Web Application & Cloud Computing What are the new threats ?

David Calligaris

OWASP Italy Day

Cagliari, 19th October 2018

$: whoami

- **Geek & Nerd**
- Director Security Testing Automation Huawei Munich (DE)
- Former CTO Emaze S.p.A.

Disclaimer

All the content of these slides represent <u>my personal view</u> not that of my employer.

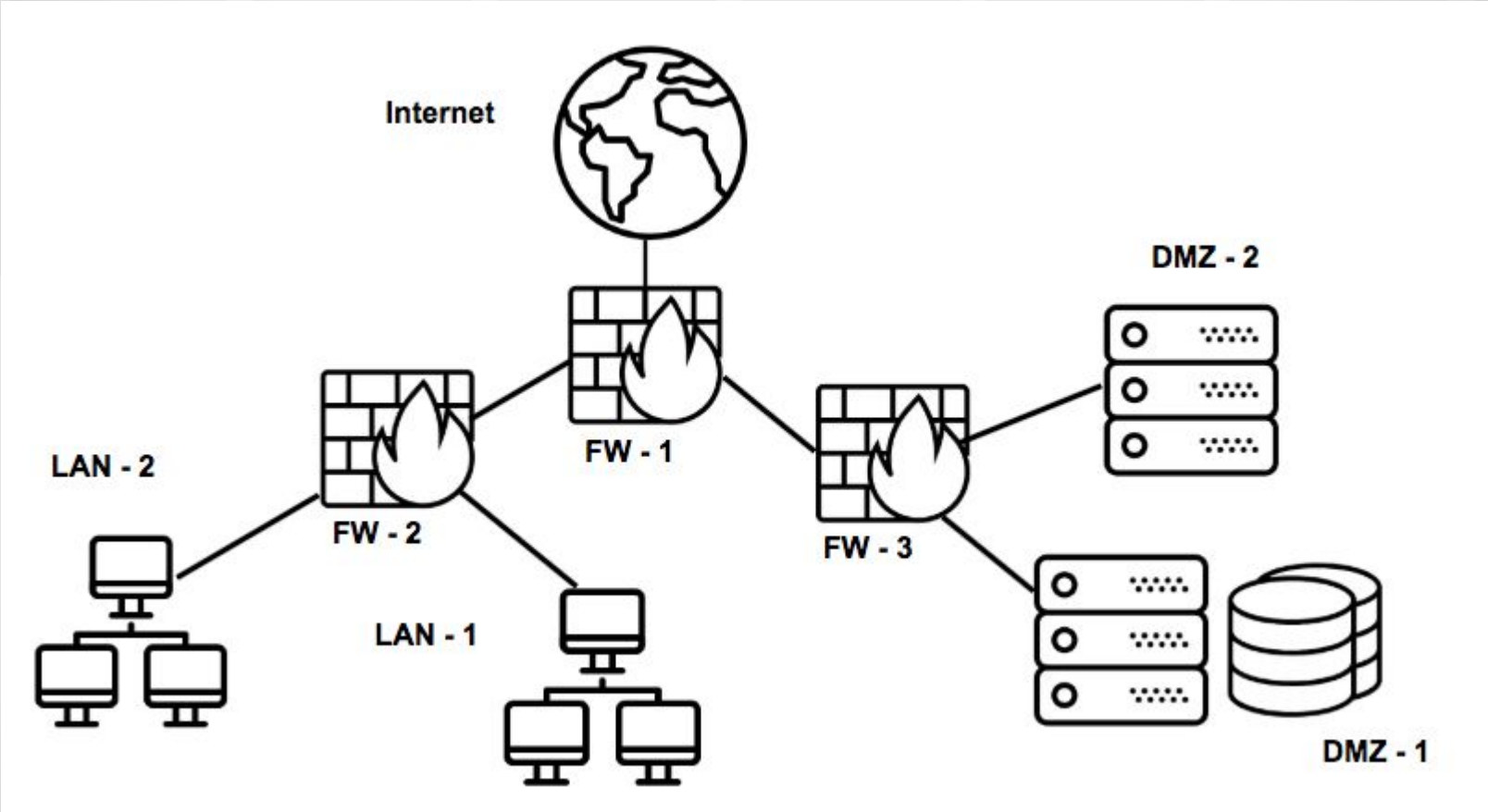
What is this presentation about ?

