19.12.2015

Targeting Amazon S3 services (Buckets)

By Amitay Dan and Samuel Cardillo

www.samuelcardillo.com www.amitaydan.com

Recently, we have realised that many Amazon customers do not understand how to use AWS Amazon Simple Storage Service (S3), leaving sensitive files and data open without any security measures. To change this issue and make better awareness, we decided to create a tool which helps to demonstrate how easy is to hunt for insecure Buckets and files in Amazon S3 service.

After creating the tool, we have found additional two documents related to this subject, but our tool is focusing on using Amazon JSON. Meaning, it is capable of attacking Amazon users, unlike the previous tools mentioned in the found documents.

Amazon employees communicated with us regularly on this issue. We were asked to share with them our findings before releasing our publication.

Time-line of our communication:

- 31.07.2015 - First email regarding the issue from our side.
- 31.07.2015 - Answer from Amazon requesting a draft before publication (the issue is already known by Amazon).
- 03.08.2015 - We sent them an email with an update about creation of a tool.
- 03.08.2015 - Amazon answered that they are looking forward to see the result.
- 02.12.2015 - The tool and the white paper sent to Amazon for review.
- 18.12.2015 - Amazon examined the review and answered positively about our further steps.

Email from Amazon:

"Hi Amitay

Thank you for sending through your paper.

As you rightly point out in the paper, buckets are completely private by default. It is a deliberate act by the customer to weaken those default controls to allow operations on their buckets by external parties. We also have a large amount of documentation covering the general use of [1[1]] and security best practices [2[2]] for all AWS services, including S3. We believe this is sufficient at this stage.

---

1 https://aws.amazon.com/documentation/s3

Thanks again for taking the time to look into the security of our customers, we always appreciate work done by external researchers like yourself, and enjoy working with them for the benefit of our customers. If you discover anything else about our services you would like to discuss with us, feel free to reach out to us again.

Best Regards

AWS Security

The review and white paper:

The cloud storage of Amazon is managed by Buckets[3], through which customers administer their files in the cloud.

"In a virtual-hosted–style URL, the bucket name is part of the domain name in the URL. For example:

`http://`*bucket*`.s3.amazonaws.com`

`http://`*bucket*`.s3-`*aws-region*`.amazonaws.com`.

In a virtual-hosted–style URL, you can use either of these endpoints. If you make a request to the `http://bucket.s3.amazonaws.com` endpoint, the DNS has sufficient information to route your request directly to the region where your bucket resides.

In a path-style URL, the bucket name is not part of the domain (unless you use a region-specific endpoint). For example:

US Standard endpoint, `http://s3.amazonaws.com/bucket`

Region-specific endpoint, `http://s3-`*aws-region*`.amazonaws.com/bucket`

In a path-style URL, the endpoint you use must match the region in which the bucket resides. For example, if your bucket is in the South America (Sao Paulo) region, you must use the `http://s3-sa-east-1.amazonaws.com/bucket` endpoint. If your bucket is in the US Standard region, you must use the `http://s3.amazonaws.com/bucket` endpoint".[4]

