



OWASP  
AppSec EU  
**Belfast**

6th to 12th  
of May  
2017

Waterfront  
Conference  
Center

# DNS hijacking using cloud providers

– no verification needed

@fransrosen

# Frans Rosén

**Security Advisor @detectify ( twitter: @fransrosen )**

**HackerOne #5 all time @ hackerone.com/thanks**

**Blog at [labs.detectify.com](https://labs.detectify.com)**

**"The Swedish Ninja"**



- **Background**
- **History**
- **Tools & Techniques**
- **Deeper levels of hijacking**
- **Evolution**
- **Mitigations**
- **Monitoring**

# Subdomain Takeover v1.0

**campaign.site.com**



**heroku**

**Campaign!**

# Subdomain Takeover v1.0

campaign.site.com



heroku

Campaign!



heroku

Fake site!





## Heroku | No such app

There is no app configured at that hostname.  
Perhaps the app owner has renamed it, or you mistyped the URL.

## 404 Not Found

- Code: NoSuchBucket
- Message: The specified bucket does not exist
- BucketName: sub.example.com
- RequestId: C7980A31H58612S3
- HostId: xcPkWtmW21xC31vZKRHOXuvxvVuY/9Y8RtM6rSWa

# 404

There isn't a GitHub Pages site here.

If you're trying to publish one, [read the full documentation](#) to learn how to set up GitHub Pages for your repository, organization, or user account.



Sorry, We Couldn't Find That Page

Please try again or try Desk.com free for 14 days.

TRY DESK.COM FREE

## First instance, 12th Oct '14

### **Onavo - CNAME records pointing to Heroku but no app configured**

Some weeks ago I found an issue in two acquisitions of Facebook. First I found the issue in Onavo and then in Parse. I will use Onavo for describe the issue because I have screen captures, but there was exactly the same issue in Parse.

<http://esevece.tumblr.com/post/99786512849/onavo-cname-records-pointing-to-heroku-but-no>



9 days later, 21st Oct '14

**detectify**  
labs

**Hostile Subdomain Takeover using  
Heroku/Github/Desk + more**

<https://labs.detectify.com/2014/10/21/hostile-subdomain-takeover-using-herokugithubdesk-more/>

# Response from services

## **Heroku:**

*“We're aware of this issue”*

## **Shopify:**

*“I had already identified that this is a security issue”*

## **GitHub:**

*“My apologies for the delayed response.  
We are aware of this issue”*

# What have we seen?



Twitter rewarded [fransrosen](#) with a \$1,680 bounty.

Thanks again for helping us keep Twitter safe and secure for our users!



[\[blurred\]](#) rewarded [fransrosen](#) with a \$10,000 bounty.

Thanks for the report Frans.



Riot Games rewarded [fransrosen](#) with a \$7,500 bounty.

GG, thanks for your help resolving this issue! We greatly appreciate your time



LinkedIn rewarded [fransrosen](#) with a \$1,000 bounty.

# What have we seen?

30

#172137

**Authentication bypass on sso.ubnt.com via subdomain takeover of ping.ubnt.com**

The session cookie of your SSO subdomain sso.ubnt.com is (deliberately?) shared with all [https://\\*.ubnt.com](https://*.ubnt.com) subdomains through its "domain=.ubnt.com" attribute. This allows leakage of this high-value session cookie to the overtaken subdomain <https://ping.ubnt.com> in all modern browsers.

<https://hackerone.com/reports/172137>



# What have we seen?

## #171942 Subdomain takeover of blog.snapchat.com - HackerOne

<https://hackerone.com/reports/171942> - Översätt den här sidan  
25 sep. 2016 - Here is the blog for this bug: <https://medium.com/@johayemal/skalemail-s4blog.snapchat.com-58883de07678#ajgqz0z>

## #159150 HackerOne Subdomain Takeover - HackerOne

<https://hackerone.com/reports/159150> - Översätt den här sidan  
20 sep. 2016 - Reputation: 2nd Rank: 4.92 Signal: 00h Personal: 18.87 Impact: 37h, 0 165 #160166 HackerOne Subdomain Takeover Share ...

## #154425 Subdomain takeover on http://fastly.co-odin.net/ - Hacker

<https://hackerone.com/reports/154425> - Översätt den här sidan  
20 sep. 2016 - Hey team, I've found a snapchat cdn domain here which had a test because setup but did not remove the dns record when the service ...

## #30007 Subdomain Takeover using blog.greenhouse.io pointing to ...

<https://hackerone.com/reports/30007> - Översätt den här sidan  
26 sep. 2016 - Hi, your subdomain blog.greenhouse.io is pointing to the service called Huestop. However, your account at Huestop has expired or has been ...

## #145224 Subdomain takeover on partners.ubuntu.com due to ncr-used ...

<https://hackerone.com/reports/145224> - Översätt den här sidan  
27 nov. 2016 - Hi, So lately I have discovered that CloudFront is not validating which user that set a CNAME rchname in a CloudFront Origin.

## #166309 Subdomain Takeover in http://gerghis.odn.shopify.io ...

<https://hackerone.com/reports/166309> - Översätt den här sidan  
8 sep. 2016 - Hi, I've found a Shopify cdn domain here which had an instance of fastly setup but did not remove the dns record when the service was ...

## #166826 Potential Subdomain Takeover Possible - HackerOne

<https://hackerone.com/reports/166826> - Översätt den här sidan  
29 okt. 2016 - 1294 Reputation: Rank: 3.36 Signal: 00h Personal: 53.38 Impact: 70h Power: 16 #169222. Potential Subdomain Takeover Possible.

## #176307 Subdomain Takeover of Brave.com - HackerOne

<https://hackerone.com/reports/176307> - Översätt den här sidan  
13 okt. 2016 - Summary: Hey I want to inform you about a subdomain takeover issue. When I did your DNS enumeration I came across 1-10 Address 18008 ...

## #148770 Subdomain takeover at api.logalrobot.com due to non-used ...

<https://hackerone.com/reports/148770> - Översätt den här sidan  
26 aug. 2016 - Hi, I noticed that the following domain: api.logalrobot.com was returning the following information: NO APPLICATION WAS FOUND FOR ...