- How Cloud Computing changes Companies
- How Cloud Computing changes Web Applications
- Web Applications & External Resources (Buckets)
- Buckets Security

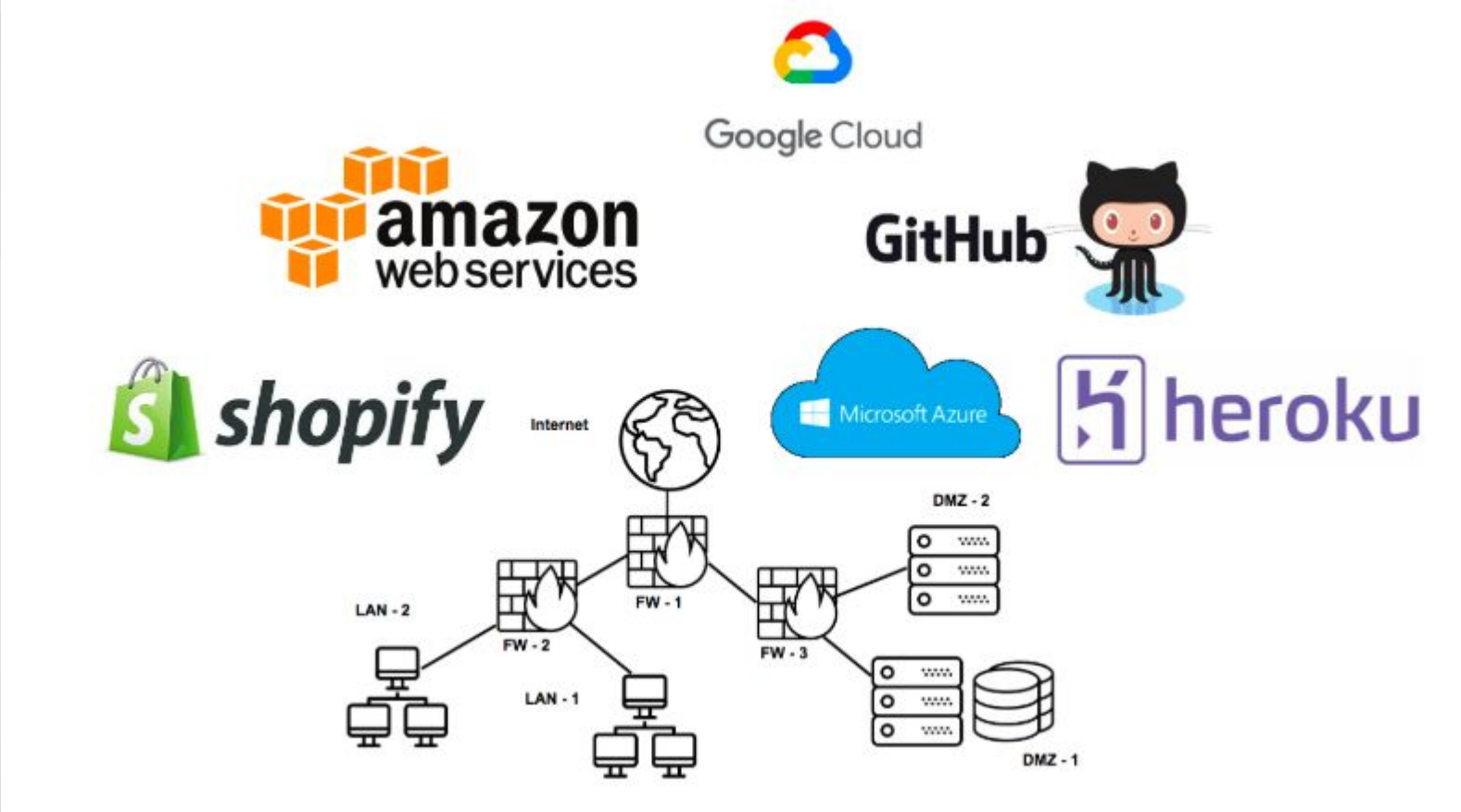
What are Clouds ?

- Virtual Machines
- Storage
- Application Providers
- Others ...

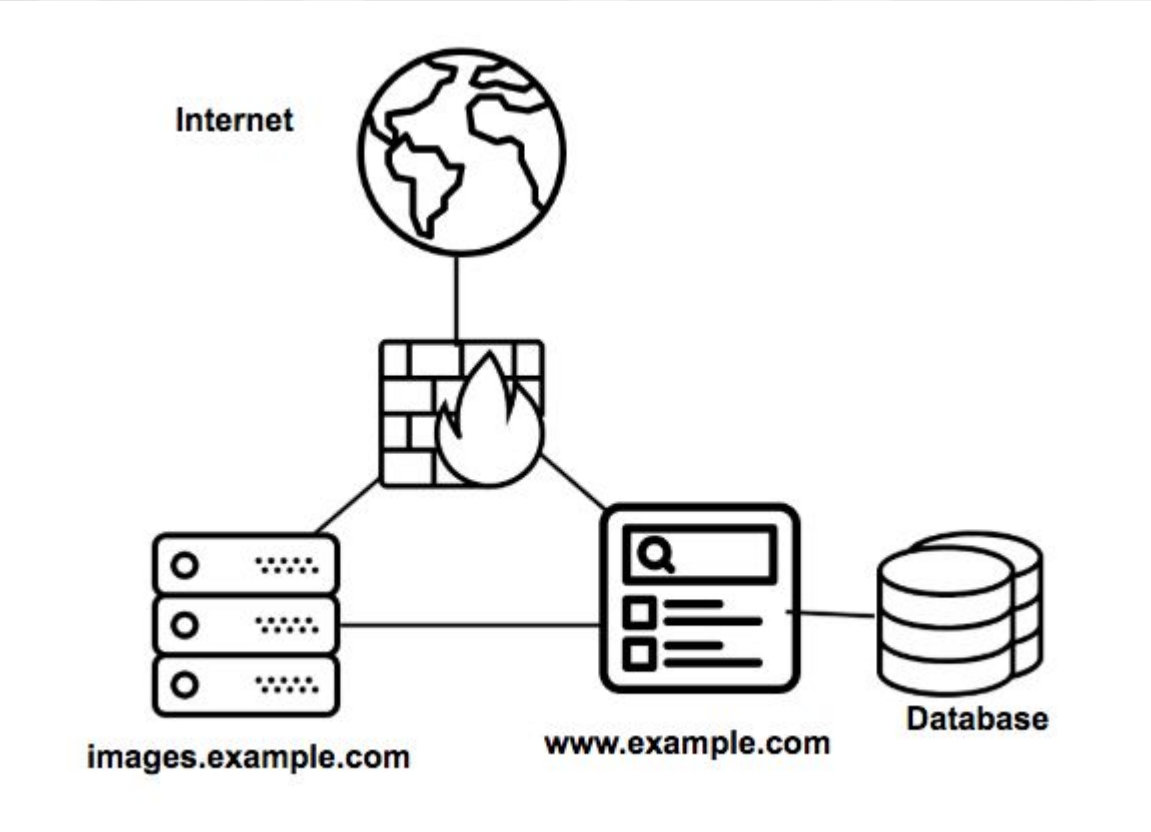
Companies <u>before</u> Cloud era:



