RISKIQ®

Advanced Use Case:

Humanitarian Aid Group Investigation

Scenario:

You are a freelancing human rights cybersecurity analyst. You have been contacted by a humanitarian aid group that claims they were attacked and need your help with conducting the cyber investigation. You have been given some background information and a twitter post to begin your investigation.

Background:

Venezuela is currently in the throes of a major political crisis as opposition leader and self-declared interim President Juan Guaidó is attempting to oust the incumbent President, Nicolas Maduro, who had been re-elected for a second term in a very controversial election that many are refusing to recognize as legitimate.

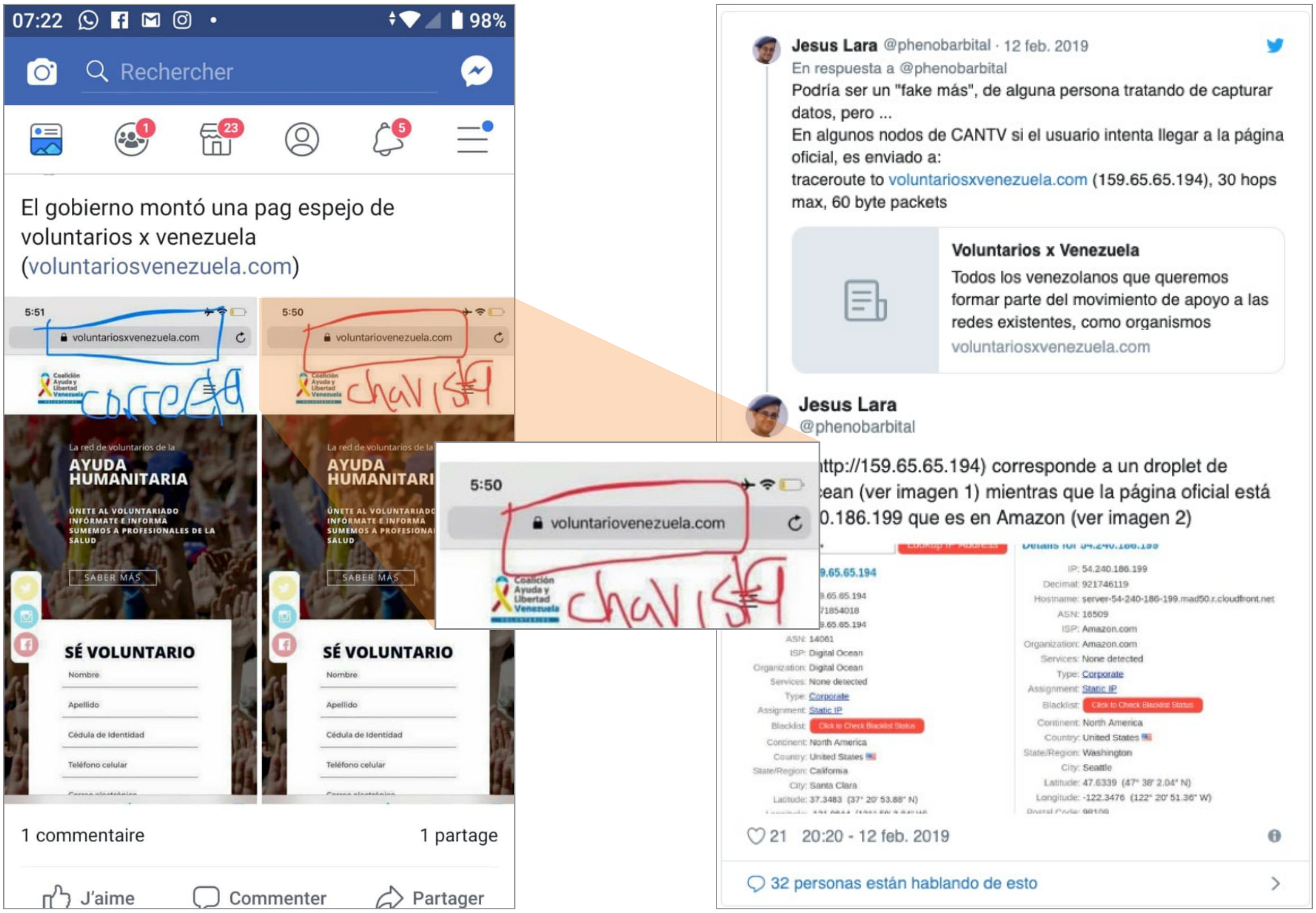
Back in February, shortly after declaring himself as interim president, Guaidó called for citizens of Venezuela to volunteer in helping international organizations deliver humanitarian aid to the country because Maduro was refusing to accept aid and blocking desperately needed supplies, food, and medicine at their borders.

A website was set up where volunteers could register to help, which required them to provide personal information such as their name, phone number, address, and whether they have things like a medical degree or a car.

This website appeared online on February 6th. Only a few days later, on February 11th, the day after the public announcement of the initiative, another almost identical website appeared with a very similar domain name and structure.

Only people inside Venezuela seemed to be affected by this attack.

Twitter posts started to be released of an identical fraudulent website. Here is a screenshot of the twitter posts.



07:22 98%

Rechercher

El gobierno montó una pag espejo de voluntarios x venezuela (voluntariosvenezuela.com)

1 commentaire 1 partage

Jesus Lara @phenobarbital · 12 feb. 2019
En respuesta a @phenobarbital
Podría ser un "fake más", de alguna persona tratando de capturar datos, pero ...
En algunos nodos de CANTV si el usuario intenta llegar a la página oficial, es enviado a:
traceroute to voluntariosxvenezuela.com (159.65.65.194), 30 hops max, 60 byte packets

Voluntarios x Venezuela
Todos los venezolanos que queremos formar parte del movimiento de apoyo a las redes existentes, como organismos
voluntariosxvenezuela.com

Jesus Lara
@phenobarbital

ttp://159.65.65.194) corresponde a un droplet de ean (ver imagen 1) mientras que la página oficial está 0.186.199 que es en Amazon (ver imagen 2)

9.65.65.194
9.65.65.194
71854018
9.65.65.194
ASN: 14061
ISP: Digital Ocean
Organization: Digital Ocean
Services: None detected
Type: Corporate
Assignment: Static IP
Blacklist: Click to Check Blacklist Status
Continent: North America
Country: United States
State/Region: California
City: Santa Clara
Latitude: 37.3483 (37° 20' 53.88" N)

IP: 54.240.186.199
Decimal: 921746119
Hostname: server-54-240-186-199.mad50.r.cloudfront.net
ASN: 16509
ISP: Amazon.com
Organization: Amazon.com
Services: None detected
Type: Corporate
Assignment: Static IP
Blacklist: Click to Check Blacklist Status
Continent: North America
Country: United States
State/Region: Washington
City: Seattle
Latitude: 47.6339 (47° 38' 2.04" N)
Longitude: -122.3476 (122° 20' 51.36" W)

♡ 21 20:20 - 12 feb. 2019

32 personas están hablando de esto

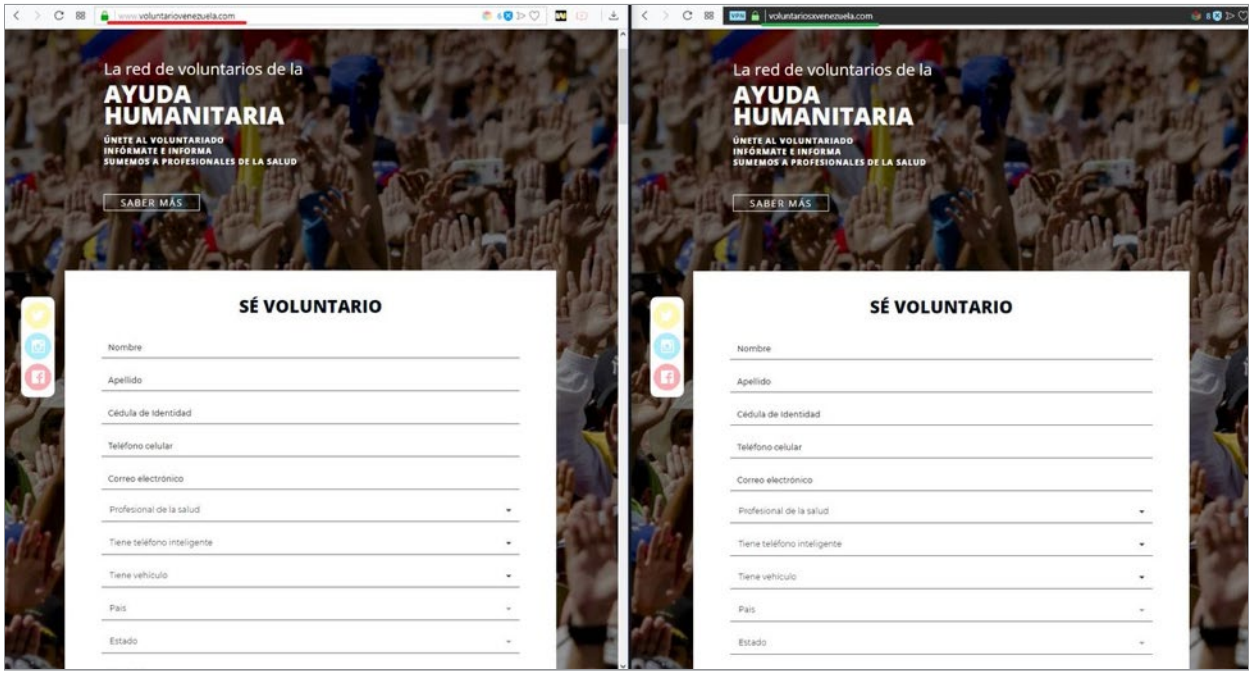
Reported fraudulent website Voluntariovenezuela[.]com, 159[.]65[.]65[.]194,

The legitimate website is www[.]voluntariosxvenezuela[.]com.

It was reported soon after that website went up that only people in Venezuela trying to visit the original website www[.]voluntariosxvenezuela[.]com was being redirected to the fake website www[.] voluntariosvenezuela[.]com via DNS spoofing.

DNS spoofing, which is a type of attack that corrupts domain name servers to redirect internet traffic from legitimate servers to malicious ones.

Below are screenshots from the two websites. The one that is underlined in red is the reported fraudulent website.



Goal:

Your goal is to investigate both websites from back in February 2019 and determine the following and provide your evidence:

1. Is www[.]voluntariovenezuela[.]com fraudulent?
2. Are any other websites also infringing on the real website www[.]voluntariosxvenezuela[.]com?
3. Can you determine or infer who is behind this domain infringing DNS poison attack?
4. Are there any other websites that the threat actor is currently using or has used in attacks?
5. What are some ways people can protect against DNS spoofing?

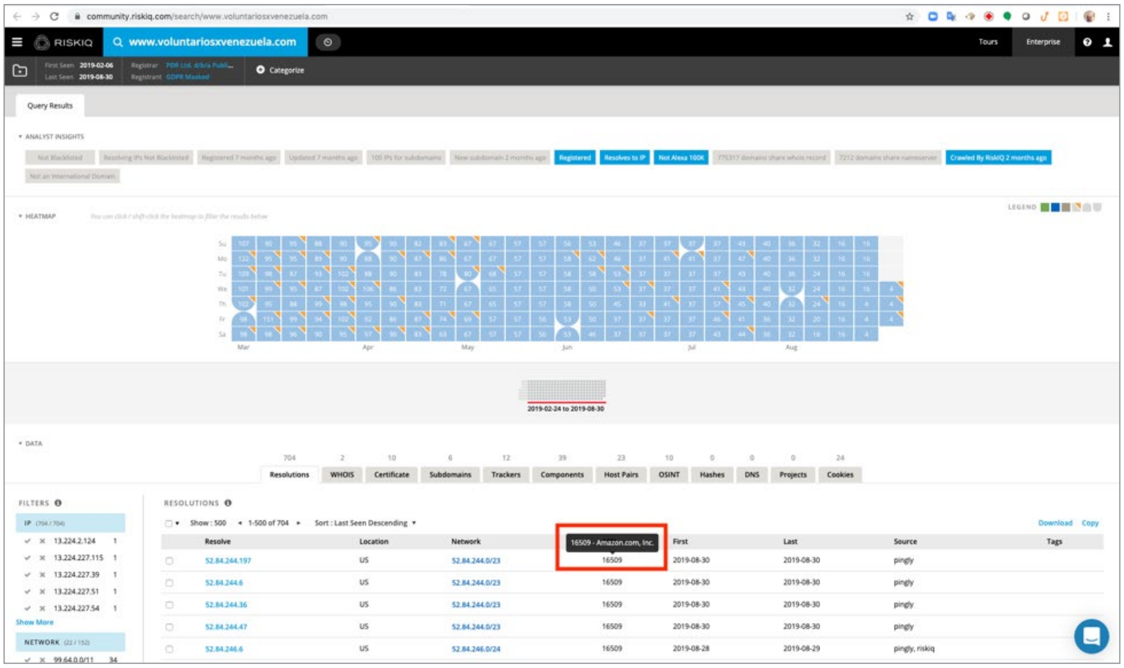
Search:

Fist Search: Perform a search for www[.]voluntariosxvenezuela[.]com
https://community.riskiq.com/search/www.voluntariosxvenezuela.com

Second Search: Perform a search for www[.]voluntariovenezuela[.]com
https://community.riskiq.com/search/www.voluntariovenezuela.com

Step 1: search for www[.]voluntariosxvenezuela[.]com

https://community.riskiq.com/search/www.voluntariosxvenezuela.com

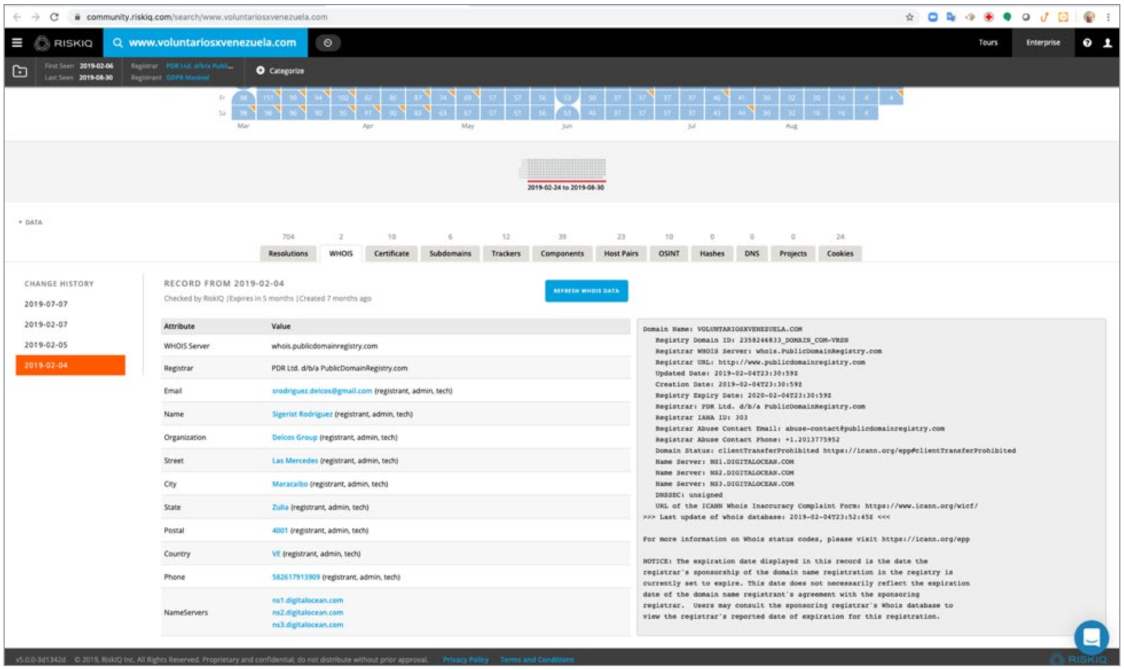


Resolve	Location	Network		First	Last	Source	Tags
52.84.244.197	US	52.84.244.0/23	16509	2019-08-30	2019-08-30	pingly	
52.84.244.6	US	52.84.244.0/23	16509	2019-08-30	2019-08-30	pingly	
52.84.244.36	US	52.84.244.0/23	16509	2019-08-30	2019-08-30	pingly	
52.84.244.47	US	52.84.244.0/23	16509	2019-08-30	2019-08-30	pingly	
52.84.246.6	US	52.84.246.0/24	16509	2019-08-28	2019-08-29	pingly, riskiq	

Determine the characteristics of the real website www[.]voluntariosxvenezuela[.]com

From the resolutions tab, we can see the IP addresses are from Amazon.com, Inc. according to the ASN number based in the United States.