## #119514 Subdomain takeover: URGENT - HackerOne

<https://hackerone.com/reports/119514> - Översätt den här sidan  
26 jan. 2016 - Reputation: 87th Rank: 1.01 Signal: 73rd Personal: 14.88 Impact: 81d Personal: 0 #119514. SUBDOMAIN TAKEOVER: URGENT STATE ...

## #161428 Subdomain takeover at wa.bimweb.com due to unconfigured ...

<https://hackerone.com/reports/161428> - Översätt den här sidan  
5 okt. 2016 - The researcher found a subdomain takeover on 'wa.bimweb.com'.

## #121461 Subdomain takeover due to unconfigured Amazon S3 bucket ...

<https://hackerone.com/reports/121461> - Översätt den här sidan  
22 juni 2016 - I noticed BIME.io is primarily built on Amazon AWS, which sparsely reytended. I started looking for DNS entries that were still pointing to S3 ...

## #71718 URGENT - Subdomain Takeover on the hired.com. due to ...

<https://hackerone.com/reports/71718> - Översätt den här sidan  
1 okt. 2016 - Hi, Brief This is an urgent issue and I hope you will act on it quickly. Your subdomain on hired.com is pointing to heroku.com, but so heroku ...

## #116243 Potential Subdomain Takeover - http://storfrontnews.rfc ...

<https://hackerone.com/reports/116243> - Översätt den här sidan  
19 juni 2016 - Depending on whether Fastly permits it, a subdomain takeover similar to that of <https://hackerone.com/reports/102955> could be possible.

## #119220 Sub-Domain Takeover - HackerOne

<https://hackerone.com/reports/119220> - Översätt den här sidan  
18 mars 2016 - @spiker Yes, its Fixed Now, But I Guess The Issue Worth A 300 Subdomain Takeover After All. Please Check The Above ...

## #109099 Subdomain Takeover in http://assets.goubiquit.com

<https://hackerone.com/reports/109099> - Översätt den här sidan  
14 feb. 2016 - Hi there. Its urgent issue about your subdomain http://assets.goubiquit.com AWS S3 but no auth/webake-configuration is made.

## #105350 Subdomain takeover on pe6ccars.slack-ecre.com

<https://hackerone.com/reports/105350> - Översätt den här sidan  
4 jun. 2017 - I noticed 'slack-ecre.com' is used for Slack's call infrastructure. I have domain before, so I decided to find out what else was ...

## #115578 SUBDOMAIN TAKEOVER(FIXED) - HackerOne

<https://hackerone.com/reports/115578> - Översätt den här sidan  
20 maj 2016 - Hello, I Already Reported This issue Though #190498 Support Ticket Now! Your Subdomain go.hackerone.com is pointing to ...

## #163790 [Critical] Subdomain Takeover - HackerOne

<https://hackerone.com/reports/163790> - Översätt den här sidan  
20 sep. 2016 - Your subdomains are pointing to unconfigured heroku app. You sh

## #150707 Subdomain takeover on slider.uber.com due to non-

<https://hackerone.com/reports/150707> - Översätt den här sidan  
12 dec. 2016 - Hi, 5 hours ago, slider.uber.com was responding like this: #121137 both HTTP and HTTPS. Now, as our bug post from last ...

## #142096 [Screenhare] Subdomain takeover - HackerOne

<https://hackerone.com/reports/142096> - Översätt den här sidan  
Hi & flagger action - Hi, I found out some registered DNS records that can be exploited subdomain of Slack's acquisition 'feedback@weehere.com' ...

## #103432 URGENT - Subdomain Takeover in support.ubuntu

<https://hackerone.com/reports/103432> - Översätt den här sidan  
3 jan. 2016 - I found out that one of your subdomain which is http://support.ubuntu.com taken over or is vulnerable to subdomains takeover.

# What have we seen?

#32825

**URGENT - Subdomain Takeover on media.vine.co due to unclaimed domain pointing to AWS**

We've written an advisory about this at Detectify:

<http://blog.detectify.com/post/100600514143/hostile-subdomain-takeover->

Where you can read more about this sort of attack.

<https://hackerone.com/reports/32825>

# What have we seen?

Hey Frans

I hope all is well dude. I have a guy who claims to have found a vuln and tried to submit it into us. He's not on SRT yet but it was interesting to see that he claimed to have written a DSN blog at Detectify:

**We've written an advisory about this at Detectify:**

**<http://blog.detectify.com/post/100600514143/hostile-subdomain-takeover-using-heroku-github-desk>**

**where you can read more about this sort of attack.**

I was curious to see if you knew who this person is? Email is [hacklockedZZZ@gmail.com](mailto:hacklockedZZZ@gmail.com)

# What have we seen?

## [crt.sh](#) Identity Search

Criteria

Identity LIKE '%.uber.com'

Logged At ↕	Not Before	Identity	
2016-12-30	2016-12-15	beacon.uber.com	<a href="#">C=US, O=DigiCert In</a>
2016-11-30	2016-11-30	photography.uber.com	<a href="#">C=US, O=Lef's Encry</a>
2016-11-30	2016-11-30	photos.uber.com	<a href="#">C=US, O=Lef's Encry</a>
2016-11-30	2016-11-30	photo.uber.com	<a href="#">C=US, O=Lef's Encry</a>
2016-10-19	2016-10-10	ride.uber.com	<a href="#">C=US, O=DigiCert In</a>
2016-10-17	2016-10-17	signup.uber.com	<a href="#">C=US, O=Lef's Encry</a>
2016-10-16	2016-09-27	prod2.uber.com	<a href="#">C=IL, O=StartCom LI</a>
2016-10-16	2016-09-27	<a href="#">szymon.gruszecki.has.hacked.prod2.uber.com</a>	<a href="#">C=IL, O=StartCom LI</a>
2016-10-12	2015-12-23	*.cn.gcp.uber.com	<a href="#">C=US, O=DigiCert In</a>

<https://crt.sh/?q=%25.uber.com>



# What have we seen?

Jonathan Claudius

---

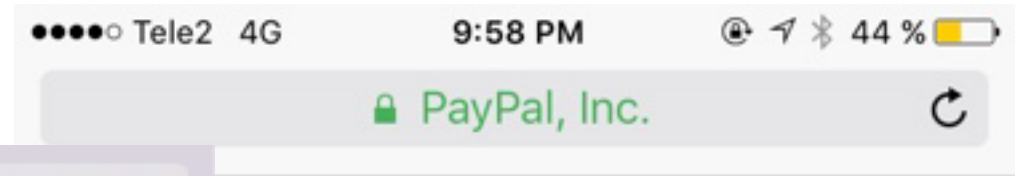
## 'Deep Thoughts' on Subdomain Takeover Vulnerabilities

Feb 3, 2017

In this post, I would like to reiterate how important and likely prolific this vulnerability is and will continue to be for some time. I even went so far as referring to "subdomain takeover as the new XSS" when describing it to my bug bounty peers when we first started seeing these roll in. Now, I could be

<https://blog.rubidus.com/2017/02/03/deep-thoughts-on-subdomain-takeovers/>

# What have we seen?



Open "www.card.io." in a new tab

## Example Domain

This domain is established to be used for illustrative examples in documents. You may use this domain in examples without prior coordination or asking for permission.

