

Splunk 3 – More AWS Events

You'll return your focus to AWS-related events with some questions focusing on email-related events in this task.

The questions below are from the 200 series of the BOTSv3 dataset.

You're tasked to identify which IAM user access key generates the most distinct errors when attempting to access IAM resources.

You should have an idea of which source type you'll need to query.

The question is, which field or fields you need to expand your query?

Question 1:

What IAM user access key generates the most distinct errors when attempting to access IAM resources?

Answer: AKIAJOGCDXJ5NW5PXUPA

I used the query below with the keyword "IAM*"

The screenshot shows the Splunk search interface. The search bar contains the query: `1 index=botsv3 sourcetype="aws:cloudtrail" IAM*`. Below the search bar, it indicates **6,571 events** (before 9/16/23 5:14:06.000 PM) with **No Event Sampling** selected. The interface has tabs for **Events (6,571)**, **Patterns**, **Statistics**, and **Visualization**.

Then went through and analysed field name "errorCode". From the question we can see that errors occurred when attempting to access IAM resources. Therefore I looked and researched further errorCode value "AccessDenied"

The screenshot shows the 'errorCode' field analysis report. It indicates 16 values, 100% of events. The report includes tabs for 'Top values', 'Top values by time', and 'Rare values'. The 'Top 10 Values' table is displayed below.

Top 10 Values	Count	%
success	5,504	83.762%
Client.InstanceLimitExceeded	280	4.261%
Client.UnauthorizedOperation	231	3.515%
NoSuchCORSConfiguration	151	2.298%
NoSuchLifecycleConfiguration	147	2.237%
Client.Unsupported	104	1.583%
NoSuchTagSet	57	0.867%
NoSuchBucketPolicy	51	0.776%
NoSuchEntityException	11	0.167%
AccessDenied	7	0.106%

From here I searched through the events looking for access keys until I found the answer below

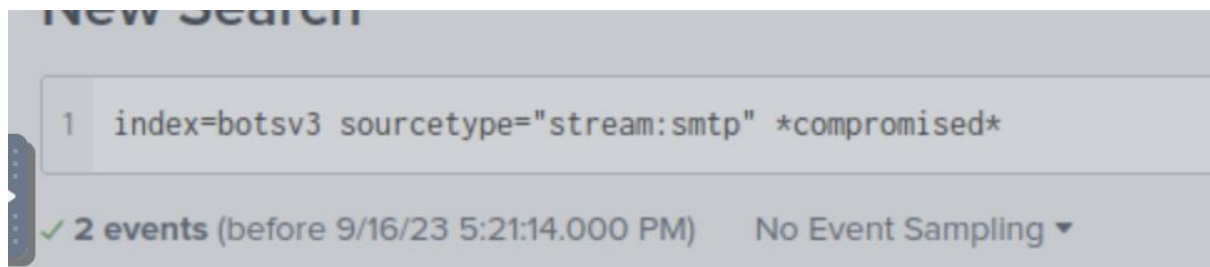
```
errorCode: AccessDenied
errorMessage: User: arn:aws:iam::622676721278:user/web_ac
eventID: f42a75ca-fda2-44fc-b9ef-084ac6922534
eventName: GetUser
eventSource: iam.amazonaws.com
eventTime: 2018-08-20T09:27:07Z
eventType: AwsApiCall
eventVersion: 1.02
recipientAccountId: 622676721278
requestID: 998cefe3-9094-11e8-9f0d-dfb84f749fa0
requestParameters: null
responseElements: null
sourceIPAddress: 82.102.18.111
userAgent: ElasticWolf/5.1.6
userIdentity: { [-]
  accessKeyId: AKIAJOGCDXJ5NW5PXUPA
  accountId: 622676721278
```

Question 2:

Bud accidentally commits AWS access keys to an external code repository. Shortly after, he receives a notification from AWS that the account had been compromised. What is the support case ID that Amazon opens on his behalf?