Step 2: Click on the WHOIS tab



RECORD FROM 2019-02-04

Checked by RiskIQ |Expires in 5 months |Created 7 months ago

Attribute	Value
WHOIS Server	whois.publicdomainregistry.com
Registrar	PDR Ltd. d/b/a PublicDomainRegistry.com
Email	srodriguez.delcos@gmail.com (registrant, admin, tech)
Name	Sigerist Rodriguez (registrant, admin, tech)
Organization	Delcos Group (registrant, admin, tech)
Street	Las Mercedes (registrant, admin, tech)
City	Maracaibo (registrant, admin, tech)
State	Zulia (registrant, admin, tech)
Postal	4001 (registrant, admin, tech)
Country	VE (registrant, admin, tech)
Phone	582617913909 (registrant, admin, tech)
NameServers	ns1.digitalocean.com ns2.digitalocean.com ns3.digitalocean.com

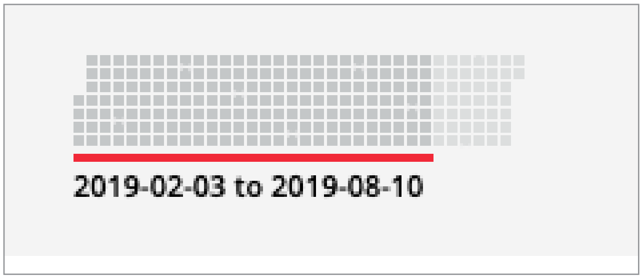
```
Domain Name: VOLUNTARIOSXVENEZUELA.COM
   Registry Domain ID: 2358246833_DOMAIN_COM-VRSN
   Registrar WHOIS Server: whois.PublicDomainRegistry.com
   Registrar URL: http://www.publicdomainregistry.com
   Updated Date: 2019-02-04T23:30:59Z
   Creation Date: 2019-02-04T23:30:59Z
   Registry Expiry Date: 2020-02-04T23:30:59Z
   Registrar: PDR Ltd. d/b/a PublicDomainRegistry.com
   Registrar IANA ID: 303
   Registrar Abuse Contact Email: abuse-contact@publicdomainregistry.com
   Registrar Abuse Contact Phone: +1.2013775952
   Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
   Name Server: NS1.DIGITALOCEAN.COM
   Name Server: NS2.DIGITALOCEAN.COM
   Name Server: NS3.DIGITALOCEAN.COM
   DNSSEC: unsigned
   URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2019-02-04T23:52:45Z <<<

For more information on Whois status codes, please visit https://icann.org/epp

NOTICE: The expiration date displayed in this record is the date the
registrar's sponsorship of the domain name registration in the registry is
currently set to expire. This date does not necessarily reflect the expiration
date of the domain name registrant's agreement with the sponsoring
registrar.  Users may consult the sponsoring registrar's Whois database to
view the registrar's reported date of expiration for this registration.
```

In the change history section on the left side of the screen click on the earliest date.

The WHOIS information shows the website was originally registered to Delcos Group in the city of Maracaibo in Venezuela. The registrant is Sigerist Rodriguez.

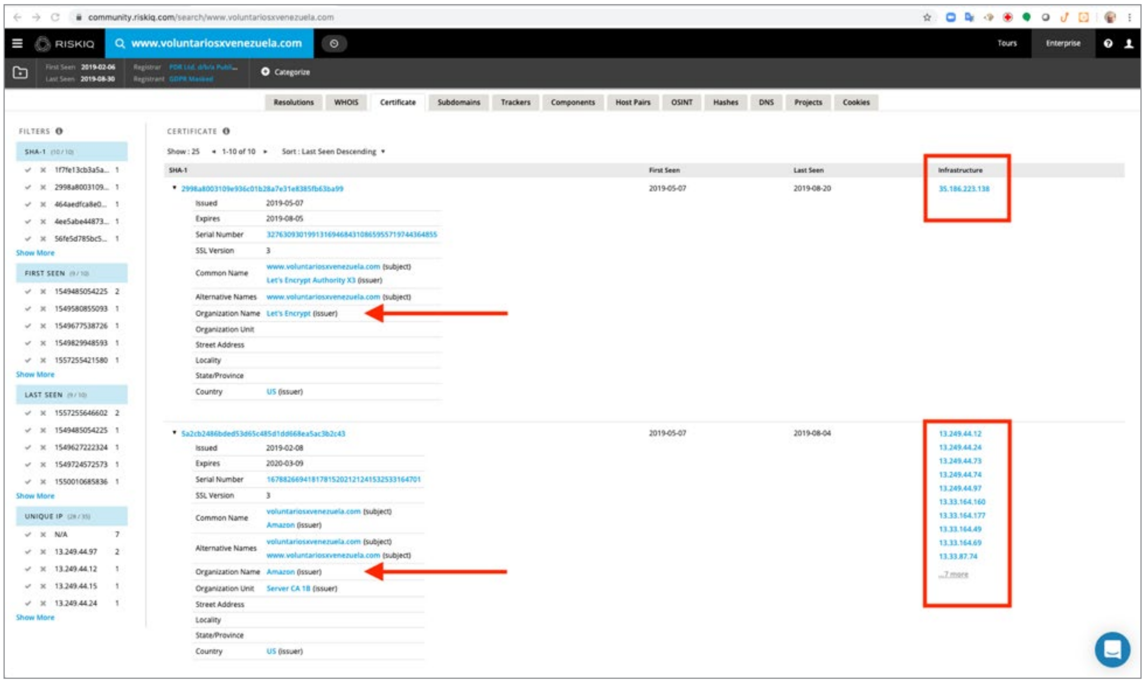
Step 3: Click on the Certificate tab

In order to see the results that occurred back in February, you will need to use the timebar. Click on the far left side of the timebar.



2019-02-03 to 2019-08-10

The results will now refresh and display six months of data starting on February 3, 2019.



community.riskiq.com/search/www.voluntariosxvenezuela.com

First Seen 2019-02-06
Last Seen 2019-08-30
Registrar PDR Ltd. d/b/a Publi...
Registrant GDPR Masked

FILTERS

SHA-1 (10 / 10)

1f7fe13cb3a5a...	1
2998a8003109...	1
464aedfca8e0...	1
4ee5abe44873...	1
56fe5d785bc5...	1

Show More

FIRST SEEN (9 / 10)

1549485054225	2
1549580855093	1
1549677538726	1
1549829948593	1
1557255421580	1

Show More

LAST SEEN (9 / 10)

1557255646602	2
1549485054225	1
1549627222324	1
1549724572573	1
1550010685836	1

Show More

UNIQUE IP (28 / 35)

N/A	7
13.249.44.97	2
13.249.44.12	1
13.249.44.15	1
13.249.44.24	1

Show More

CERTIFICATE

Show : 25 ◂ 1-10 of 10 ▸ Sort : Last Seen Descending ▾

SHA-1	First Seen	Last Seen	Infrastructure
2998a8003109e936c01b28a7e31e8385fb63ba99	2019-05-07	2019-08-20	35.186.223.138
5a2cb2486bded53d65c485d1dd668ea5ac3b2c43	2019-05-07	2019-08-04	13.249.44.12 13.249.44.24 13.249.44.73 13.249.44.74 13.249.44.97 13.33.164.160 13.33.164.177 13.33.164.49 13.33.164.69 13.33.87.74 ...7 more

2998a8003109e936c01b28a7e31e8385fb63ba99

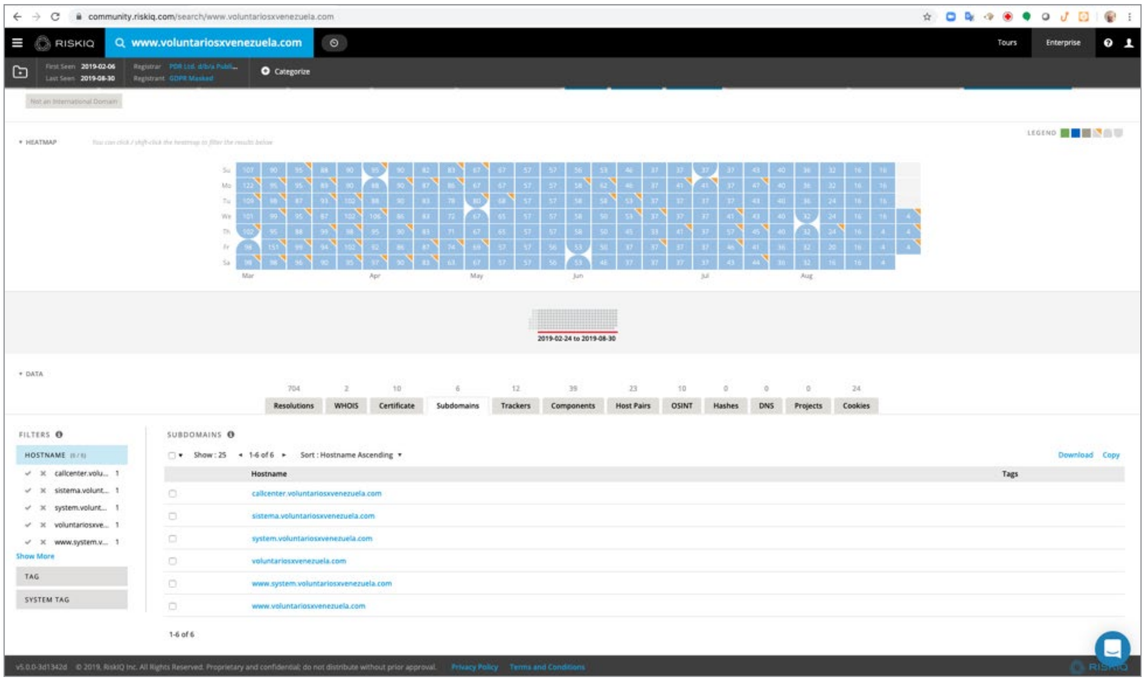
Issued	2019-05-07
Expires	2019-08-05
Serial Number	327630930199131694684310865955719744364855
SSL Version	3
Common Name	www.voluntariosxvenezuela.com (subject) Let's Encrypt Authority X3 (issuer)
Alternative Names	www.voluntariosxvenezuela.com (subject)
Organization Name	Let's Encrypt (issuer)
Organization Unit	
Street Address	
Locality	
State/Province	
Country	US (issuer)

5a2cb2486bded53d65c485d1dd668ea5ac3b2c43

Issued	2019-02-08
Expires	2020-03-09
Serial Number	16788266941817815202121241532533164701
SSL Version	3
Common Name	voluntariosxvenezuela.com (subject) Amazon (issuer)
Alternative Names	voluntariosxvenezuela.com (subject) www.voluntariosxvenezuela.com (subject)
Organization Name	Amazon (issuer)
Organization Unit	Server CA 1B (issuer)
Street Address	
Locality	
State/Province	
Country	US (issuer)

Certificates are a combination of paid Amazon and Let's Encrypt free certificates. The DNS spoofing could have tainted the results because the domain was redirecting to fraudulent infrastructure. Until the other domain has been examined, we will not be able to conclusively determine if the real domain also had free Let's Encrypt SSL certificates.

Step 4: Click on the Subdomains Tab



704	2	10	6	12	39	23	10	0	0	0	24
Resolutions	WHOIS	Certificate	Subdomains	Trackers	Components	Host Pairs	OSINT	Hashes	DNS	Projects	Cookies

SUBDOMAINS

Show : 25 ◂ 1-6 of 6 ▸ Sort : Hostname Ascending

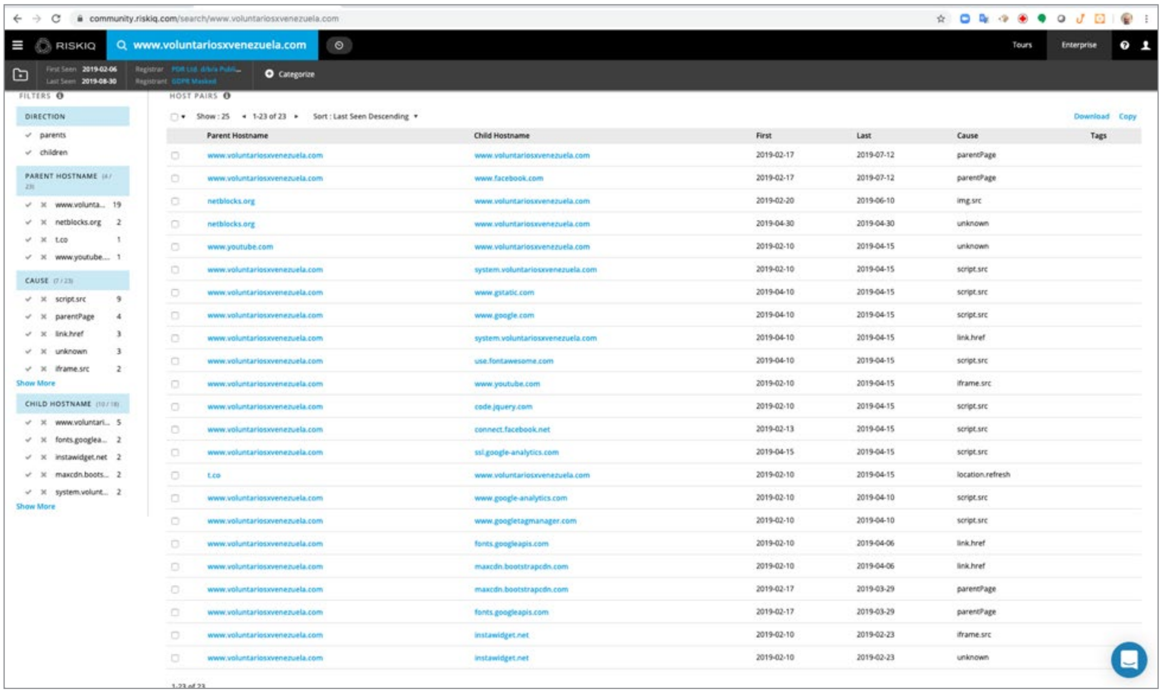
Hostname	Tags
callcenter.voluntariosxvenezuela.com	
sistema.voluntariosxvenezuela.com	
system.voluntariosxvenezuela.com	
voluntariosxvenezuela.com	
www.system.voluntariosxvenezuela.com	
www.voluntariosxvenezuela.com	

