

Furado no fundo

Como Buckets S3 mal configurados expõem milhões em dados e atacantes exploram isso

-R3d0lx01

Gustavo Redol



- Analista de CloudSec
- Pentester
- Apaixonado por CyberSec

Mas oque são buckets S3

- AWS S3 (Simple Storage Service) é o serviço de armazenamento da Amazon AWS.
- O Google tem o GCP(Google Cloud Provider) Buckets .
- A Microsoft tem os Azure Blobs.

Acessando seu 1º bucket publico



- Como todo arquivo no bucket tem uma URL própria conseguimos fazer um fuzzing para encontrar arquivos interessantes dentro dos buckets.

Mas quão real é esse problema?

- Em Junho/2017 Dados dos registros de eleitores dos EUA armazenados em um bucket exposto abertamente, causou o vazamento de informações pessoais de 198 milhões de eleitores.
- A Deep Root Analytics, uma empresa de big data apoiada pelo Partido Republicano, colocou em risco informações pessoais e dados de perfis de eleitores armazenando-os em um servidor S3 aberto. Esse s3 combinava informações de eleitores acessíveis ao público com dados adicionais de pesquisa de mercado para perfilar eleitores individuais a ponto de ser utilizáveis para calcular a probabilidade de voto nas próximas eleições.

Mas quão real é esse problema?

- Foi divulgado em 6 de novembro de 2020 por pesquisadores um vazamento de dados do booking.com e Hostels.com e totalizando 24,4 GB de dados, pelo menos 10 milhões de arquivos .
- Os dados do dump incluem detalhes de cartão de crédito de viajantes e agentes de viagens, incluindo o código CVV, detalhes de pagamento, detalhes de reserva e informações de identificação pessoal (PII), incluindo nomes, endereços de e-mail, números de identificação nacionais e números de telefone .
- O bucket ainda estava em uso, com novos registros sendo constantemente carregados e, embora tenha sido protegido poucas horas após a equipe de pesquisa entrar em contato com a AWS, é impossível dizer que o banco de dados não foi acessado ou roubado.


Mas como encontramos esses vazamentos?

- Ferramentas browser-based como GreyHatWarfare.
- Ferramentas CLI como AWSBucketDump e S3Scanner e Gobuster / Feroxbuster.

GreyhatWarfare

Buckets

Shorteners

GRAYHAT
WARFARE
CAUSE WHITE IS BORING

Home

Filter Buckets

Search Files

Docs / API


Top Keywords


Buckets Stream


★ Pricing

🔗 FAQ


✉ Contact Us









Files
2.8bn of 14.8bn




Amazon Web Services
35.1k of 325.8k




Azure Blob Storage
42.9k of 62.6k




Digital Ocean Spaces
9.1k



Google Cloud Platform
32.0k of 75.7k



Alibaba Cloud
2.5k




Last Update
22 Nov 2024


Search Public Buckets


✕ Random Files

Wondering what is this website ? Read details here: [How to search for Open Amazon s3 Buckets and their contents](#)

Keywords - Stopwords (start with minus -) 

keyword1 keyword2 -stopword1 -stopword2

☐ Full Path 

☐ Treat as regex 

Additional filters

Filename Extensions (php, xlsx, docx, pdf)

php, xlsx, docx, pdf

+ Include

✕ Exclude

🔍 Search

GreyhatWarfare

Buckets

Shorteners

GRAYHAT
WARFARE

causes white to boring

★ Pricing

🔗 FAQ

✉ Contact Us

Home

Filter Buckets

Search Files

Docs / API

Top Keywords

Buckets Stream

Search files

Saved searchesRandom Files

Keywords - Stopwords (start with minus -)

php config

Full Path

Treat as regex

Additional filters

Filename Extensions (php, xlsx, docx, pdf)

phptxtphp, xlsx, docx, pdf

IncludeExclude

Search

Results for "php config"

★ Save & notifySee corresponding API Call

Showing 1 - 20 out of 7272 results

Premium users using this query see 31427 more results. More info here.