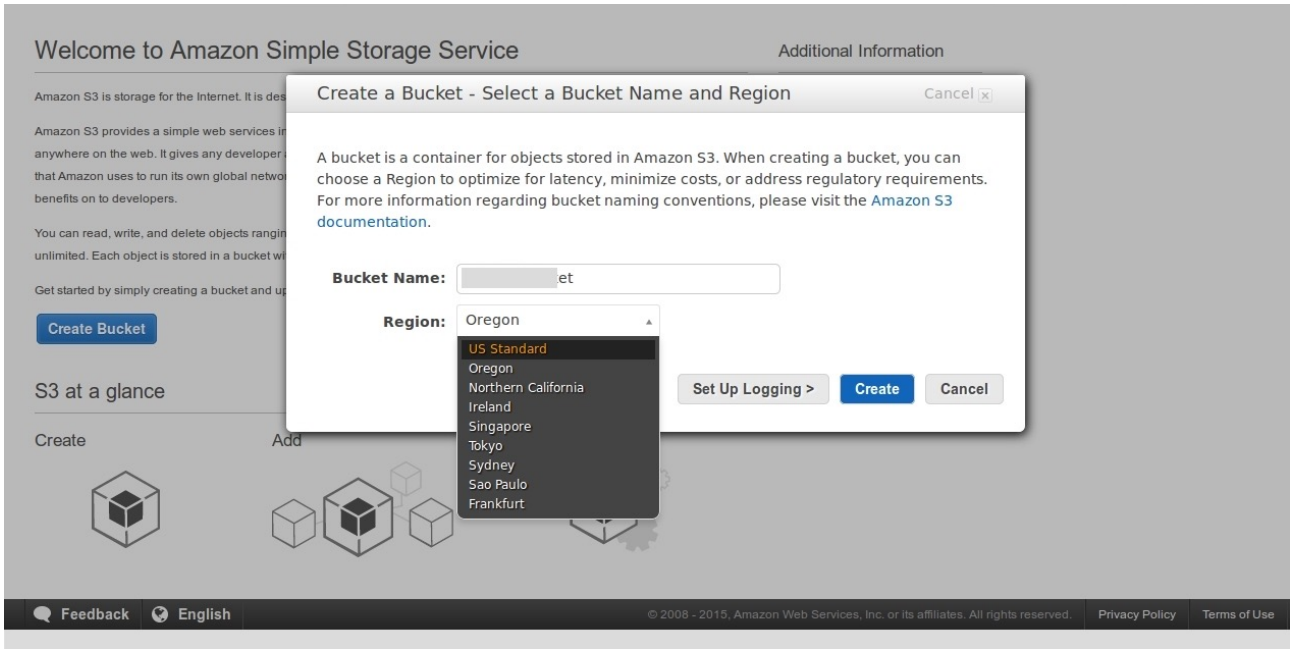
---

2 http://media.amazonwebservices.com/AWS_Security_Best_Practices.pdf

3 http://docs.aws.amazon.com/AmazonS3/latest/dev/UsingBucket.html

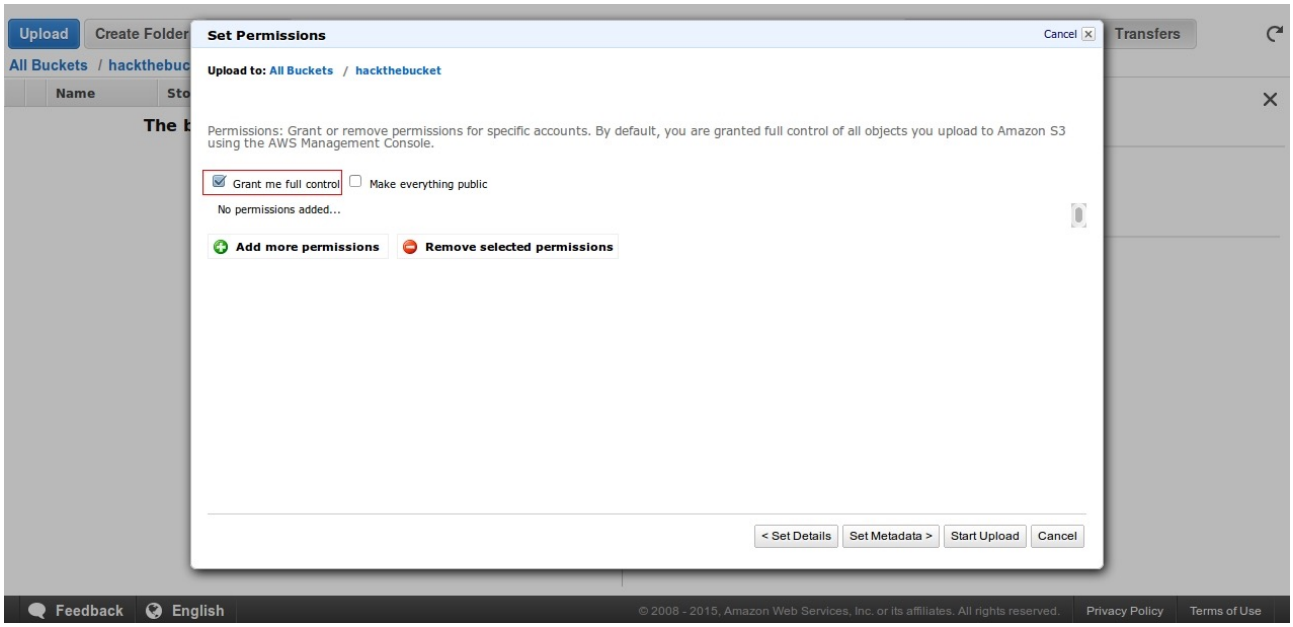
Customers can create by default up to 100 buckets, but also can request more. Administration of 100s of Buckets and 1000s of files might lead into problems, but the main issue is that there is a lack of understanding of cloud. Since the Buckets are private by default, it is really the user's problem if they decided to change it to be open. Yet we believe that Amazon needs to be more proactive with the (graphic) explanation related to the security. Additionally step by step clarification of the effect having public access to the main buckets, as well as for the files under it, should be released.

Here are some example of S3 interface:

