POLITECNICO
MILANO 1863

UCSB

There’s a Hole in that Bucket!
A Large-scale Analysis of Misconfigured S3 Buckets

Andrea Continella, Mario Polino, Marcello Pogliani, Stefano Zanero

7 December 2018
ACSAC 2018

Cloud Storage Services

Amazon S3

- Users create **buckets** (storage containers)
- Amazon S3 supports various **access control policies**
  - User-level
  - Bucket-level
  - Resource-level

Amazon S3

- Users create **buckets** (storage containers)
- Amazon S3 supports various **access control policies**
  - User-level
  - Bucket-level
  - Resource-level
- REST API to read/write:
  - `http[s]://<BUCKET_NAME>.s3[-region].amazonaws.com/`
  - `http[s]://s3[-region].amazonaws.com/<BUCKET_NAME>/`

```
HTTP/1.1 403 Forbidden
x-amz-bucket-region: ap-southeast-2
Content-Type: application/xml
Transfer-Encoding: chunked
Date: Mon, 19 Mar 2018 13:22:24 GMT
Server: AmazonS3

<Error>
    <Code>AccessDenied</Code>
    <Message>Access Denied</Message>
    <RequestId>4CBC01F61S808F69</RequestId>
    <HostId>zPQX088xyzUTAH704xQLZFg9toDH</HostId>
</Error>
```

What could possibly go wrong?

Threats

Misconfigurations in access control rules can be really **dangerous**

Threats

Misconfigurations in access control rules can be really **dangerous**

Data Leakage

Threats

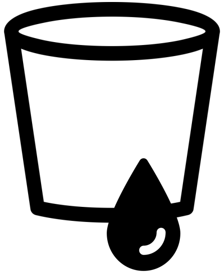
Misconfigurations in access control rules can be really **dangerous**

Data Leakage

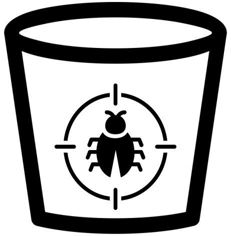
Resource Infection

Threats

Misconfigurations in access control rules can be really **dangerous**



Data Leakage

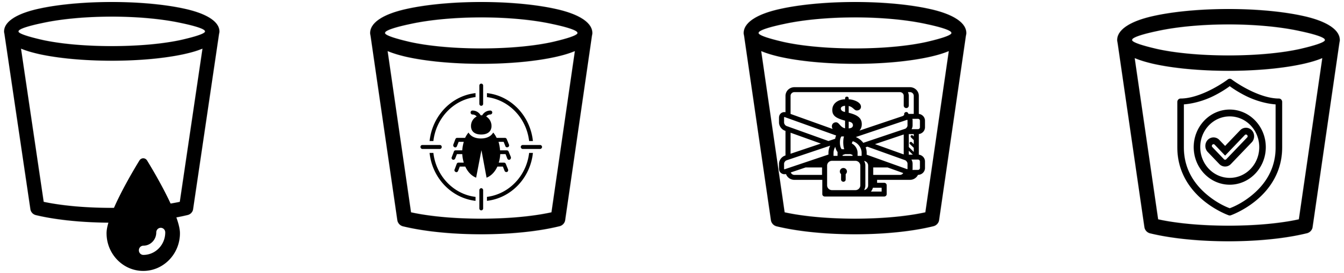


Resource Infection

Ransom Demand

Threats

Misconfigurations in access control rules can be really **dangerous**



Data Leakage

Resource Infection

Ransom Demand

Domain Name Trust Exploiting

Threats

Misconfigurations in access control rules can be really **dangerous**

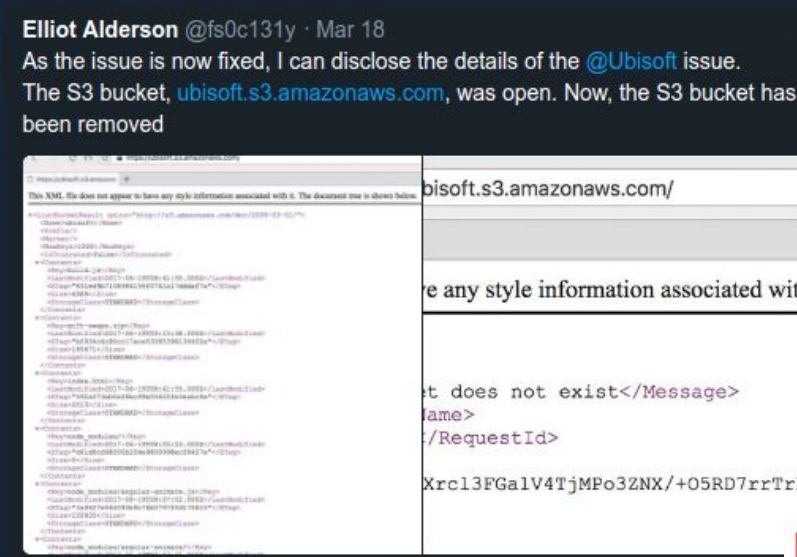
Data Leakage

Resource Infection

Ransom Demand

Domain Name Trust Exploiting

Subdomain Takeover



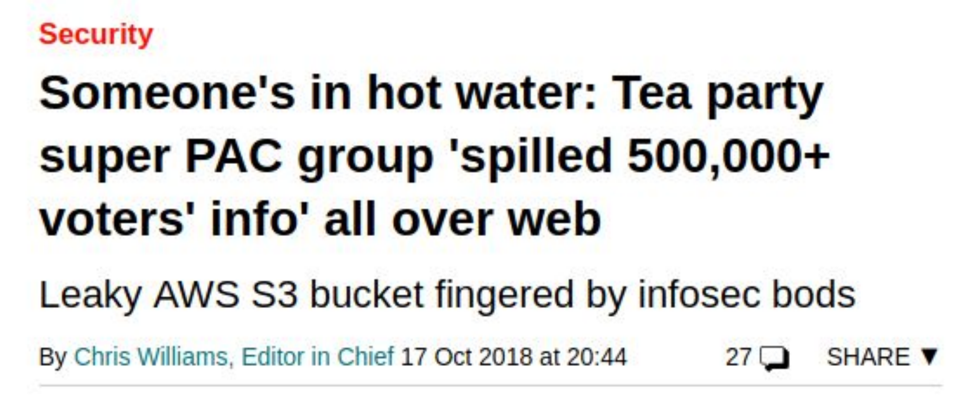
Elliot Alderson @fs0c131y · Mar 18

As the issue is now fixed, I can disclose the details of the @Ubisoft issue.
The S3 bucket, ubisoft.s3.amazonaws.com, was open. Now, the S3 bucket has been removed

This XML file does not appear to have any style information associated with it. The document tree is shown below.

[illegible]

```
bisoft.s3.amazonaws.com/
e any style information associated with i
t does not exist</Message>
ame>
/RequestId>
Xrcl3FGalV4TjMPo3ZNX/+O5RD7rrTrLF
```

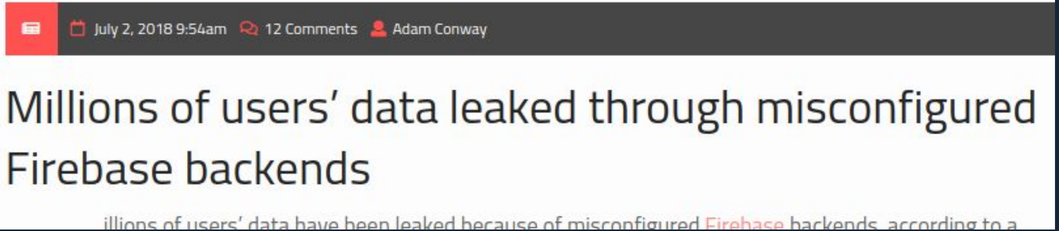


Security

Someone's in hot water: Tea party super PAC group 'spilled 500,000+ voters' info' all over web

Leaky AWS S3 bucket fingered by infosec bods

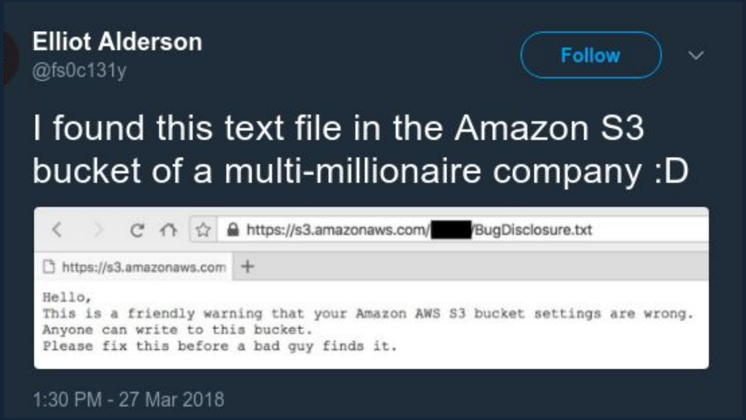
By Chris Williams, Editor in Chief 17 Oct 2018 at 20:44 27 SHARE ▼



July 2, 2018 9:54am 12 Comments Adam Conway

Millions of users' data leaked through misconfigured Firebase backends

illions of users' data have been leaked because of misconfigured Firebase backends, according to a



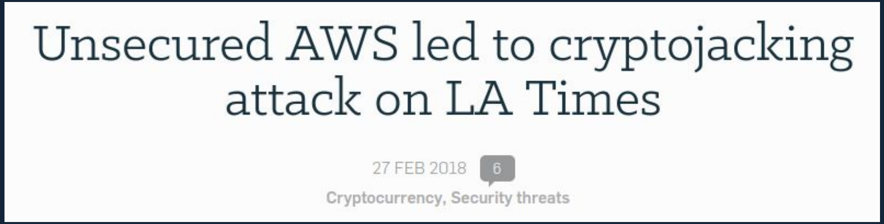
Elliot Alderson
@fs0c131y

I found this text file in the Amazon S3 bucket of a multi-millionaire company :D

https://s3.amazonaws.com/[redacted]/BugDisclosure.txt

```
Hello,
This is a friendly warning that your Amazon AWS S3 bucket settings are wrong.
Anyone can write to this bucket.
Please fix this before a bad guy finds it.
```

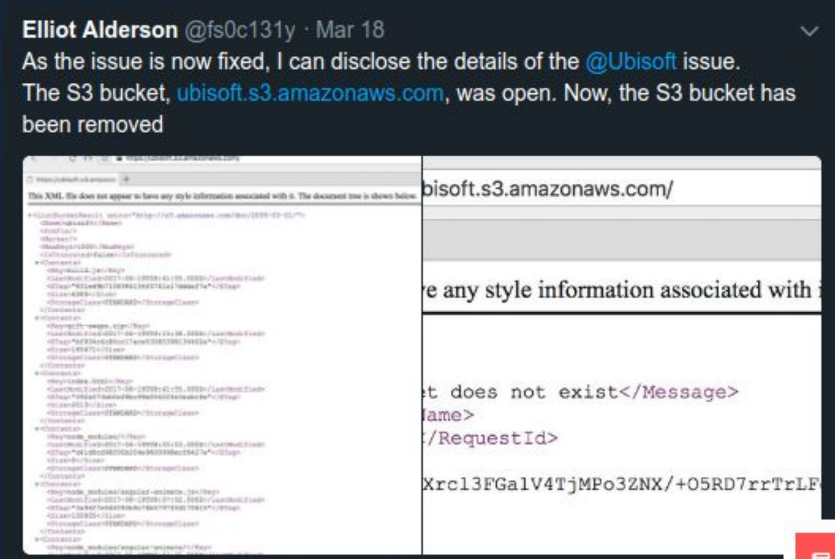
1:30 PM - 27 Mar 2018



Unsecured AWS led to cryptojacking attack on LA Times

27 FEB 2018 6

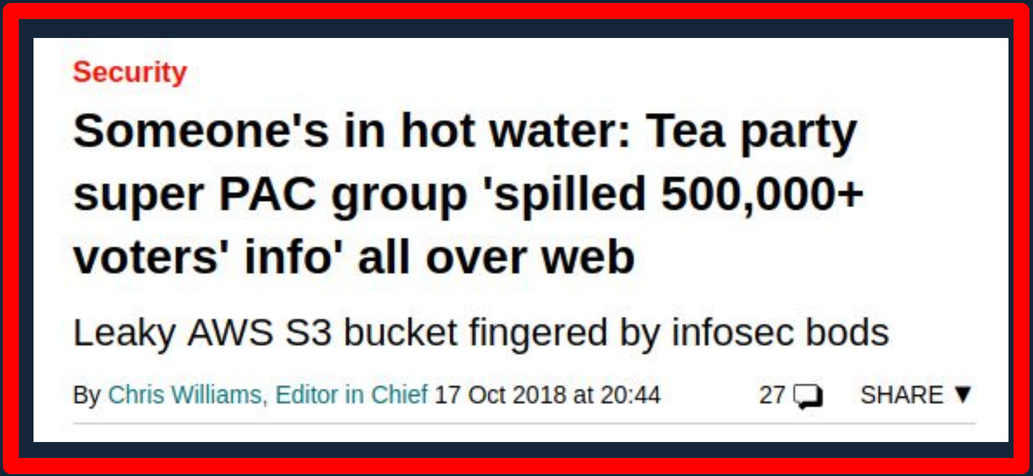
Cryptocurrency, Security threats



Elliot Alderson @fs0c131y · Mar 18

As the issue is now fixed, I can disclose the details of the @Ubisoft issue. The S3 bucket, ubisoft.s3.amazonaws.com, was open. Now, the S3 bucket has been removed

```
bisoft.s3.amazonaws.com/
e any style information associated with i
t does not exist</Message>
ame>
/RequestId>
Xrcl3FGalV4TjMPo3ZNX/+O5RD7rrTrLF
```