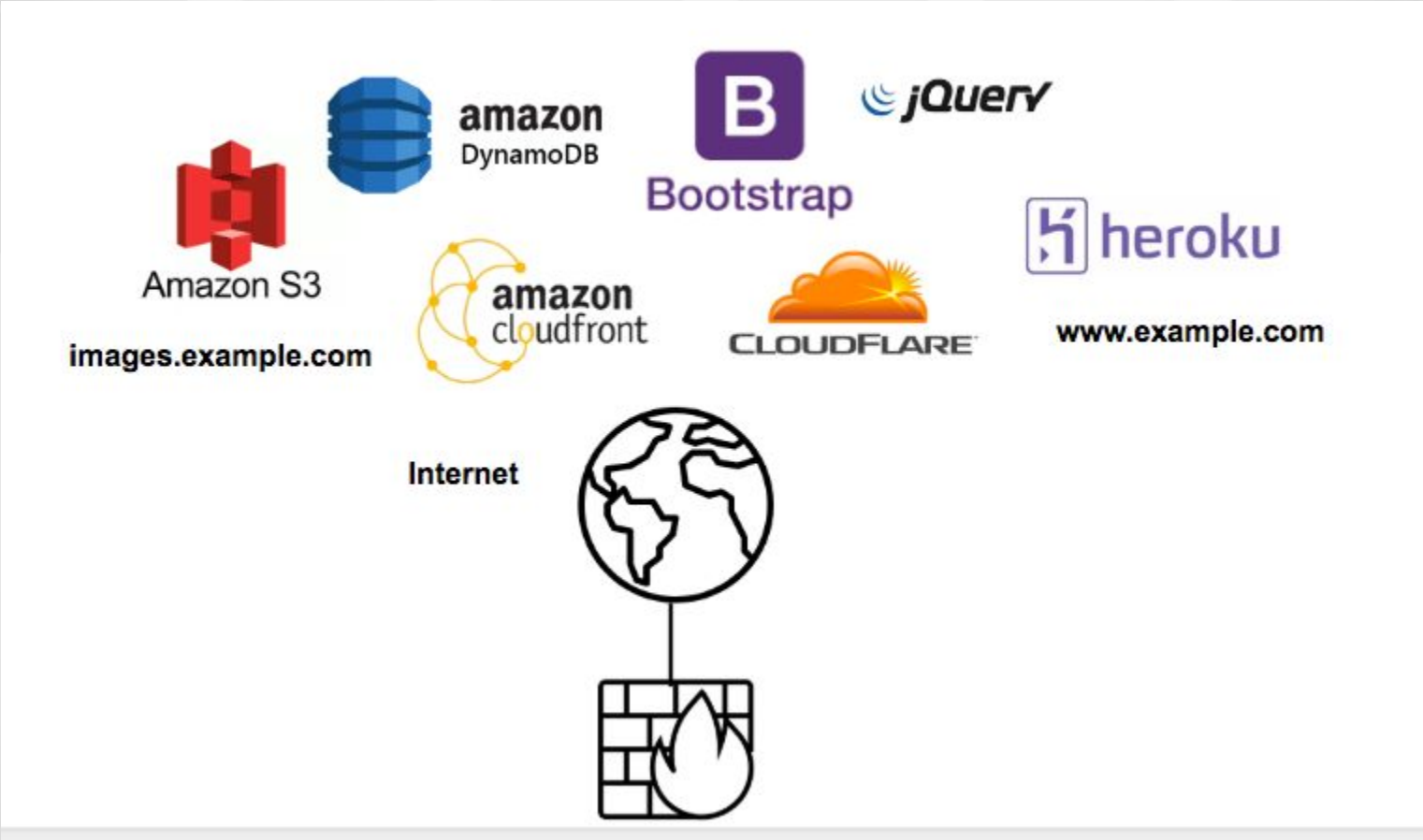
Companies in Cloud era:



