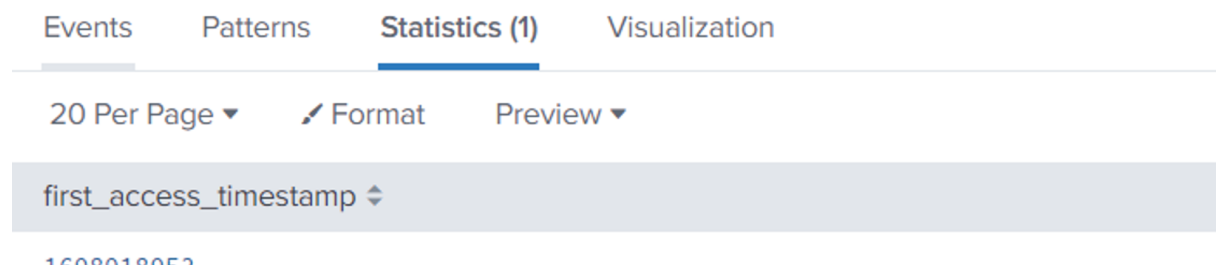
Q2

We must investigate the events following the initial compromise to understand

the attacker's motives. What's the UTC timestamp of the attacker's first access to an S3 object?

Query

index="aws_cloudtrail" eventName=GetObject userIdentity.userName=put it here
| stats min(_time) as first_access_timestamp



in unix

convert using

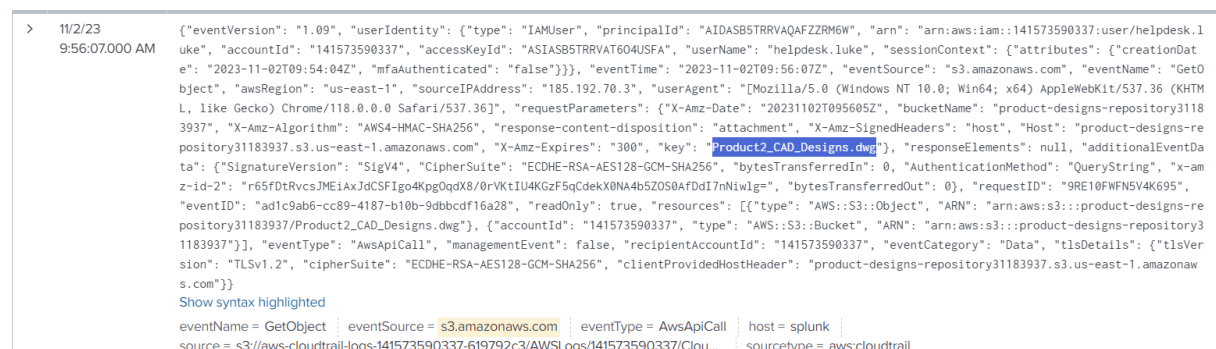
<https://www.unixtimestamp.com/>

Q3

Among the S3 buckets accessed by the attacker, one contains a DWG file. What is the name of this bucket?

Query

index="aws_cloudtrail" eventSource="s3.amazonaws.com"
| search requestParameters.key="*.dwg"



a eventCategory 1
a eventID 6
a eventTime 4
eventVersion 1
a index 1
linecount 1
a managementEvent 1
a punct 1
a readOnly 1
recipientAccountId 1
a requestID 6
a requestParameters.bucketName 1

requestParameters.bucketName

1 Value, 100% of events

Selected

Reports

Top values
Top values by time
Rare values

Events with this field

Values

Count

%

product-designs-repository31183937	6	100%
------------------------------------	---	------

Q4

We've identified changes to a bucket's configuration that allowed public access, a significant security concern. What is the name of this particular S3 bucket?

Query

this link helped me <https://community.splunk.com/t5/Splunk-Search/Splunk-query-to-check-for-S3-Buckets-in-AWS-using/m-p/571106>

it gives me the EventName which i should search with

"eventName": "PutBucketPolicy"

index="aws_cloudtrail" eventSource="s3.amazonaws.com"

eventName=GetBucketPublicAccessBlock "userIdentity.userName"="put it here"

```
> 11/2/23 9:58:03.000 AM {"eventVersion": "1.09", "userIdentity": {"type": "IAMUser", "principalId": "AIDASB5TRRVAQAFZZRM6W", "arn": "arn:aws:iam::141573590337:user/helpdesk.luke", "accountId": "141573590337", "accessKeyId": "ASIASB5TRRVA4YINUVJD", "userName": "helpdesk.luke", "sessionContext": {"attributes": {"creationDate": "2023-11-02T09:54:04Z", "mfaAuthenticated": "false"}}}, "eventTime": "2023-11-02T09:58:03Z", "eventSource": "s3.amazonaws.com", "eventName": "GetBucketPublicAccessBlock", "awsRegion": "us-east-1", "sourceIPAddress": "185.192.70.78", "userAgent": "[S3Console/0.4, aws-internal/3 aws-sdk-java/1.12.488 Linux/5.10.196-163.744.amzn2int.x86_64 OpenJDK_64-Bit_Server_VM/25.372-b08 java/1.8.0_372 vendor/Oracle_Corporation cfg/retry-mode/standard]", "requestParameters": {"publicAccessBlock": "", "bucketName": "backup-and-restore98825501", "Host": "s3.amazonaws.com"}, "responseElements": null, "additionalEventData": {"SignatureVersion": "SigV4", "CipherSuite": "ECDHE-RSA-AES128-GCM-SHA256", "bytesTransferredIn": 0, "AuthenticationMethod": "AuthHeader", "x-amz-id-2": "deNbG+MIXBwyaXZHPAUtwVEJ9sBUBWw6d0BPESF7ziNqe7WPgGoWIFcAw7bp5qBtqUiuxQ0wyQ=", "bytesTransferredOut": 330}, "requestID": "71TR01XXQDXRTTB7", "eventID": "e9b1a827-4b01-42ff-a40b-d5f7edffcd92", "readOnly": true, "resources": [{"accountId": "141573590337", "type": "AWS::S3::Bucket", "ARN": "arn:aws:s3:::backup-and-restore98825501"}], "eventType": "AwsApiCall", "managementEvent": true, "recipientAccountId": "141573590337", "vpceEndpointId": "vpce-f40dc59d", "eventCategory": "Management", "tlsDetails": {"tlsVersion": "TLSv1.2", "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256", "clientProvidedHostHeader": "s3.amazonaws.com"}}
Show syntax highlighted
eventName = GetBucketPublicAccessBlock | eventSource = s3.amazonaws.com | eventType = AwsApiCall | host = splunk | source = s3://aws-cloudtrail-logs-141573590337-619792c3/AWSLogs/141573590337/Cloud... | sourcetype = aws:cloudtrail
```

Q5

Creating a new user account is a common tactic attackers use to establish

persistence in a compromised environment. What is the username of the account created by the attacker?

Query

```
index="aws_cloudtrail" eventSource="iam.amazonaws.com"  
eventName="CreateUser"
```

Q6

Following account creation, the attacker added the account to a specific group. What is the name of the group to which the account was added?

Query

```
index="aws_cloudtrail" eventSource="iam.amazonaws.com"  
eventName="AddUserToGroup"  
| search requestParameters.userName="put it here"  
| stats values(requestParameters.groupName) as group_name by  
requestParameters.userName
```