#	Bucket	Filename	Container	Size	Last Modified
1	absoluteadmin.s3.amazonaws.com	/plugins/datatables/extensions/E/php/config.php		767.00B	10-12-2015 13:36:05
2	n.blob.core.windows.net	/wp-content/themes/dante/s/sf-shortcodes/config.php	static	731.00B	16-09-2014 01:03:40

AwsBucketDump

```
(myenv) guga@guga-desk:~/Desktop/palestra/AWSBucketDump$ python3 AWSBucketDump.py -l BucketNames.txt -g interesting_Keywords.txt
```

```
Downloads were not enabled (-D), not saving results locally.
```

```
Starting thread...
```

```
Download worker running...
```

```
Queuing http://0.s3.amazonaws.com...
```

```
Queuing http://01.s3.amazonaws.com...
```

```
Queuing http://02.s3.amazonaws.com...
```

```
Queuing http://03.s3.amazonaws.com...
```

```
Queuing http://1.s3.amazonaws.com...
```

```
Queuing http://10.s3.amazonaws.com...
```

```
Queuing http://11.s3.amazonaws.com...
```

```
Queuing http://12.s3.amazonaws.com...
```

```
Queuing http://13.s3.amazonaws.com...
```

```
Queuing http://14.s3.amazonaws.com...
```

```
Fetching http://0.s3.amazonaws.com...
```

```
Queuing http://15.s3.amazonaws.com...
```

```
Pilfering http://espanol.s3.amazonaws.com...
```

```
Collectable: http://espanol.s3.amazonaws.com/Membresias Rentables Files/estimador.xls
```

```
Downloading http://espanol.s3.amazonaws.com/Membresias Rentables Files/estimador.xls...
```

```
Collectable: http://espanol.s3.amazonaws.com/Membresias Rentables Files/estimador.xlsx
```

```
Collectable: http://espanol.s3.amazonaws.com/afiliado VIP/Autoayuda_gap.csv
```

```
Collectable: http://espanol.s3.amazonaws.com/afiliado VIP/antiguedades analysis.csv
```

```
Collectable: http://espanol.s3.amazonaws.com/afiliado VIP/auto_ayuda_analysis.csv
```

```
Local espanol.s3.amazonaws.com/Membresias Rentables Files/estimador.xls
```

```
Collectable: http://espanol.s3.amazonaws.com/afiliado VIP/belleza analysis.csv
```

```
Collectable: http://espanol.s3.amazonaws.com/afiliado VIP/dietas para quemar grasas analysis.csv
```

```
Collectable: http://espanol.s3.amazonaws.com/afiliado VIP/gap_antiguedades.csv
```

```
Collectable: http://espanol.s3.amazonaws.com/afiliado VIP/gap_belleza.csv
```

```
Collectable: http://espanol.s3.amazonaws.com/afiliado VIP/gap_liderazgo.csv
```

```
Collectable: http://espanol.s3.amazonaws.com/afiliado VIP/gap_manualidades.csv
```

```
Collectable: http://espanol.s3.amazonaws.com/afiliado VIP/liderazgo analysis.csv
```

```
Collectable: http://espanol.s3.amazonaws.com/afiliado VIP/manualidades analysis.csv
```

```
Collectable: http://espanol.s3.amazonaws.com/afiliado VIP/tercera edad analysis.csv
```

```
Collectable: http://espanol.s3.amazonaws.com/citypopulation.xlsx
```

```
Collectable: http://espanol.s3.amazonaws.com/clickbank/00Avanzado/week1/images/Thumbs.db
```

```
Collectable: http://espanol.s3.amazonaws.com/clickbank/00Avanzado/week1/images/arrow_s1_red3_sh.png
```