Web Applications before Cloud era:



Web Applications in Cloud era:



Loading External Files

- Web application could load images, javascripts, css from external sources

```
/- og:type  content= website ><script nonce= 5515127
v.cookieBannerEnabled = true; window.cookieBannerMod
 src='https://cdn.optimizely.com/js/8148824632.js'>
.js'></script><style
```

```
";__WEBPACK_PUBLIC_PATH__ = "https://d3i4yxtzktqr9n.cloudfront.net/uber-sites";</script><script nonce="
"https://d3i4yxtzktqr9n.cloudfront.net/uber-sites/client-vendor-6483a6d09e4acd4595e2.js"></script><script
"anonymous" src="https://d3i4yxtzktqr9n.cloudfront.net/uber-sites/client-main-c16f43518a810360017a.js"></
```

Loading External Files

- In general this puts your application at risk because the security of your web application depends on the security of these external sources

Loading External Files

- We have several examples and write-ups of security issues of Web Applications loading contents from expired domains

https://blog.hboeck.de/archives/889-Abandoned-Domain-Takeover-as-a-Web-Security-Risk.html

Abandoned Domain Takeover a

Tuesday, September 5. 2017

Abandoned Domain Takeover as a Web Security Risk

In the modern web it's extremely common to include thirdparty content on web pages. Youtube videos, social media buttons, ads, statistic tools, CDNs for fonts and common javascript files - there are plenty of good and many not so good reasons for this. What is often forgotten is that including other peoples content means giving other people control over your webpage. This is obviously particularly risky if it involves javascript, as this gives a third party full code execution rights in the context of your webpage.

I recently helped a person whose Wordpress blog had a problem: The layout looked broken. The cause was that the theme used a font from a web host - and that host was down. This was easy to fix. I was able to extract the font file from the Internet Archive and store a copy locally. But it made me thinking: What happens if you include third party content on your webpage and the service from which you're including it disappears?

I put together a simple script that would check webpages for HTML tags with the src attribute. If the src attribute points to an external host it checks if the host name actually can be resolved to an IP address. I ran that check on the Alexa Top 1 Million list. It gave me some interesting results. (This methodology has some limits, as it won't discover indirect src references or includes within javascript code, but it should be good enough to get a rough picture.)

Loading External Files

- The consequences could have a high impact:
  - Load in-browser JavaScript cryptominer
  - Steal cookies
  - Inject Malicious code (e.g. malware, exploit)

Loading External Files Buckets

- Sometimes we can see a web application loading content from buckets

```
re - Snowboards" data-sizes="auto" data-srcset="https://s3.amazonaws.com/shopify-theme-store
  https://s3.amazonaws.com/shopify-theme-store/screenshots/1019/main/fullsize.jpg 500w,
  https://s3.amazonaws.com/shopify-theme-store/screenshots/1019/main/fullsize_2x.jpg 1000w"

src="https://s3.amazonaws.com/shopify-theme-store/screenshots/1019/main/optimized_large.jpg"
```

Loading External Files Buckets

- What are the differences if an application is loading content from a bucket ?
- What are buckets ?

What are Buckets ?

Services served by different cloud providers (e.g. Amazon S3, Google Storage, DigitalOcean Spaces, etc) that offer storage resources.

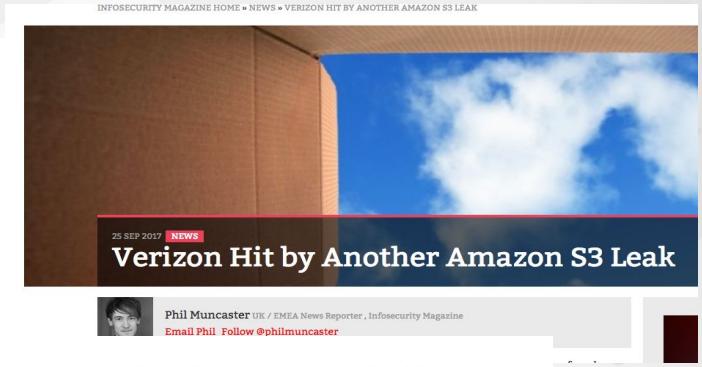
Bucket Security ?

In recent years buckets misconfiguration issues were on the news for several security incidents

Accenture latest to breach client data due to misconfigured AWS server

Hundreds of gigabytes of sensitive client and company data were exposed when the tech and cloud giant accidentally left four of its AWS S3 buckets open to the public.