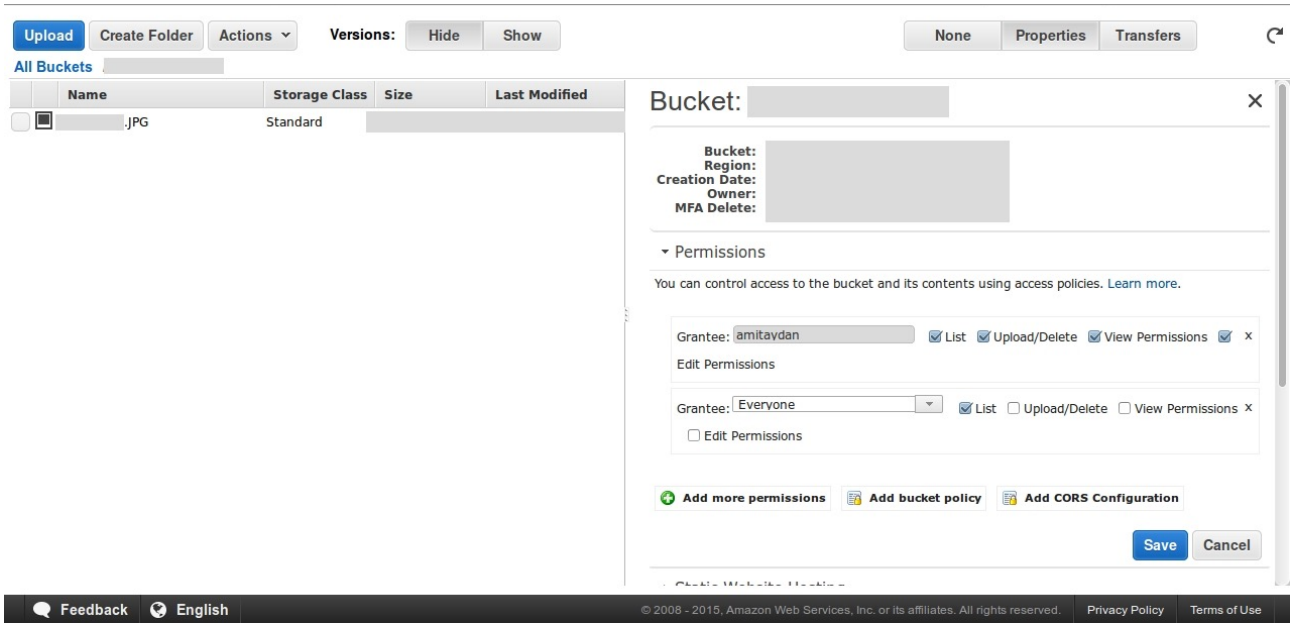


After choosing the bucket name, we are heading into the next steps

4 http://docs.aws.amazon.com/AmazonS3/latest/dev/UsingBucket.html



Amazon actually shares with a user that he/she has a full control, but they do not warn him/her by proactive means what will be the effect if he/she changes it.



Now, you can see what's happening when the users is adding more permissions and allows the public to see is list of file,which are stored under the buckets.

Even when a user has cloud front service as a protection in front of S3 service , misconfiguration will show the name of Bucket as well as the files inside.

Our tool is based on Amazon opening JSON [5], which helps us to target the full list[6] of Amazon IP range without the need for a brute force.

Since there was a need for passive DNS resolvers, for our project to run we have checked couple of options[7] and we chose a very effective tool.

Technical part:

Lets look here: https://1d4.us/54.231.136.58

5 https://aws.amazon.com/blogs/aws/aws-ip-ranges-json

6 https://ip-ranges.amazonaws.com/ip-ranges.json

7 http://www.bfk.de/bfk_dnslogger_en.html
https://www.passivetotal.org/api/docs
https://www.circl.lu/services/passive-dns
https://www.dnsdb.info

What we get is a list of clients who chose Amazon S3 service.
(*CLIENT SUBDOMAIN).s3(THIS CAN BE CHANGE).amazonaws.com.
→ 1234.s3.amazonws.com
Sometime the client domain comes after the amazonaws.com.

Now, protected client will be given XML results like that:
1.NoSuchBucket

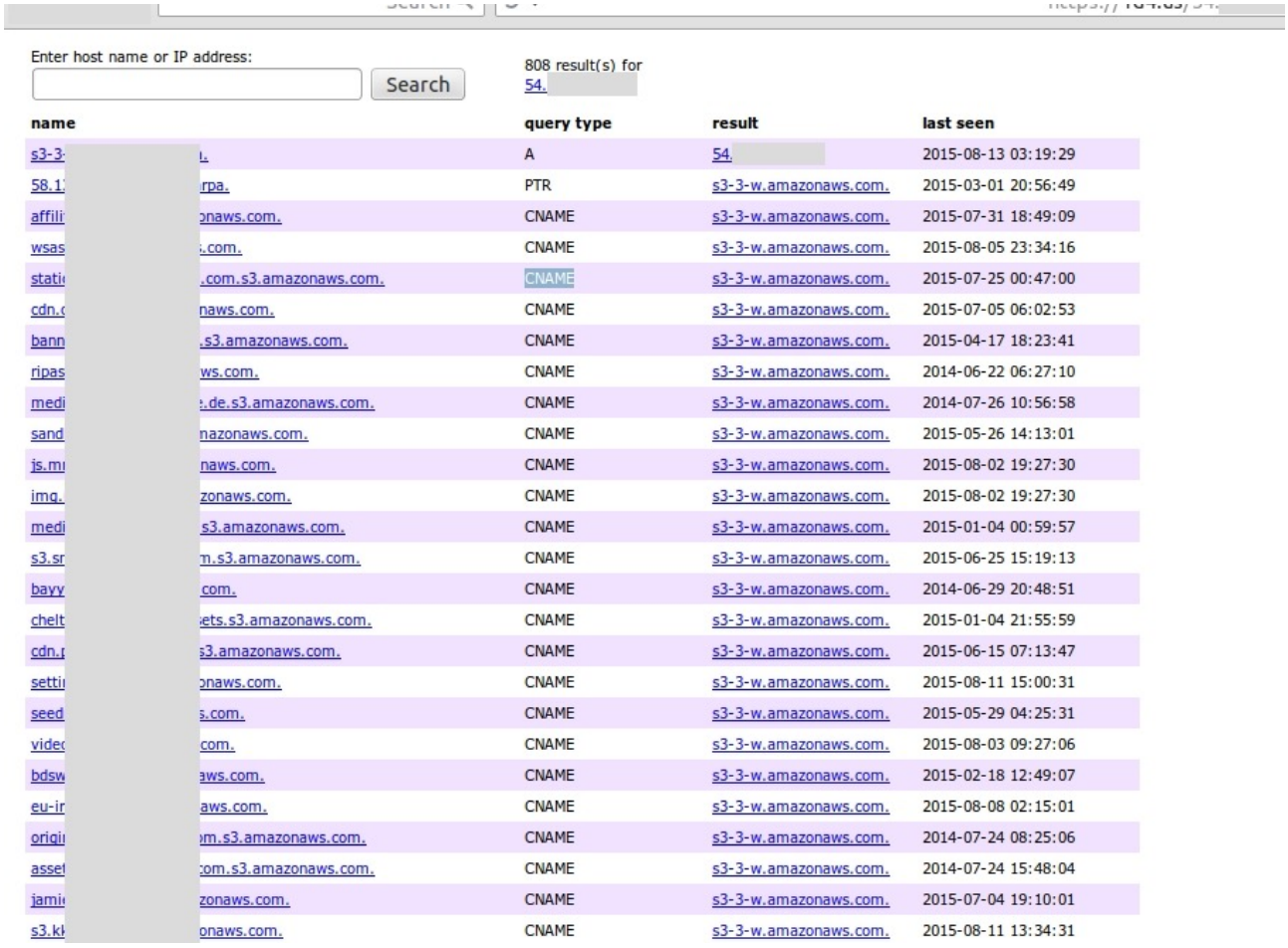
<Error><Code>NoSuchBucket</Code><Message>The specified bucket does not exist</Message><BucketName>***.s3.amazonaws.com.</BucketName><RequestId>***</RequestId><HostId>*******=</HostId></Error>**
Or
2.AccessDenied
<Error><Code>**AccessDenied**</Code><Message>Access Denied</Message><RequestId>******</RequestId><HostId>****=</HostId></Error>