Answer: 5244329601

The question noted that “Bud” receives a “notification from AWS”. Because of this I decided to search within the “stream:smtp” sourcetype. I also tried a few keywords without any success until “compromised” did the trick.



It was easy to then search through the events as there were only 2. After going through I found the "Support Case ID" shown highlighted below

```
ort-CrossTenantHeadersStamped: BN7PR17MB2258\r\n", "Amazon Web Services has opened cas  
"Case ID: 5244329601\r\nSubject: Your AWS account 622676721278", " is compromised\r\nS  
ised! Please review the following notice and take immediate action to secure your acc  
Key AKIAJOGCDXJ5NW5PXUPA (belonging to IAM user \"web_admin\") along with the corresp
```

Question 3:

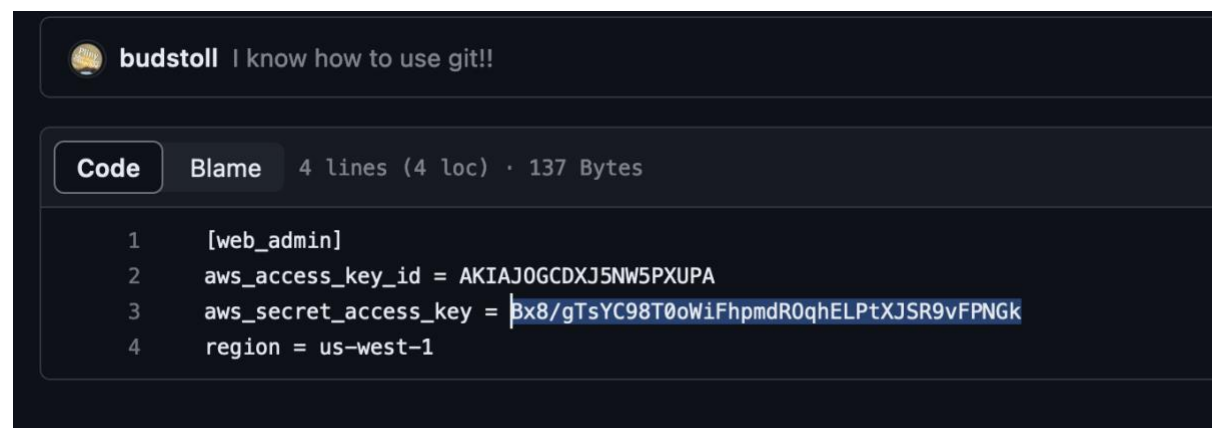
AWS access keys consist of two parts: an access key ID (e.g., AKIAIOSFODNN7EXAMPLE) and a secret access key (e.g., wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY). What is the secret access key of the key that was leaked to the external code repository?

Answer: Bx8/gTsYC98T0oWiFhpmdR0qhELPtXJSR9vFPNGk

Using the access key ID from the 1st question I was able to use that in the search query which provided the event and information below. As you can see the link highlighted takes you to a webpage shown further below providing the aws_secret_access_key, the answer to this question.

We have become aware that the AWS Access Key AKIAJOGCDXJ5NW5PXUPA (belonging to IAM user \"web_admin\") along with the corresponding Secret Key is publicly available online at https://github.com/FrothyBeers/BrewingIoT/blob/e4a98cc997de12bb7a59f18aea207a28bcec566c/MyDocuments/aws_credentials.bak. This poses a security risk to your account.

We have become aware that the AWS Access Key AKIAJOGCDXJ5NW5PXUPA (belonging to IAM user \"web_admin\") along with the corresponding Secret Key is publicly available online at https://github.com/FrothyBeers/BrewingIoT/blob/e4a98cc997de12bb7a59f18aea207a28bcec566c/MyDocuments/aws_credentials.bak.