By Jessica Davis | October 10, 2017 | 03:35 PM



INFOSECURITY MAGAZINE HOME » NEWS » VERIZON HIT BY ANOTHER AMAZON S3 LEAK

25 SEP 2017 NEWS

Verizon Hit by Another Amazon S3 Leak

Phil Muncaster UK / EMEA News Reporter , Infosecurity Magazine

Email Phil Follow @philmuncaster

GoDaddy Leaks 'Map of the Internet' via Amazon S3 Cloud Bucket Misconfig

Author:

Tara Seals

August 13, 2018 / 1:26 pm

Identify buckets

Buckets have a particular name format and are easy to identify:

- bucket-name.s3.amazonaws.com
- s3.amazonaws.com/bucket-name
- bucket-name.s3-us-west-2.amazonaws.com
- s3-us-west-2.amazonaws.com/bucket-name
- bucket-name.storage.googleapis.com
- storage.googleapis.com/bucket-name

Identify buckets

Sometimes buckets are behind a CNAME or CDN:

- d1l27wvezozmw4.cloudfront.net
- images.owaspdaycagliari2018.it

Identify buckets

There are several techniques to identify buckets:

- CNAME
- Server Header
- Default Page
- Error Message

How to identify buckets ?

- DNS CNAME

```
sh-3.2$ nslookup download.intel.com
Server:         8.8.8.8
Address:        8.8.8.8#53

Non-authoritative answer:
download.intel.com      canonical name = download.intel.com.s3-us-west-2.amazonaws.com.
download.intel.com.s3-us-west-2.amazonaws.com   canonical name = s3-us-west-2-r-w.amazon
aws.com.
Name:   s3-us-west-2-r-w.amazonaws.com
Address: 52.218.201.217
```

How to identify buckets ?

- Server Headers (1/2)

```
HTTP/1.1 403 Forbidden
x-amz-bucket-region: us-east-1
x-amz-request-id: 8F5D2E041612C5AA
x-amz-id-2: 6hAAqc4axNEt/TAXh0TaX0eo27RV0GpsADNk5K94Q4+NA2fpgjchY5T5Q8jmZEH9SDsc6R0cl44=
Content-Type: application/xml
Transfer-Encoding: chunked
Date: Fri, 12 Oct 2018 14:39:42 GMT
Server: AmazonS3
```

How to identify buckets ?

- Server Headers (2/2)

```
HTTP/1.0 403 Forbidden
X-GUploader-UploadID: AEnB2Up44XuL0q5VC8T2xQDa7Sz0jt25Ns62H__U57UvFRo9ew_Qjw0e66W8rGEPCCaTt7sTi3nJDcXGydCQWbX5A9_xrM5ZqQ
Content-Type: application/xml; charset=UTF-8
Content-Length: 204
Date: Fri, 12 Oct 2018 14:42:50 GMT
Expires: Fri, 12 Oct 2018 14:42:50 GMT
Cache-Control: private, max-age=0
Server: UploadServer
```

How to identify buckets ?

- “Index” default page


```
▼<ListBucketResult xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
  <Name>owaspdaytest2018</Name>
  <Prefix/>
  <Marker/>
  <MaxKeys>1000</MaxKeys>
  <IsTruncated>false</IsTruncated>
 ▼<Contents>
    <Key>test1.txt</Key>
    <LastModified>2018-10-12T12:06:37.000Z</LastModified>
    <ETag>"d41d8cd98f00b204e9800998ecf8427e"</ETag>
    <Size>0</Size>
    <StorageClass>STANDARD</StorageClass>
  </Contents>
 ▼<Contents>
    <Key>test2.txt</Key>
    <LastModified>2018-10-12T12:06:36.000Z</LastModified>
    <ETag>"d41d8cd98f00b204e9800998ecf8427e"</ETag>
    <Size>0</Size>
    <StorageClass>STANDARD</StorageClass>
  </Contents>
 ▼<Contents>
    <Key>test3.txt</Key>
    <LastModified>2018-10-12T12:06:35.000Z</LastModified>
    <ETag>"d41d8cd98f00b204e9800998ecf8427e"</ETag>
    <Size>0</Size>
    <StorageClass>STANDARD</StorageClass>
  </Contents>
 ▼<Contents>
    <Key>test4.txt</Key>
    <LastModified>2018-10-12T12:06:35.000Z</LastModified>
    <ETag>"d41d8cd98f00b204e9800998ecf8427e"</ETag>
    <Size>0</Size>
    <StorageClass>STANDARD</StorageClass>
  </Contents>
</ListBucketResult>
```

How to identify buckets ?