Many clients are not protected and then what we get is:
<ListBucketResult></ListBucketResult>
If we open the XML ,we see:

<ListBucketResult>
<Name>****</Name>
<Prefix/>
<Marker/>
<MaxKeys>1000</MaxKeys>
<IsTruncated>true</IsTruncated>
<Contents>
<Key>banners/</Key>
<LastModified>2015-05-**T**:**:**1.000Z</LastModified>
<Etag>"******"</Etag>
<Size>0</Size>
<StorageClass>STANDARD</StorageClass>
</Contents>
<Contents><Key>*****.png</Key>
<LastModified>20**-**-**T**:**:**.000Z</LastModified>
<Etag>"**********"</Etag>
<Size>****</Size>
<StorageClass>STANDARD</StorageClass></Contents>
</ListBucketResult>

All you need to do now is to download the “Key”
1234.s3.amazonws.com will be now
1234.s3.amazonws.com/*****.png

Information about previous work can be found in here: Rapid7[8] Robin Wood[9] (akadigi ninja) as a might check for Cloudefigo[10] which is a project made by Nir Valtman and Moshe Ferber



Enter host name or IP address:

Search

808 result(s) for 54.

name	query type	result	last seen
s3-3- .amazonaws.com.	A	54.	2015-08-13 03:19:29
58.1 .in-addr.arpa.	PTR	s3-3-w.amazonaws.com.	2015-03-01 20:56:49
affili .s3.amazonaws.com.	CNAME	s3-3-w.amazonaws.com.	2015-07-31 18:49:09
wsas .com.	CNAME	s3-3-w.amazonaws.com.	2015-08-05 23:34:16
stati .com.s3.amazonaws.com.	CNAME	s3-3-w.amazonaws.com.	2015-07-25 00:47:00
cdn.c .amazonaws.com.	CNAME	s3-3-w.amazonaws.com.	2015-07-05 06:02:53
bann .s3.amazonaws.com.	CNAME	s3-3-w.amazonaws.com.	2015-04-17 18:23:41
ripas .aws.com.	CNAME	s3-3-w.amazonaws.com.	2014-06-22 06:27:10
medi .de.s3.amazonaws.com.	CNAME	s3-3-w.amazonaws.com.	2014-07-26 10:56:58
sand .amazonaws.com.	CNAME	s3-3-w.amazonaws.com.	2015-05-26 14:13:01
js.mi .amazonaws.com.	CNAME	s3-3-w.amazonaws.com.	2015-08-02 19:27:30
img. .amazonaws.com.	CNAME	s3-3-w.amazonaws.com.	2015-08-02 19:27:30
medi .s3.amazonaws.com.	CNAME	s3-3-w.amazonaws.com.	2015-01-04 00:59:57
s3.sr .m.s3.amazonaws.com.	CNAME	s3-3-w.amazonaws.com.	2015-06-25 15:19:13
bayy .com.	CNAME	s3-3-w.amazonaws.com.	2014-06-29 20:48:51
chelt .ets.s3.amazonaws.com.	CNAME	s3-3-w.amazonaws.com.	2015-01-04 21:55:59
cdn.p .s3.amazonaws.com.	CNAME	s3-3-w.amazonaws.com.	2015-06-15 07:13:47
setti .amazonaws.com.	CNAME	s3-3-w.amazonaws.com.	2015-08-11 15:00:31
seed .s.com.	CNAME	s3-3-w.amazonaws.com.	2015-05-29 04:25:31
video .com.	CNAME	s3-3-w.amazonaws.com.	2015-08-03 09:27:06
bdsw .aws.com.	CNAME	s3-3-w.amazonaws.com.	2015-02-18 12:49:07
eu-ir .aws.com.	CNAME	s3-3-w.amazonaws.com.	2015-08-08 02:15:01
origi .m.s3.amazonaws.com.	CNAME	s3-3-w.amazonaws.com.	2014-07-24 08:25:06
asset .com.s3.amazonaws.com.	CNAME	s3-3-w.amazonaws.com.	2014-07-24 15:48:04
jami .amazonaws.com.	CNAME	s3-3-w.amazonaws.com.	2015-07-04 19:10:01
s3.kl .amazonaws.com.	CNAME	s3-3-w.amazonaws.com.	2015-08-11 13:34:31