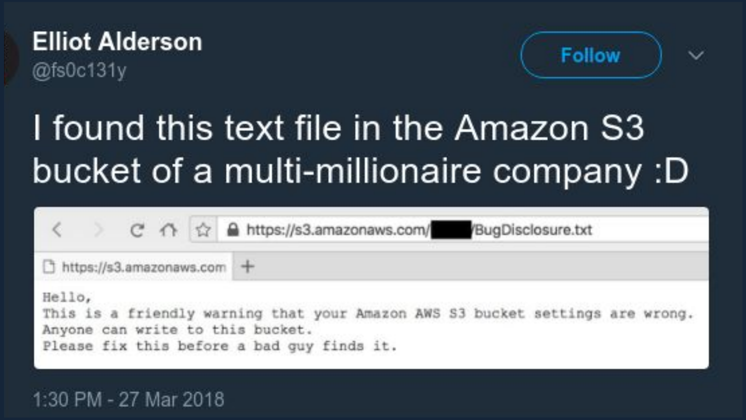


Security

Someone's in hot water: Tea party super PAC group 'spilled 500,000+ voters' info' all over web

Leaky AWS S3 bucket fingered by infosec bods

By Chris Williams, Editor in Chief 17 Oct 2018 at 20:44 27 SHARE ▼



Elliot Alderson
@fs0c131y

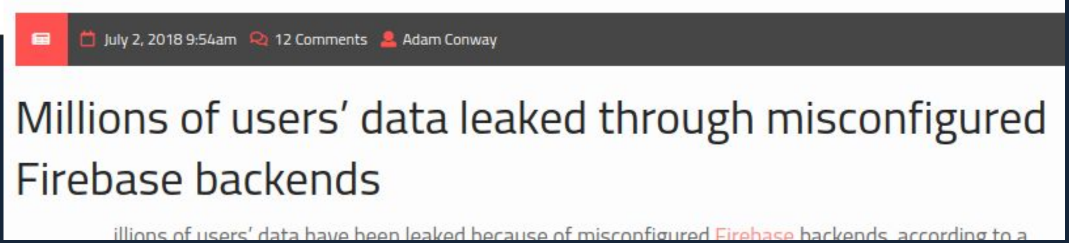
I found this text file in the Amazon S3 bucket of a multi-millionaire company :D

https://s3.amazonaws.com/[redacted]/BugDisclosure.txt

https://s3.amazonaws.com

```
Hello,
This is a friendly warning that your Amazon AWS S3 bucket settings are wrong.
Anyone can write to this bucket.
Please fix this before a bad guy finds it.
```

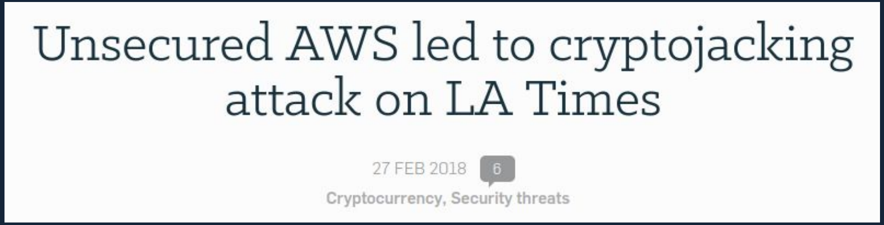
1:30 PM - 27 Mar 2018



July 2, 2018 9:54am 12 Comments Adam Conway

Millions of users' data leaked through misconfigured Firebase backends

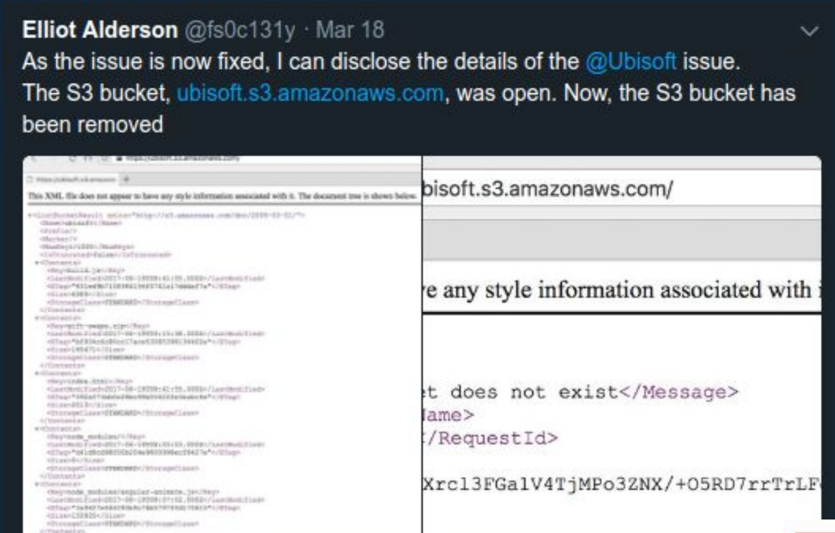
illions of users' data have been leaked because of misconfigured Firebase backends, according to a



Unsecured AWS led to cryptojacking attack on LA Times

27 FEB 2018 6

Cryptocurrency, Security threats

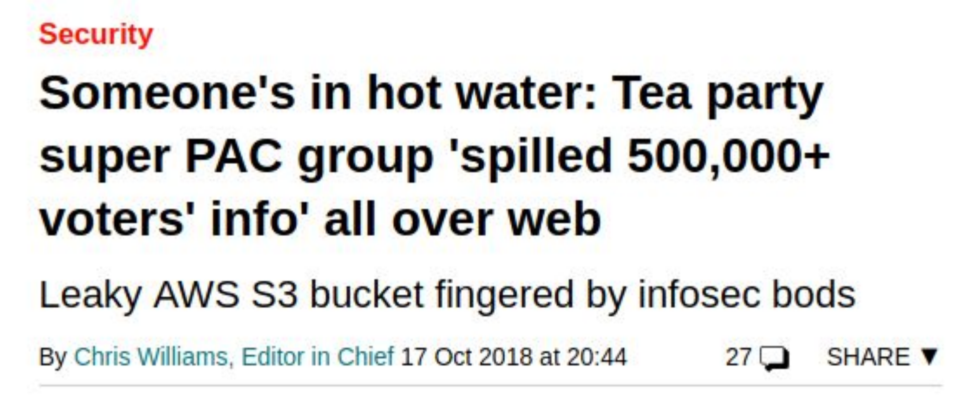


Elliot Alderson @fs0c131y · Mar 18

As the issue is now fixed, I can disclose the details of the @Ubisoft issue. The S3 bucket, ubisoft.s3.amazonaws.com, was open. Now, the S3 bucket has been removed

This XML file does not appear to have any style information associated with it. The document tree is shown below.

```
bisoft.s3.amazonaws.com/
e any style information associated with i
t does not exist</Message>
ame>
/RequestId>
Xrcl3FGalV4TjMPo3ZNX/+O5RD7rrTrLF
```

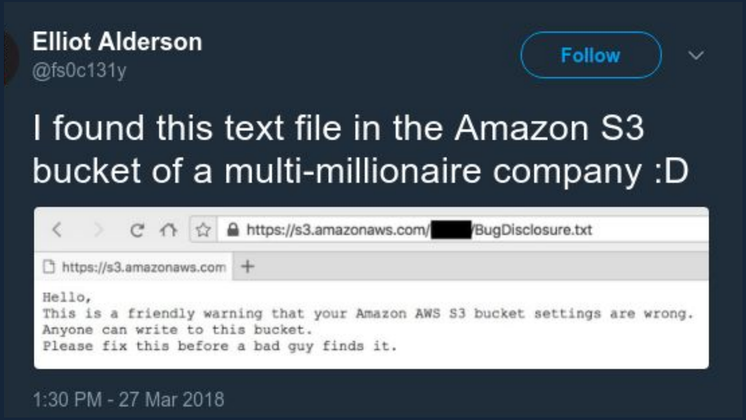


Security

Someone's in hot water: Tea party super PAC group 'spilled 500,000+ voters' info' all over web

Leaky AWS S3 bucket fingered by infosec bods

By Chris Williams, Editor in Chief 17 Oct 2018 at 20:44 27 SHARE ▼



Elliot Alderson
@fs0c131y

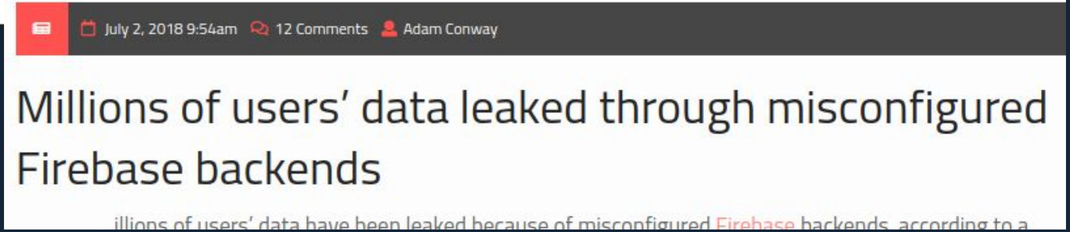
I found this text file in the Amazon S3 bucket of a multi-millionaire company :D

https://s3.amazonaws.com/[redacted]/BugDisclosure.txt

https://s3.amazonaws.com

```
Hello,
This is a friendly warning that your Amazon AWS S3 bucket settings are wrong.
Anyone can write to this bucket.
Please fix this before a bad guy finds it.
```

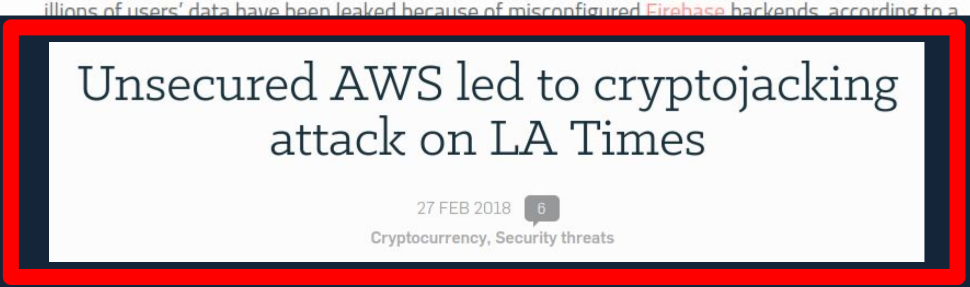
1:30 PM - 27 Mar 2018



July 2, 2018 9:54am 12 Comments Adam Conway

Millions of users' data leaked through misconfigured Firebase backends

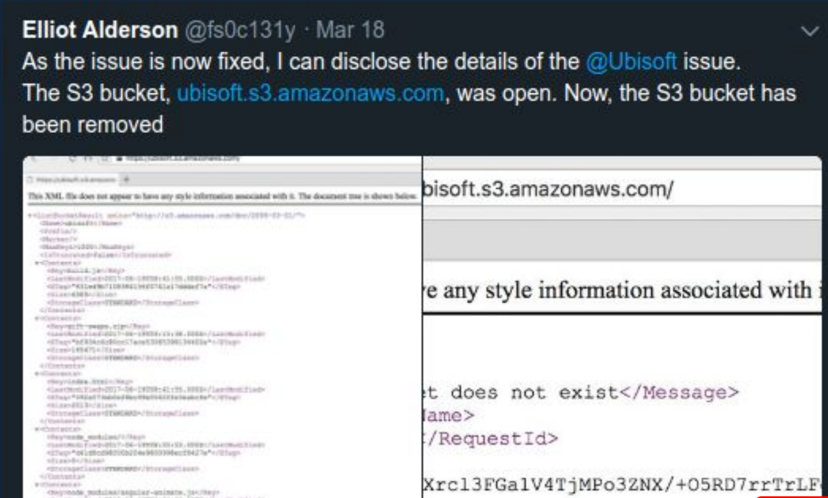
illions of users' data have been leaked because of misconfigured Firebase backends, according to a