1-6 of 6

v5.0.0-3d1342d © 2019, RiskIQ Inc. All Rights Reserved. Proprietary and confidential; do not distribute without prior approval. Privacy Policy Terms and Conditions

Subdomains are not showing anything unusual and are all part of the same domain voluntariosxvenexuela[.]com

Step 5: Click on the Hoist Pairs tab



HOST PAIRS

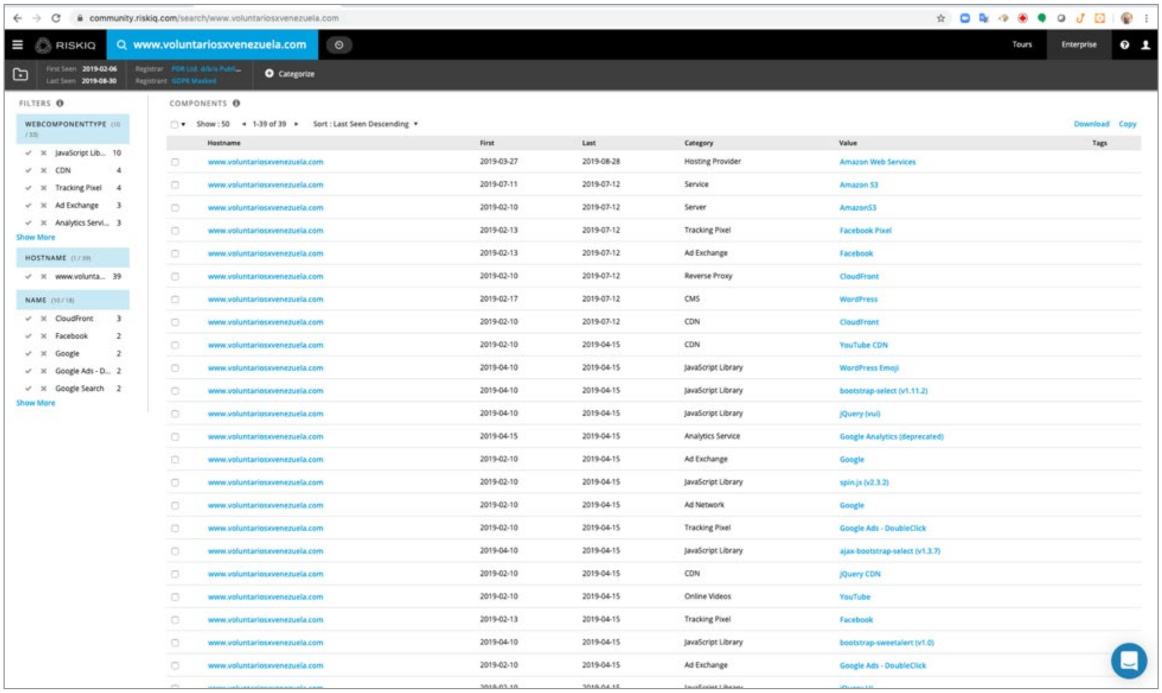
Show : 25 ◂ 1-23 of 23 ▸ Sort : Last Seen Descending

Parent Hostname	Child Hostname	First	Last	Cause	Tags
www.voluntariosxvenezuela.com	www.voluntariosxvenezuela.com	2019-02-17	2019-07-12	parentPage	
www.voluntariosxvenezuela.com	www.facebook.com	2019-02-17	2019-07-12	parentPage	
netblocks.org	www.voluntariosxvenezuela.com	2019-02-20	2019-06-10	img.src	
netblocks.org	www.voluntariosxvenezuela.com	2019-04-30	2019-04-30	unknown	
www.youtube.com	www.voluntariosxvenezuela.com	2019-02-10	2019-04-15	unknown	
www.voluntariosxvenezuela.com	system.voluntariosxvenezuela.com	2019-02-10	2019-04-15	script.src	
www.voluntariosxvenezuela.com	www.gstatic.com	2019-04-10	2019-04-15	script.src	
www.voluntariosxvenezuela.com	www.google.com	2019-04-10	2019-04-15	script.src	
www.voluntariosxvenezuela.com	system.voluntariosxvenezuela.com	2019-04-10	2019-04-15	link.href	
www.voluntariosxvenezuela.com	use.fontawesome.com	2019-04-10	2019-04-15	script.src	
www.voluntariosxvenezuela.com	www.youtube.com	2019-02-10	2019-04-15	iframe.src	
www.voluntariosxvenezuela.com	code.jquery.com	2019-02-10	2019-04-15	script.src	
www.voluntariosxvenezuela.com	connect.facebook.net	2019-02-13	2019-04-15	script.src	
www.voluntariosxvenezuela.com	ssl.google-analytics.com	2019-04-15	2019-04-15	script.src	
t.co	www.voluntariosxvenezuela.com	2019-02-10	2019-04-15	location.refresh	
www.voluntariosxvenezuela.com	www.google-analytics.com	2019-02-10	2019-04-10	script.src	
www.voluntariosxvenezuela.com	www.googletagmanager.com	2019-02-10	2019-04-10	script.src	
www.voluntariosxvenezuela.com	fonts.googleapis.com	2019-02-10	2019-04-06	link.href	
www.voluntariosxvenezuela.com	maxcdn.bootstrapcdn.com	2019-02-10	2019-04-06	link.href	
www.voluntariosxvenezuela.com	maxcdn.bootstrapcdn.com	2019-02-17	2019-03-29	parentPage	
www.voluntariosxvenezuela.com	fonts.googleapis.com	2019-02-17	2019-03-29	parentPage	
www.voluntariosxvenezuela.com	instawidget.net	2019-02-10	2019-02-23	iframe.src	
www.voluntariosxvenezuela.com	instawidget.net	2019-02-10	2019-02-23	unknown	

1-23 of 23

The Host Pairs tab does not show any current or past relationship with content going to or coming from the fraudulent website under investigation. Sometimes threat actors will create their website, and have it pull content directly from the real website. In this particular case, we do not see any of that type of activity on www[.] voluntariosxvenexuela[.]com.

Step 6: Click on the Components tab


community.riskiq.com/search/www.voluntariosxvenezuela.com

RISKIQ | www.voluntariosxvenezuela.com | Tours | Enterprise

First Seen 2019-02-06 · Last Seen 2019-08-30 · Registrar PDR Ltd. d/b/a Publi... · Registrant GDPR Masked · Categorize

FILTERS

WEBCOMPONENTTYPE (10 / 33)

JavaScript Lib...	10
CDN	4
Tracking Pixel	4
Ad Exchange	3
Analytics Servi...	3

Show More

HOSTNAME (1 / 39)

www.volunta...	39

NAME (10 / 18)

CloudFront	3
Facebook	2
Google	2
Google Ads - D...	2
Google Search	2

Show More

COMPONENTS

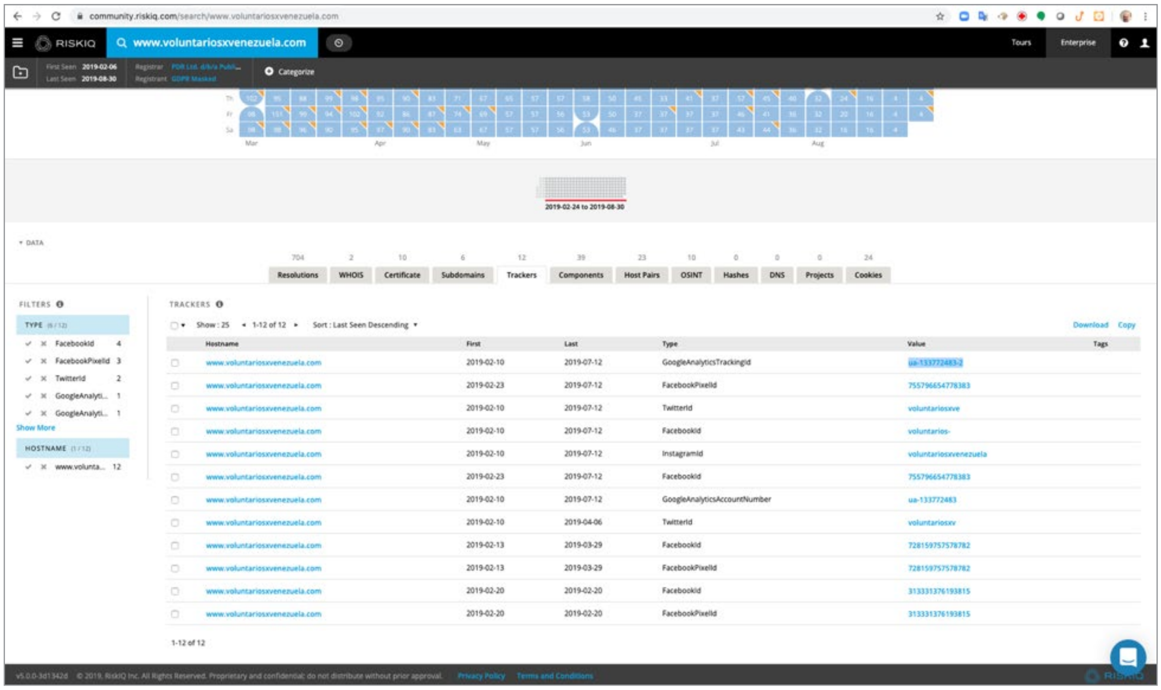
Show : 50 · 1-39 of 39 · Sort : Last Seen Descending · Download · Copy

Hostname	First	Last	Category	Value	Tags
www.voluntariosxvenezuela.com	2019-03-27	2019-08-28	Hosting Provider	Amazon Web Services	
www.voluntariosxvenezuela.com	2019-07-11	2019-07-12	Service	Amazon S3	
www.voluntariosxvenezuela.com	2019-02-10	2019-07-12	Server	AmazonS3	
www.voluntariosxvenezuela.com	2019-02-13	2019-07-12	Tracking Pixel	Facebook Pixel	
www.voluntariosxvenezuela.com	2019-02-13	2019-07-12	Ad Exchange	Facebook	
www.voluntariosxvenezuela.com	2019-02-10	2019-07-12	Reverse Proxy	CloudFront	
www.voluntariosxvenezuela.com	2019-02-17	2019-07-12	CMS	WordPress	
www.voluntariosxvenezuela.com	2019-02-10	2019-07-12	CDN	CloudFront	
www.voluntariosxvenezuela.com	2019-02-10	2019-04-15	CDN	YouTube CDN	
www.voluntariosxvenezuela.com	2019-04-10	2019-04-15	JavaScript Library	WordPress Emoji	
www.voluntariosxvenezuela.com	2019-04-10	2019-04-15	JavaScript Library	bootstrap-select (v1.11.2)	
www.voluntariosxvenezuela.com	2019-04-10	2019-04-15	JavaScript Library	jQuery (vui)	
www.voluntariosxvenezuela.com	2019-04-15	2019-04-15	Analytics Service	Google Analytics (deprecated)	
www.voluntariosxvenezuela.com	2019-02-10	2019-04-15	Ad Exchange	Google	
www.voluntariosxvenezuela.com	2019-02-10	2019-04-15	JavaScript Library	spin.js (v2.3.2)	
www.voluntariosxvenezuela.com	2019-02-10	2019-04-15	Ad Network	Google	
www.voluntariosxvenezuela.com	2019-02-10	2019-04-15	Tracking Pixel	Google Ads - DoubleClick	
www.voluntariosxvenezuela.com	2019-04-10	2019-04-15	JavaScript Library	ajax-bootstrap-select (v1.3.7)	
www.voluntariosxvenezuela.com	2019-02-10	2019-04-15	CDN	jQuery CDN	
www.voluntariosxvenezuela.com	2019-02-10	2019-04-15	Online Videos	YouTube	
www.voluntariosxvenezuela.com	2019-02-13	2019-04-15	Tracking Pixel	Facebook	
www.voluntariosxvenezuela.com	2019-04-10	2019-04-15	JavaScript Library	bootstrap-sweetalert (v1.0)	
www.voluntariosxvenezuela.com	2019-02-10	2019-04-15	Ad Exchange	Google Ads - DoubleClick	

None of the components appear to be associated with malicious activity.