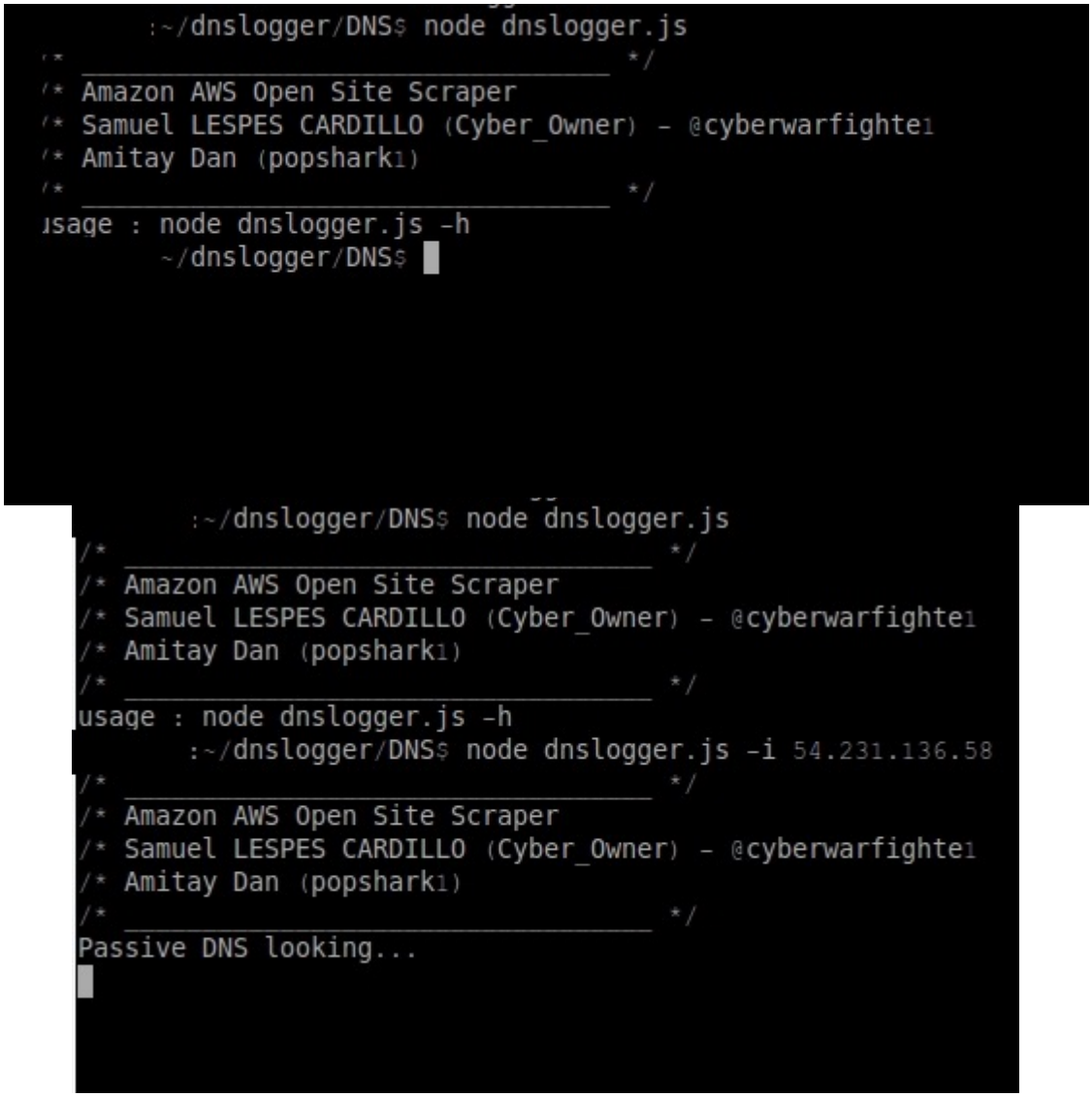
8 https://community.rapid7.com/community/infosec/blog/2013/03/27/1951-open-s3-buckets
http://www.rapid7.com/resources/videos/amazon-s3-bucket-misconfiguration.jsp