Unsecured AWS led to cryptojacking attack on LA Times

27 FEB 2018 6

Cryptocurrency, Security threats



Elliot Alderson @fs0c131y · Mar 18

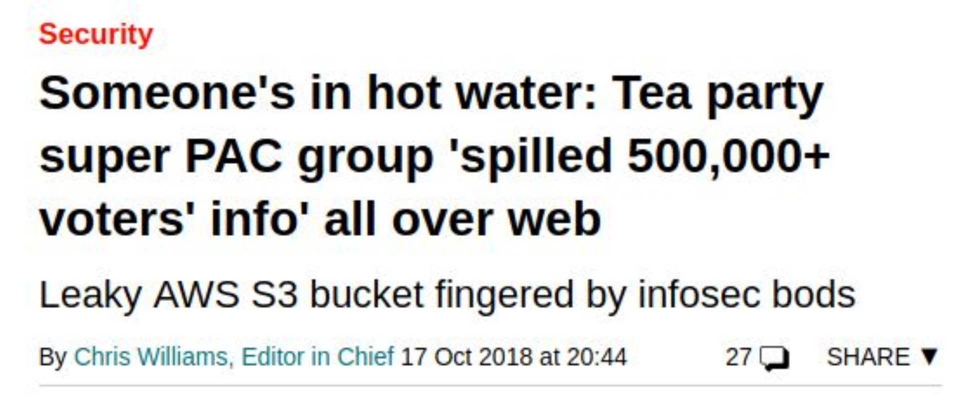
As the issue is now fixed, I can disclose the details of the @Ubisoft issue.
The S3 bucket, ubisoft.s3.amazonaws.com, was open. Now, the S3 bucket has been removed

This XML file does not appear to have any style information associated with it. The document tree is shown below.

bisoft.s3.amazonaws.com/

e any style information associated with i

```
t does not exist</Message>
Name>
/RequestId>
Xrcl3FGa1V4TjMPo3ZNX/+O5RD7rrTrLF
```

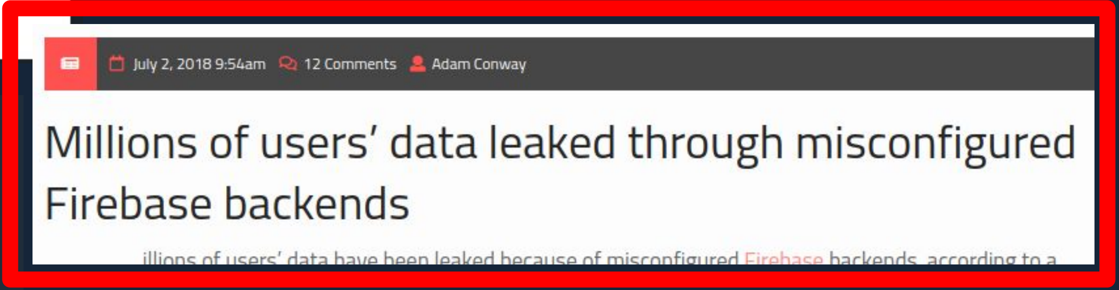


Security

Someone's in hot water: Tea party super PAC group 'spilled 500,000+ voters' info' all over web

Leaky AWS S3 bucket fingered by infosec bods

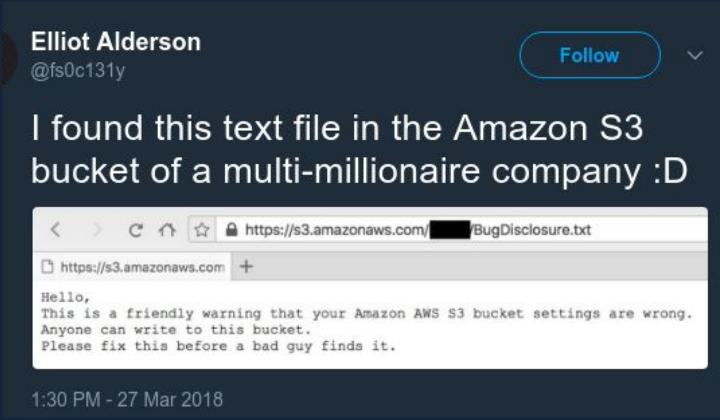
By Chris Williams, Editor in Chief 17 Oct 2018 at 20:44 27 SHARE ▼



July 2, 2018 9:54am 12 Comments Adam Conway

Millions of users' data leaked through misconfigured Firebase backends

illions of users' data have been leaked because of misconfigured Firebase backends, according to a



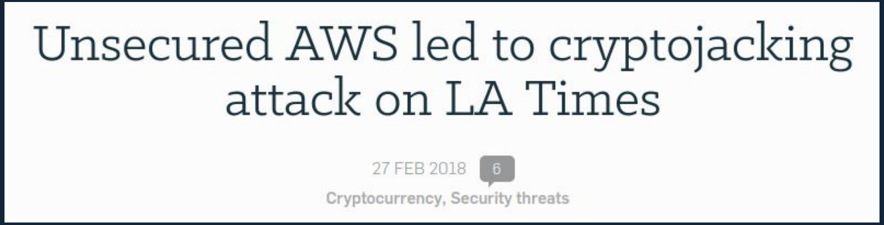
Elliot Alderson
@fs0c131y

I found this text file in the Amazon S3 bucket of a multi-millionaire company :D

https://s3.amazonaws.com/[redacted]/BugDisclosure.txt

```
Hello,
This is a friendly warning that your Amazon AWS S3 bucket settings are wrong.
Anyone can write to this bucket.
Please fix this before a bad guy finds it.
```