# What have we seen?



**Frans Rosén**

@fransrosen



And yeah, subdomain takeover + CloudFront is a thing. Look for "Bad Request" + CloudFront on both http/https + and do a proper PoC...

RETWEETS

2

LIKES

23



7:02 PM - 5 Oct 2016

# What have we seen?



The image shows a screenshot of a news article on a website. The browser's address bar at the top displays 'secure2.donaldtrump.com'. The main headline is 'Trump site hacked by attacker purportedly from Iraq' in large, bold, red text. Below the headline, there is a small circular profile picture of the author, followed by the text 'by ABHIMANYU GHOSHAL — 11 weeks ago in UNITED STATES'. At the bottom of the article, there is a black box containing green and blue text: 'Hacked By Pro\_Mast3r - Attacker Gov Nothing Is Impossible Peace From Iraq'. In the bottom right corner of this black box, it says 'Credit: Ars Technica'.

## Trump site hacked by attacker purportedly from Iraq



by **ABHIMANYU GHOSHAL** — 11 weeks ago in **UNITED STATES**

Hacked By Pro\_Mast3r -

Attacker Gov

Nothing Is Impossible

Peace From Iraq

Credit: Ars Technica

# What have we seen?



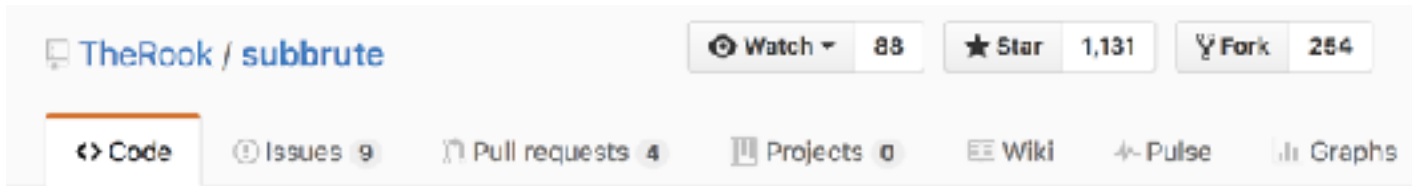
**briankrebs** ✓

@briankrebs

the Iraqi hacker who took credit for the Trump site "defacement" told me he used this [labs.detectify.com/2014/10/21/hos...](https://labs.detectify.com/2014/10/21/hos...) from Oct. 2014..

# Tools

# subbrute



TheRook / subbrute

Watch 88 Star 1,131 Fork 254

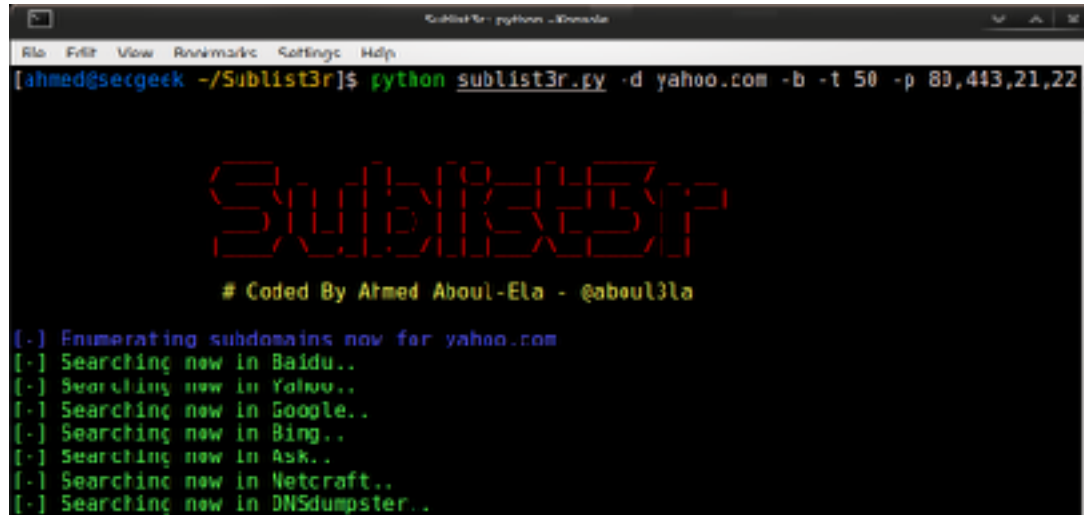
Code Issues 9 Pull requests 4 Projects 0 Wiki Pulse Graphs

A DNS meta-query spider that enumerates DNS records, and subdomains.