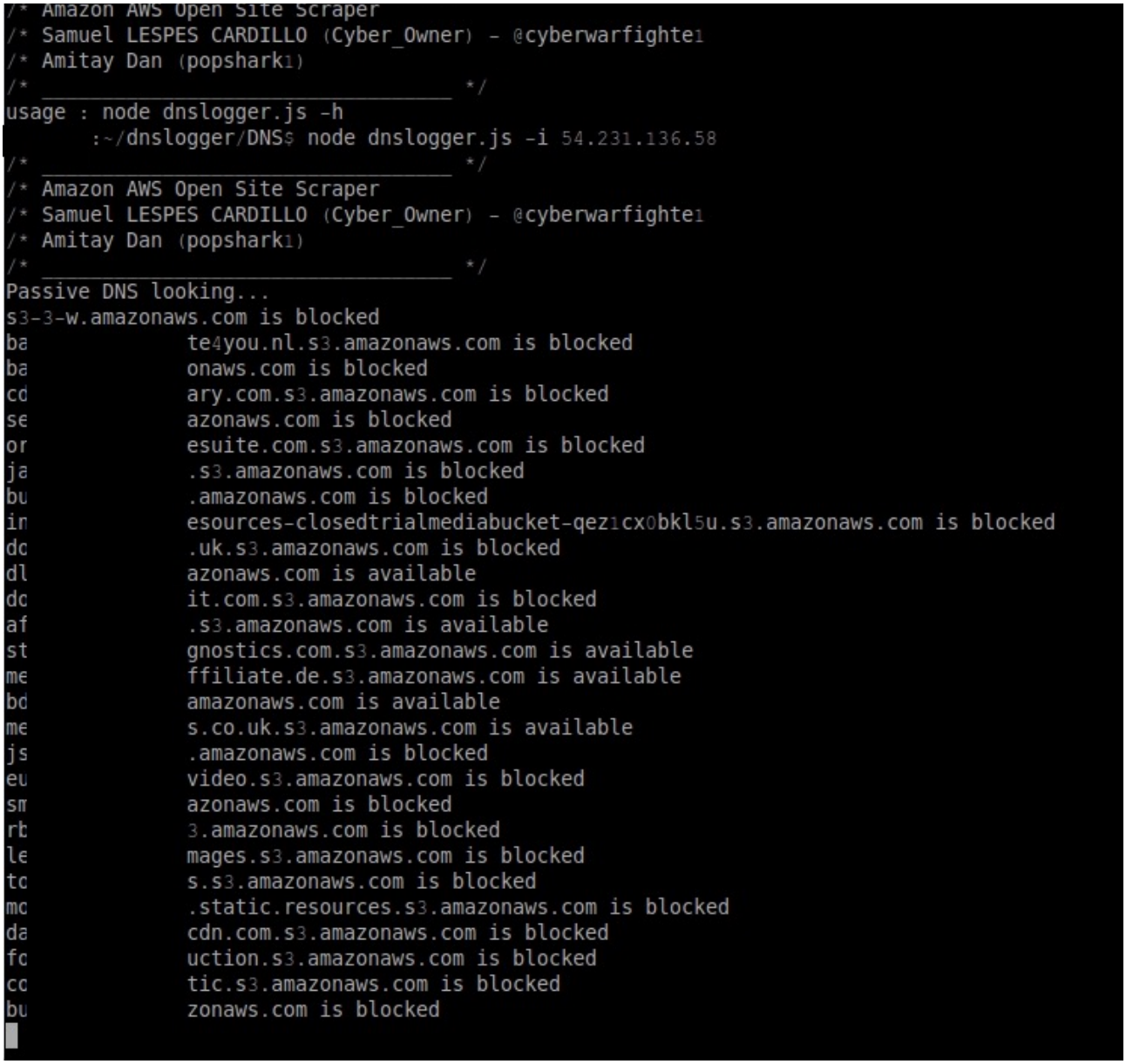
9 https://digi.ninja/blog/whats_in_amazons_buckets.php

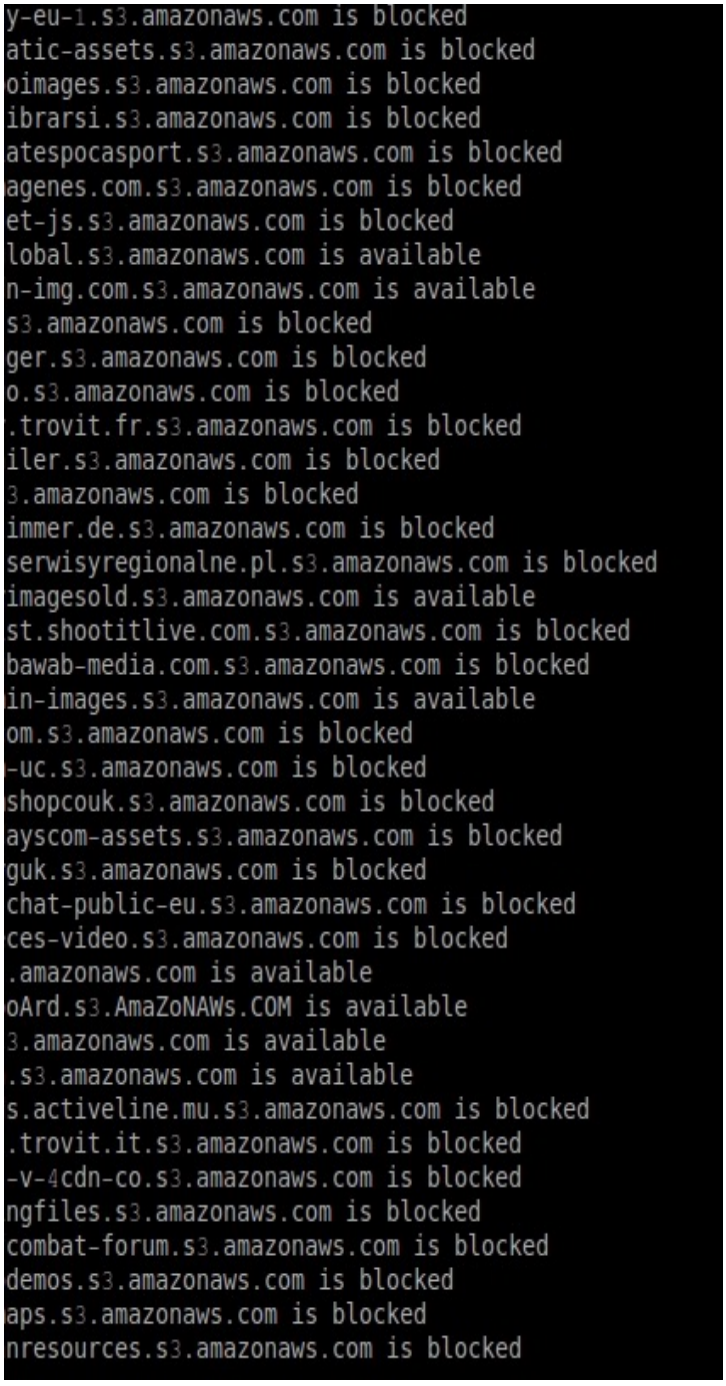
10 http://www.cloudefigo.org/
https://media.defcon.org/DEF%20CON%2023/DEF%20CON%2023%20presentations/DEFCON-23-Nir-Valtman-Moshe-Ferber-From-zero-to-secure-in-1-minute-UPDATED.pdf