AwsBucketDump

```
Downloading http://espanol.s3.amazonaws.com/Membresias Rentables Files/estimador.xlsx...  
local espanol.s3.amazonaws.com/Membresias Rentables Files/estimador.xlsx  
This file is greater than the specified max size... skipping...
```

```
Downloading http://espanol.s3.amazonaws.com/afiliado VIP/Autoayuda_gap.csv...  
local espanol.s3.amazonaws.com/afiliado VIP/Autoayuda_gap.csv  
Pilfering http://esx.s3.amazonaws.com...  
Collectable: http://esx.s3.amazonaws.com/_users/org.couchdb.user:poc  
Fetching http://et.s3.amazonaws.com...  
This file is greater than the specified max size... skipping...
```

```
Downloading http://espanol.s3.amazonaws.com/afiliado VIP/antiguedades analysis.csv...  
local espanol.s3.amazonaws.com/afiliado VIP/antiguedades analysis.csv  
Fetching http://eta.s3.amazonaws.com...  
This file is greater than the specified max size... skipping...
```

```
Downloading http://espanol.s3.amazonaws.com/afiliado VIP/auto_ayuda_analysis.csv...  
local espanol.s3.amazonaws.com/afiliado VIP/auto_ayuda_analysis.csv  
http://eta.s3.amazonaws.com is not accessible.  
Fetching http://europe.s3.amazonaws.com...  
This file is greater than the specified max size... skipping...
```

AwsBucketDump

```
(myenv) guga@guga-desk:~/Desktop/palestra/AWSBucketDump$ ls -la
total 132
drwxrwxr-x 10 guga guga 4096 Feb  5 23:45 .
drwxrwxr-x  5 guga guga 4096 Feb  5 22:59 ..
-rwxrwxr-x  1 guga guga 7235 Feb  2 22:53 AWSBucketDump.py
-rw-rw-r--  1 guga guga 18679 Feb  2 23:18 aws-s3-names-list.txt
-rw-rw-r--  1 guga guga 11957 Feb  2 22:53 BucketNames.txt
drwxrwxr-x  2 guga guga 4096 Feb  5 23:43 database01.s3.amazonaws.com
drwxrwxr-x  6 guga guga 4096 Feb  5 23:45 espanol.s3.amazonaws.com
drwxrwxr-x  3 guga guga 4096 Feb  5 23:45 esx.s3.amazonaws.com
drwxrwxr-x  5 guga guga 4096 Feb  5 23:45 formacion.s3.amazonaws.com
drwxrwxr-x  8 guga guga 4096 Feb  2 22:53 .git
-rw-rw-r--  1 guga guga    6 Feb  2 22:53 .gitignore
-rw-rw-r--  1 guga guga 25646 Feb  5 23:45 interesting_file.txt
-rw-rw-r--  1 guga guga   84 Feb  2 22:53 interesting_Keywords.txt
drwxrwxr-x  3 guga guga 4096 Feb  5 23:45 kansas.s3.amazonaws.com
-rw-rw-r--  1 guga guga 1059 Feb  2 22:53 LICENSE
drwxrwxr-x  5 guga guga 4096 Feb  2 22:54 myenv
-rw-rw-r--  1 guga guga 2837 Feb  2 22:53 README.md
-rw-rw-r--  1 guga guga   89 Feb  2 22:53 requirements.txt
drwxrwxr-x 15 guga guga 4096 Feb  2 23:06 SecLists
-rw-rw-r--  1 guga guga  125 Feb  2 22:53 .travis.yml
(myenv) guga@guga-desk:~/Desktop/palestra/AWSBucketDump$
```