Via “Error Messages”


```
<Error>
  <Code>AllAccessDisabled</Code>
  <Message>All access to this object has b
  <RequestId>FDCF69793BBE0606</RequestId>
  <HostId>
    IlkqQqucHhGFiUV+nuy4n+cBPPZeSN8uicExEcMOiayxFrQlF5zYL9hChpllkyJPHbrmgzWF9AA=
  </HostId>
</Error>
```


404 Not Found

- Code: NoSuchKey
- Message: The specified key does not exist.
- Key: index.html
- RequestId: B3722D678AE7E5BF
- HostId: 6Bo0HJ55fuQct93GUe1ZLXwkxssLILSKlpkdhMUghFOqGSQK7aBiK/F8cO1qSK1n3YL3Q4UxmQ4=


```
<Error>
  <Code>AccessDenied</Code>
  <Message>Access Denied</Message>
  <RequestId>418A5C13D444CE05</RequestId>
  <HostId>
    U7CKSDYFS7Ow+hkTDgBsC5Hecb37qCf7yQhW6W+LPwqQ9AlSm6XJ7hNPVGoGzUc5ymN+w1j6J0E=
  </HostId>
```


404 Not Found

- Code: NoSuchWebsiteConfiguration
- Message: The specified bucket does not have a website configuration

How to identify buckets ?

- Via 404 “NoSuchBucket” Error Message


```
▼<Error>
  <Code>NoSuchBucket</Code>
  <Message>The specified bucket does not exist</Message>
  <BucketName>test111111111.x</BucketName>
  <RequestId>521DE2B76A2B0E3D</RequestId>
 ▼<HostId>
   ChboJZ6acvwVDocxnMK7fLKPwnvU9rtxmN61wemBHA/rx1dDkU84Nzip3wutnIyRs2ObIwGnbs0=
  </HostId>
 </Error>
```


NOTE: This can enable a <u>SubDomain Takeover Vulnerability</u>

Special Note: Subdomain TakeOver

- The first article regarding this vulnerability is from Franz Rosen from 2014

https://labs.detectify.com/tag/hostile-subdomain-takeover/

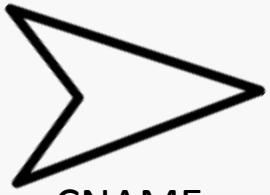
Special Note: Subdomain TakeOver

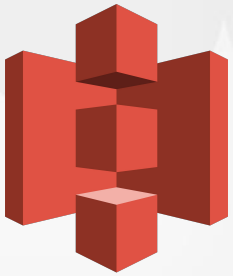
- Companies decide to use a bucket for storing website images:

- images-owasp.s3.amazonaws.com

Special Note: Subdomain TakeOver

- The company decides to associate this name with a company DNS entry:



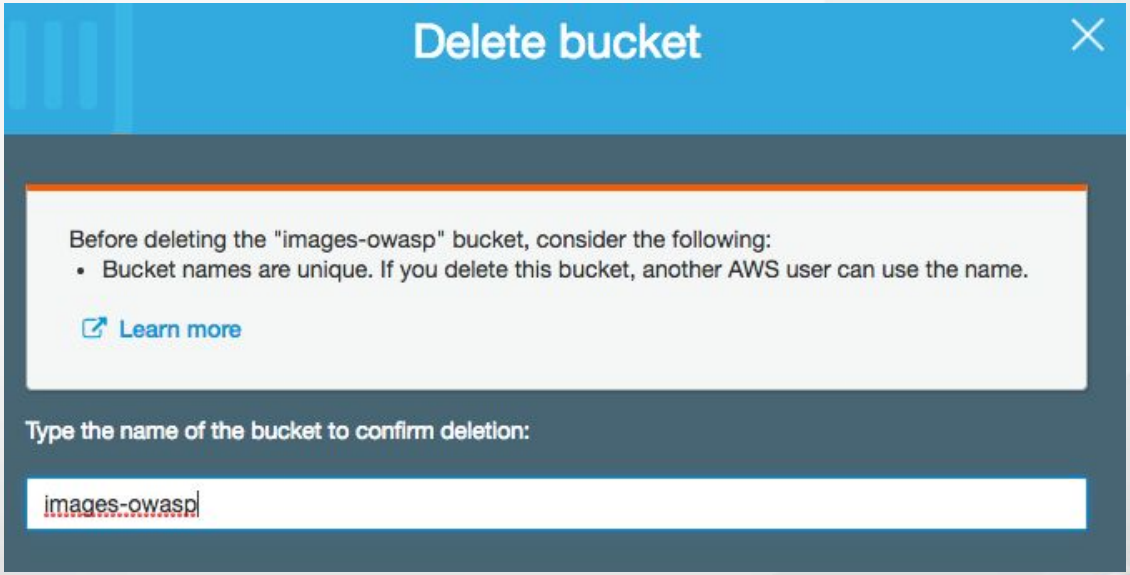


images-owasp.example.com

images-owasp.s3.amazonaws.com

Special Note: Subdomain TakeOver

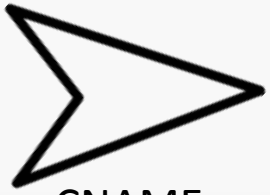
- After some time the company decides to use a different cloud provider for hosting the images and deletes the bucket …