1:30 PM - 27 Mar 2018

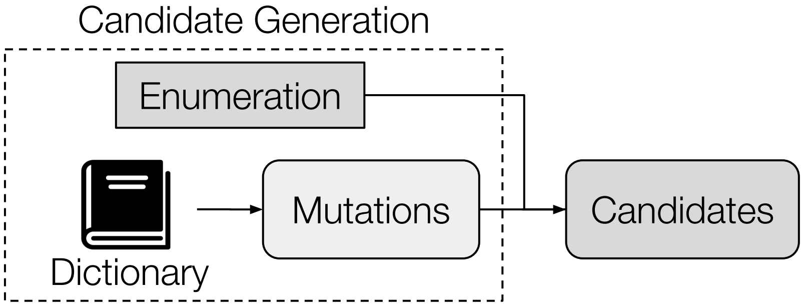


Unsecured AWS led to cryptojacking attack on LA Times

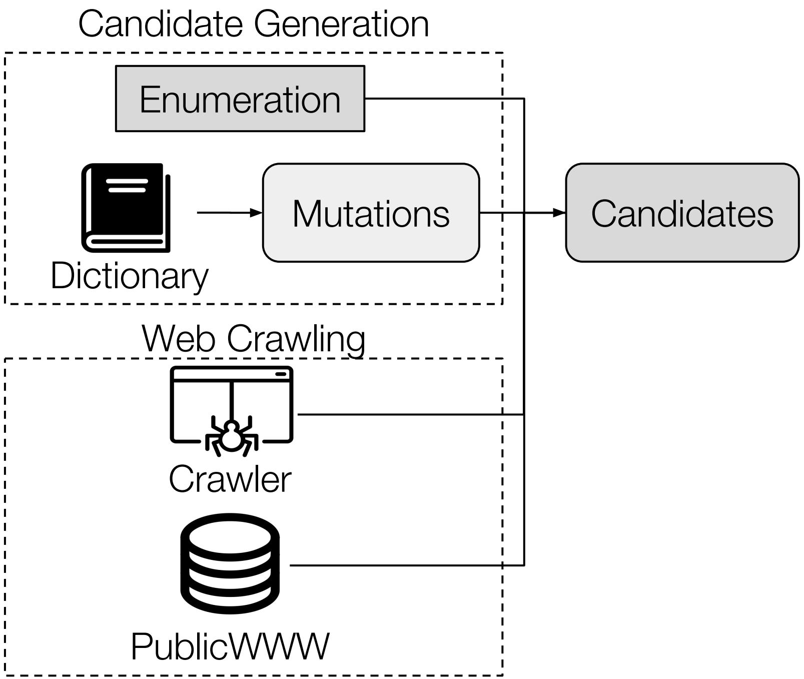
27 FEB 2018 6

Cryptocurrency, Security threats

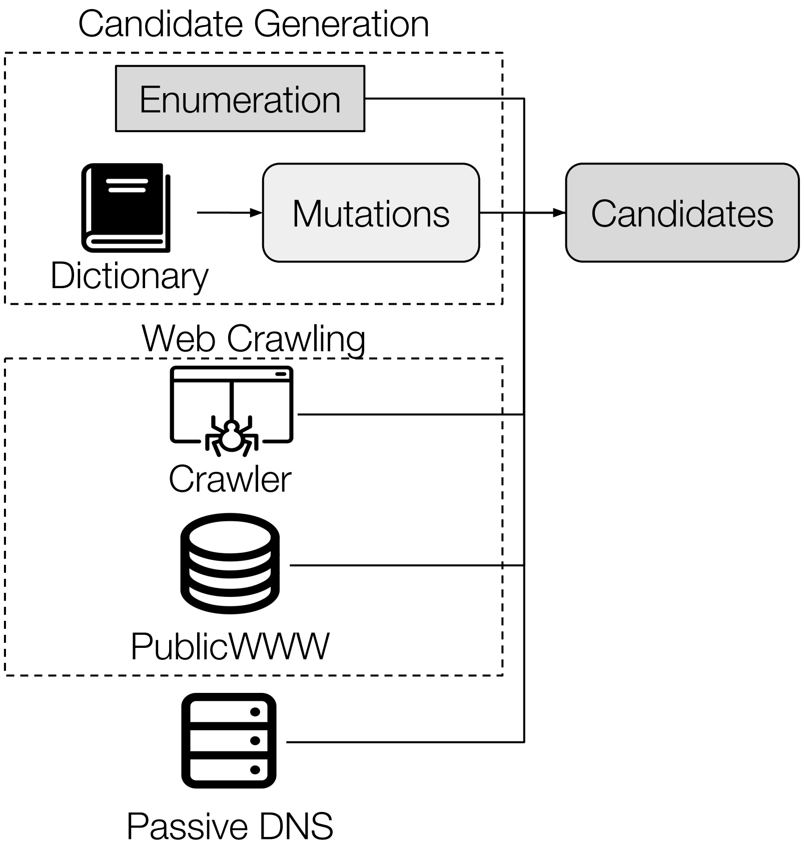
Methodology



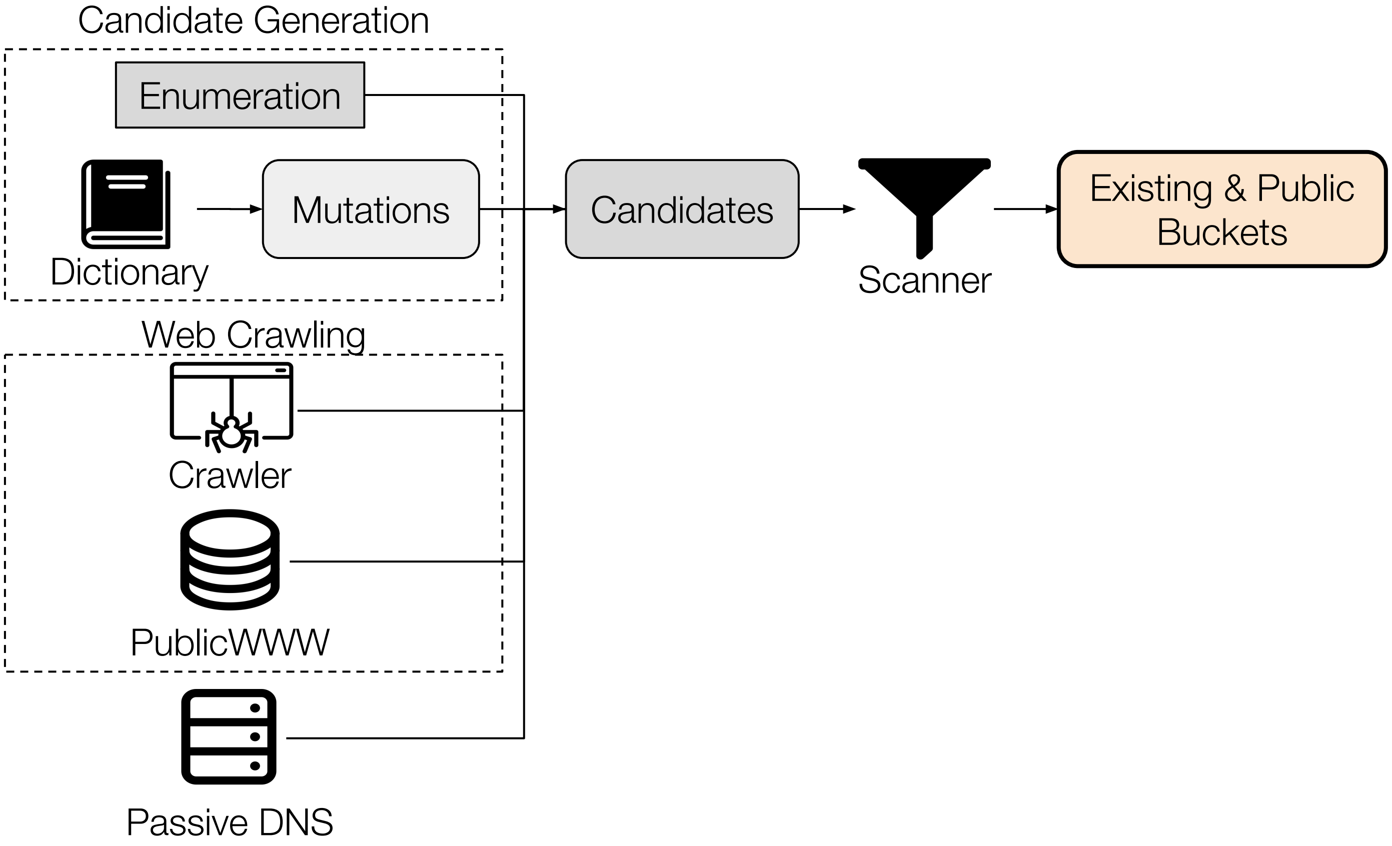
Methodology



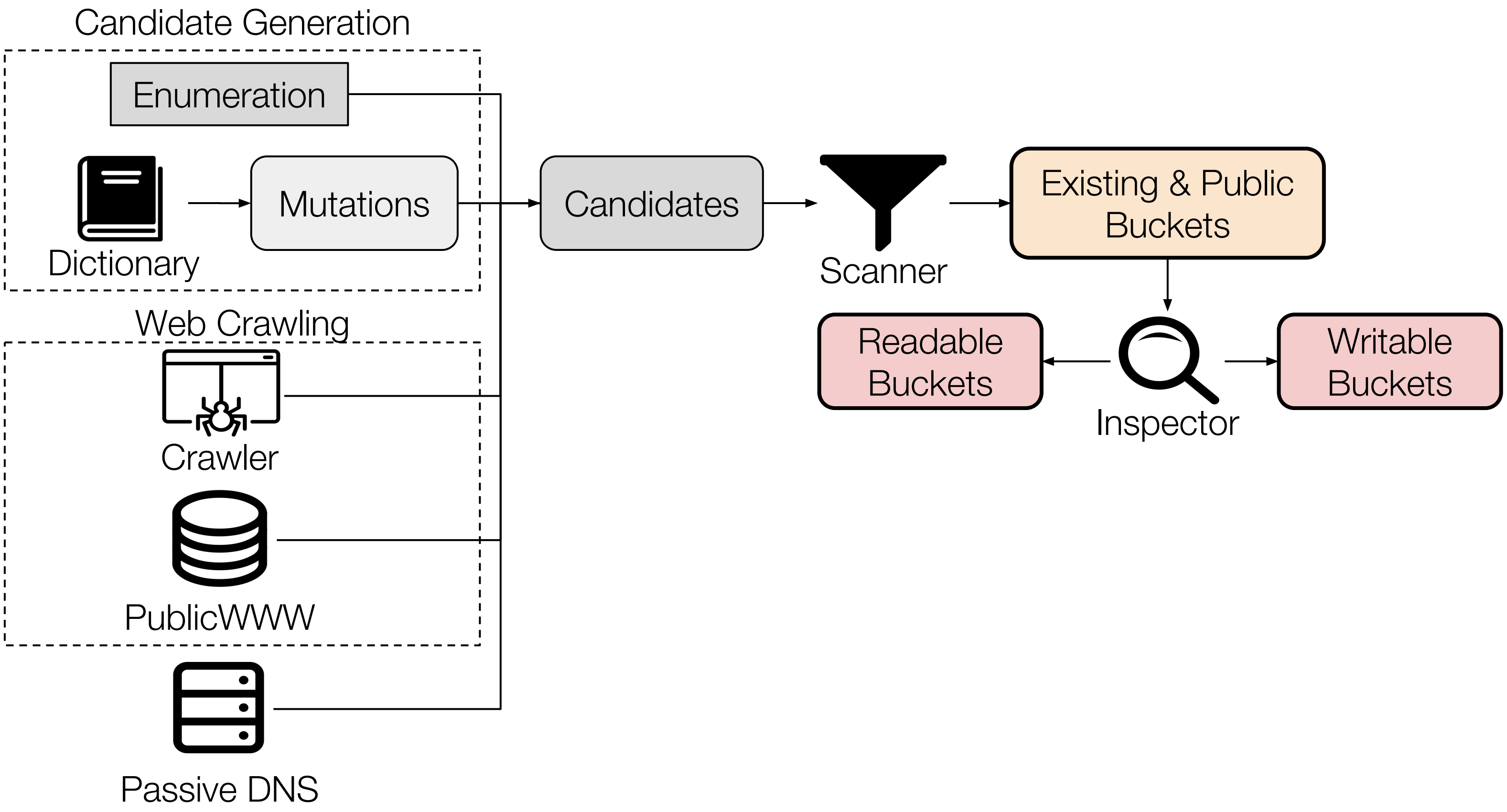
Methodology



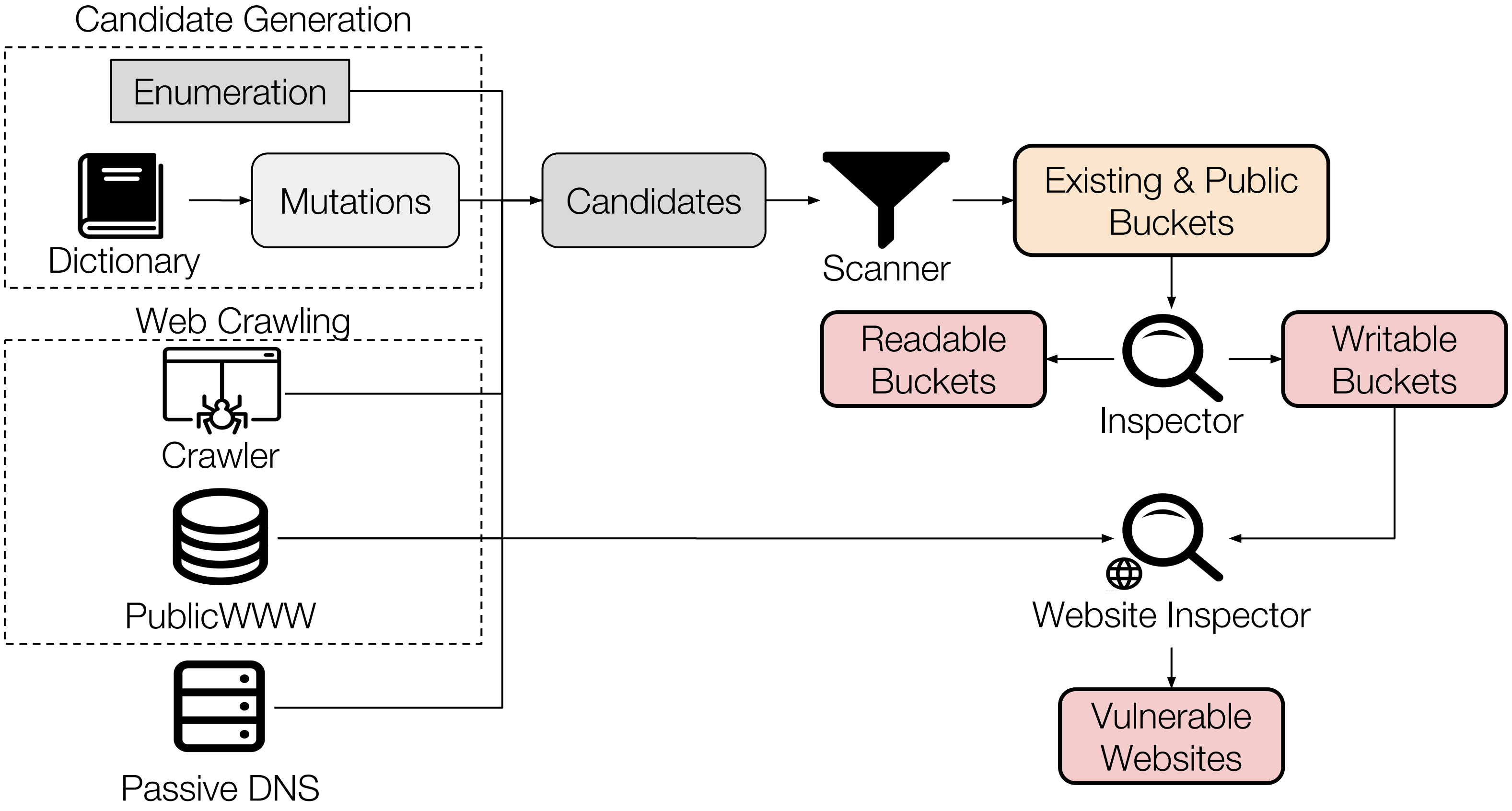
Methodology



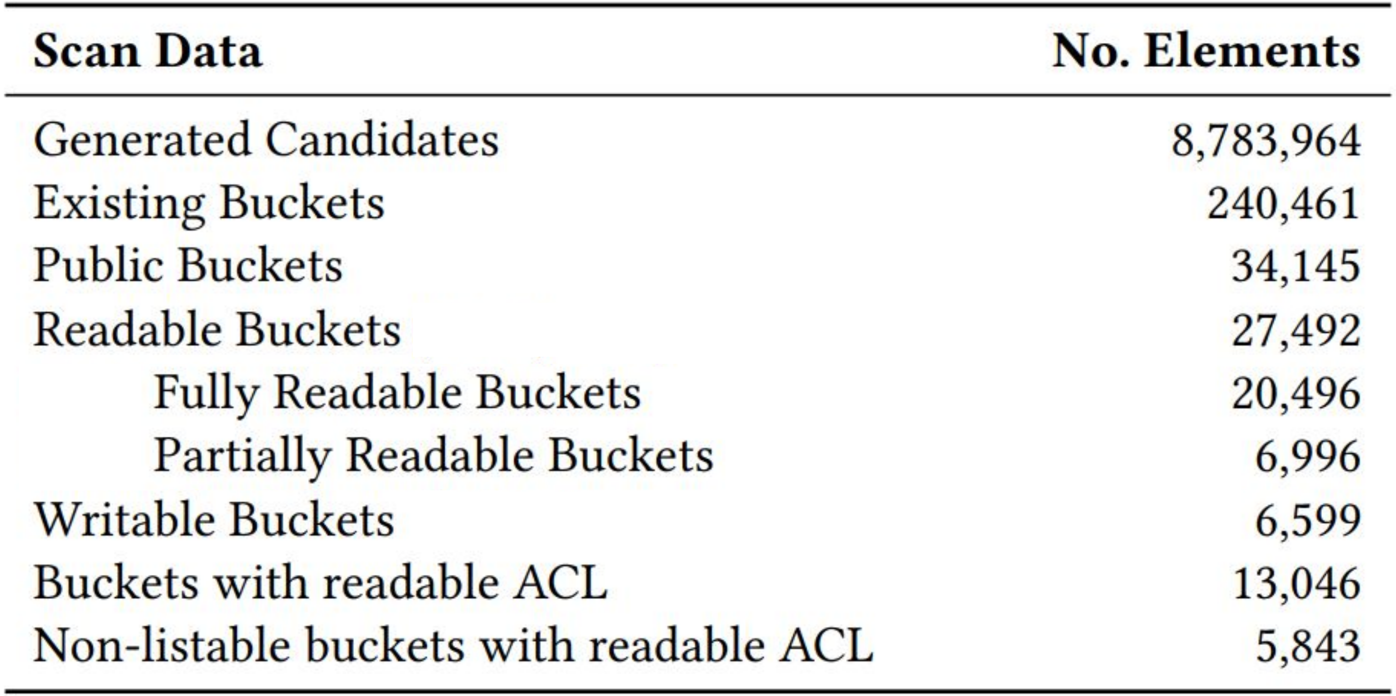
Methodology



Methodology

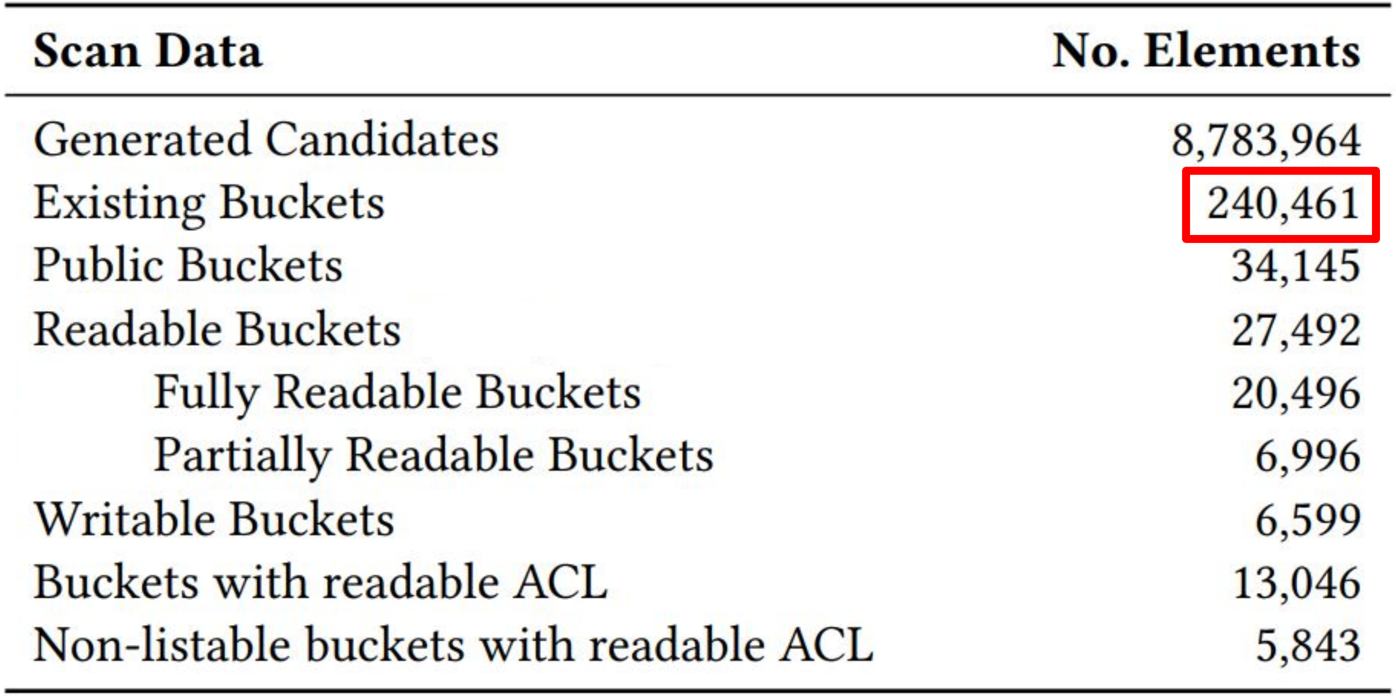


Scanning Result Summary



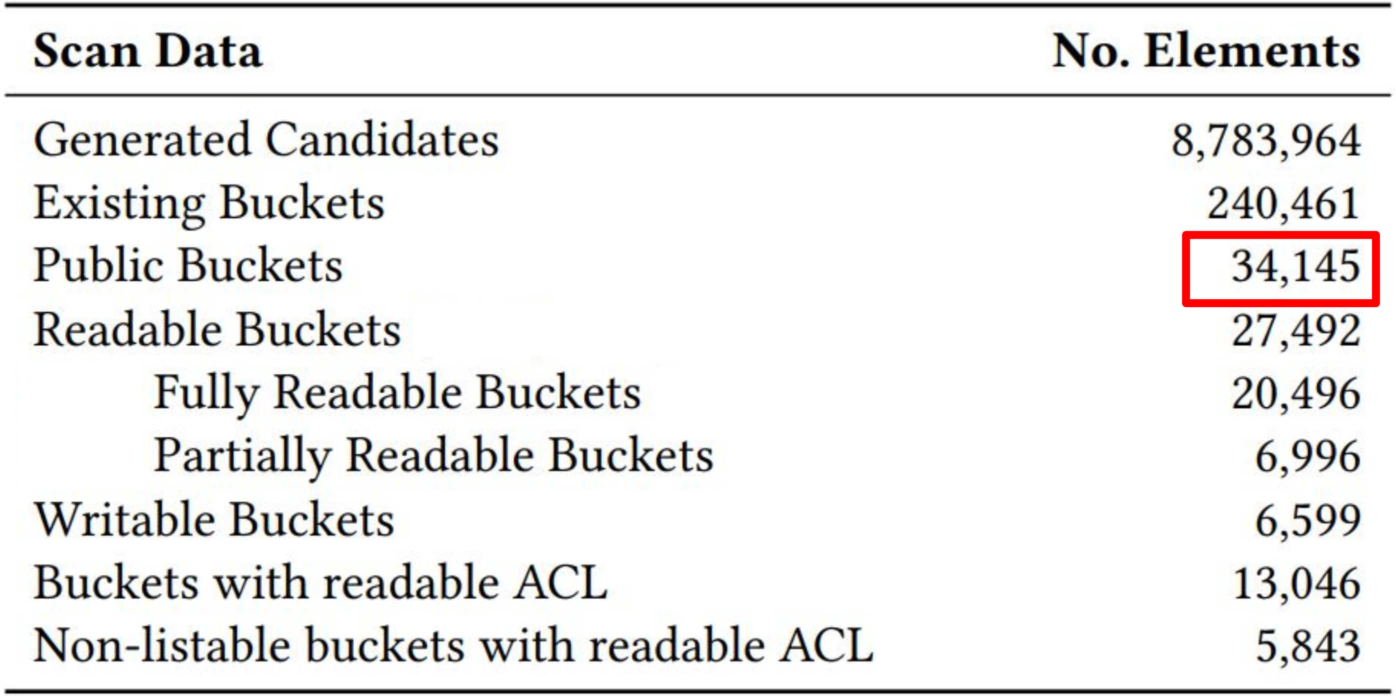
Scan Data	No. Elements
Generated Candidates	8,783,964
Existing Buckets	240,461
Public Buckets	34,145
Readable Buckets	27,492
Fully Readable Buckets	20,496
Partially Readable Buckets	6,996