Exemplo de query de vulneraveis no AWS CLI

```
guga@guga-desk:~$ aws --profile flaws ec2 describe-snapshots --region us-west-2
{
  "Snapshots": [
    {
      "StorageTier": "standard",
      "TransferType": "standard",
      "CompletionTime": "2018-04-19T17:51:52+00:00",
      "SnapshotId": "snap-[REDACTED]",
      "VolumeId": "vol-[REDACTED]",
      "State": "completed",
      "StartTime": "2018-04-19T17:48:27+00:00",
      "Progress": "100%",
      "OwnerId": "364390758643",
      "Description": "Copied for DestinationAmi ami-4baec133 from SourceAmi ami-18d8ca78 for SourceSnapshot snap-002644fdf2d5b6a98. Task created on 1,524,160,078,444.",
      "VolumeSize": 8,
      "Encrypted": false
    },
    {
      "StorageTier": "standard",
      "TransferType": "standard",
      "CompletionTime": "2018-04-17T14:43:00+00:00",
      "SnapshotId": "snap-[REDACTED]",
      "VolumeId": "vol-[REDACTED]",
      "State": "completed",
      "StartTime": "2018-04-17T14:39:59+00:00",
      "Progress": "100%",
      "OwnerId": "364390758643",
      "Description": "Copied for DestinationAmi ami-691c7011 from SourceAmi ami-b90b19d9 for SourceSnapshot snap-04bd78ba14a8e4ab8. Task created on 1,523,975,997,720.",
      "VolumeSize": 8,
      "Encrypted": false
    },
    {
      "OwnerAlias": "amazon",
      "StorageTier": "standard",
      "TransferType": "standard",
      "CompletionTime": "2018-04-16T06:05:58+00:00",
      "SnapshotId": "snap-[REDACTED]",
      "VolumeId": "vol-[REDACTED]",
      "State": "completed",
      "StartTime": "2018-04-16T05:52:45+00:00",
      "Progress": "100%",
      "OwnerId": "102837901569",
      "Description": "Created by CreateImage(i-0d0dadd6aa2c825a2) for ami-7a781502 from vol-07d90aab87ede5d69",
      "VolumeSize": 30,
      "Encrypted": false
    },
    {
      "OwnerAlias": "amazon",
      "StorageTier": "standard",
      "TransferType": "standard",
      "CompletionTime": "2018-04-16T05:07:20+00:00",
      "SnapshotId": "snap-[REDACTED]",
      "VolumeId": "vol-[REDACTED]",
      "State": "completed",
      "StartTime": "2018-04-16T04:54:18+00:00",
      "Progress": "100%",

```

Mas oquê causa isso?

```
1 ▼ {  
2   "Version": "2012-10-17",  
3 ▼   "Statement": [  
4 ▼     {  
5       "Sid": "PublicRead",  
6       "Effect": "Allow",  
7       "Principal": "*",  
8       "Action": "s3:GetObject",  
9       "Resource": "arn:aws:s3:::dataco-salesreps/*"  
10    },  
11 ▼    {  
12      "Sid": "PublicList",  
13      "Effect": "Allow",  
14      "Principal": "*",  
15      "Action": "s3:ListBucket",  
16      "Resource": "arn:aws:s3:::dataco-salesreps"  
17    }  
18  ]  
19 }
```

- Políticas de acesso permissivas
- Más praticas de deploy
- Falta de conhecimento do ambiente cloud

E como deveria ser?

```
{
  "Version": "2012-10-17",
  "Id": "ExamplePolicy01",
  "Statement": [
    {
      "Sid": "ExampleStatement01",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::123456789012:user/Dave"
      },
      "Action": [
        "s3:GetObject",
        "s3:GetBucketLocation",
        "s3:ListBucket"
      ],
      "Resource": [
        "arn:aws:s3:::awsexamplebucket1/*",
        "arn:aws:s3:::awsexamplebucket1"
      ]
    }
  ]
}
```

- Allow específico para o ARN do usuário/grupo que deve ter o acesso.
- Viu como é fácil errar isso?

Ok, mas como impedimos isso?

- Habilitar bloqueio de acesso público: Os buckets do S3 não devem ser acessíveis publicamente, a menos que seja absolutamente necessário. Use a configuração "Bloquear acesso público" para evitar exposição não autorizada.
- Use políticas do IAM e políticas de bucket: Conceda permissões com base no princípio do menor privilégio. Evite usar permissões curinga (por exemplo, "s3:*") e defina ações e recursos explícitos.

Ok, mas como impedimos isso?

