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
"The Swedish Ninja"
- Background
- History
- Tools & Techniques
- Deeper levels of hijacking
- Evolution
- Mitigations
- Monitoring
Subdomain Takeover v1.0

campaign.site.com  

Campaign!
Subdomain Takeover v1.0

campaign.site.com  

Campaign!  

Fake site!
Ever seen one of these?

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: C7980A38158b619283
- HostId: xePlWWmW21xC3rVZKRGGXwVxVY9Y8Ru6KrSWa

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.
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

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 fransrogen with a $1,680 bounty.
Thanks again for helping us keep Twitter safe and secure for our users!

[Logo] rewarded fransrogen with a $10,000 bounty.
Thanks for the report Frans.

Riot Games rewarded fransrogen with a $7,500 bounty.
GG, thanks for your help resolving this issue! We greatly appreciate your time.

LinkedIn rewarded fransrogen with a $1,000 bounty.
What have we seen?

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 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?
What have we seen?

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:


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
What have we seen?

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...
What have we seen?

What have we seen?

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

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?

the Iraqi hacker who took credit for the Trump site "defacement" told me he used this labs.detectify.com/2014/10/21/hos... from Oct. 2014.
Tools
subbrute

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

Not active dev.

https://github.com/TheRook/subbrute
Sublist3r

Active dev! Took over subbrute!
Fetching from multiple sources

https://github.com/aboul3la/Sublist3r
**massdns**

A high-performance DNS stub resolver in C

Fast as hell!
Needs good resolver lists

https://github.com/blechschmidt/massdns
Soo soo powerful if you have good mutations
Combine with massdns == success
Can resolve, but better for just creating the lists
tko-sub

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

https://github.com/anshumanbh/tko-sub
We could look here?
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
```

**:winking:** thewesternuniongame.com is available! only $14.90
SERVFAIL/REFUSED

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.example.com.  172800  IN  NS  ns-1574.awsdns-04.co.uk.
labs.example.com.  172800  IN  NS  ns-875.awsdns-45.net.
```
Subdomain delegation

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

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

...  
ex

example.com. 172800 IN NS ns-272.awsdns-34.com.
ex
example.com. 172800 IN NS ns-895.awsdns-48.net.
ex
example.com. 172800 IN NS ns-1600.awsdns-08.co.uk.
ex
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.example.com. 172800 IN NS ns-1574.awsdns-04.co.uk.
labs.example.com. 172800 IN NS ns-875.awsdns-45.net.
```
Brute add/delete R53 DNS RR
We now control the domain!

```
$ dig TXT lab.example.com +short "this is just a test /FR"
```
Orphaned EC2 IPs

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 Anywhere | Prezi Mobility</title>
schema.prezi.com: <title>404 Not Found</title>
blog-es.prezi.com: <title>Prezi Blog | Noticias, trucos y consejos de pres</title>
cdn01.prezi.com: <title>404 Not Found</title>
blog-pt.prezi.com: <title>Prezi Blog | Notícias, dicas e truques sobre ap</title>
smartrouter.prezi.com: <title>404 Not Found</title>
prototypes.prezi.com: <title>Prezi</title>
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</title>
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

$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
New domain: bounces.uber.com

no-reply@zapiermail.com
to me

2017-01-20 04:29:12 - FOUND S3!! bounces.uber.com
404 Not Found

- Code: NoSuchBucket
- Message: The specified bucket does not exist
- BucketName: bounces.uber.com
- RequestId: D94DDD7B6DB4B5F5
- HostId: Hz8hPqt2DfgLaTq5w0i7ssrUGZ+pJ7fLpz1DODA1SecI
Jan 2017

```
$ dig bounces.uber.com

sparkpostmail.com. 4 IN A 52.218.128.135
```
Jan 2017

```bash
$ dig bounces.uber.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.
```
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

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
Email snoopining
September 2016

White Hats - Nepal

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

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

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

<table>
<thead>
<tr>
<th>State</th>
<th>Domain Name</th>
<th>Ou</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unverified</td>
<td>email.parse.com</td>
<td>0</td>
</tr>
<tr>
<td>Active</td>
<td>sandbox40d7e593015449359c781aTea...</td>
<td>0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>HOST</th>
<th>URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>link.westernunion.com</td>
<td><a href="https://2b8ece60598e7">https://2b8ece60598e7</a>...</td>
</tr>
<tr>
<td>mail.prod.uber.com</td>
<td><a href="https://2b8ece60598e7">https://2b8ece60598e7</a>...</td>
</tr>
<tr>
<td>mail.uberinternal.com</td>
<td><a href="https://2b8ece60598e7">https://2b8ece60598e7</a>...</td>
</tr>
</tbody>
</table>
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.
3. Add DNS Records For Tracking

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

<table>
<thead>
<tr>
<th>Type</th>
<th>Hostname</th>
<th>Enter This Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>CNAME</td>
<td>email.example.com</td>
<td>mailgun.org</td>
</tr>
</tbody>
</table>
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.
3. Add DNS Records For Tracking

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

<table>
<thead>
<tr>
<th>Type</th>
<th>Hostname</th>
<th>Enter This Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>CNAME</td>
<td>email.example.com</td>
<td>mailgun.org</td>
</tr>
</tbody>
</table>
Tadaa!

Success! Your domain email.example.com was created.
We now get postmaster@
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

404 Not Found

- Code: NoSuchBucket
- Message: The specified bucket does not exist
- BucketName: hacked.i.am
- RequestId: DB1ED0F29B47452E
- HostId:
  QN5AeeHTm8OYXVIOTxadneBHqUXkY9UI18tZkl+6YbGt689
On a final note

ERROR

The request could not be satisfied.

Bad request.

Generated by cloudfront (CloudFront)
Request ID: PtuuK4pcPXlAz235X7t8tUstWUDeABqIbqfrwDRRNoKq-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)