Writable Buckets	6,599
Buckets with readable ACL	13,046
Non-listable buckets with readable ACL	5,843

Scanning Result Summary



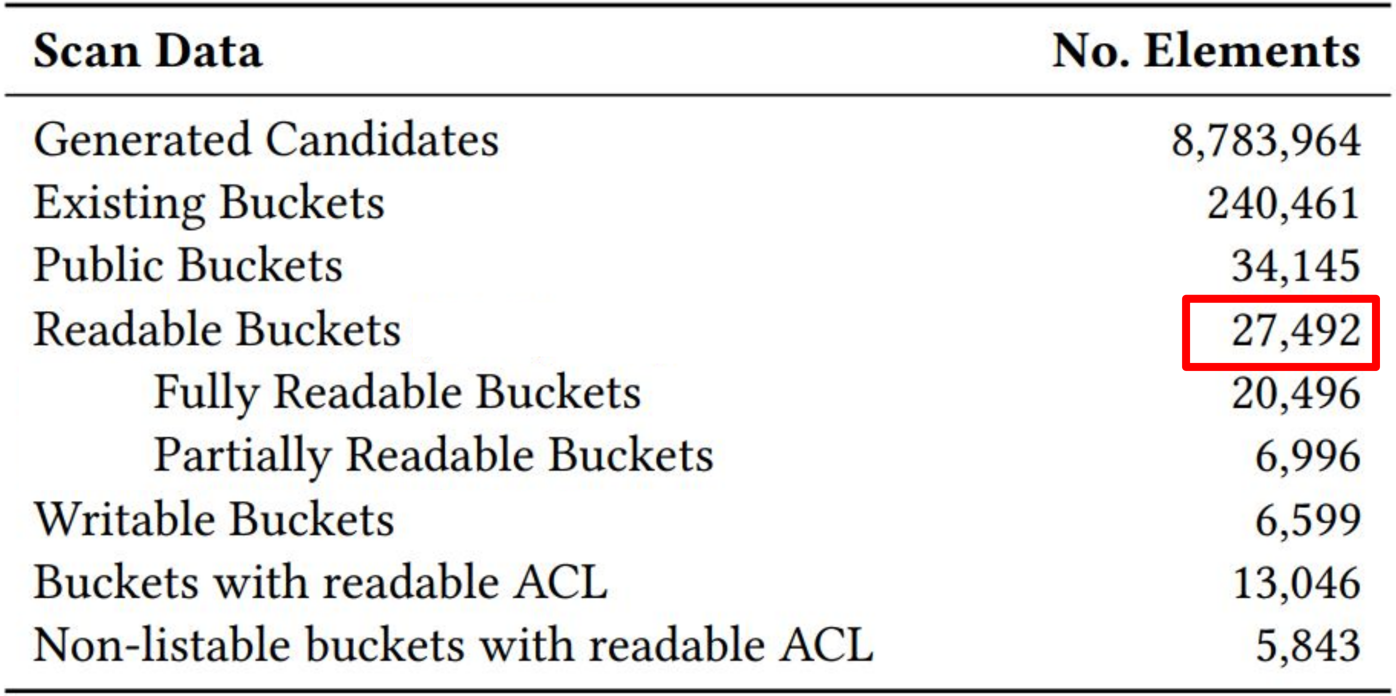
Scan Data	No. Elements
Generated Candidates	8,783,964
Existing Buckets	240,461
Public Buckets	34,145
Readable Buckets	27,492
Fully Readable Buckets	20,496
Partially Readable Buckets	6,996
Writable Buckets	6,599
Buckets with readable ACL	13,046
Non-listable buckets with readable ACL	5,843

Scanning Result Summary



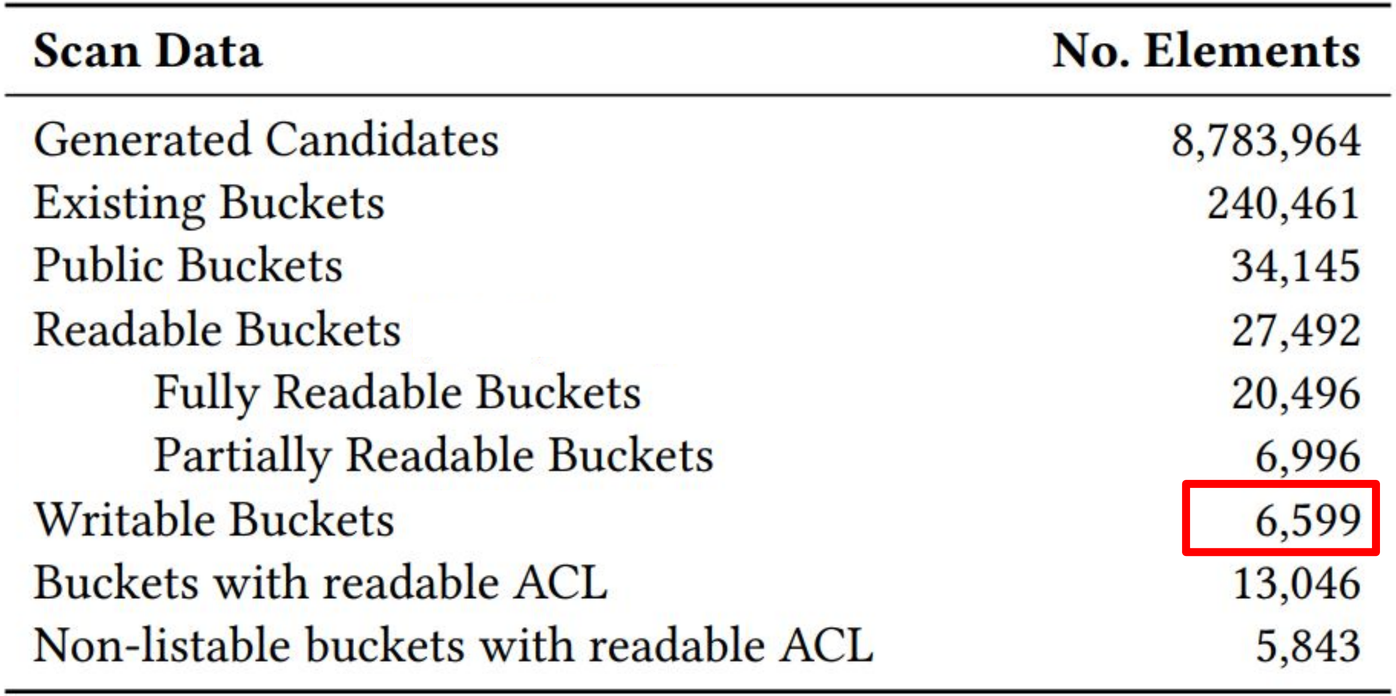
Scan Data	No. Elements
Generated Candidates	8,783,964
Existing Buckets	240,461
Public Buckets	34,145
Readable Buckets	27,492
Fully Readable Buckets	20,496
Partially Readable Buckets	6,996
Writable Buckets	6,599
Buckets with readable ACL	13,046
Non-listable buckets with readable ACL	5,843