Step 7: Click on the Trackers tab

Now we want to examine the tracker and cookies from www[.]voluntariosxvenexuela[.]com to see if the threat actor duplicated the real website's cookies and trackers into the fraudulent website.



community.riskiq.com/search/www.voluntariosxvenezuela.com

RISKIQ | www.voluntariosxvenezuela.com | Tours | Enterprise

First Seen 2019-02-06 · Last Seen 2019-08-30 · Registrar PDR Ltd. d/b/a Publi... · Registrant GDPR Masked · Categorize

DATA

Resolutions	WHOIS	Certificate	Subdomains	Trackers	Components	Host Pairs	OSINT	Hashes	DNS	Projects	Cookies
704	2	10	6	12	39	23	10	0	0	0	24

FILTERS

TYPE (6 / 12)

FacebookId	4
FacebookPixelId	3
TwitterId	2
GoogleAnalyti...	1
GoogleAnalyti...	1

Show More

HOSTNAME (1 / 12)

www.volunta...	12

TRACKERS

Show : 25 · 1-12 of 12 · Sort : Last Seen Descending · Download · Copy

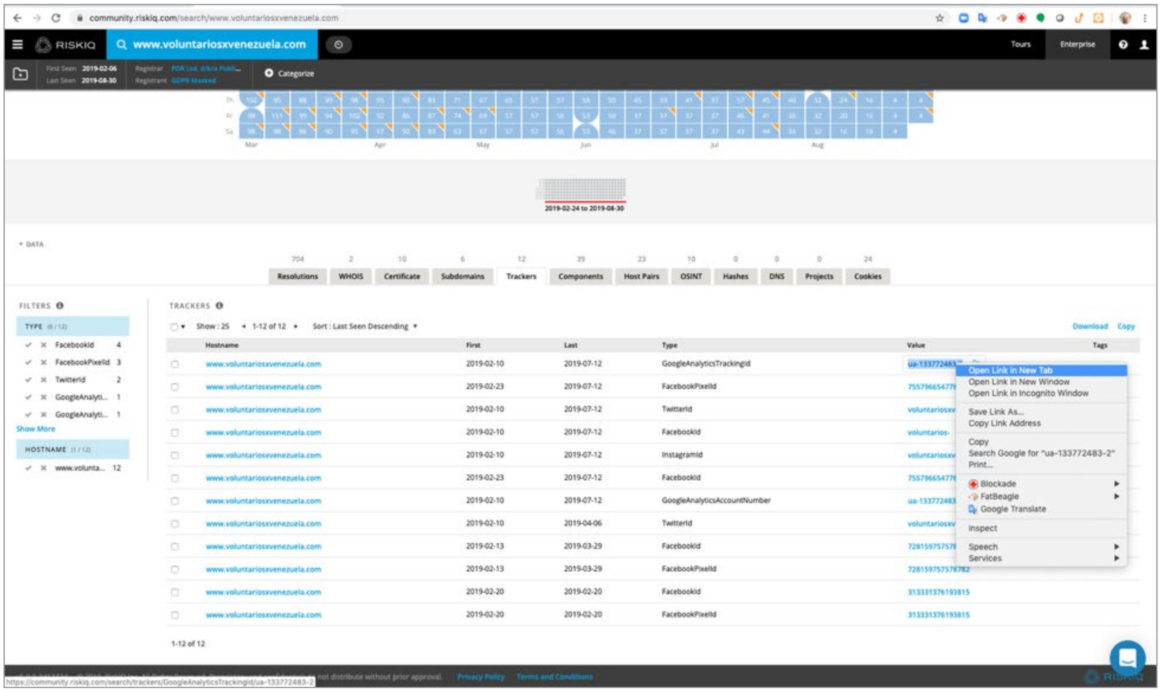
Hostname	First	Last	Type	Value	Tags
www.voluntariosxvenezuela.com	2019-02-10	2019-07-12	GoogleAnalyticsTrackingId	ua-133772483-2	
www.voluntariosxvenezuela.com	2019-02-23	2019-07-12	FacebookPixelId	755796654778383	
www.voluntariosxvenezuela.com	2019-02-10	2019-07-12	TwitterId	voluntariosxve	
www.voluntariosxvenezuela.com	2019-02-10	2019-07-12	FacebookId	voluntarios-	
www.voluntariosxvenezuela.com	2019-02-10	2019-07-12	InstagramId	voluntariosxvenezuela	
www.voluntariosxvenezuela.com	2019-02-23	2019-07-12	FacebookId	755796654778383	
www.voluntariosxvenezuela.com	2019-02-10	2019-07-12	GoogleAnalyticsAccountNumber	ua-133772483	
www.voluntariosxvenezuela.com	2019-02-10	2019-04-06	TwitterId	voluntariosxv	
www.voluntariosxvenezuela.com	2019-02-13	2019-03-29	FacebookId	728159757578782	
www.voluntariosxvenezuela.com	2019-02-13	2019-03-29	FacebookPixelId	728159757578782	
www.voluntariosxvenezuela.com	2019-02-20	2019-02-20	FacebookId	313331376193815	
www.voluntariosxvenezuela.com	2019-02-20	2019-02-20	FacebookPixelId	313331376193815	

1-12 of 12

v5.0.0-3d1342d © 2019, RiskIQ Inc. All Rights Reserved. Proprietary and confidential; do not distribute without prior approval. Privacy Policy Terms and Conditions

Here we see a list of trackers used to track user experience on the website. We will now pivot search on the first value for the GoogleAnalyticsTrackingId ua-133772483-2.

Step 8: Pivot search on the GoogleAnalyticsTrackingId value ua-133772483-2


community.riskiq.com/search/www.voluntariosxvenezuela.com
RISKIQ
www.voluntariosxvenezuela.com
Tours
Enterprise
Categorize
2019-02-24 to 2019-08-30
Open Link in New Tab
Open Link in New Window
Open Link in Incognito Window
Save Link As...
Copy Link Address
Copy
Search Google for "ua-133772483-2"
Print...
Blockade
FatBeagle
Google Translate
Inspect
Speech
Services
https://community.riskiq.com/search/trackers/GoogleAnalyticsTrackingId/ua-133772483-2
Privacy Policy
Terms and Conditions

DATA

Resolutions	WHOIS	Certificate	Subdomains	Trackers	Components	Host Pairs	OSINT	Hashes	DNS	Projects	Cookies
704	2	10	6	12	39	23	10	0	0	0	24

FILTERS

TYPE (6 / 12)

FacebookId	4
FacebookPixelId	3
TwitterId	2
GoogleAnalyti...	1
GoogleAnalyti...	1

Show More

HOSTNAME (1 / 12)

www.volunta...	12

TRACKERS

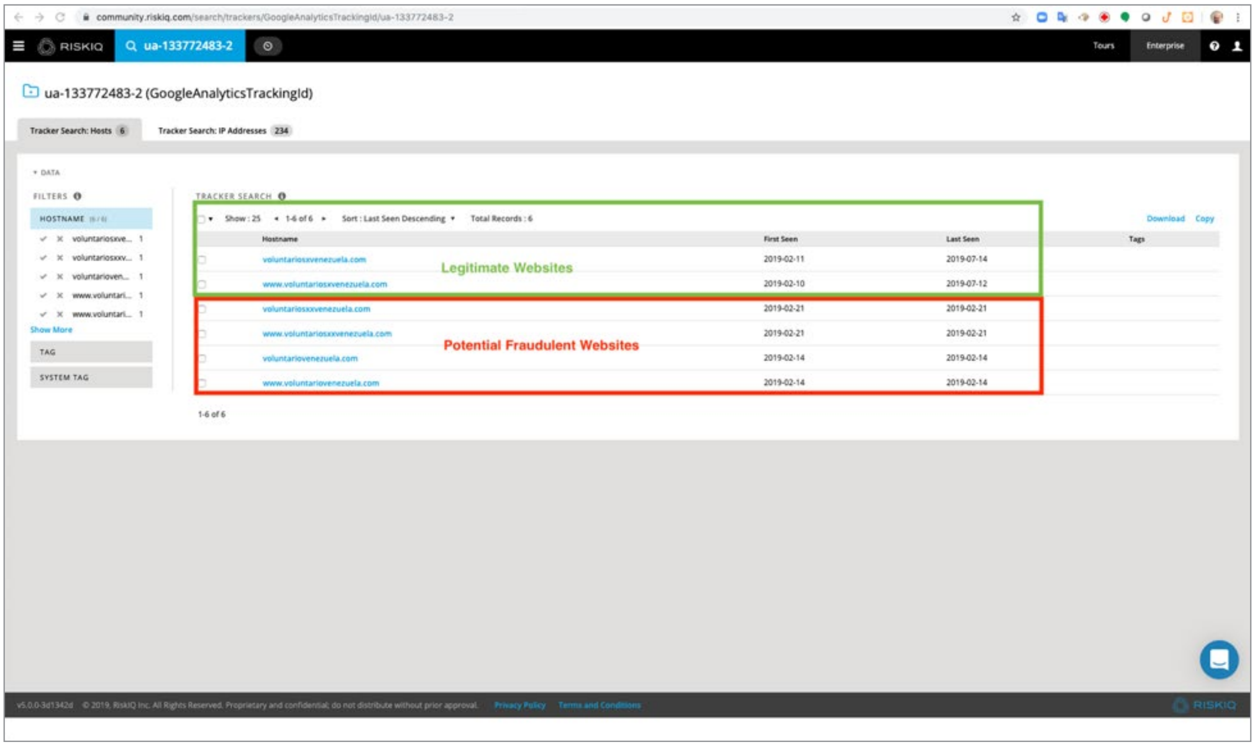
Show : 25 · 1-12 of 12 · Sort : Last Seen Descending · Download · Copy

Hostname	First	Last	Type	Value	Tags
www.voluntariosxvenezuela.com	2019-02-10	2019-07-12	GoogleAnalyticsTrackingId	ua-133772483-2	
www.voluntariosxvenezuela.com	2019-02-23	2019-07-12	FacebookPixelId	755796654778	
www.voluntariosxvenezuela.com	2019-02-10	2019-07-12	TwitterId	voluntariosxv	
www.voluntariosxvenezuela.com	2019-02-10	2019-07-12	FacebookId	voluntarios-	
www.voluntariosxvenezuela.com	2019-02-10	2019-07-12	InstagramId	voluntariosxv	
www.voluntariosxvenezuela.com	2019-02-23	2019-07-12	FacebookId	755796654778	
www.voluntariosxvenezuela.com	2019-02-10	2019-07-12	GoogleAnalyticsAccountNumber	ua-133772483	
www.voluntariosxvenezuela.com	2019-02-10	2019-04-06	TwitterId	voluntariosxv	
www.voluntariosxvenezuela.com	2019-02-13	2019-03-29	FacebookId	728159757578	
www.voluntariosxvenezuela.com	2019-02-13	2019-03-29	FacebookPixelId	728159757578782	
www.voluntariosxvenezuela.com	2019-02-20	2019-02-20	FacebookId	313331376193815	
www.voluntariosxvenezuela.com	2019-02-20	2019-02-20	FacebookPixelId	313331376193815	

1-12 of 12

Right-click on ua-133772483-2 and open it in a new tab.

The URL should be https://community.riskiq.com/search/trackers/GoogleAnalyticsTrackingId/ua-133772483-2
We now see some interesting results.


community.riskiq.com/search/trackers/GoogleAnalyticsTrackingId/ua-133772483-2
RISKIQ
ua-133772483-2
Tours
Enterprise
v5.0.0-3d1342d © 2019, RiskIQ Inc. All Rights Reserved. Proprietary and confidential; do not distribute without prior approval.
Privacy Policy
Terms and Conditions
RISKIQ
Legitimate Websites
Potential Fraudulent Websites

ua-133772483-2 (GoogleAnalyticsTrackingId)

Tracker Search: Hosts 6 · Tracker Search: IP Addresses 234

DATA

FILTERS

HOSTNAME (6 / 6)

voluntariosxve...	1
voluntariosxxv...	1
voluntarioven...	1
www.voluntari...	1
www.voluntari...	1

Show More

TAG

SYSTEM TAG

TRACKER SEARCH

Show : 25 · 1-6 of 6 · Sort : Last Seen Descending · Total Records : 6 · Download · Copy

Hostname	First Seen	Last Seen	Tags
voluntariosxvenezuela.com	2019-02-11	2019-07-14	
www.voluntariosxvenezuela.com	2019-02-10	2019-07-12	
voluntariosxxvenezuela.com	2019-02-21	2019-02-21	
www.voluntariosxxvenezuela.com	2019-02-21	2019-02-21	
voluntariovenezuela.com	2019-02-14	2019-02-14	
www.voluntariovenezuela.com	2019-02-14	2019-02-14	

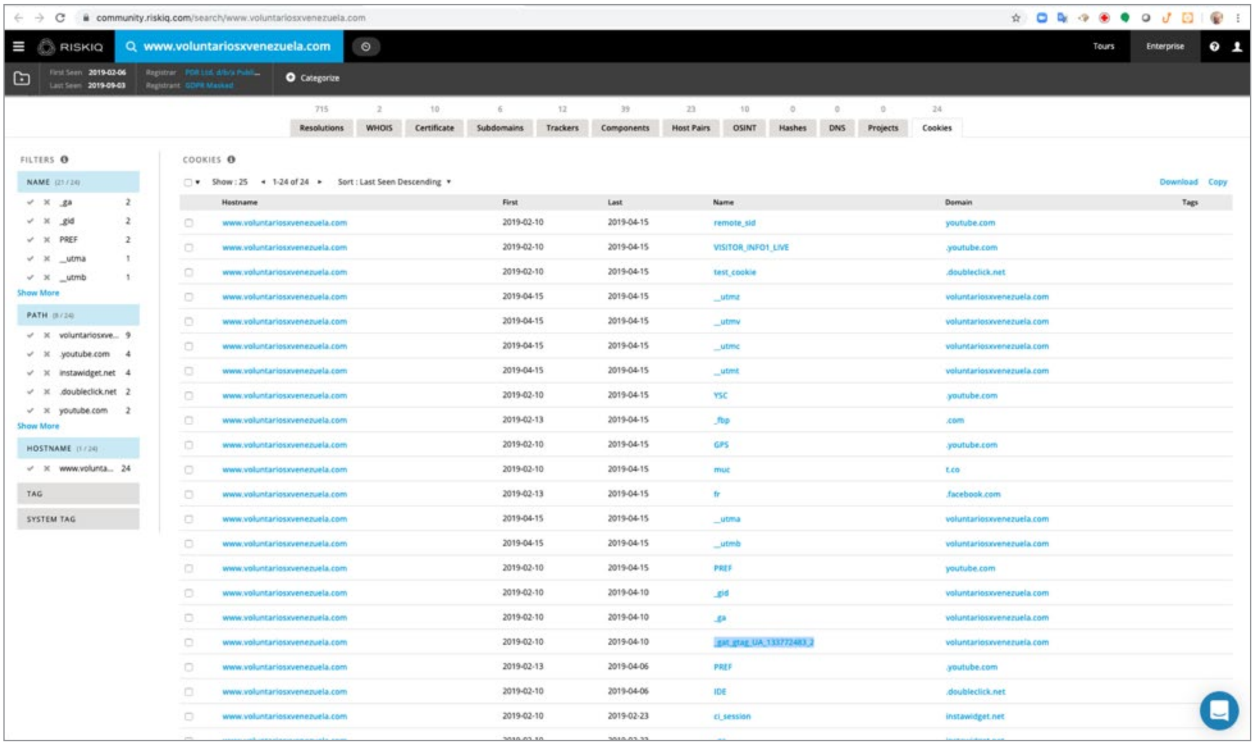
1-6 of 6

voluntariosxvenexuela[.]com and www[.]voluntariosxvenexuela[.]com is using Google Analytics Tracking Id as expected. But four different websites now appear to be using the same Google Analytics tracking id.

voluntariosxxvenzuela[.]com, www[.]voluntariosxxvenzuela[.]com, voluntariovenezuela[.]com, and www.voluntariovenezuela[.]com

Step 9: Now go back to the previous tab for www[.]voluntariosxvenezuela[.]com and click on the cookies tab