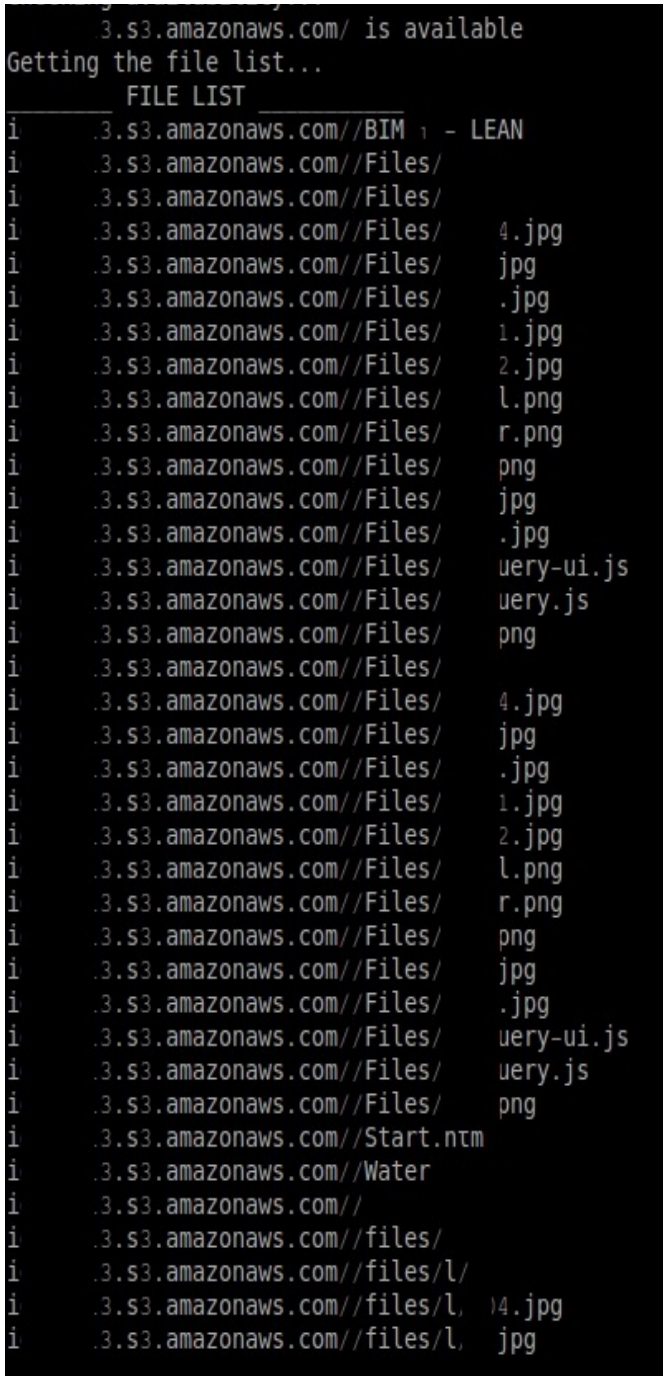
The tool

After covering the background of Amazon buckets, here are some screen shots from the tool we created as POC. The tool itself can be downloaded from Github.(link)