Scanning Result Summary



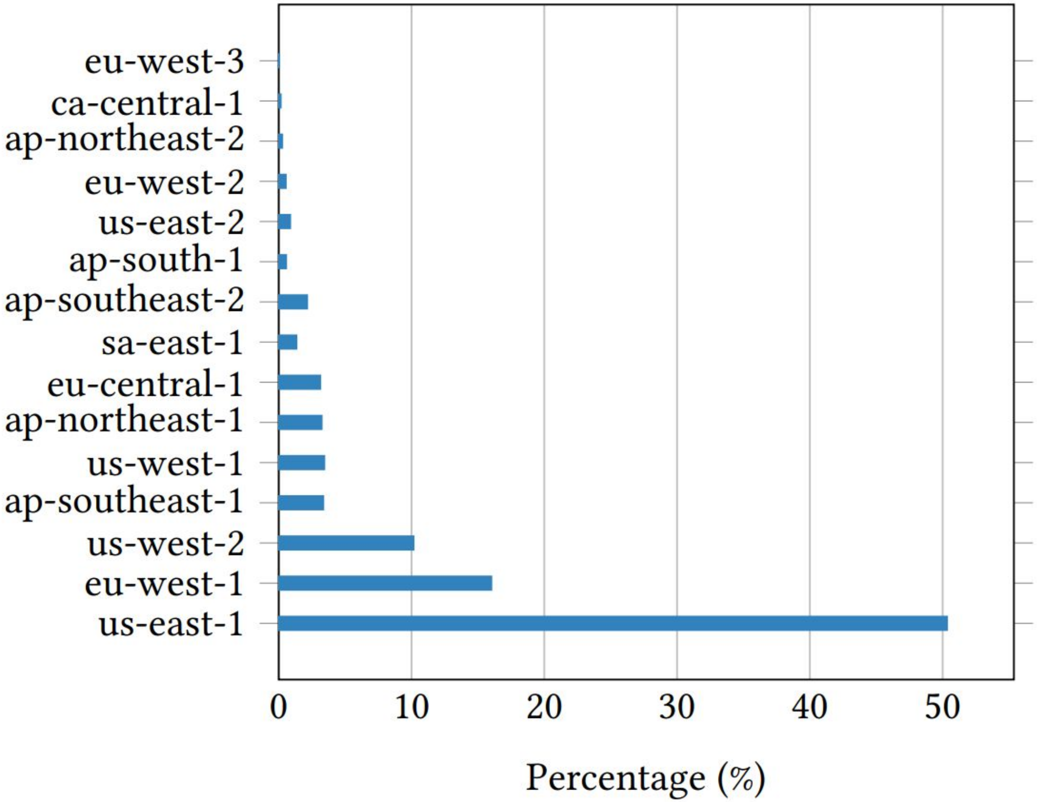
Scan Data	No. Elements
Generated Candidates	8,783,964
Existing Buckets	240,461
Public Buckets	34,145
Readable Buckets	27,492
Fully Readable Buckets	20,496
Partially Readable Buckets	6,996
Writable Buckets	6,599
Buckets with readable ACL	13,046
Non-listable buckets with readable ACL	5,843

Scanning Result Summary

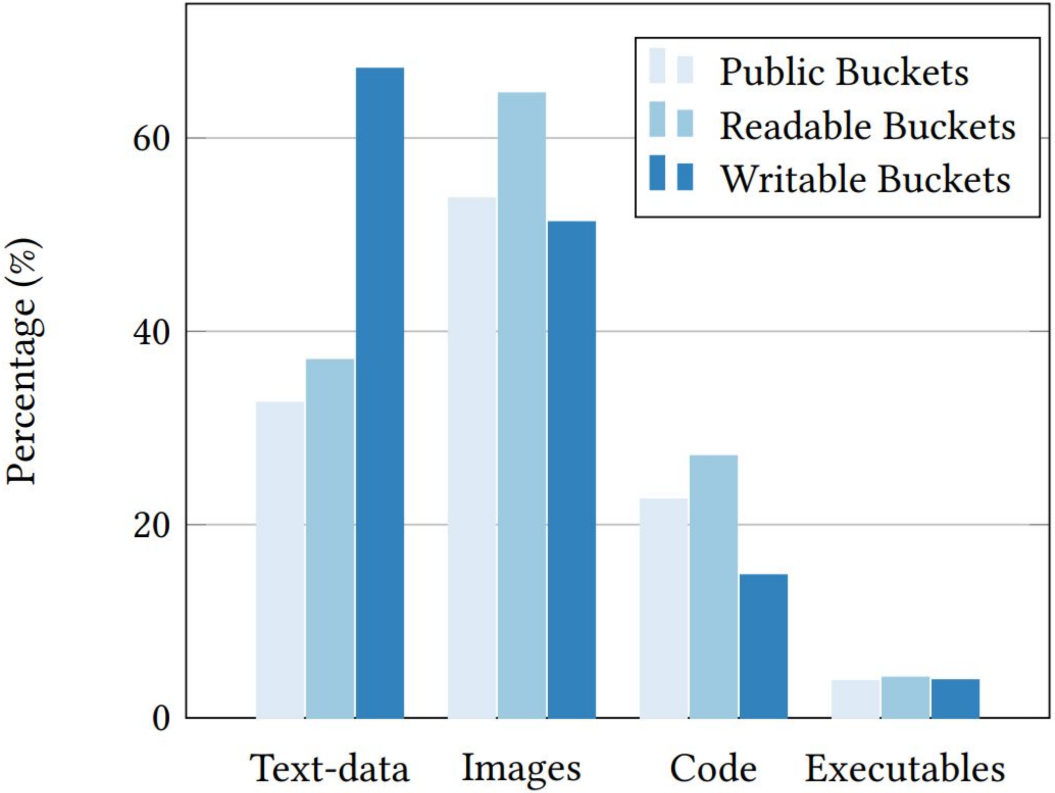


Scan Data	No. Elements
Generated Candidates	8,783,964
Existing Buckets	240,461
Public Buckets	34,145
Readable Buckets	27,492
Fully Readable Buckets	20,496
Partially Readable Buckets	6,996
Writable Buckets	6,599
Buckets with readable ACL	13,046
Non-listable buckets with readable ACL	5,843

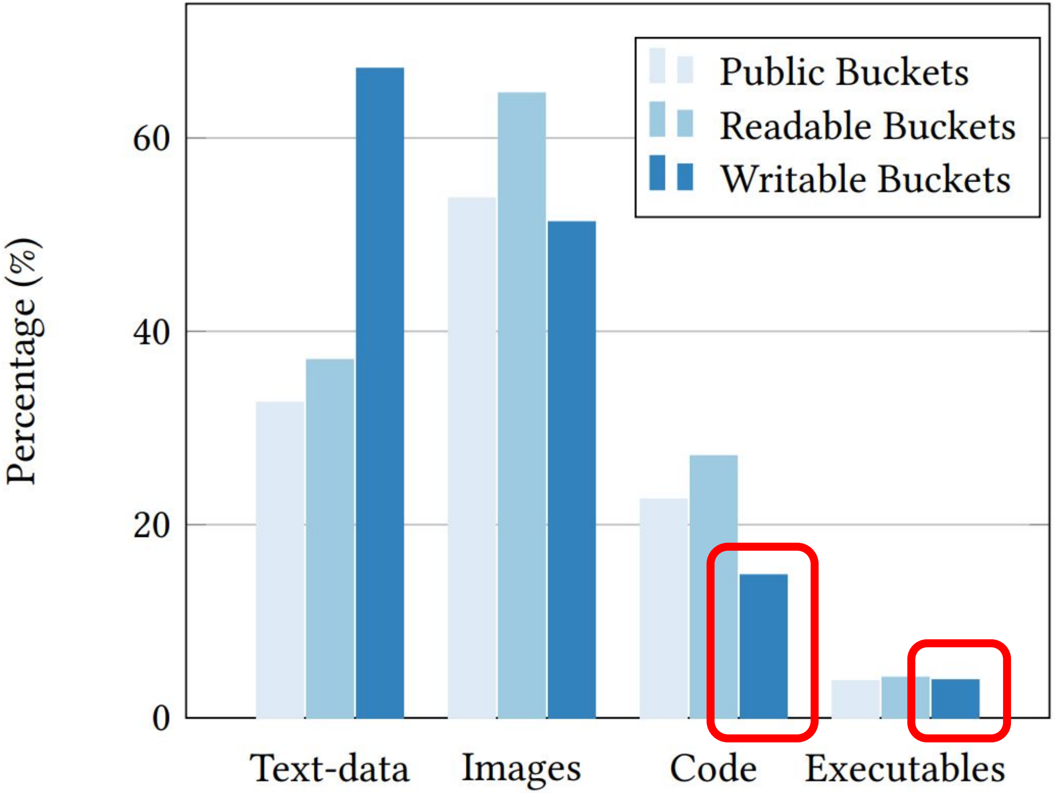
Region Distribution



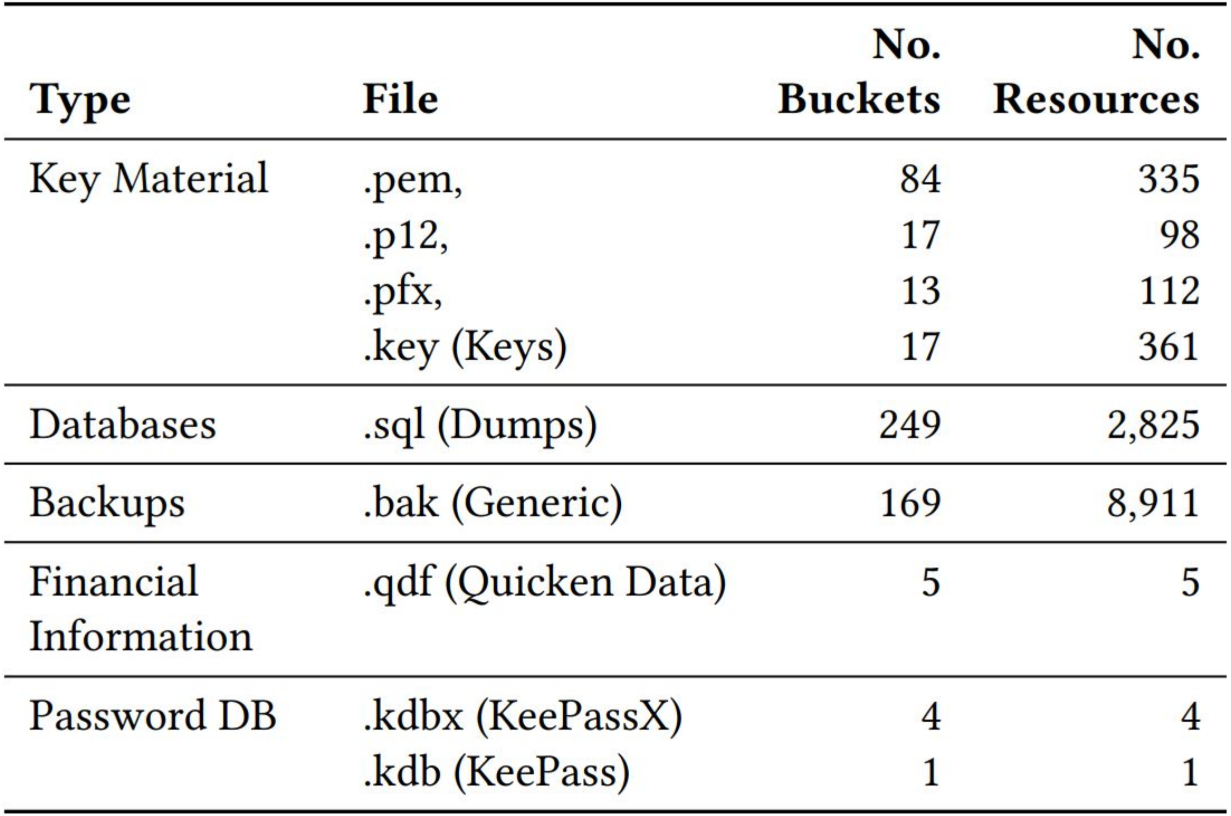
File Types


Public Buckets
Readable Buckets
Writable Buckets
Percentage (%)
60
40
20
0
Text-data
Images
Code
Executables

File Types


Public Buckets
Readable Buckets
Writable Buckets
Percentage (%)
0
20
40
60
Text-data
Images
Code
Executables