**Not active dev.**

<https://github.com/TheRook/subbrute>

# Sublist3r



```
Sublist3r: python -Konsola
File Edit View Run/Bookmark Settings Help
[ahmed@secgeek ~/Sublist3r]$ python sublist3r.py -d yahoo.com -b -t 50 -p 80,443,21,22

Sublist3r
# Coded By Ahmed Aboul-Ela - @aboul3la

[.] Enumerating subdomains now for yahoo.com
[.] Searching now in Baidu..
[.] Searching now in Yahoo..
[.] Searching now in Google..
[.] Searching now in Bing..
[.] Searching now in Ask..
[.] Searching now in Netcraft..
[.] Searching now in DNSdumpster..
```

**Active dev! Took over subbrute!**  
**Fetching from multiple sources**



# massdns

blehschmidt / massdns

Watch ▾

22

★ Star

286

🍴 Fork

21

↔ Code

🕒 Issues 2

🔗 Pull requests 0

📁 Projects 0

📖 Wiki

↔ Pulse

📊 Graphs

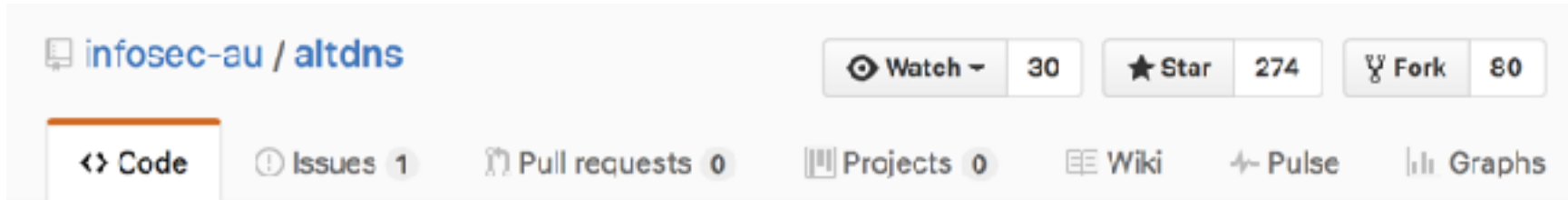
A high-performance DNS stub resolver in C

**Fast as hell!**

**Needs good resolver lists**

<https://github.com/blehschmidt/massdns>

# altdns



infosec-au / altdns

Watch 30 Star 274 Fork 80

Code Issues 1 Pull requests 0 Projects 0 Wiki Pulse Graphs

Generates permutations, alterations and mutations of subdomains and then resolves them

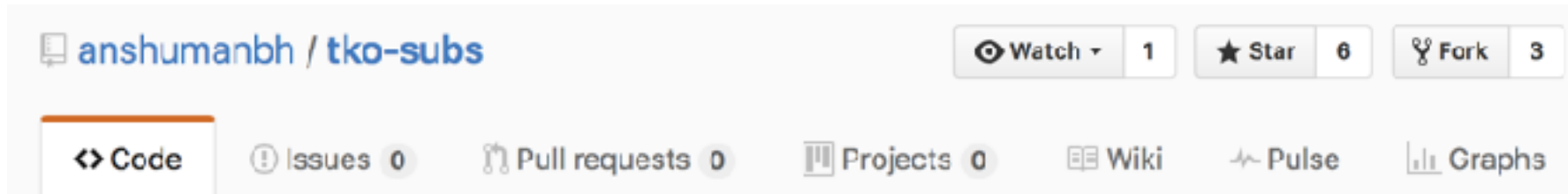
**Soo soo powerful if you have good mutations**

**Combine with massdns == success**

**Can resolve, but better for just creating the lists**

<https://github.com/infosec-au/altdns>

# tko-sub



anshumanbh / tko-sub

Watch 1 Star 6 Fork 3

Code Issues 0 Pull requests 0 Projects 0 Wiki Pulse Graphs

Takeover Domains that have dangling CNAMEs pointing to various CMS websites

**Interesting idea, auto takeover when finding issues**  
**Might be a liittle bit too aggressive**

## We could look here?

```
$ host sub.example.com  
sub.example.com is an alias for mybucketname.s3.amazonaws.com.  
mybucketname.s3.amazonaws.com is an alias for s3-directional-w.amazonaws.com.  
s3-directional-w.amazonaws.com is an alias for s3-directional-w.a-geo.amazonaws.com.  
s3-directional-w.a-geo.amazonaws.com is an alias for s3-1-w.amazonaws.com.  
s3-1-w.amazonaws.com has address 54.231.64.185
```

```
$ host sub.example.com  
sub.example.com is an alias for myrepository.github.io.  
myrepository.github.io is an alias for github.map.fastly.net.  
github.map.fastly.net has address 185.31.17.133
```

```
$ host sub.example.com  
sub.example.com is an alias for mycoolapp.herokuapp.com.  
mycoolapp.herokuapp.com is an alias for us-east-1-a.route.heroku.  
us-east-1-a.route.heroku.com has address 23.21.41.210
```

**WRONG!**

**WRONG!**

**WRONG!**

**WRONG!**

**WRONG!**

**WRONG!**

**WRONG!**

WRONG!

**Resolve and not resolve is what matters.**



# Dead DNS records

## A dead record?

```
[local @ ~ $ host blablabla.trello.com  
Host blablabla.trello.com not found: 3(NXDOMAIN)
```



## A dead record?

```
[local @ ~ $ host blablabla.trello.com  
Host blablabla.trello.com not found: 3(NXDOMAIN)
```

```
[local @ ~ $ host admin.trello.com  
Host admin.trello.com not found: 3(NXDOMAIN)
```

dig is your friend

```
local @ ~ $ dig admin.trello.com +short  
prod.trello.local.
```

## 9 year old bug

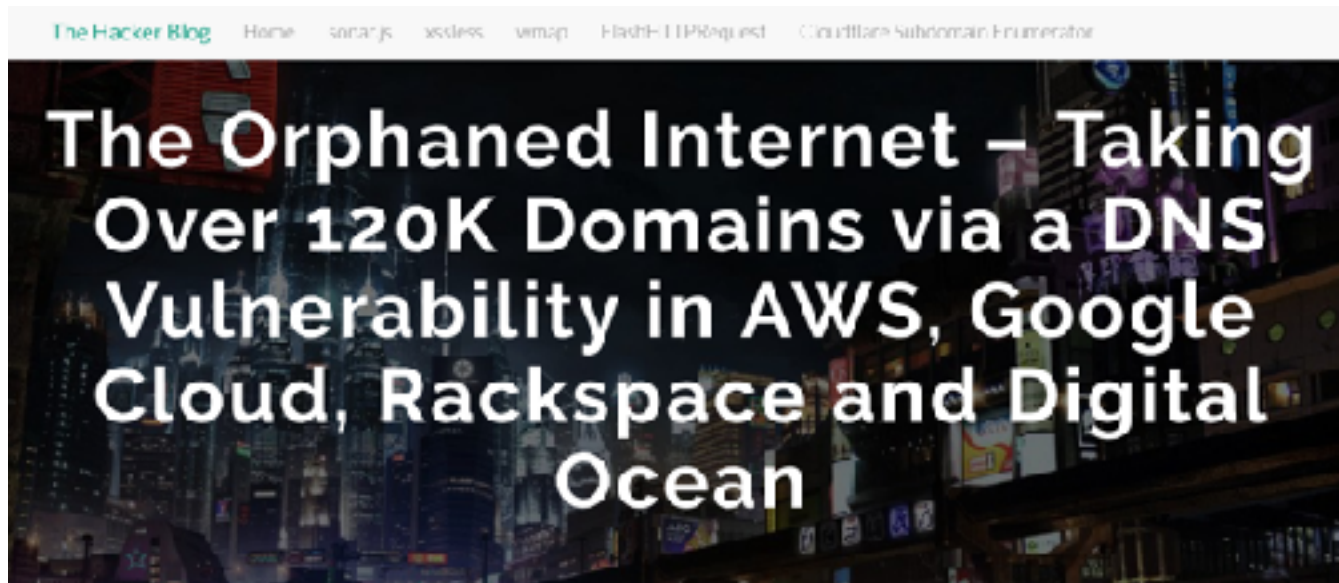
```
$ dig CNAME +short game.westernunion.com  
www.thewesternuniongame.com.
```