The screenshot shows a GitHub interface for a file named `aws_credentials.bak`. The user `budstoll` is shown with the profile picture of a gold coin and the bio "I know how to use git!!". The file is 4 lines long and 137 bytes. The code content is as follows:

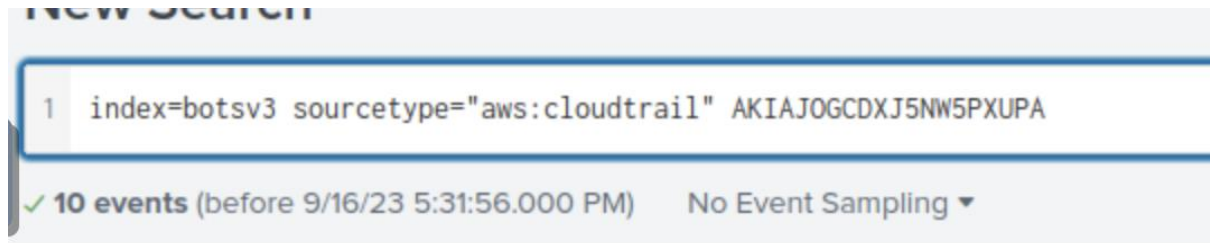
```
1 [web_admin]
2 aws_access_key_id = AKIAJOGCDXJ5NW5PXUPA
3 aws_secret_access_key = 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
4 region = us-west-1
```

Question 4:

Using the leaked key, the adversary makes an unauthorized attempt to create a key for a specific resource. What is the name of that resource? Answer guidance: One word.

Answer: nullweb_admin

This question was incredibly frustrating because I was convinced the answer was web_admin as it cropped up in most of the events when using the leaked secret access key from the previous question.



However after going through all the events I was finally able to find the answer highlighted below

```
awsRegion: us-east-1
errorCode: AccessDenied
errorMessage: User: arn:aws:iam::622676721278:user/web_admin is not authorized to perform: iam:ListAccessKeys on resource: user: nullweb_admin
eventID: 7ea7fdd1-b32d-4ac2-b543-2d2214cad35c
eventName: ListAccessKeys
eventSource: iam.amazonaws.com
eventTime: 2018-08-20T09:16:18Z
eventType: AwsApiCall
```

Question 5:

Using the leaked key, the adversary makes an unauthorized attempt to describe an account. What is the full user agent string of the application that originated the request?

Answer: ElasticWolf/5.1.6

This was another incredibly frustrating question, but mostly because I didn't understand the term "describe an account" after some research I understood the meaning and was able to find the value in the "eventName" field.

The screenshot shows the AWS CloudTrail console with the 'eventName' field selected in the filter sidebar. The main panel displays a table of event names and their counts.

Values	Count	%
ListAccessKeys	2	20%
CreateAccessKey	1	10%
CreateUser	1	10%
DeleteAccessKey	1	10%
DescribeAccountAttributes	1	10%
GetCallerIdentity	1	10%
GetSessionToken	1	10%
GetUser	1	10%
UpdateAccessKey	1	10%

From there I went through and analysed the event trying to find anything related to User Agent. Answer highlighted below.

```
{ [-]
  awsRegion: us-east-1
  errorCode: Client.UnauthorizedOperation
  errorMessage: You are not authorized to perform this operation
  eventId: c077df0d-2435-4152-9127-09e579dd1fb2
  eventName: DescribeAccountAttributes
  eventSource: ec2.amazonaws.com
  eventTime: 2018-08-20T09:27:06Z
  eventType: AwsApiCall
  eventVersion: 1.05
  recipientAccountId: 622676721278
  requestId: f94dfb04-2d7b-40a8-b3cc-3664b9463db8
  requestParameters: { [+]
  }
  responseElements: null
  sourceIPAddress: 82.102.18.111
  userAgent: ElasticWolf/5.1.6
  userIdentity: { [-]
    accessKeyId: AKIAJOGCDXJ5NW5PXUPA
    accountId: 622676721278
    arn: arn:aws:iam::622676721278:user/ek-admin
```