Special Note: Subdomain TakeOver

- … but they don't delete the DNS CNAME entry

images-owasp.example.com



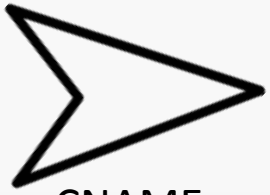
CNAME

images-owasp.s3.amazonaws.com

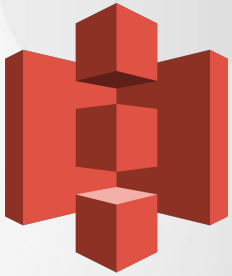
Special Note: Subdomain TakeOver

- Anyone now can create a bucket with the original name and take control of it

images-owasp.example.com



CNAME



images-owasp.s3.amazonaws.com

Special Note: Subdomain TakeOver

- What are the consequences of the SubDomain TakeOver ?
  - Phishing Attacks
  - In some conditions Steal Cookies with scope *.example.com
  - In some conditions bypass CORS/CSP Policy

Special Note: Subdomain TakeOver

- Additional Resources:
  - https://github.com/EdOverflow/can-i-take-over-xyz
  - https://0xpatrik.com/subdomain-takeover-basics/

Special Note: Subdomain TakeOver

- Who is to blame ?
  - SysAdmins ?
  - Cloud Service Providers ?

Special Note: Subdomain TakeOver

https://blog.cloudsecurityalliance.org/2018/08/13/cve-cloud-services-part-1/

cloud security alliance®

Blog Press CSA Network CSA Products Search Search ...

CVE and Cloud Services, Part 1: The Exclusion of Cloud Service Vulnerabilities

By Kurt Seifried, Director of IT, Cloud Security Alliance and Victor Chin, Research Analyst, Cl

The vulnerability management process has traditionally been supported by a finely balanc enterprises, and vendors. At the crux of this ecosystem is the Common Vulnerabilities and vulnerabilities have to fulfill certain criteria. In recent times, these criteria have become pro are becoming more and more common.

This is the first in a series of blogposts that will explore the challenges and opportunities ir cloud services.

https://blog.cloudsecurityalliance.org/2018/09/28/cve-impacts-cloud-vulnerability-risk-management/

cloud security alliance®

Blog Press CSA Network CSA Products

CVE and Cloud Services, Part 2: Impacts on Cloud Vulnerability and Risk Management

By Victor Chin, Research Analyst, Cloud Security Alliance, and Kurt Seifried, Director of IT, Cloud Security Alliance

This is the second post in a series, where we'll discuss cloud service vulnerability and risk management trends in relation to the Common Vulnerability and Exposures (CVE) system. In the first blog post, we wrote about the Inclusion Rule 3 (INC3) and how it affects the counting of cloud service vulnerabilities. Here, we will delve deeper into how the exclusion of cloud service vulnerabilities impacts enterprise vulnerability and risk management.

https://blog.cloudsecurityalliance.org/2018/08/13/cve-cloud-services-part-1/

Testing Buckets Security

- Buckets can be misconfigured in different ways:
  - READ Access
  - WRITE Access
  - Readable ACL
  - Writable ACL
  - …

Testing Buckets Security

- Buckets can have different types of access:
  - Anonymous
  - Authenticated User (*)
  - Owner

Testing Buckets Security

- Checking for READ Access:

Amazon

$ aws s3 ls s3://bucket-name

Google

$ gsutil ls gs://bucket-name

Testing Buckets Security

- READ Access:
  - Backups (.tar.gz, .zip)
  - SQL Databases (.sql)
  - Source Code (.php, .aspx, .rb)

Testing Buckets Security

- Checking for WRITE Access:

Amazon

$ aws cp TestUpload.txt s3://bucket-name

Google

$ gsutil cp TestUpload.txt gs://bucket-name

NOTE: remember to delete the file!!!

Testing Buckets Security

- WRITE Access:
  - Overwrite files (.js, css, jpg, html)
  - Create phishing pages (.html)
  - Overwrite executables (.exe, .sh)
  - Malware drop zone
  - Warez Hosting

Testing Buckets Security

- Checking ACL READ ACCESS

Amazon

$ aws s3api get-bucket-acl --bucket bucket-name

Testing Buckets Security

```
sh-3.2$ aws s3api get-bucket-acl --bucket images-owasp
{
    "Owner": {
        "DisplayName": "[redacted]",
        "ID": "[redacted]"
    },
    "Grants": [
        {
            "Grantee": {
                "DisplayName": "[redacted]",
                "ID": "[redacted]",
                "Type": "CanonicalUser"
            },
            "Permission": "FULL_CONTROL"
        },
        {
            "Grantee": {
                "Type": "Group",
                "URI": "http://acs.amazonaws.com/groups/global/AllUsers"
            },
            "Permission": "READ"
        },
        {
            "Grantee": {
                "Type": "Group",
                "URI": "http://acs.amazonaws.com/groups/global/AllUsers"
            },
            "Permission": "WRITE"
        },
        {
            "Grantee": {
                "Type": "Group",
                "URI": "http://acs.amazonaws.com/groups/global/AllUsers"
            },
            "Permission": "READ_ACP"
        }
    ]
}
```

Testing Buckets Security

- Checking ACL WRITE ACCESS

Amazon

$ aws s3api put-bucket-acl --bucket bucket-name NEW_ACL

Testing Buckets Security

```
        },
        {
            "Grantee": {
                "Type": "Group",
                "URI": "http://acs.amazonaws.com/groups/global/AllUsers"
            },
            "Permission": "WRITE_ACP"
        }
    ]
}
```

Testing Buckets Security

- The topic is not over; in this presentation we did not cover some aspects like:
  - Bucket Name Identification
  - Bucket Policies
  - Pre-Signed URLs

Bucket Security

Bad Packets Report @bad_packets · 7 Nov 2017
ICYMI: This was caused by an open @awscloud bucket. After someone found that, installing #Coinhive was a breeze on @Politifact's website!