thewesternuniongame.com is available!

only \$14.90

# SERVFAIL/REFUSED



<https://thehackerblog.com/the-orphaned-internet-taking-over-120k-domains-via-a-dns-vulnerability-in-aws-google-cloud-rackspace-and-digital-ocean/index.html>



Also works on  
subdomain delegations!

# DNS status codes

**NOERROR**

**Resolves. All OK.**

# DNS status codes

## **NXDOMAIN**

**Doesn't exist. Could still have a DNS RR.  
Query NS to find out more.**

# DNS status codes

**REFUSED**

**NS does not like this domain.**



# DNS status codes

**SERVFAIL**

**Not even responding. Very interesting!**

The tools find what?

**NOERROR**

????

NXDOMAIN

SERVFAIL

REFUSED

# Subdomain delegation

```
$ dig lab.example.com

; <<>> DiG 9.8.3-P1 <<>> lab.example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: SERVFAIL, id: 46773
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 0
```

# Subdomain delegation

```
$ dig NS labs.example.com +trace

: <<>> DiG 9.8.3-P1 <<>> NS labs.example.com +trace
:: global options: +cmd

...

example.com.      172800  IN      NS      ns-272.awsdns-34.com.
example.com.      172800  IN      NS      ns-896.awsdns-48.net.
example.com.      172800  IN      NS      ns-1600.awsdns-08.co.uk.
example.com.      172800  IN      NS      ns-1271.awsdns-30.org.
;; Received 207 bytes from 192.33.10.3#53(192.33.10.3) in 402 ms

labs.exanple.com. 172800  IN      NS      ns-1415.awsdns-48.org.
labs.exanple.com. 172800  IN      NS      ns-1574.awsdns-04.co.uk.
labs.exanple.com. 172800  IN      NS      ns-230.awsdns-28.com.
labs.exanple.com. 172800  IN      NS      ns-875.awsdns-45.net.
```

# Subdomain delegation

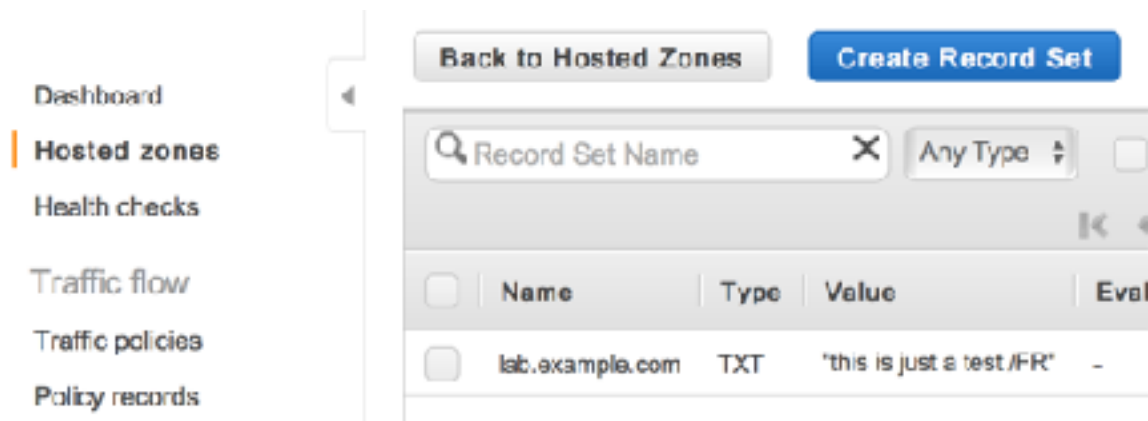
```
$ dig NS labs.example.com +trace
; <<>> DiG 9.8.3-P1 <<>> NS labs.example.com +trace
;; global options: +cmd
...
example.com.      172800  IN      NS      ns-272.awsdns-34.com.
example.com.      172800  IN      NS      ns-896.awsdns-48.net.
example.com.      172800  IN      NS      ns-1600.awsdns-08.co.uk.
example.com.      172800  IN      NS      ns-1271.awsdns-30.org.
;; Received 207 bytes from 192.33.10.3#53(192.33.10.3) in 402 ms

labs.exanple.com. 172800  IN      NS      ns-1415.awsdns-48.org.
labs.exanple.com. 172800  IN      NS      ns-1574.awsdns-04.co.uk.
labs.exanple.com. 172800  IN      NS      ns-230.awsdns-28.com.
labs.exanple.com. 172800  IN      NS      ns-875.awsdns-45.net.
```

# Brute add/delete R53 DNS RR

```
ns-875.awsdns-45.net
creating zone
id is Z5G2TM7GNMQXG
created:
ns-1965.awsdns-53.co.uk ns-283.awsdns-25.com ns-1434.awsdns-51.org ns-913.awsdns-58.net
checking match...
deleting zone
{
  "ChangeInfo": {
    "Status": "PENDING",
    "SubmittedAt": "2016-12-11T22:20:28.921Z",
    "Id": "/change/C2Y735BLG4WL15"
  }
}
deleted
creating zone
id is Z1VL4H5HBEP747
created:
ns-1987.awsdns-46.co.uk ns-693.awsdns-22.net ns-1345.awsdns-48.org ns-454.awsdns-56.com
checking match...
deleting zone
```