/* Amazon AWS Open Site Scraper
/* Samuel LESPES CARDILLO (Cyber_Owner) - @cyberwarfighte1
/* Amitay Dan (popshark1)
/* ____________________________________ */
usage : node dnslogger.js -h
:~/dnslogger/DNS$ node dnslogger.js -i 54.231.136.58
/* ____________________________________ */
/* Amazon AWS Open Site Scraper
/* Samuel LESPES CARDILLO (Cyber_Owner) - @cyberwarfighte1
/* Amitay Dan (popshark1)
/* ____________________________________ */
Passive DNS looking...
s3-3-w.amazonaws.com is blocked
te4you.nl.s3.amazonaws.com is blocked
onaws.com is blocked
ary.com.s3.amazonaws.com is blocked
azonaws.com is blocked
esuite.com.s3.amazonaws.com is blocked
.s3.amazonaws.com is blocked
.amazonaws.com is blocked
esources-closedtrialmediabucket-qez1cx0bkl5u.s3.amazonaws.com is blocked
.uk.s3.amazonaws.com is blocked
azonaws.com is available
it.com.s3.amazonaws.com is blocked
.s3.amazonaws.com is available
gnostics.com.s3.amazonaws.com is available
ffiliate.de.s3.amazonaws.com is available
amazonaws.com is available
s.co.uk.s3.amazonaws.com is available
.amazonaws.com is blocked
video.s3.amazonaws.com is blocked
azonaws.com is blocked
3.amazonaws.com is blocked
mages.s3.amazonaws.com is blocked
s.s3.amazonaws.com is blocked
.static.resources.s3.amazonaws.com is blocked
cdn.com.s3.amazonaws.com is blocked
uction.s3.amazonaws.com is blocked
tic.s3.amazonaws.com is blocked
zonaws.com is blocked


y-eu-1.s3.amazonaws.com is blocked
atic-assets.s3.amazonaws.com is blocked
oimages.s3.amazonaws.com is blocked
ibrarsi.s3.amazonaws.com is blocked
atespocasport.s3.amazonaws.com is blocked
agenes.com.s3.amazonaws.com is blocked
et-js.s3.amazonaws.com is blocked
lobal.s3.amazonaws.com is available
n-img.com.s3.amazonaws.com is available
s3.amazonaws.com is blocked
ger.s3.amazonaws.com is blocked
o.s3.amazonaws.com is blocked
.trovit.fr.s3.amazonaws.com is blocked
iler.s3.amazonaws.com is blocked
3.amazonaws.com is blocked
immer.de.s3.amazonaws.com is blocked
serwisyregionalne.pl.s3.amazonaws.com is blocked
imagesold.s3.amazonaws.com is available
st.shootitlive.com.s3.amazonaws.com is blocked
bawab-media.com.s3.amazonaws.com is blocked
in-images.s3.amazonaws.com is available
om.s3.amazonaws.com is blocked
-uc.s3.amazonaws.com is blocked
shopcouk.s3.amazonaws.com is blocked
ayscom-assets.s3.amazonaws.com is blocked
guk.s3.amazonaws.com is blocked
chat-public-eu.s3.amazonaws.com is blocked
ces-video.s3.amazonaws.com is blocked
.amazonaws.com is available
oArd.s3.AmaZoNAWs.COM is available
3.amazonaws.com is available
.s3.amazonaws.com is available
s.activeline.mu.s3.amazonaws.com is blocked
.trovit.it.s3.amazonaws.com is blocked
-v-4cdn-co.s3.amazonaws.com is blocked
ngfiles.s3.amazonaws.com is blocked
combat-forum.s3.amazonaws.com is blocked
demos.s3.amazonaws.com is blocked
aps.s3.amazonaws.com is blocked
nresources.s3.amazonaws.com is blocked


3.s3.amazonaws.com/ is available
Getting the file list...
FILE LIST
.3.s3.amazonaws.com//BIM - LEAN
.3.s3.amazonaws.com//Files/
.3.s3.amazonaws.com//Files/
.3.s3.amazonaws.com//Files/ 4.jpg
.3.s3.amazonaws.com//Files/ jpg
.3.s3.amazonaws.com//Files/ .jpg
.3.s3.amazonaws.com//Files/ 1.jpg
.3.s3.amazonaws.com//Files/ 2.jpg
.3.s3.amazonaws.com//Files/ l.png
.3.s3.amazonaws.com//Files/ r.png
.3.s3.amazonaws.com//Files/ png
.3.s3.amazonaws.com//Files/ jpg
.3.s3.amazonaws.com//Files/ .jpg
.3.s3.amazonaws.com//Files/ uery-ui.js
.3.s3.amazonaws.com//Files/ uery.js
.3.s3.amazonaws.com//Files/ png
.3.s3.amazonaws.com//Files/
.3.s3.amazonaws.com//Files/ 4.jpg
.3.s3.amazonaws.com//Files/ jpg
.3.s3.amazonaws.com//Files/ .jpg
.3.s3.amazonaws.com//Files/ 1.jpg
.3.s3.amazonaws.com//Files/ 2.jpg
.3.s3.amazonaws.com//Files/ l.png
.3.s3.amazonaws.com//Files/ r.png
.3.s3.amazonaws.com//Files/ png
.3.s3.amazonaws.com//Files/ jpg
.3.s3.amazonaws.com//Files/ .jpg
.3.s3.amazonaws.com//Files/ uery-ui.js
.3.s3.amazonaws.com//Files/ uery.js
.3.s3.amazonaws.com//Files/ png
.3.s3.amazonaws.com//Start.ntm
.3.s3.amazonaws.com//Water
.3.s3.amazonaws.com//
.3.s3.amazonaws.com//files/
.3.s3.amazonaws.com//files/l/
.3.s3.amazonaws.com//files/l, 4.jpg
.3.s3.amazonaws.com//files/l, jpg