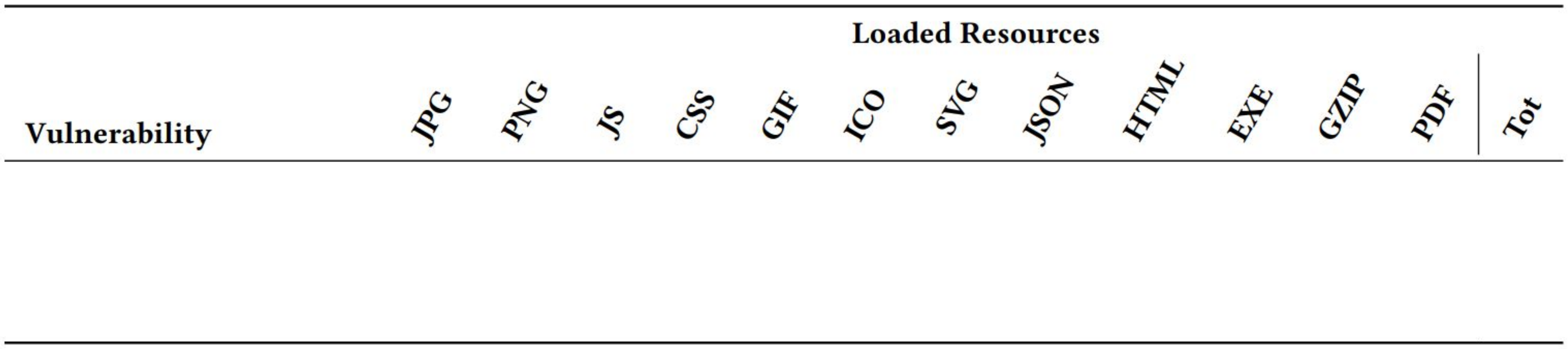
Sensitive Exposure



Type	File	No. Buckets	No. Resources
Key Material	.pem,	84	335
	.p12,	17	98
	.pfx,	13	112
	.key (Keys)	17	361
Databases	.sql (Dumps)	249	2,825
Backups	.bak (Generic)	169	8,911
Financial Information	.qdf (Quicken Data)	5	5
Password DB	.kdbx (KeePassX)	4	4
	.kdb (KeePass)	1	1

Vulnerable Websites

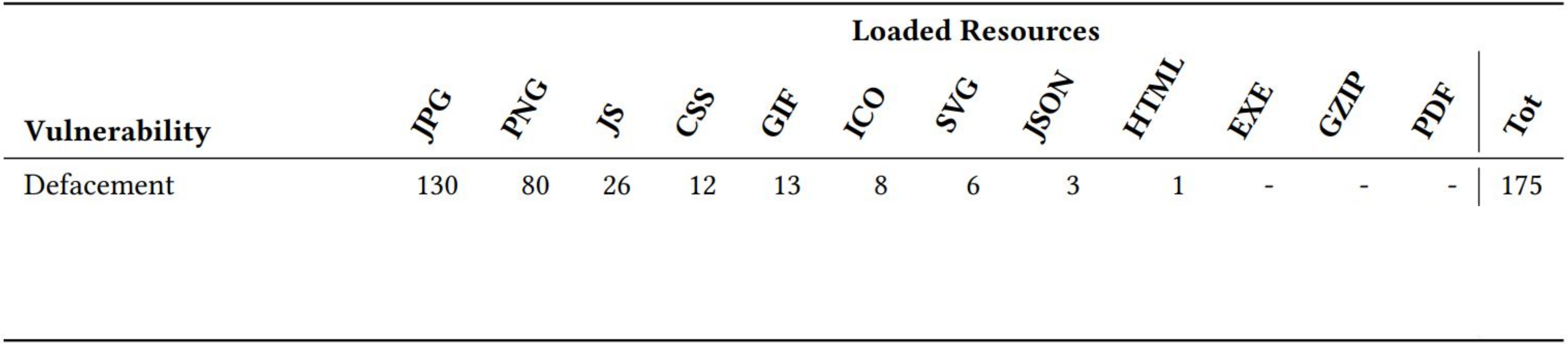
We collected 5,196 websites relying on 2,468 buckets



	Loaded Resources												
Vulnerability	JPG	PNG	JS	CSS	GIF	ICO	SVG	JSON	HTML	EXE	GZIP	PDF	Tot

Vulnerable Websites

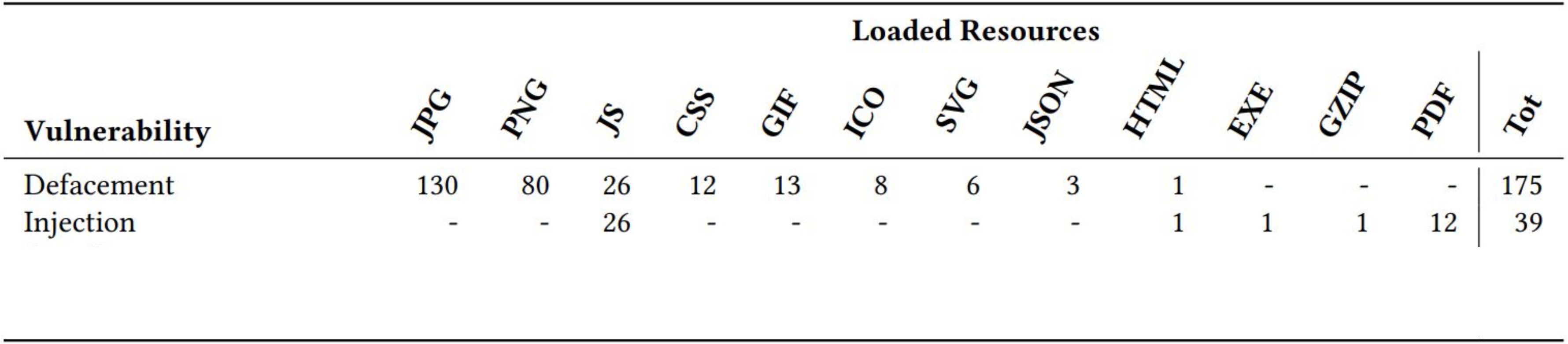
We collected 5,196 websites relying on 2,468 buckets



	Loaded Resources												
Vulnerability	JPG	PNG	JS	CSS	GIF	ICO	SVG	JSON	HTML	EXE	GZIP	PDF	Tot
Defacement	130	80	26	12	13	8	6	3	1	-	-	-	175

Vulnerable Websites

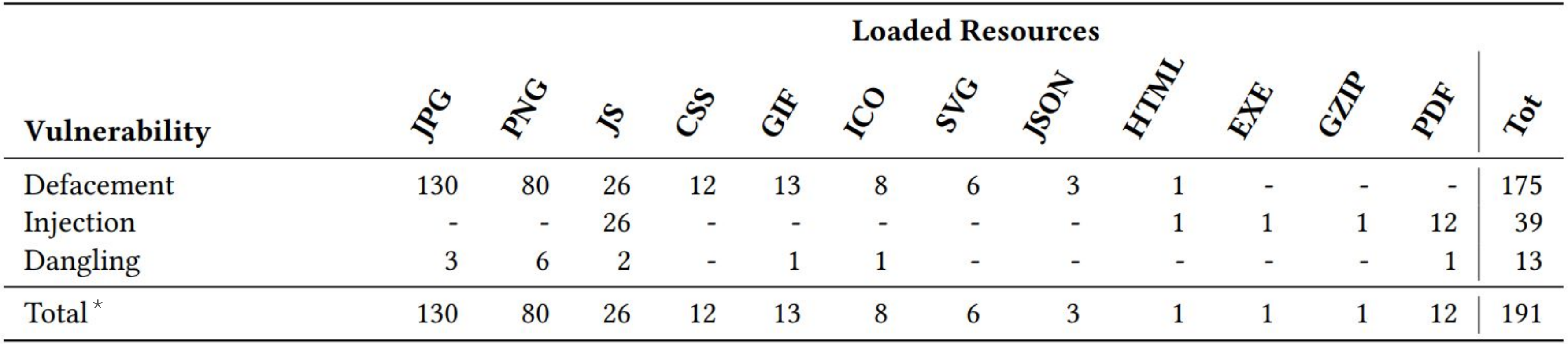
We collected 5,196 websites relying on 2,468 buckets



	Loaded Resources												
Vulnerability	JPG	PNG	JS	CSS	GIF	ICO	SVG	JSON	HTML	EXE	GZIP	PDF	Tot
Defacement	130	80	26	12	13	8	6	3	1	-	-	-	175
Injection	-	-	26	-	-	-	-	-	1	1	1	12	39

Vulnerable Websites

We collected 5,196 websites relying on 2,468 buckets



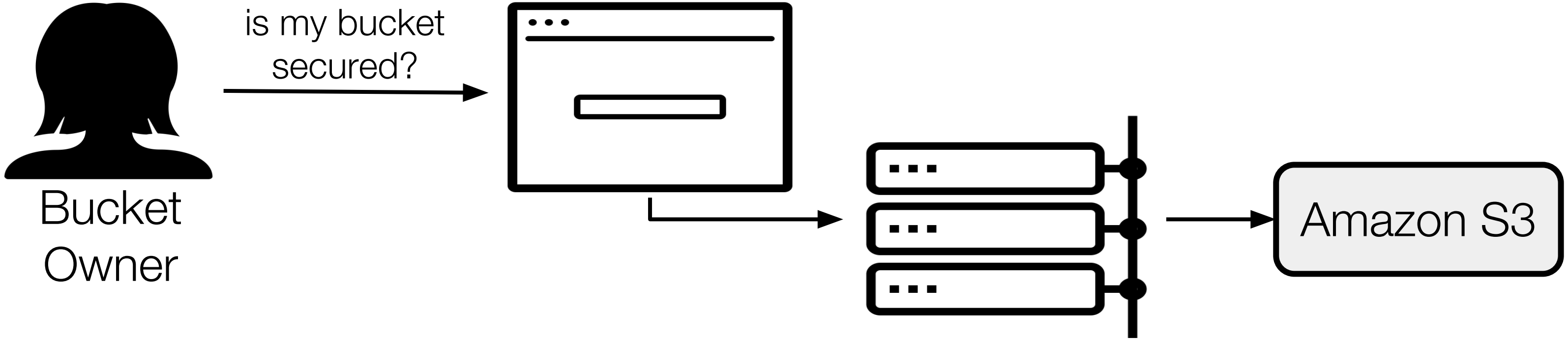
	Loaded Resources												
Vulnerability	**JPG**	**PNG**	**JS**	**CSS**	**GIF**	**ICO**	**SVG**	**JSON**	**HTML**	**EXE**	**GZIP**	**PDF**	**Tot**
Defacement	130	80	26	12	13	8	6	3	1	-	-	-	175
Injection	-	-	26	-	-	-	-	-	1	1	1	12	39
Dangling	3	6	2	-	1	1	-	-	-	-	-	1	13
Total *	130	80	26	12	13	8	6	3	1	1	1	12	191