# We now control the domain!



The screenshot shows the AWS Route 53 console interface. On the left is a navigation menu with the following items: Dashboard, Hosted zones (highlighted with an orange bar), Health checks, Traffic flow, Traffic policies, and Policy records. The main content area has two buttons at the top: 'Back to Hosted Zones' and 'Create Record Set'. Below these is a search bar labeled 'Record Set Name' with a search icon and a clear button, and a dropdown menu set to 'Any Type'. A table below displays a list of records:

<input type="checkbox"/>	Name	Type	Value	Eval
<input type="checkbox"/>	lab.example.com	TXT	"this is just a test /FR"	-

```
$ dig TXT lab.example.com +short  
"this is just a test /FR"
```

# Orphaned EC2 IPs

OCTOBER 7, 2015

## Fishing the AWS IP Pool for Dangling Domains

<https://www.bishopfox.com/blog/2015/10/fishing-the-aws-ip-pool-for-dangling-domains/>



# Orphaned EC2 IPs

```
beautifulbits.prezi.com:<title>Beautiful bits</title>  
href.prezi.com:<title>Sign in - Google Accounts</title>  
bugbounty.prezi.com:<title>Prezi Bug Bounty Program | Prezi</title>  
mobility.prezi.com:<title>Great Presenters AnywherePrezi Mobility</title>  
schema.prezi.com:<title>404 Not Found</title>  
blog-es.prezi.com:<title>Prezi Blog | Novedades, trucos y consejos de pres  
cdn01.prezi.com:<title>404 Not Found</title>  
blog-pt.prezi.com:<title>Prezi Blog | Novidades, dicas e truques sobre apr  
smartrouter.prezi.com:<title>404 Not Found</title>  
prototypes.prezi.com:<title>Prezi</title>  
charge.prezi.com:<title>Why Was My Card Charged? | Prezi Classic Support</  
bin.prezi.com:<title>403 Forbidden</title>  
preprod-w.prezi.com:<title>404 Not Found</title>  
princess.prezi.com:<title>404 Not Found</title>  
evangelism.prezi.com:<title>Prezi Evangelism</title>  
preprod.prezi.com:<title>Presentation Software | Online Presentation Tools  
0501.cdn01.prezi.com:<title>404 Not Found</title>  
0401.cdn01.prezi.com:<title>404 Not Found</title>  
0104.cdn01.prezi.com:<title>404 Not Found</title>
```

dev.on.site.com



The screenshot shows a product page with a green background. At the top, there are two tabs: "product" and "ingredient". Under "product", there are two buttons: "Chamomile/Valerian/Elder Flower Sleepy Time Tea" (which is selected) and "Hibiscus/Lime/Lemon Haze Afternoon Cooler Herbal Tea". Under "ingredient", there are three buttons: "Nature's Joy hot", "Organic, Vegan, Lemon Coconut Macaroons", and "Organic, Vegan, Raspberry Bars". Below the tabs is a large image of the tea ingredients with a "Read More!" button on the right. A text box over the image reads: "Chamomile/Valerian/Elder Flower Sleepy Time Tea Set of 10 hand-packed, unbleached, tea bags contain dry organic". At the bottom, there are five small images with captions: 1. Chamomile/Valerian/Elder Flower Sleepy Time; 2. Hibiscus/Lime/Lemon Haze Afternoon; 3. Nature's Joy hot; 4. Organic, Vegan, Lemon Coconut; 5. Organic, Vegan, Raspberry Bars.

**product** Chamomile/Valerian/Elder Flower Sleepy Time Tea Hibiscus/Lime/Lemon Haze Afternoon Cooler Herbal Tea

**ingredient** Nature's Joy hot Organic, Vegan, Lemon Coconut Macaroons Organic, Vegan, Raspberry Bars

Read More!

Chamomile/Valerian/Elder Flower Sleepy Time Tea  
Set of 10 hand-packed, unbleached, tea bags contain dry organic

Chamomile/Valerian/Elder Flower Sleepy Time

Hibiscus/Lime/Lemon Haze Afternoon

Nature's Joy hot

Organic, Vegan, Lemon Coconut

Organic, Vegan, Raspberry Bars

dev.on.site.com



\$300.00

dev.on.site.com



\$300.00



+ \$250.00 bonus

# Flow

## Brute

- \* **Collect NOERROR**
- \* **Collect SERVFAIL / REFUSED +trace the NS**
- \* **Collect NXDOMAIN if CNAME, +trace**

# Flow

## Resolve

- \* Check NOERROR for patterns
- \* SERVFAIL/REFUSED, Check NS for patterns
- \* NXDOMAIN, traverse up to apex, check:

`NXDOMAIN | SERVFAIL | REFUSED | no servers could be reached`

# Flow

## Improve

- \* **Collect all subdomain names**
- \* **Sort them by popularity**
- \* **Sort www below all names with  $p > 2$**

# Flow

## Analyze unknowns

- \* **Collect titles of all sites**
- \* **Filter out common titles + name of company**
- \* **Generate screenshots, create a image map**




# Flow

## Repeat

- \* **Do it every day**
- \* **Push notification changes**

# Jan 2017

---

New domain: [bounces.uber.com](https://bounces.uber.com) 



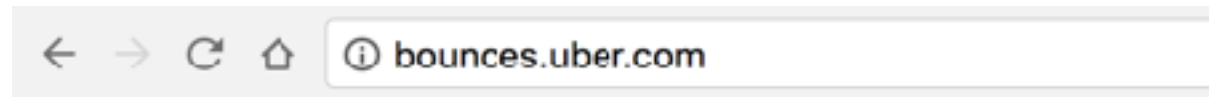
no-reply@zapiemail.com

to me 

2017-01-20 04:29:12 - FOUND S3!! [bounces.uber.com](https://bounces.uber.com)

---

Jan 2017



## 404 Not Found

- Code: NoSuchBucket
- Message: The specified bucket does not exist
- BucketName: bounces.uber.com
- RequestId: D94DDD7B6DB4B5F5
- HostId: Hz8hPqt2DfgLaTq5w0i7ssrUGZ+pJ7fLpz1DODA1Sec1

# Jan 2017

```
$ dig bounces.uber.com
```

```
bounces.uber.com. 299 IN CNAME sparkpostmail.com.  
sparkpostmail.com. 4 IN A 52.218.128.135
```

## Jan 2017

```
$ dig bounces.uber.com
```

```
bounces.uber.com. 299 IN CNAME sparkpostmail.com.  
sparkpostmail.com. 4 IN A 52.218.128.135
```

```
$ host 52.218.128.135
```

```
135.128.218.52.in-addr.arpa domain name pointer s3-website-us-west-2.amazonaws.com.
```

# Jan 2017

bounces.uber.com/login123

## Subdomain takeover

This is just a placeholder to show that it is indeed possible to hijack URLs on this domain, providing content which is not under your control anymore.