- Ativar versionamento e criptografia para reter os dados, mesmo que eles sejam excluídos acidentalmente.
- Use a criptografia do lado do servidor “SSE” (padrão novo) ou a criptografia do lado do cliente para proteger os dados estacionários.
- Utilize Access Analyzer: Use o AWS Identity and Access Management (IAM) Access Analyzer para identificar buckets compartilhados com contas ou organizações externas.

AWS CloudWatch

The screenshot displays the AWS CloudWatch Alarms console. The top navigation bar includes the AWS logo, a search bar, and the region 'United States (Oregon)'. The left sidebar shows the 'CloudWatch' menu with options like 'Alarms', 'Logs', 'Metrics', 'X-Ray traces', 'Events', 'Application Signals', 'Network Monitoring', and 'Insights'. The main content area is titled 'Alarms (0)' and features a search bar, filters for 'Alarm state: Any', 'Alarm type: Any', and 'Actions status: Any', and a 'Create alarm' button. The table below the filters is empty, displaying the message 'No alarms' and 'No alarms to display'. A 'Create alarm' button is visible at the bottom of the table.

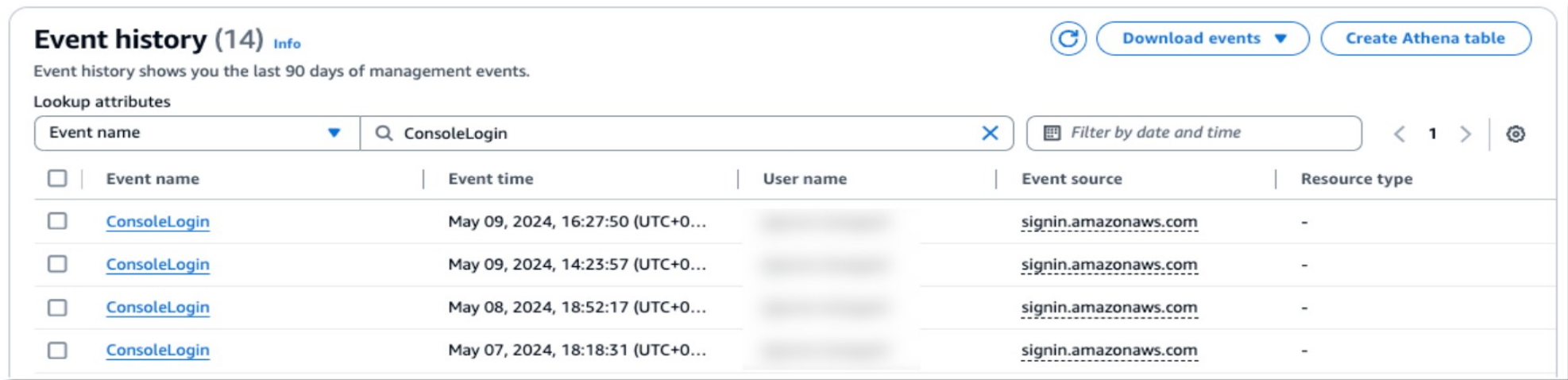
Name	State	Last state update (UTC)	Conditions	Actions
No alarms				
No alarms to display				
Read more about Alarms				
Create alarm				

- Mesmo com configurações corretas, o monitoramento contínuo é essencial para manter a segurança do S3. O CloudWatch fornece monitoramento e alertas em tempo real sobre possíveis problemas.

Integração com o CloudTrail

- Integre com o AWS CloudTrail: use os logs do CloudTrail no CloudWatch para identificar chamadas de API e detectar tentativas de acesso não autorizado.

The CloudTrail Event history page filtered on the ConsoleLogin event.



The screenshot shows the AWS CloudTrail Event history page. At the top, it says "Event history (14) Info" and "Event history shows you the last 90 days of management events." There are buttons for "Download events" and "Create Athena table". Below this is a "Lookup attributes" section with a search bar containing "ConsoleLogin" and a "Filter by date and time" button. The main table displays four events, all of which are "ConsoleLogin" events. Each row has a checkbox, the event name, the event time, the user name (blurred), the event source (signin.amazonaws.com), and the resource type (-).