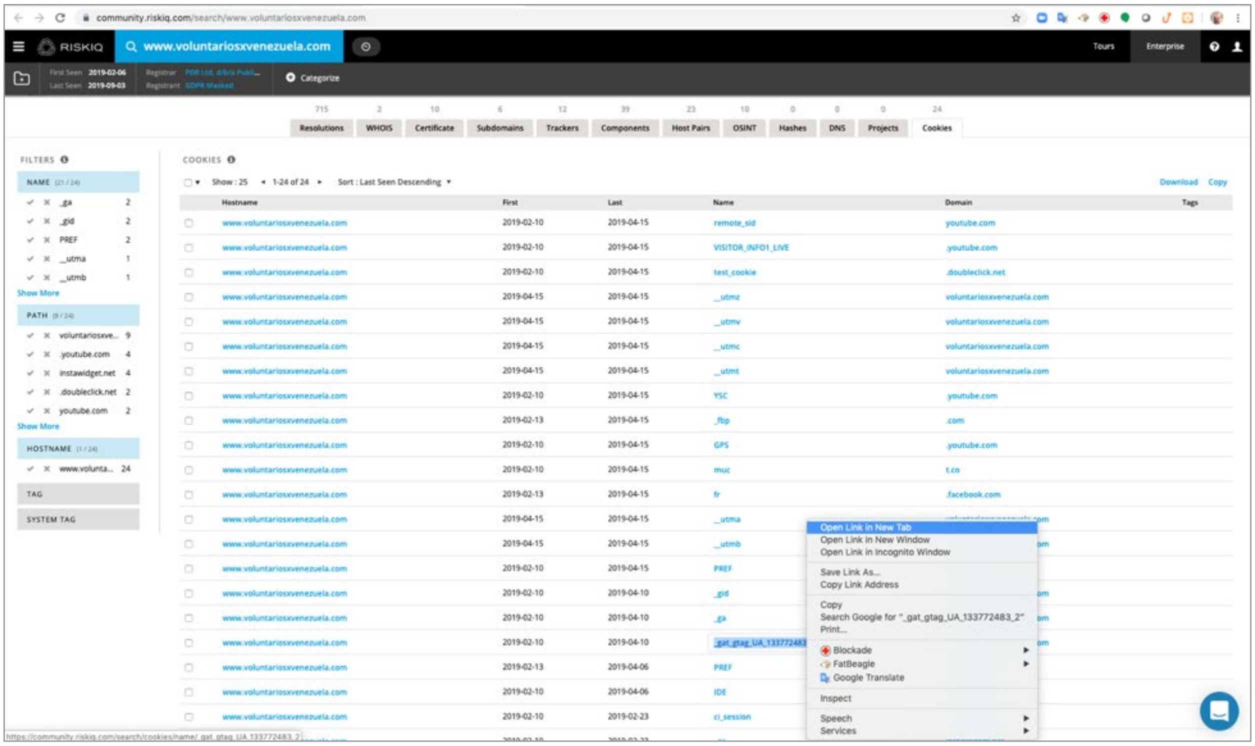
https://community.riskiq.com/search/www.voluntariosxvenezuela.com



Hostname	First	Last	Name	Domain	Tags
www.voluntariosxvenezuela.com	2019-02-10	2019-04-15	remote_sid	youtube.com	
www.voluntariosxvenezuela.com	2019-02-10	2019-04-15	VISITOR_INFO1_LIVE	.youtube.com	
www.voluntariosxvenezuela.com	2019-02-10	2019-04-15	test_cookie	.doubleclick.net	
www.voluntariosxvenezuela.com	2019-04-15	2019-04-15	__utmz	voluntariosxvenezuela.com	
www.voluntariosxvenezuela.com	2019-04-15	2019-04-15	__utmv	voluntariosxvenezuela.com	
www.voluntariosxvenezuela.com	2019-04-15	2019-04-15	__utmc	voluntariosxvenezuela.com	
www.voluntariosxvenezuela.com	2019-04-15	2019-04-15	__utmt	voluntariosxvenezuela.com	
www.voluntariosxvenezuela.com	2019-02-10	2019-04-15	YSC	.youtube.com	
www.voluntariosxvenezuela.com	2019-02-13	2019-04-15	_fbp	.com	
www.voluntariosxvenezuela.com	2019-02-10	2019-04-15	GPS	.youtube.com	
www.voluntariosxvenezuela.com	2019-02-10	2019-04-15	muc	t.co	
www.voluntariosxvenezuela.com	2019-02-13	2019-04-15	fr	.facebook.com	
www.voluntariosxvenezuela.com	2019-04-15	2019-04-15	__utma	voluntariosxvenezuela.com	
www.voluntariosxvenezuela.com	2019-04-15	2019-04-15	__utmb	voluntariosxvenezuela.com	
www.voluntariosxvenezuela.com	2019-02-10	2019-04-15	PREF	youtube.com	
www.voluntariosxvenezuela.com	2019-02-10	2019-04-10	_gid	voluntariosxvenezuela.com	
www.voluntariosxvenezuela.com	2019-02-10	2019-04-10	_ga	voluntariosxvenezuela.com	
www.voluntariosxvenezuela.com	2019-02-10	2019-04-10	_gat_gtag_UA_133772483_2	voluntariosxvenezuela.com	
www.voluntariosxvenezuela.com	2019-02-13	2019-04-06	PREF	.youtube.com	
www.voluntariosxvenezuela.com	2019-02-10	2019-04-06	IDE	.doubleclick.net	
www.voluntariosxvenezuela.com	2019-02-10	2019-02-23	ci_session	instawidget.net	

Here we see just one cookie name that appears to be unique associated with legitimate domain voluntariosxvenezuela[.]com.

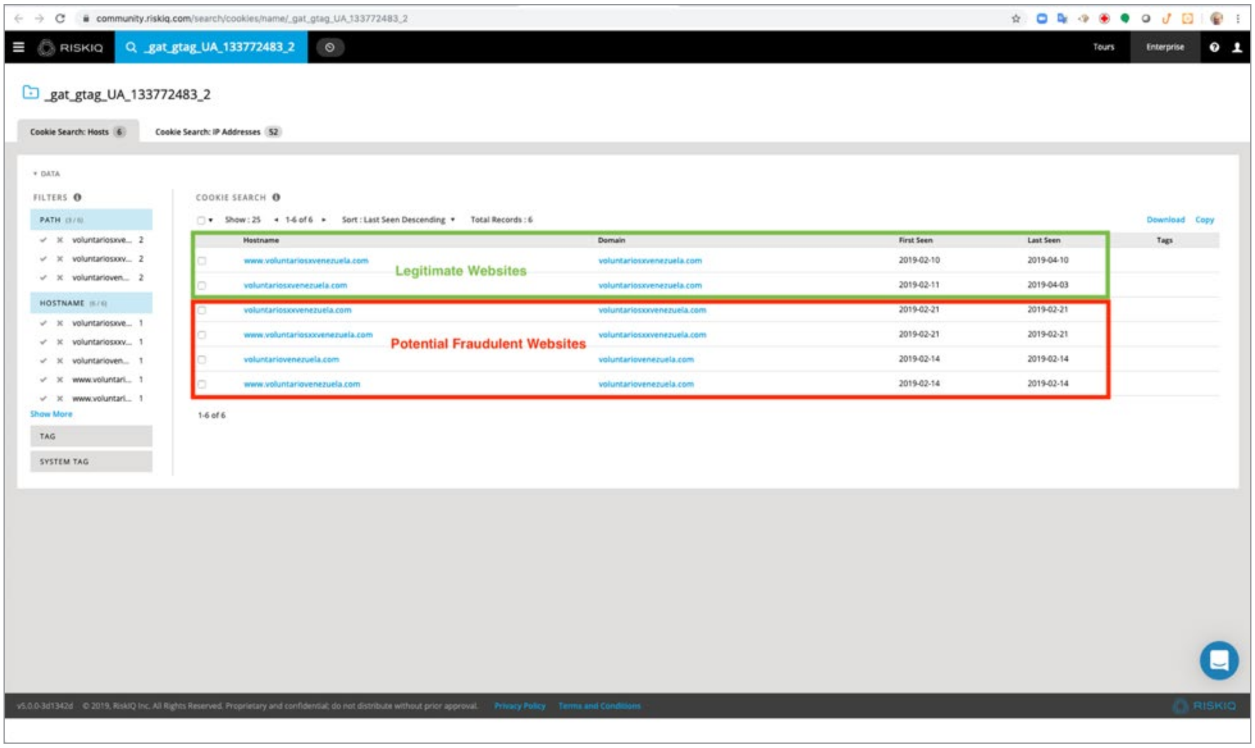
Step 10: Pivot search on the cookie name _gat_gtag_UA_133772483_2



Hostname	First	Last	Name	Domain	Tags
www.voluntariosxvenezuela.com	2019-02-10	2019-04-15	remote_sid	youtube.com	
www.voluntariosxvenezuela.com	2019-02-10	2019-04-15	VISITOR_INFO1_LIVE	.youtube.com	
www.voluntariosxvenezuela.com	2019-02-10	2019-04-15	test_cookie	.doubleclick.net	
www.voluntariosxvenezuela.com	2019-04-15	2019-04-15	__utmz	voluntariosxvenezuela.com	
www.voluntariosxvenezuela.com	2019-04-15	2019-04-15	__utmv	voluntariosxvenezuela.com	
www.voluntariosxvenezuela.com	2019-04-15	2019-04-15	__utmc	voluntariosxvenezuela.com	
www.voluntariosxvenezuela.com	2019-04-15	2019-04-15	__utmt	voluntariosxvenezuela.com	
www.voluntariosxvenezuela.com	2019-02-10	2019-04-15	YSC	.youtube.com	
www.voluntariosxvenezuela.com	2019-02-13	2019-04-15	_fbp	.com	
www.voluntariosxvenezuela.com	2019-02-10	2019-04-15	GPS	.youtube.com	
www.voluntariosxvenezuela.com	2019-02-10	2019-04-15	muc	t.co	
www.voluntariosxvenezuela.com	2019-02-13	2019-04-15	fr	.facebook.com	
www.voluntariosxvenezuela.com	2019-04-15	2019-04-15	__utma	om	
www.voluntariosxvenezuela.com	2019-04-15	2019-04-15	__utmb	om	
www.voluntariosxvenezuela.com	2019-02-10	2019-04-15	PREF		
www.voluntariosxvenezuela.com	2019-02-10	2019-04-10	_gid	om	
www.voluntariosxvenezuela.com	2019-02-10	2019-04-10	_ga	om	
www.voluntariosxvenezuela.com	2019-02-10	2019-04-10	_gat_gtag_UA_133772483	om	
www.voluntariosxvenezuela.com	2019-02-13	2019-04-06	PREF		
www.voluntariosxvenezuela.com	2019-02-10	2019-04-06	IDE		
www.voluntariosxvenezuela.com	2019-02-10	2019-02-23	ci_session		

Right-click on the cookie name _gat_gtag_UA_133772483_2 and open the link in a new tab.

https://community.riskiq.com/search/cookies/name/_gat_gtag_UA_133772483_2



Hostname	Domain	First Seen	Last Seen	Tags
www.voluntariosxvenezuela.com	voluntariosxvenezuela.com	2019-02-10	2019-04-10	
voluntariosxvenezuela.com	voluntariosxvenezuela.com	2019-02-11	2019-04-03	
voluntariosxxvenezuela.com	voluntariosxxvenezuela.com	2019-02-21	2019-02-21	
www.voluntariosxxvenezuela.com	voluntariosxxvenezuela.com	2019-02-21	2019-02-21	
voluntariovenezuela.com	voluntariovenezuela.com	2019-02-14	2019-02-14	
www.voluntariovenezuela.com	voluntariovenezuela.com	2019-02-14	2019-02-14	

Now we see the two hosts using a cookie from the legitimate domain voluntariosxvenezuela.com (in green). We also see four different hostnames pointing to two different potential fraudulent domains. voluntariosxxvenzuela[.]com, www[.]voluntariosxxvenzuela[.]com, voluntariovenezuela[.]com, and www.voluntariovenezuela[.]com. These are the same domains that were also using the legitimate domain's Google Analytics Tracking Id.

Step 11: Investigating the domains utilizing web crawl data

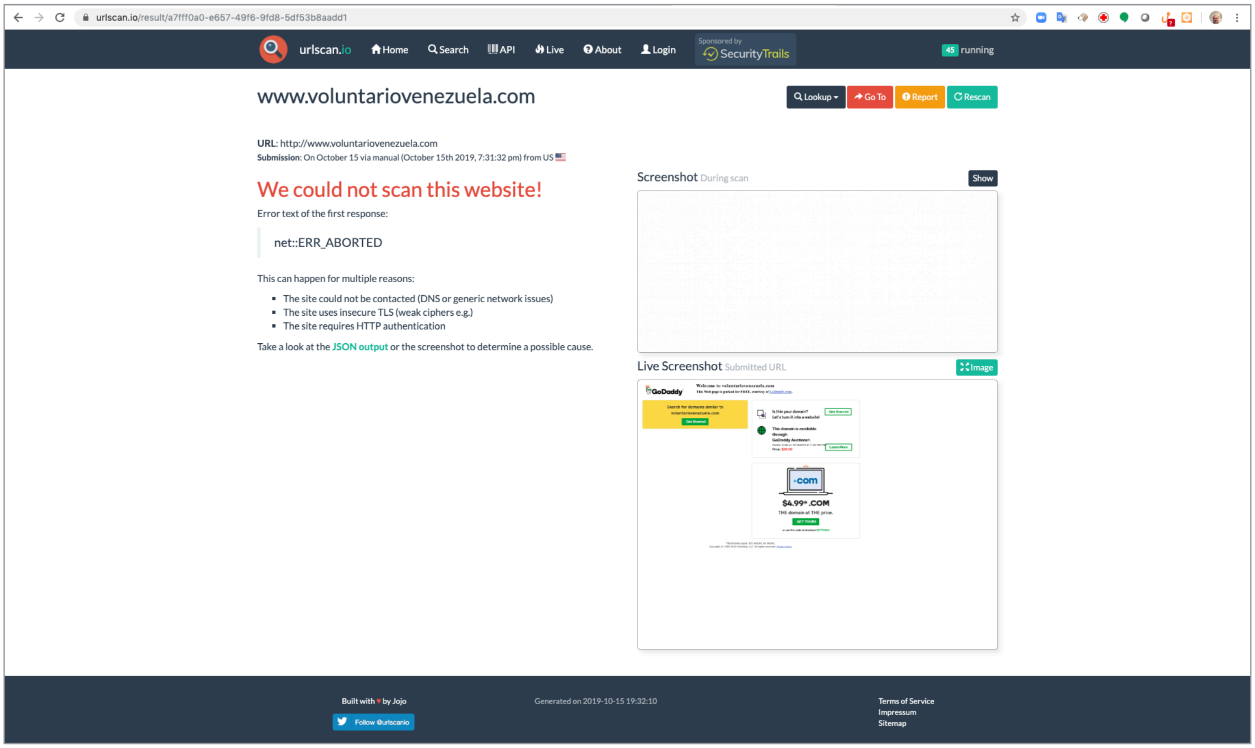
Now we will examine the legitimate and potential fraudulent domains to see how the websites appear now and back in February 2019.

It is important not to directly visit the websites you are investigating. The websites might contain malware, or the threat actors could be monitoring who is visiting the website. Also, the threat actor might be filtering traffic, to block traffic from the attacked domain or it could look different from the organization.

The attack happened back in February 2019 so the websites might not be up anymore. We will now do a web crawl of one of the fraudulent domains.

In a new tab go to https://urlscan.io

In the search field search for the domain www[.]voluntariovenezuela[.]com


urlscan.io/result/a7fff0a0-e657-49f6-9fd8-5df53b8aadd1
urlscan.io
Home
Search
API
Live
About
Login
Sponsored by
SecurityTrails
45 running
Lookup
Go To
Report
Rescan
Show
Image
GoDaddy
Welcome to voluntariovenezuela.com
This Web page is parked for FREE, courtesy of GoDaddy.com.
Search for domains similar to voluntariovenezuela.com
Get Started
Is this your domain? Let's turn it into a website!
This domain is available through GoDaddy Auctions®.
Learn More
.com
$4.99* .COM
THE domain at THE price.
GET YOURS
Built with ♥ by Jojo
Follow @urlscanio
Terms of Service
Impressum
Sitemap

www.voluntariovenezuela.com

URL: http://www.voluntariovenezuela.com
Submission: On October 15 via manual (October 15th 2019, 7:31:32 pm) from US

We could not scan this website!