*Note that websites can overlap among the different types of vulnerability

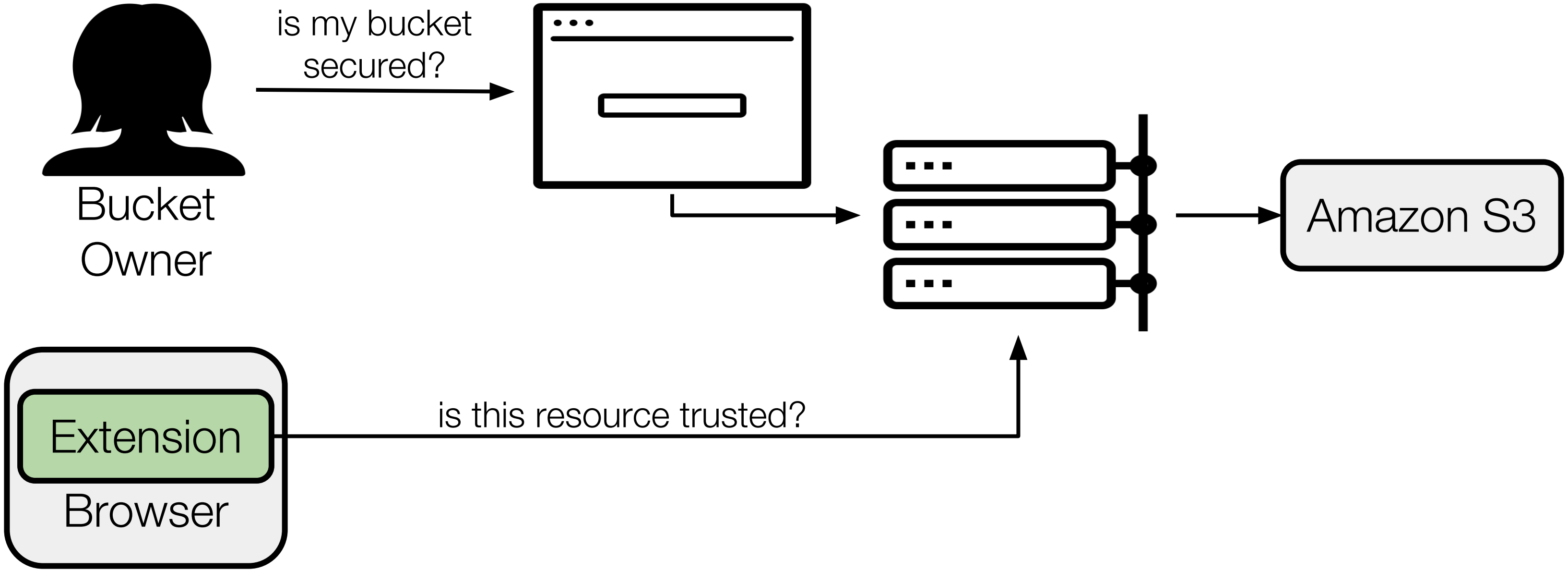
Mitigation

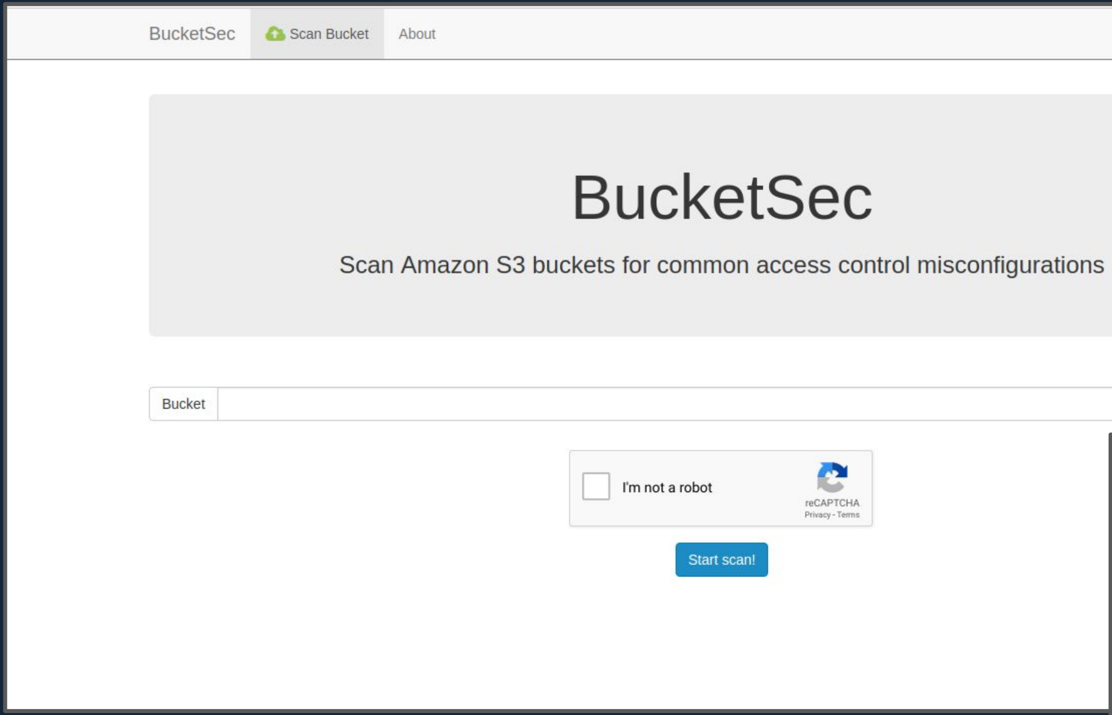
Fix the damn permissions!

Mitigation



Mitigation


is my bucket secured?
Bucket Owner
Amazon S3
Extension
Browser
is this resource trusted?

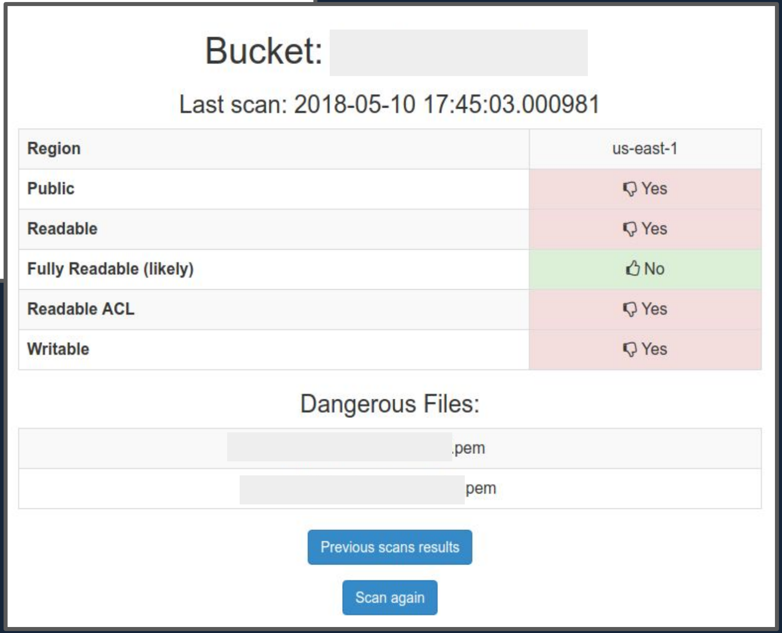


BucketSec

Scan Amazon S3 buckets for common access control misconfigurations

Bucket:

□ I'm not a robot



Bucket: [redacted]

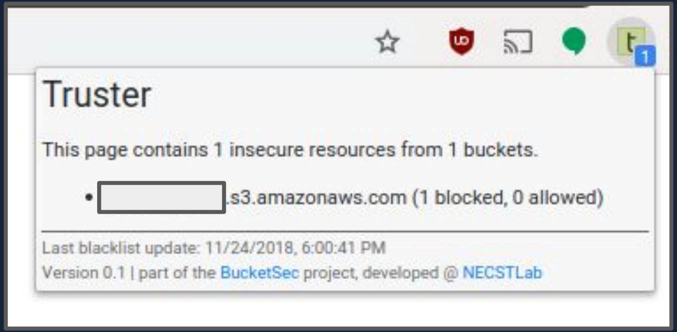
Last scan: 2018-05-10 17:45:03.000981

Region	us-east-1
Public	👎 Yes
Readable	👎 Yes
Fully Readable (likely)	👍 No
Readable ACL	👎 Yes
Writable	👎 Yes

Dangerous Files:

[redacted].pem
[redacted]pem

https://bucketsec.necst.it

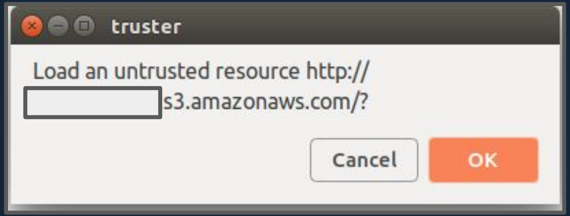


Truster

This page contains 1 insecure resources from 1 buckets.

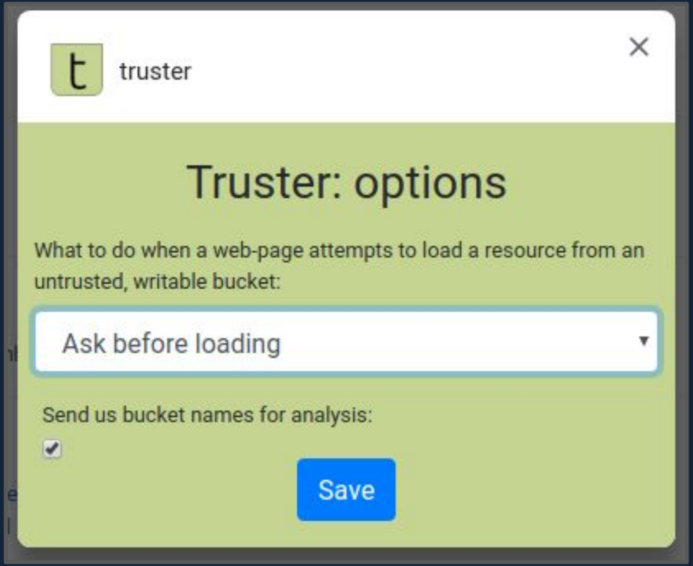
- [redacted].s3.amazonaws.com (1 blocked, 0 allowed)

Last blacklist update: 11/24/2018, 6:00:41 PM
Version 0.1 | part of the BucketSec project, developed @ NECSTLab



truster

Load an untrusted resource http://[redacted]s3.amazonaws.com/?



truster

Truster: options

What to do when a web-page attempts to load a resource from an untrusted, writable bucket:

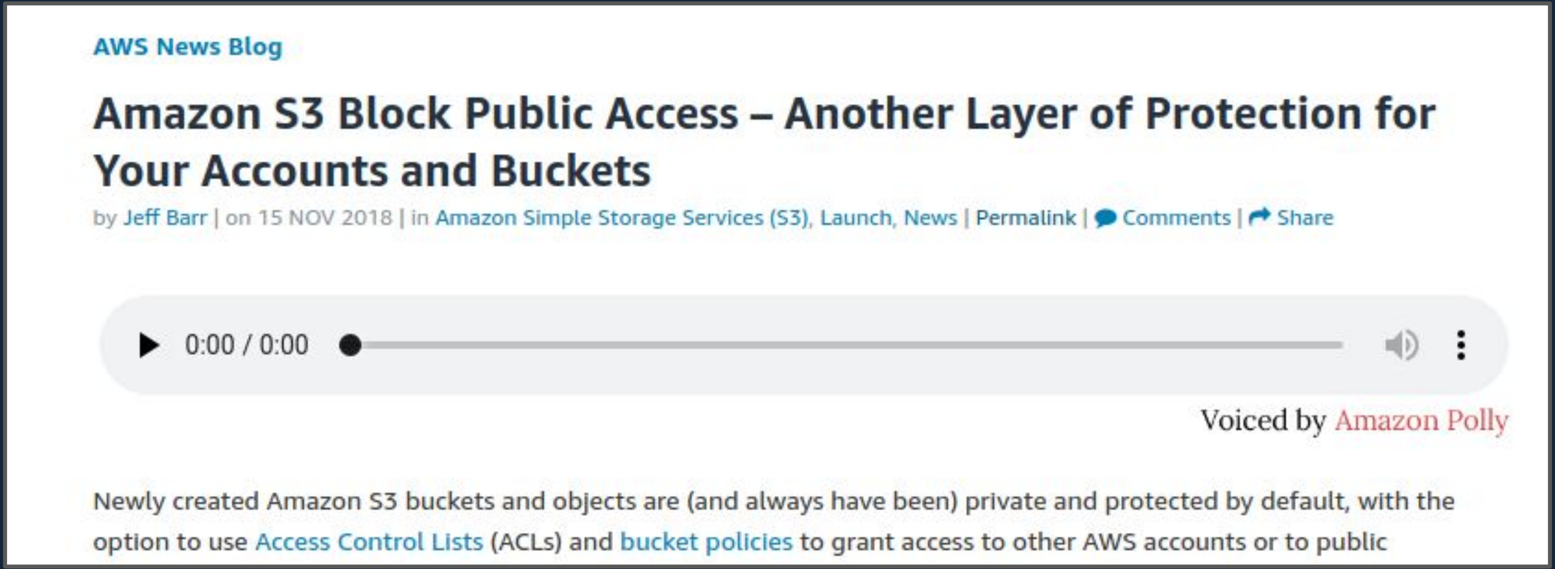
Ask before loading ▾

Send us bucket names for analysis:

☑

https://github.com/necst/truster

Responsible Disclosure



AWS News Blog

Amazon S3 Block Public Access – Another Layer of Protection for Your Accounts and Buckets

by Jeff Barr | on 15 NOV 2018 | in Amazon Simple Storage Services (S3), Launch, News | Permalink | Comments | Share

Voiced by Amazon Polly

Newly created Amazon S3 buckets and objects are (and always have been) private and protected by default, with the option to use Access Control Lists (ACLs) and bucket policies to grant access to other AWS accounts or to public

Conclusions

- We investigated **security implications** of using the Amazon S3 service
- Raise the **awareness** of a real-world security problem and warn users of its security implications
- **~14%** of S3 buckets are **public**
- **~2%** of S3 buckets are **publicly writable**
- **191** vulnerable websites
- We need **automated** solutions
  - Automatically **check** for potential misconfigurations
  - **Protect** client-side users

Thanks!
Questions?

Andrea Continella

conand@cs.ucsb.edu

https://conand.me

🐦 @_conand