**Best Regards,**

Frans Rosén  
[@fransrosen](mailto:@fransrosen)

**bounces.uber.com says:**  
bounces.uber.com

OK



dnathe4th closed the report and changed the status to **Resolved**.

Hey @fransrosen the best kind of bug fix is when we can just delete everything. Please confirm bounce.uber.com no longer resolves for you (the TTL should already have expired).

And thank you again for the report. Best of luck out there hunting!



[dnathe4th](#) closed the report and changed the status to **Resolved**.

Hey [@fransrosen](#) the best kind of bug fix is when we can just delete everything. Please confirm [bounce.uber.com](#) no longer resolves for you (the TTL should already have expired).

And thank you again for the report. Best of luck out there hunting!



Uber rewarded [fransrosen](#) with a **\$1,000** bounty.

Thanks for bringing this to our attention, [@fransrosen](#)!



# The competition



@avlidienbrunn

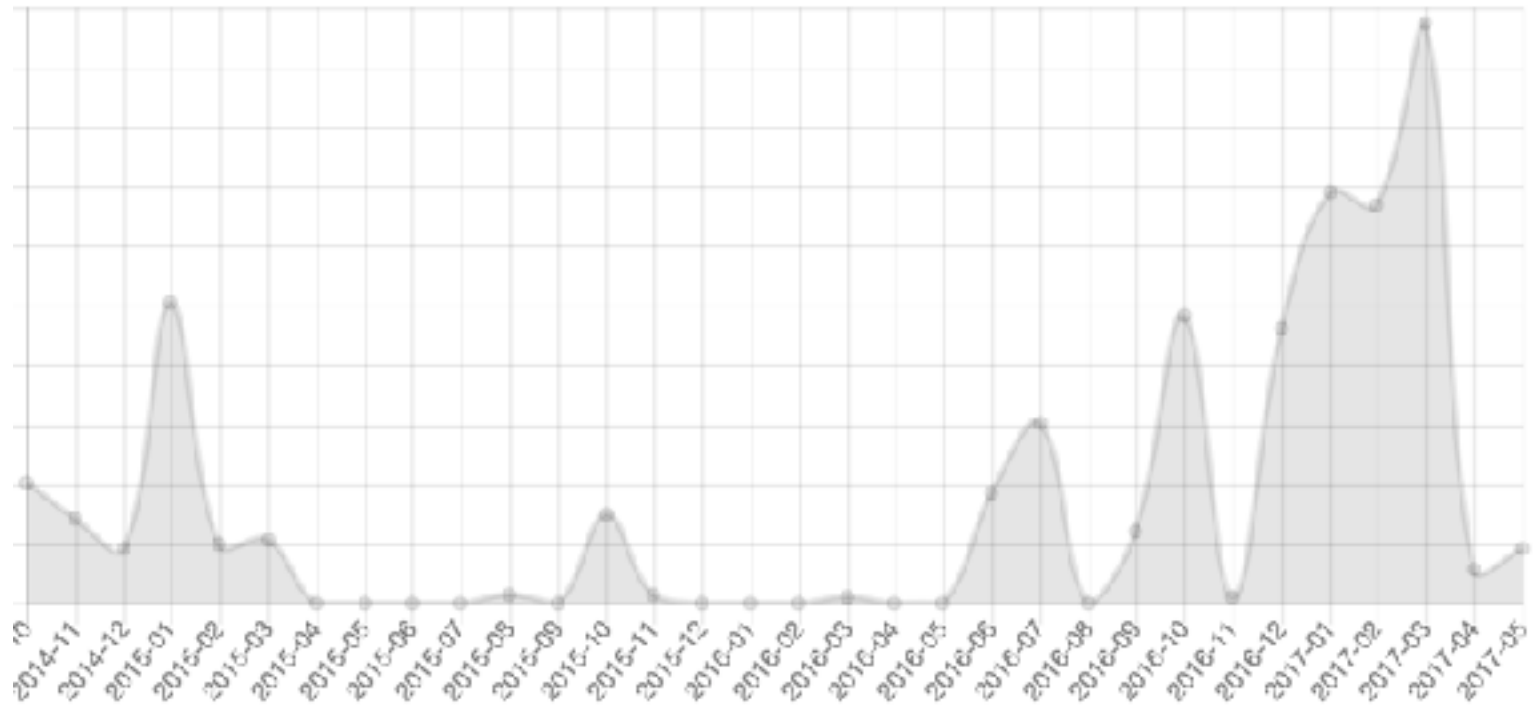


@arneswinnen



@TheBoredEng

# Takeovers since 2014-10





DILHSP  
AppSec EU  
**Belfast**





# Email snooping

# September 2016

## White Hats - Nepal

Securing the WWW

[SUBMIT](#) [ARCHIVE](#)

Reading Uber's Internal Emails [Uber Bug Bounty report worth \$10,000]

After recent finding about one of the Uber's subdomains takeover was publicly disclosed, I looked

Thanks to [detectify](#) for bringing the issue of subdomain takeover into light

<http://blog.pentestnepal.tech/post/149985438982/reading-ubers-internal-emails-uber-bug-bounty>

## 2 of 3 in action



# MX-records


**Inbound mail. This is important.**

# MX-records



Add New Domain

Some of your domains are unverified and require DNS configuration. Unverified domain.

State	Domain Name	Out
 Unverified	email.parse.com	0
 Active	sandbox40d7e593015449359d781a7ea...	0



## Inbound Parse

HOST	URL
link.westernunion.com	https://2b8ece...
mail.prod.uber.com	https://2b8ece...
mail.uberinternal.com	https://2b8ece...