Robert Marere @robertmarere · Feb 28
#OnTheRise .....#CyberCrimes reach scary new levels as #Coinhive #Monero miner #Cryptomining code was discovered #CryptoJacking on the @latimes website thanks to a poorly secured @Amazon @awscloud S3 **bucket**.

Bad Packets Report @bad
BREAKING NEWS: #Coinhi
@PolitiFact website in latest

Bad Packets Report @bad_packets · Mar 2
#Coinhive was removed from @Farmacity's website around 2:20 PM UTC time today. The compromised AWS S3 **bucket** now returns a 403 Forbidden error.

Bad Packets Report @bad_packets · Mar 1
How did #Coinhive get on @VAIOargentina's website?

Was it an unsecured AWS S3 **bucket**?

Yes.

Spotted by @VriesHd. Previously notified by @Random_Robbie (poc.txt)

ar.vaio.com

The CyberWire @thecyberwire · Feb 28
On Podcast: In today's podcast, we hear that #CoinHive was installed via a misconfigured #AWSS3 **bucket**. #cybersecurity #infosec bit.ly/cwPod02271

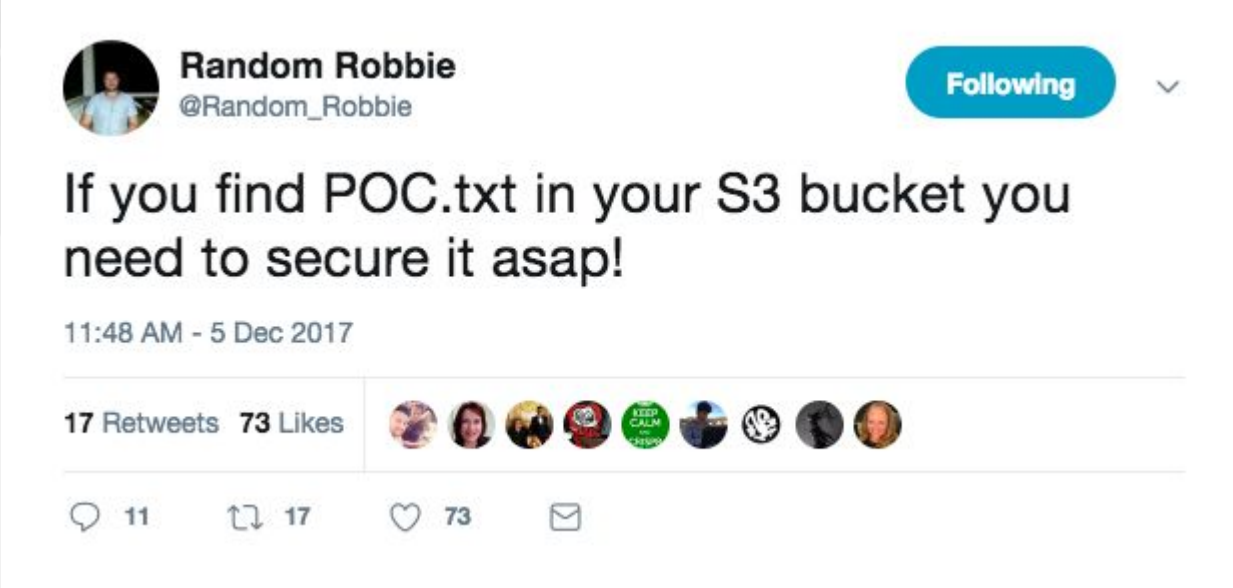
Bad Packets Report @bad_packets · Feb 25
#Coinhive found on the website of Mexican professional football league @AscensoMX.

This case of #cryptojacking appears to be caused by an open AWS S3 **bucket** as the malicious script is injected via http://s3.amazonaws[.]com/lmxwebsite/js/toastr.js

SCENSO Bancomer BBVA

Open Web Application Security Project

Bucket Security




```
Hello from https://www.twitter.com/random_robbie - this is a proof of concept to check if your S3 bucket has incorrect permissions.

Please secure your s3 bucket before a bad guy finds it!!

DM's are open if you wish to chat.

https://www.openbugbounty.org/researchers/Random_Robbie/ (little overview of me)
```

Conclusions

- Nothing New, just a new contest:
  - Writable FTP Server, Writable NFS Share, Writable Buckets
- Need of Security Automation:
  - Traditional security scanners focus on old / classic perimeter
  - We need new security scanners to check cloud deployment

Thanks !

Feedback: david.calligaris@gmail.com