Error text of the first response:

> net::ERR_ABORTED

This can happen for multiple reasons:

- The site could not be contacted (DNS or generic network issues)
- The site uses insecure TLS (weak ciphers e.g.)
- The site requires HTTP authentication

Take a look at the JSON output or the screenshot to determine a possible cause.

Screenshot During scan

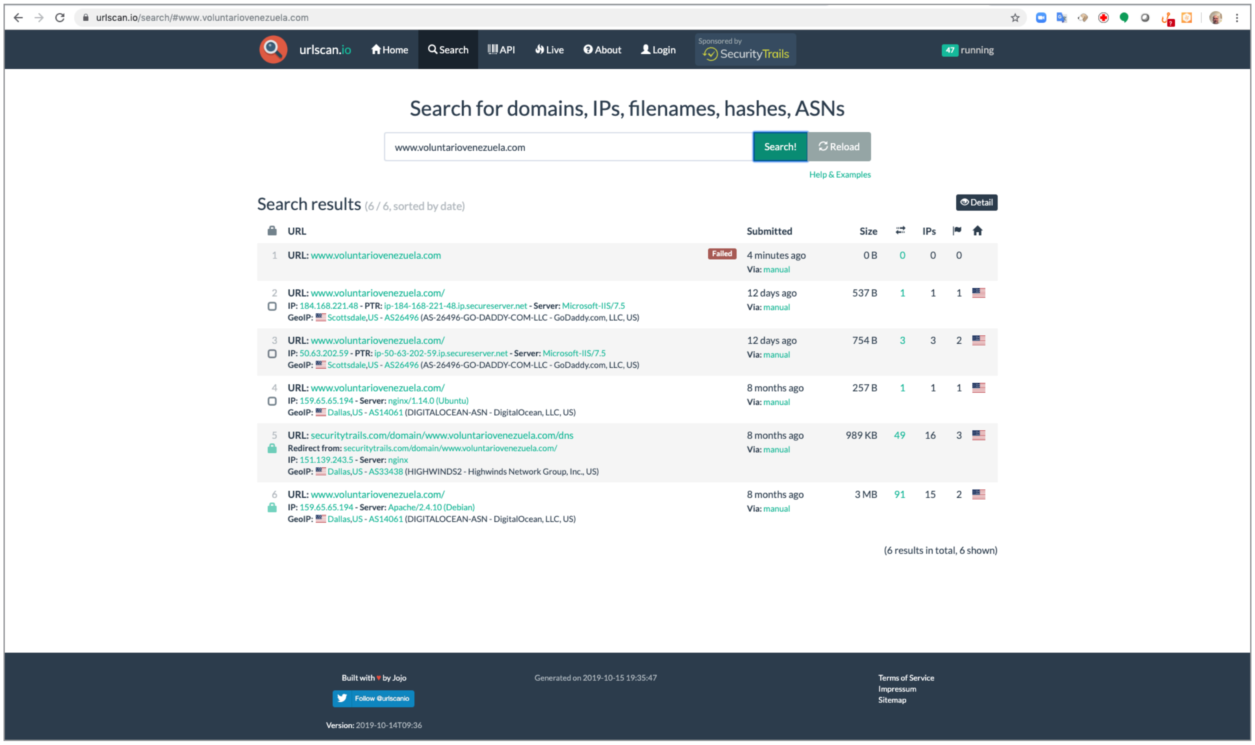
Live Screenshot Submitted URL

Generated on 2019-10-15 19:32:10

This website does not seem to be infringing at this time. Now let us search for any results in the base back in February 2019.

Step 12: Using urlscan.io look for any previous crawls for the domain www[.]voluntariovenezuela[.]com

Click on search in the title bar and search for www[.]voluntariovenezuela[.]com



Search for domains, IPs, filenames, hashes, ASNs

www.voluntariovenezuela.com

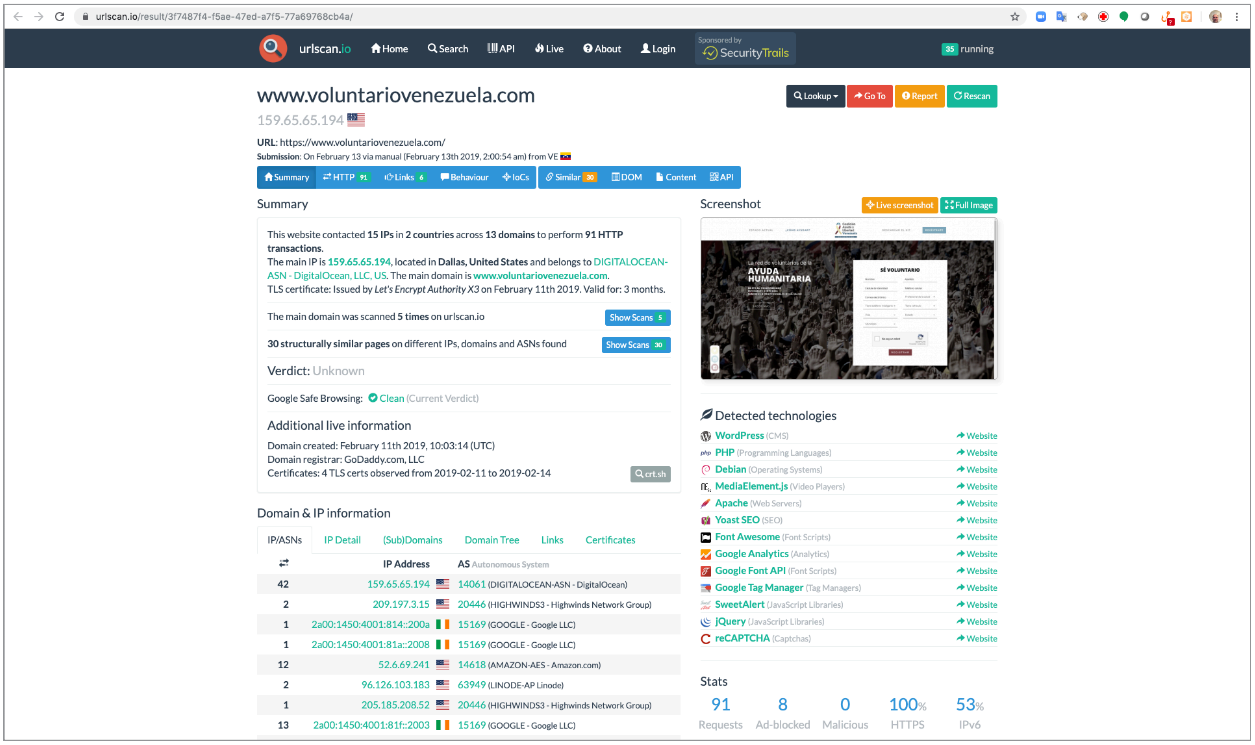
Search results (6 / 6, sorted by date)

	URL	Submitted	Size	⇄	IPs	⚑	⌂
1	URL: www.voluntariovenezuela.com	4 minutes ago Via: manual	0 B	0	0	0	
2	URL: www.voluntariovenezuela.com/ IP: 184.168.221.48 - PTR: ip-184-168-221-48.ip.secureserver.net - Server: Microsoft-IIS/7.5 GeoIP: Scottsdale,US - AS26496 (AS-26496-GO-DADDY-COM-LLC - GoDaddy.com, LLC, US)	12 days ago Via: manual	537 B	1	1	1	
3	URL: www.voluntariovenezuela.com/ IP: 50.63.202.59 - PTR: ip-50-63-202-59.ip.secureserver.net - Server: Microsoft-IIS/7.5 GeoIP: Scottsdale,US - AS26496 (AS-26496-GO-DADDY-COM-LLC - GoDaddy.com, LLC, US)	12 days ago Via: manual	754 B	3	3	2	
4	URL: www.voluntariovenezuela.com/ IP: 159.65.65.194 - Server: nginx/1.14.0 (Ubuntu) GeoIP: Dallas,US - AS14061 (DIGITALOCEAN-ASN - DigitalOcean, LLC, US)	8 months ago Via: manual	257 B	1	1	1	
5	URL: securitytrails.com/domain/www.voluntariovenezuela.com/dns Redirect from: securitytrails.com/domain/www.voluntariovenezuela.com/ IP: 151.139.243.5 - Server: nginx GeoIP: Dallas,US - AS33438 (HIGHWINDS2 - Highwinds Network Group, Inc., US)	8 months ago Via: manual	989 KB	49	16	3	
6	URL: www.voluntariovenezuela.com/ IP: 159.65.65.194 - Server: Apache/2.4.10 (Debian) GeoIP: Dallas,US - AS14061 (DIGITALOCEAN-ASN - DigitalOcean, LLC, US)	8 months ago Via: manual	3 MB	91	15	2	

(6 results in total, 6 shown)

Built with ♥ by Jojo
Follow @urlscanio
Version: 2019-10-14T09:36
Generated on 2019-10-15 19:35:47
Terms of Service
Impressum
Sitemap

Click on the last result about 8 months ago.



www.voluntariovenezuela.com

159.65.65.194

URL: https://www.voluntariovenezuela.com/
Submission: On February 13 via manual (February 13th 2019, 2:00:54 am) from VE

Summary

This website contacted **15 IPs** in **2 countries** across **13 domains** to perform **91 HTTP transactions**.
The main IP is **159.65.65.194**, located in **Dallas, United States** and belongs to DIGITALOCEAN-ASN - DigitalOcean, LLC, US. The main domain is **www.voluntariovenezuela.com**.
TLS certificate: Issued by *Let's Encrypt Authority X3* on February 11th 2019. Valid for: 3 months.

The main domain was scanned **5 times** on urlscan.io

30 structurally similar pages on different IPs, domains and ASNs found

Verdict: Unknown

Google Safe Browsing: ✓ Clean (Current Verdict)

Additional live information

Domain created: February 11th 2019, 10:03:14 (UTC)
Domain registrar: GoDaddy.com, LLC
Certificates: 4 TLS certs observed from 2019-02-11 to 2019-02-14

Domain & IP information

IP/ASNs | IP Detail | (Sub)Domains | Domain Tree | Links | Certificates

⇄	IP Address	AS Autonomous System
42	159.65.65.194	14061 (DIGITALOCEAN-ASN - DigitalOcean)
2	209.197.3.15	20446 (HIGHWINDS3 - Highwinds Network Group)
1	2a00:1450:4001:814::200a	15169 (GOOGLE - Google LLC)
1	2a00:1450:4001:81a::2008	15169 (GOOGLE - Google LLC)
12	52.6.69.241	14618 (AMAZON-AES - Amazon.com)
2	96.126.103.183	63949 (LINODE-AP Linode)
1	205.185.208.52	20446 (HIGHWINDS3 - Highwinds Network Group)
13	2a00:1450:4001:81f::2003	15169 (GOOGLE - Google LLC)

Screenshot

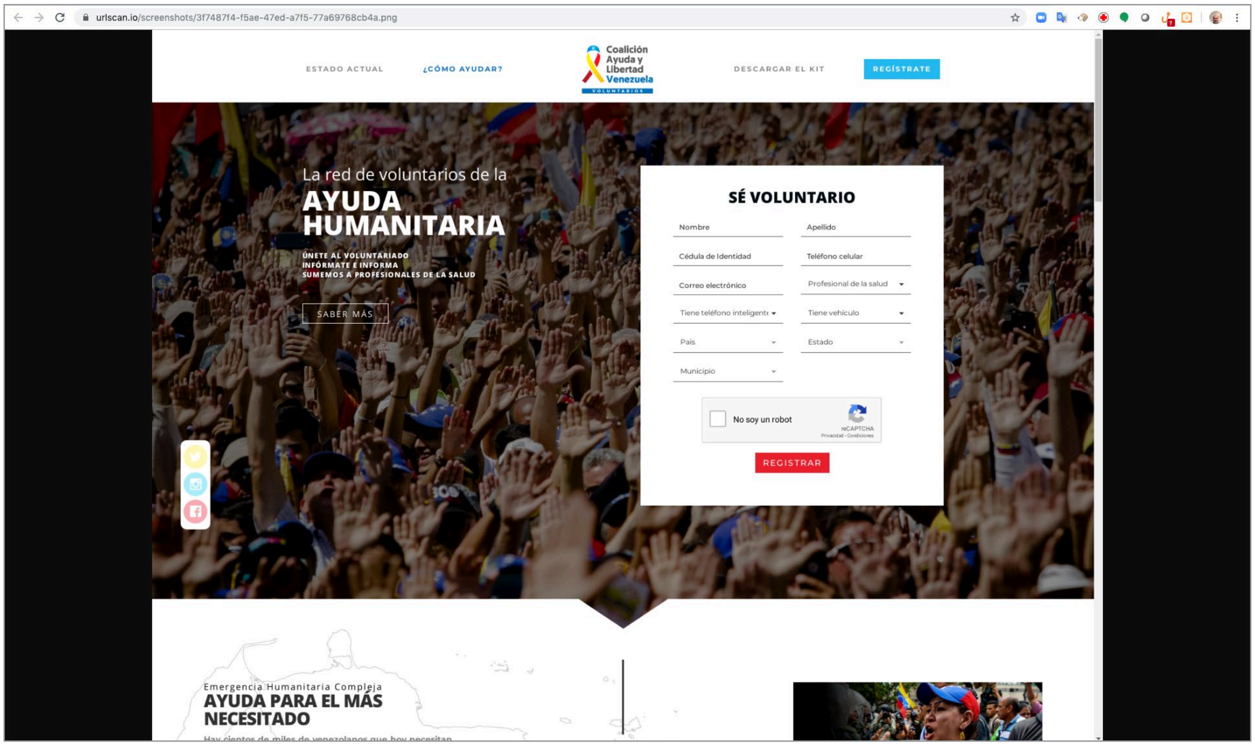
Detected technologies

WordPress (CMS)	Website
PHP (Programming Languages)	Website
Debian (Operating Systems)	Website
MediaElement.js (Video Players)	Website
Apache (Web Servers)	Website
Yoast SEO (SEO)	Website
Font Awesome (Font Scripts)	Website
Google Analytics (Analytics)	Website
Google Font API (Font Scripts)	Website
Google Tag Manager (Tag Managers)	Website
SweetAlert (JavaScript Libraries)	Website
jQuery (JavaScript Libraries)	Website
reCAPTCHA (Captchas)	Website