# Conflict check + Validation

This domain name is already taken

**TO USE INBOUND PARSE, YOU MUST  
FIRST WHITELABEL YOUR DOMAIN.**

Creating a whitelabel proves that you are  
authorized to receive mail at that domain.

# Oh, add this!

## 3. Add DNS Records For Tracking

The CNAME record is necessary for **tracking opens, clicks and unsubscribes**.

Type	Hostname	Enter This Value
CNAME	email.example.com	mailgun.org

# CNAME -> MX

`CNAME` causes queries for all RR types (excluding `CNAME` itself) to be directed to the target name. That includes `MX`. So yes, the above zone data will cause queries for `otherdomain.com.`'s `MX` to resolve to `mail.base.com.`

# Whitelisted aliases for verification

The approval email typically can be sent to the following addresses, called administrative emails:

- admin@example.com
- administrator@example.com
- hostmaster@example.com
- postmaster@example.com
- webmaster@example.com

Where `example.com` is the domain for the certificate being purchased.

# Back to this

## 3. Add DNS Records For Tracking

The CNAME record is necessary for **tracking opens, clicks and unsubscribes**.

Type	Hostname	Enter This Value
CNAME	email.example.com	mailgun.org

Tadaa!

Success! Your domain `email.example.com` was created.

# We now get postmaster@

## Message

To postmaster@email.parse.com  
From Frans Rosén <frans@detectify.com>  
Subject this is to confirm  
Body

```
X-Mailgun-Incoming: Yes  
X-Envelope-From: <frans@detectify.com>  
Received: from mail-lf0-f54.google.com (mail-lf0-f54.google.com [209.85.215.54])  
  by mx1.mailgun.org with ESMTA id 57d9e52a.7fb048057d70-in8;  
  Thu, 15 Sep 2016 00:02:50 -0000 (UTC)  
Received: by mail-lf0-f54.google.com with SMTP id g62so213277781fe.3  
  for <postmaster@email.parse.com>; Wed, 14 Sep 2016 17:02:50 -0700 (PDT)  
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;
```

# Response the day after

Hey Frans thanks for sending this over!

We are acknowledging the report in H1 and will reach out to you either tonight (possibly tomorrow) when we are ready to take the domain over from you. We should be good and no further POC is necessary. Thanks again!



# Response the day after

Hey Frans thanks for sending this over!

We are acknowledging the report in H1 and will reach out to you either tonight (possibly tomorrow) when we are ready to take the domain over from you. We should be good and no further POC is necessary. Thanks again!

Nice!

Just FYI

I called it about 3 hours ago that you were going to do it

Lol

---

# Response the day after

Hey Frans thanks for sending this over!

We are acknowledging the report in H1 and will reach out to you either tonight (possibly tomorrow) when we are ready to take the domain over from you. We should be good and no further POC is necessary. Thanks again!

Nice!

Just FYI

I called it about 3 hours ago that you were going to do it

Lol



I wish I had found it ;)

6h

## On a final note

De Ceukelaire noticed that Donald Trump had linked to the website of the National Achievers Congress in a tweet in 2012, which at the time was using the domain name nac2012.com. However since that time the domain registration lapsed and De Ceukelaire was able to register the domain name for himself on January 22th 2017 giving him the ability to redirect it to wherever he liked. Which he did: the link in the Trump tweet

# On a final note

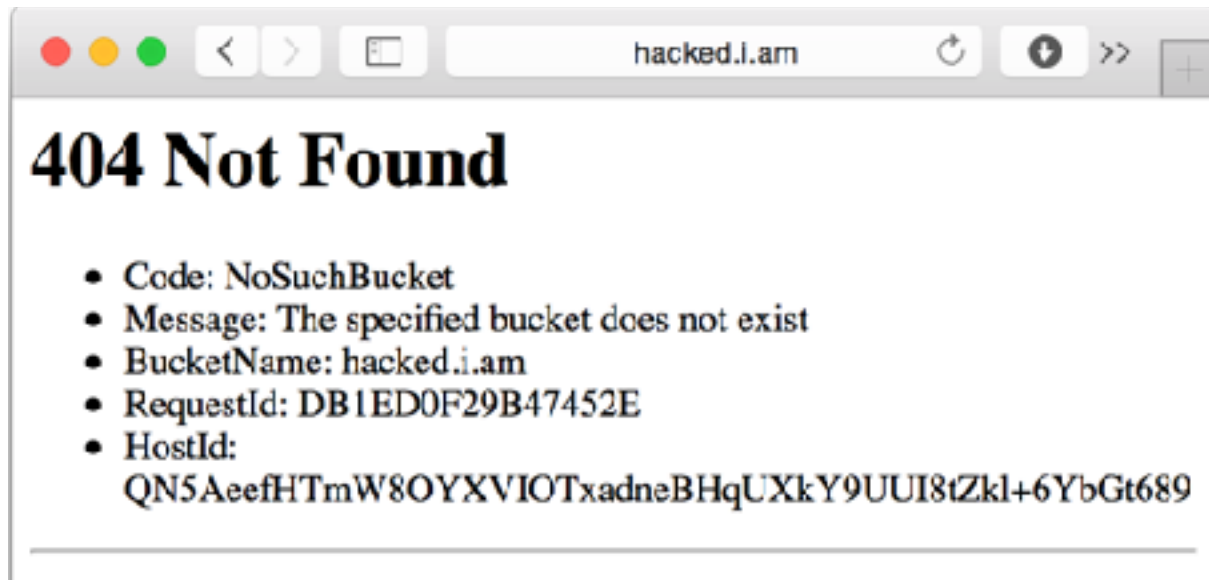


<https://twitter.com/realdonaldtrump/status/190093504939163648>

# On a final note



## On a final note



## On a final note



# ERROR

**The request could not be satisfied.**

---

Bad request.

---

Generated by cloudfront (CloudFront)

Request ID: PtuuK4poPXlAz235X7t8tUstWUDeABqIbqfrwDRRNoKq-Wwacc9R2A==

# Recap

- **Know your DNS Zone file**  
**MX, CNAME, A, AAAA, ALIAS. Everything.**
- **AUTOMATION, probably the only proper solution**
- **will.i.am loves this**



# Thanks!

**Frans Rosén (@fransrosen)**