<input type="checkbox"/>	Event name	Event time	User name	Event source	Resource type
<input type="checkbox"/>	ConsoleLogin	May 09, 2024, 16:27:50 (UTC+0...	[blurred]	signin.amazonaws.com	-
<input type="checkbox"/>	ConsoleLogin	May 09, 2024, 14:23:57 (UTC+0...	[blurred]	signin.amazonaws.com	-
<input type="checkbox"/>	ConsoleLogin	May 08, 2024, 18:52:17 (UTC+0...	[blurred]	signin.amazonaws.com	-
<input type="checkbox"/>	ConsoleLogin	May 07, 2024, 18:18:31 (UTC+0...	[blurred]	signin.amazonaws.com	-

Mas, e o RED TEAM?

```
(myenv) root@guga-Aspire-A515-56G:/home/guga/Desktop/yes3-scanner# python3 yes3.py --profile r3d0lx01
YES3 SCANNER RESULTS
```

```
-----
AWS Account: 345594608173
```

```
Account Settings
```

```
Account Block Public Access Overall Status: WARN
```

```
Account BPA Block Public ACLs WARN
```

```
Account BPA Ignore Public ACLs: WARN
```

```
Account BPA Block Public Policy: WARN
```

```
Account BPA Restrict Public Buckets: WARN
```

```
-----
```

```
Bucket Summary
```

```
Total Buckets: 1
```

```
-----
```

```
Buckets potentially public: 0
```

```
-----
```

```
Buckets with Visibility Issues: 0
```

```
Buckets with default S3-Owned Encryption: 1
```

```
Buckets with a Block Public Access setting disabled: 1
```

```
Buckets with Bucket ACLs Enabled: 0
```

```
Buckets with ACLs set to public: 0
```

```
Buckets with Bucket Policy set to public: 0
```

```
Buckets with Object Lock disabled: 1
```

```
Buckets with Versioning disabled: 1
```

```
Buckets with Lifecycle Config Set to Expiration: 0
```

```
Buckets with Public Access from Website Setting: 0
```

```
Buckets with Server Access Logs Disabled: 1
```

```
-----
```

```
Additional Bucket Details
```

```
Buckets with default S3-Owned Encryption: balde-da-palestra
```

```
Buckets with a Block Public Access setting disabled: balde-da-palestra
```

```
Buckets with Bucket ACLs Enabled:
```

Mas, e o RED TEAM?

```
Account BPA Ignore Public ACLs: WARN
Account BPA Block Public Policy: WARN
Account BPA Restrict Public Buckets: WARN
-----
Bucket Summary
Total Buckets: 1
-----
Buckets potentially public: 0
-----
Buckets with Visibility Issues: 0
-----
Buckets with default S3-Owned Encryption: 1
Buckets with a Block Public Access setting disabled: 1
Buckets with Bucket ACLs Enabled: 0
Buckets with ACLs set to public: 0
Buckets with Bucket Policy set to public: 0
Buckets with Object Lock disabled: 1
Buckets with Versioning disabled: 1
Buckets with Lifecycle Config Set to Expiration: 0
Buckets with Public Access from Website Setting: 0
Buckets with Server Access Logs Disabled: 1
-----
Additional Bucket Details
Buckets with default S3-Owned Encryption: balde-da-palestra

Buckets with a Block Public Access setting disabled: balde-da-palestra

Buckets with Bucket ACLs Enabled:

Buckets with ACLs set to public:

Buckets with Bucket Policy set to public:

Buckets with Object Lock disabled: balde-da-palestra

Buckets with Versioning disabled: balde-da-palestra

Buckets with Lifecycle Config Set to Expiration:

Buckets with Public Access from Website Setting:

Buckets with Server Access Logs Disabled: balde-da-palestra
(myenv) root@guga-Aspire-A515-56G:/home/guga/Desktop/yes3-scanner#
```

OBRIGADO!