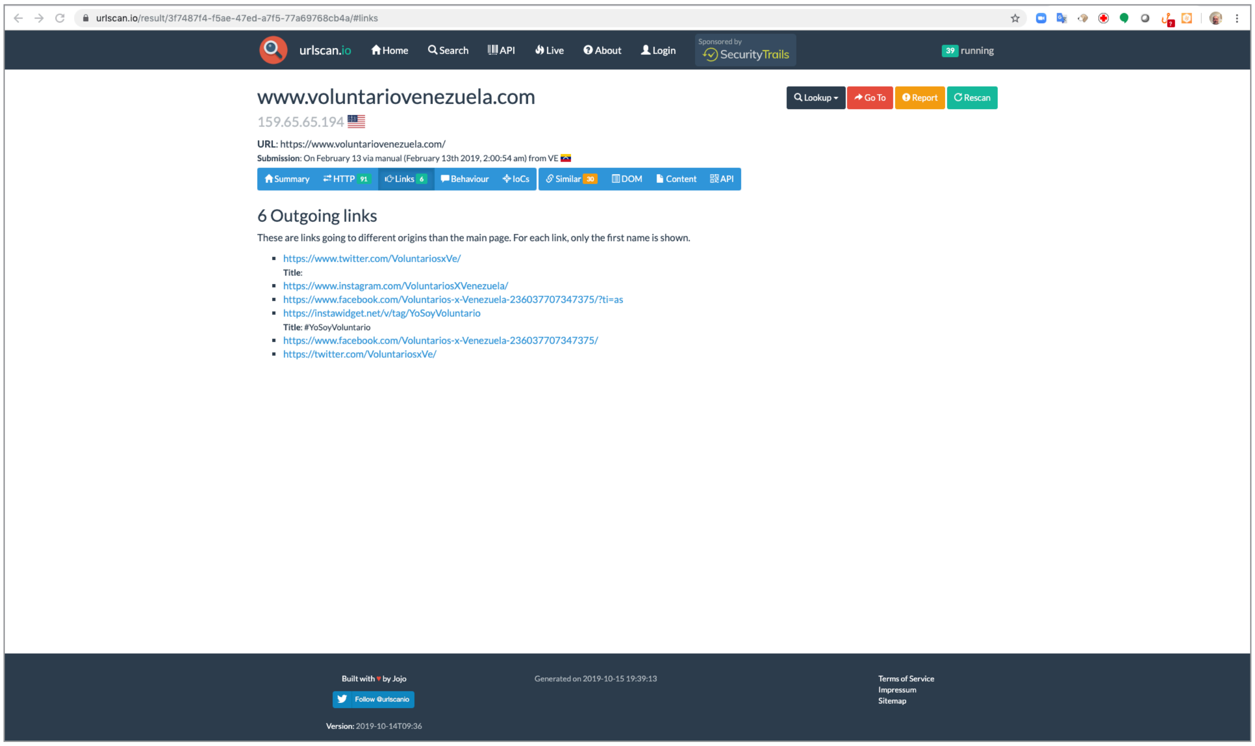
Stats

91	8	0	100%	53%
Requests	Ad-blocked	Malicious	HTTPS	IPv6

Here we see that the domain www[.]voluntariovenezuela[.]com was infringing on the real domain www[.]voluntariosxvenezuela[.]com.



If you click on the Links section.



www.voluntariovenezuela.com

159.65.65.194

URL: https://www.voluntariovenezuela.com/

Submission: On February 13 via manual (February 13th 2019, 2:00:54 am) from VE

6 Outgoing links

These are links going to different origins than the main page. For each link, only the first name is shown.

- https://www.twitter.com/VoluntariosxVe/
  Title:
- https://www.instagram.com/VoluntariosXVenezuela/
- https://www.facebook.com/Voluntarios-x-Venezuela-236037707347375/?ti=as
- https://instawidget.net/v/tag/YoSoyVoluntario
  Title: #YoSoyVoluntario
- https://www.facebook.com/Voluntarios-x-Venezuela-236037707347375/
- https://twitter.com/VoluntariosxVe/

Built with ♥ by Jojo

Follow @urlscanio

Version: 2019-10-14T09:36

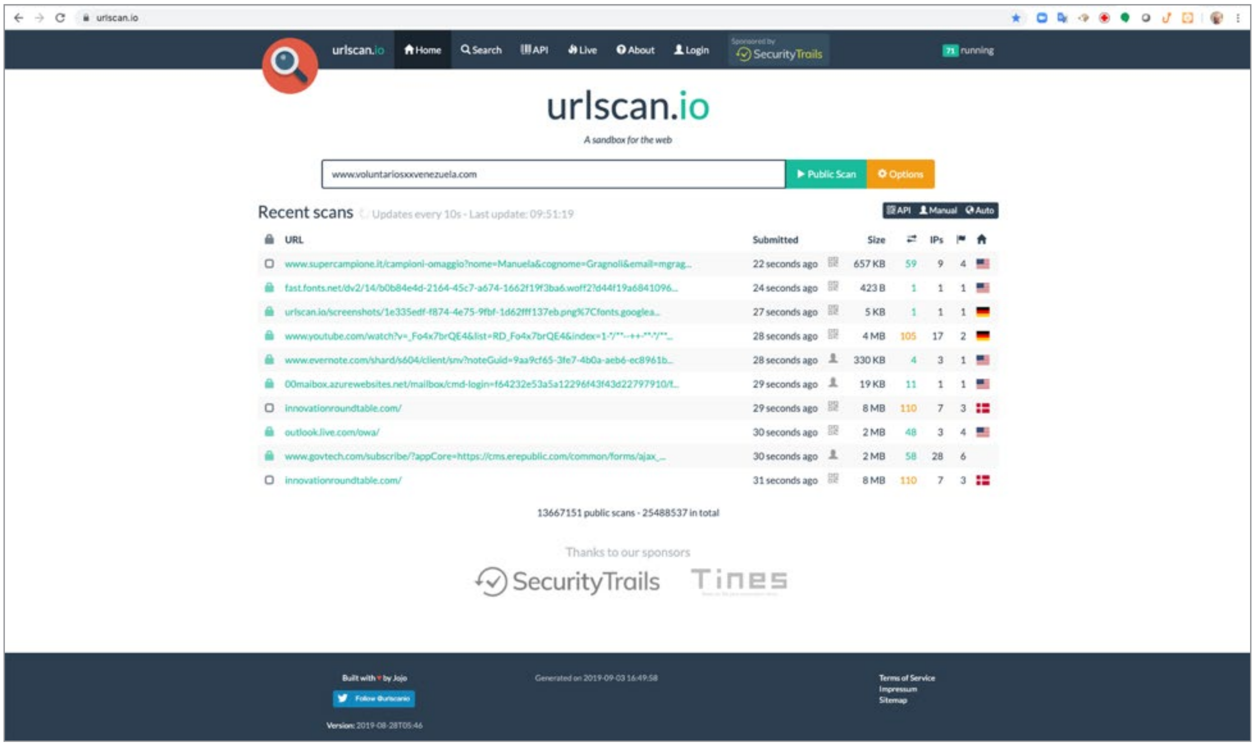
Generated on 2019-10-15 19:39:13

Terms of Service
Impressum
Sitemap

You can see that the fake www[.]voluntarovenzuela[.]com domain is linking to the real domain voluntariosxvenezuela twitter, instragram, and facebook accounts.

Step 13: Using urlscan.io for the domain www[.]voluntariosxxvenezuela[.]com

Do a public scan for www[.]voluntariosxxvenezuela[.]com



urlscan.io

www.voluntariosxxvenezuela.com

Recent scans Updates every 10s - Last update: 09:51:19

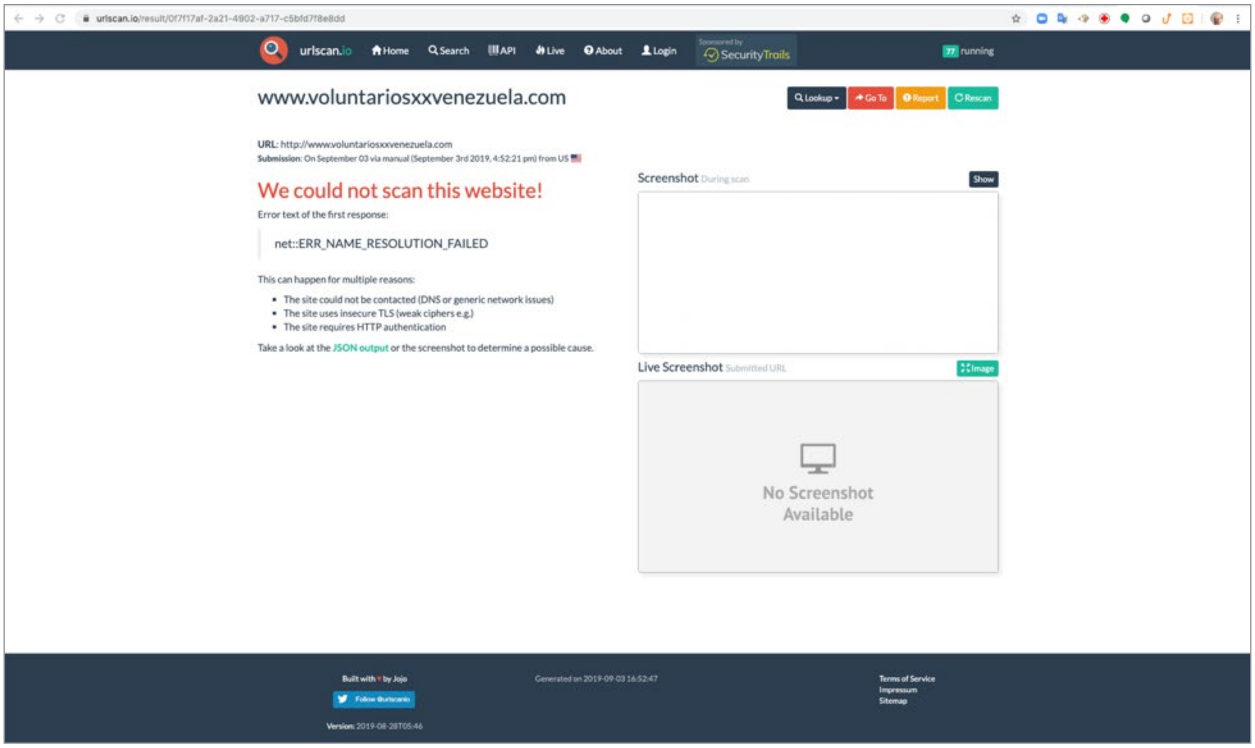
	URL	Submitted		Size	⇄	IPs	⚑	🏠
□	www.supercampione.it/campioni-omaggio?nome=Manuela&cognome=Gragnoli&email=mgrag...	22 seconds ago		657 KB	59	9	4	🇺🇸
🔒	fast.fonts.net/dv2/14/b0b84e4d-2164-45c7-a674-1662f19f3ba6.woff2?d44f19a6841096...	24 seconds ago		423 B	1	1	1	🇺🇸
🔒	urlscan.io/screenshots/1e335edf-f874-4e75-9fbf-1d62fff137eb.png%7Cfonts.googlea...	27 seconds ago		5 KB	1	1	1	🇩🇪
🔒	www.youtube.com/watch?v=_Fo4x7brQE4&list=RD_Fo4x7brQE4&index=1-'/""--++-""-'/""...	28 seconds ago		4 MB	105	17	2	🇩🇪
🔒	www.evernote.com/shard/s604/client/snv?noteGuid=9aa9cf65-3fe7-4b0a-aeb6-ec8961b...	28 seconds ago	👤	330 KB	4	3	1	🇺🇸
🔒	00maibox.azurewebsites.net/mailbox/cmd-login=f64232e53a5a12296f43f43d22797910/f...	29 seconds ago	👤	19 KB	11	1	1	🇺🇸
□	innovationroundtable.com/	29 seconds ago		8 MB	110	7	3	🇩🇰
🔒	outlook.live.com/owa/	30 seconds ago		2 MB	48	3	4	🇺🇸
🔒	www.govtech.com/subscribe/?appCore=https://cms.erepublic.com/common/forms/ajax_...	30 seconds ago	👤	2 MB	58	28	6	
□	innovationroundtable.com/	31 seconds ago		8 MB	110	7	3	🇩🇰

13667151 public scans - 25488537 in total

Built with ♥ by Jojo

Generated on 2019-09-03 16:49:58

Version: 2019-08-28T05:46



urlscan.io/result/0f7f17af-2a21-4902-a717-c5bfd7f8e8dd

www.voluntariosxxvenezuela.com

URL: http://www.voluntariosxxvenezuela.com
Submission: On September 03 via manual (September 3rd 2019, 4:52:21 pm) from US 🇺🇸

We could not scan this website!

Error text of the first response:

```
net::ERR_NAME_RESOLUTION_FAILED
```

This can happen for multiple reasons:

- The site could not be contacted (DNS or generic network issues)
- The site uses insecure TLS (weak ciphers e.g.)
- The site requires HTTP authentication

Take a look at the JSON output or the screenshot to determine a possible cause.

Built with ♥ by Jojo

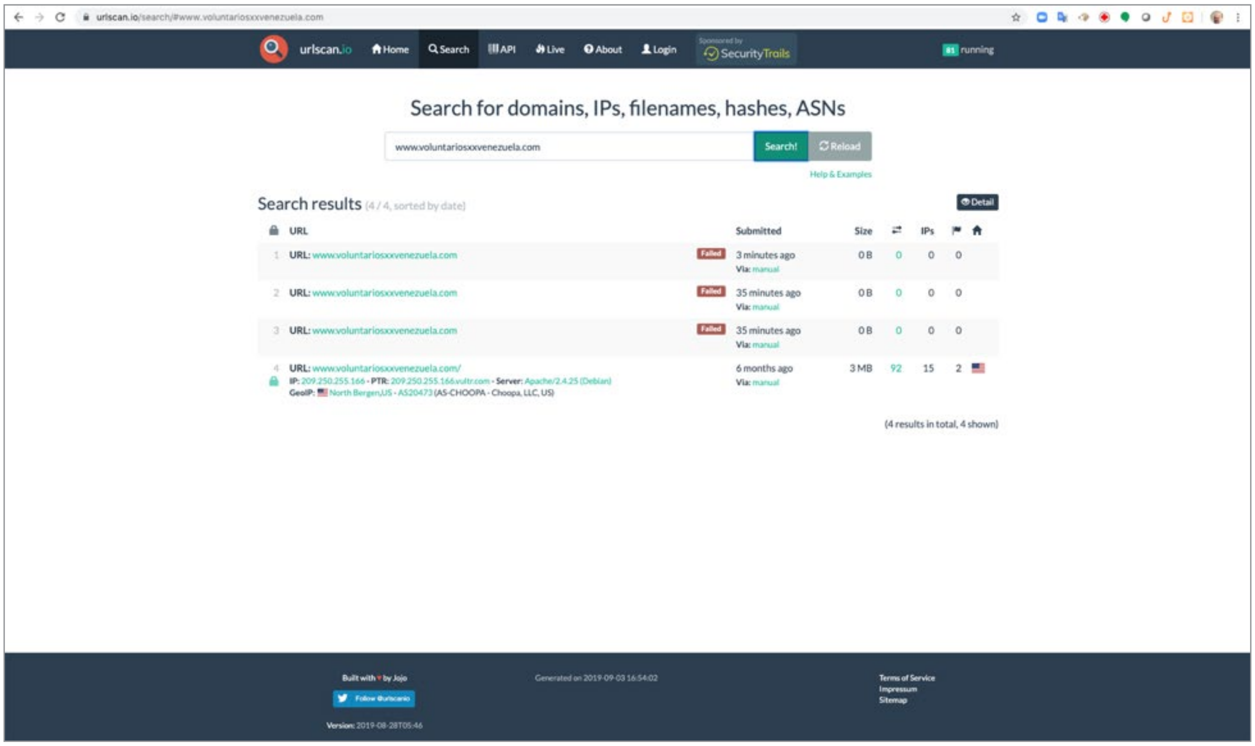
Generated on 2019-09-03 16:52:47

Version: 2019-08-28T05:46

The results come back as failed.

Step 14: Using urlscan.io look for any previous crawls for the domain www[.]voluntariosxxvenezuela[.]com (potential fraudulent domain)

Click on search in the title bar and search for www[.]voluntariosxxvenezuela[.]com



Search for domains, IPs, filenames, hashes, ASNs

www.voluntariosxxvenezuela.com

Search results (4 / 4, sorted by date)

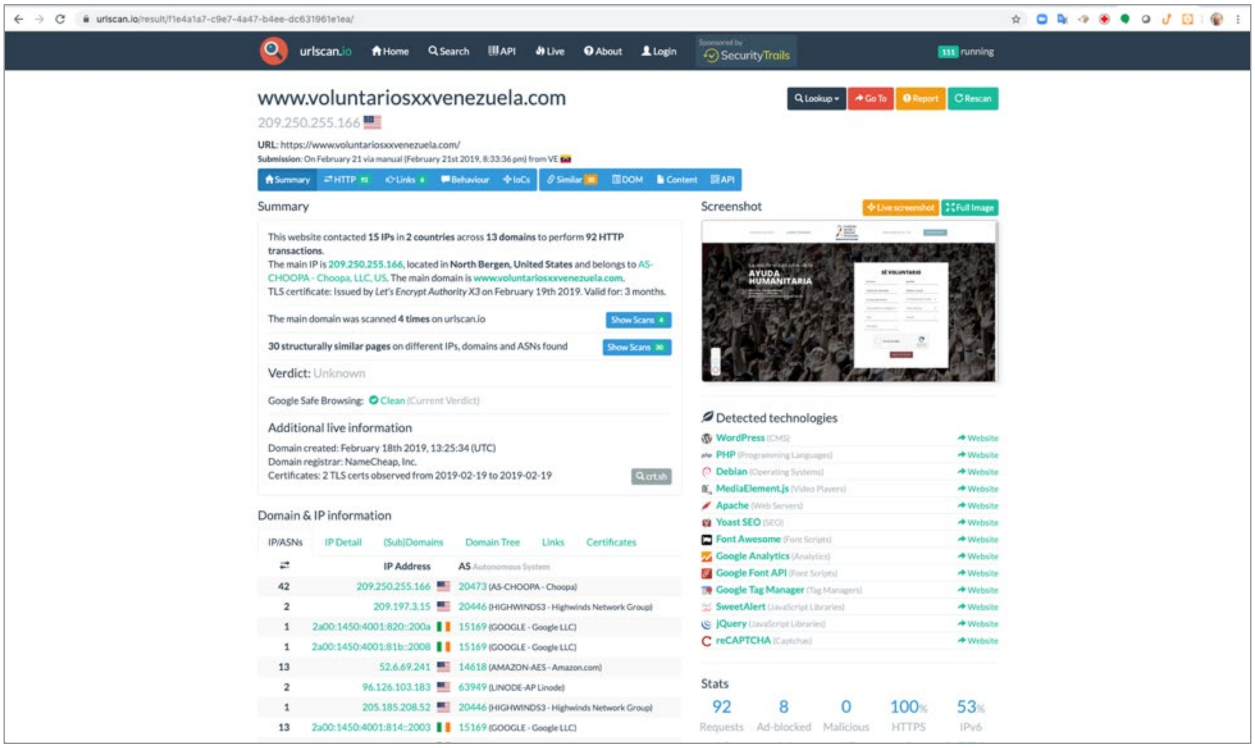
	URL		Submitted	Size	⇄	IPs	⚑	🏠
1	URL: www.voluntariosxxvenezuela.com	Failed	3 minutes ago Via: manual	0 B	0	0	0	
2	URL: www.voluntariosxxvenezuela.com	Failed	35 minutes ago Via: manual	0 B	0	0	0	
3	URL: www.voluntariosxxvenezuela.com	Failed	35 minutes ago Via: manual	0 B	0	0	0	
4	URL: www.voluntariosxxvenezuela.com/ IP: 209.250.255.166 - PTR: 209.250.255.166.vultr.com - Server: Apache/2.4.25 (Debian) GeoIP: North Bergen,US - AS20473 (AS-CHOOPA - Choopa, LLC, US)		6 months ago Via: manual	3 MB	92	15	2	

(4 results in total, 4 shown)

Generated on 2019-09-03 16:54:02

Version: 2019-08-28T05:46

In the result click on the item that did not fail over 6 months ago that has the IP address 209[.]250[.]255[.]166.



www.voluntariosxxvenezuela.com

209.250.255.166

URL: https://www.voluntariosxxvenezuela.com/

Submission: On February 21 via manual (February 21st 2019, 8:33:36 pm) from VE

Summary

This website contacted **15 IPs** in **2 countries** across **13 domains** to perform **92 HTTP transactions**.
The main IP is 209.250.255.166, located in **North Bergen, United States** and belongs to AS-CHOOPA - Choopa, LLC, US. The main domain is www.voluntariosxxvenezuela.com.
TLS certificate: Issued by *Let's Encrypt Authority X3* on February 19th 2019. Valid for: 3 months.

The main domain was scanned **4 times** on urlscan.io

30 structurally similar pages on different IPs, domains and ASNs found

Verdict: Unknown

Google Safe Browsing: Clean (Current Verdict)

Additional live information

Domain created: February 18th 2019, 13:25:34 (UTC)
Domain registrar: NameCheap, Inc.
Certificates: 2 TLS certs observed from 2019-02-19 to 2019-02-19

Domain & IP information

⇄	IP Address	AS Autonomous System
42	209.250.255.166	20473 (AS-CHOOPA - Choopa)
2	209.197.3.15	20446 (HIGHWINDS3 - Highwinds Network Group)
1	2a00:1450:4001:820::200a	15169 (GOOGLE - Google LLC)
1	2a00:1450:4001:81b::2008	15169 (GOOGLE - Google LLC)
13	52.6.69.241	14618 (AMAZON-AES - Amazon.com)
2	96.126.103.183	63949 (LINODE-AP Linode)
1	205.185.208.52	20446 (HIGHWINDS3 - Highwinds Network Group)
13	2a00:1450:4001:814::2003	15169 (GOOGLE - Google LLC)

Screenshot

Detected technologies

Technology	
WordPress (CMS)	Website
PHP (Programming Languages)	Website
Debian (Operating Systems)	Website
MediaElement.js (Video Players)	Website
Apache (Web Servers)	Website
Yoast SEO (SEO)	Website
Font Awesome (Font Scripts)	Website
Google Analytics (Analytics)	Website
Google Font API (Font Scripts)	Website
Google Tag Manager (Tag Managers)	Website
SweetAlert (JavaScript Libraries)	Website
jQuery (JavaScript Libraries)	Website
reCAPTCHA (Captchas)	Website

Stats

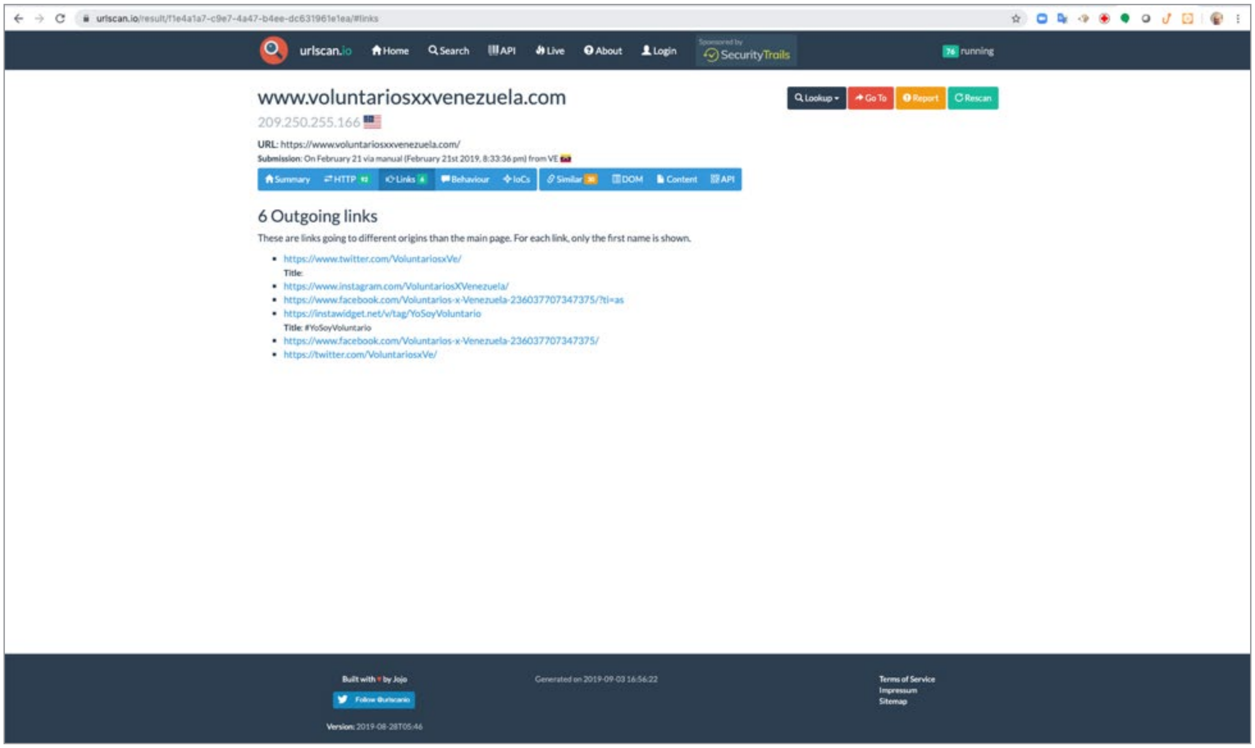
92	8	0	100%	53%
Requests	Ad-blocked	Malicious	HTTPS	IPv6

https://urlscan.io/result/f1e4a1a7-c9e7-4a47-b4ee-dc631961e1ea/

Now we see results from a previous web crawl during the time in question. We can also see a screenshot of the website and all of the information that was captured during that scan. This domain in the past appeared to have infringed against the legitimate domain.

Step 15: Click on the links tab.

https://urlscan.io/result/f1e4a1a7-c9e7-4a47-b4ee-dc631961e1ea/#links



www.voluntariosxxvenezuela.com

209.250.255.166

URL: https://www.voluntariosxxvenezuela.com/
Submission: On February 21 via manual (February 21st 2019, 8:33:36 pm) from VE

6 Outgoing links

These are links going to different origins than the main page. For each link, only the first name is shown.

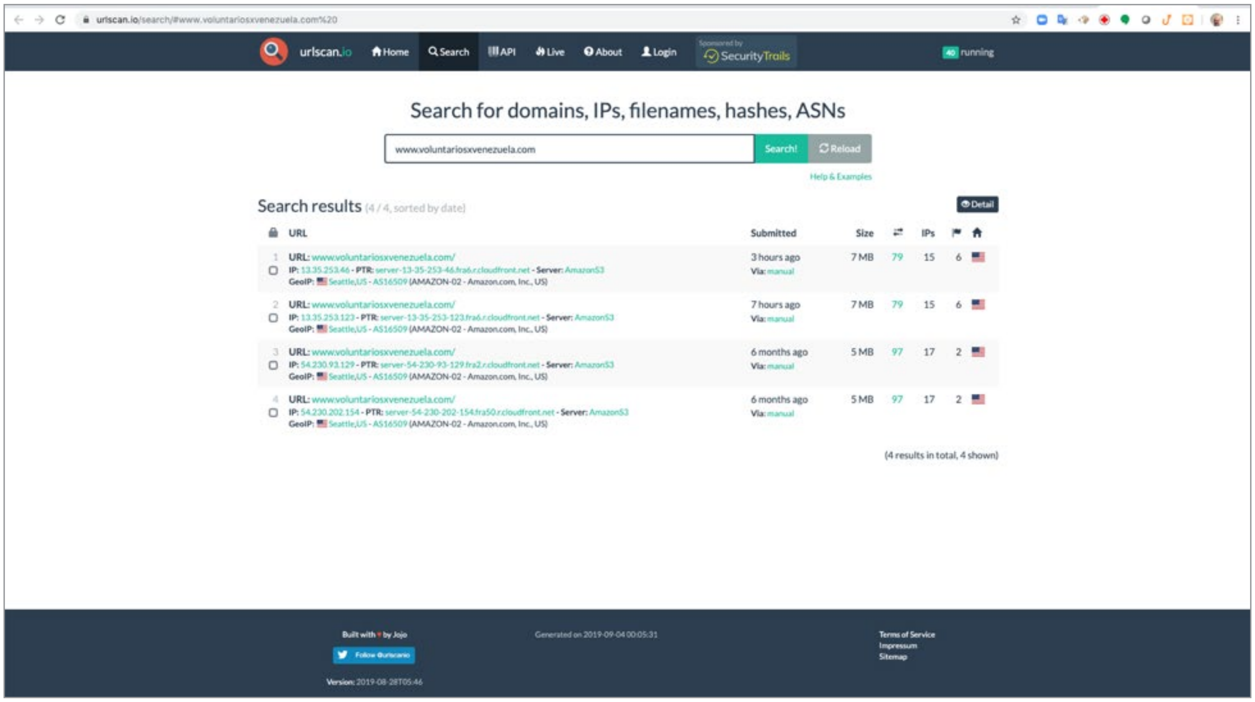
- https://www.twitter.com/VoluntariosxVe/
  Title:
- https://www.instagram.com/VoluntariosXVenezuela/
- https://www.facebook.com/Voluntarios-x-Venezuela-236037707347375/?ti=as
- https://instawidget.net/v/tag/YoSoyVoluntario
  Title: #YoSoyVoluntario
- https://www.facebook.com/Voluntarios-x-Venezuela-236037707347375/
- https://twitter.com/VoluntariosxVe/

Here we see that this potential fraudulent domain is linking to the legitimate Twitter, Instagram, and Facebook accounts. This information was gathered when urlscan.io previously visited the domain.

Step 16: In urlscan.io search for previous results for the legitimate domain www[.]voluntariosxvenezuela[.]com

Click on search in the title bar and search for www[.]voluntariosxvenezuela[.]com

https://urlscan.io/search/#www.voluntariosxvenezuela.com



Search for domains, IPs, filenames, hashes, ASNs

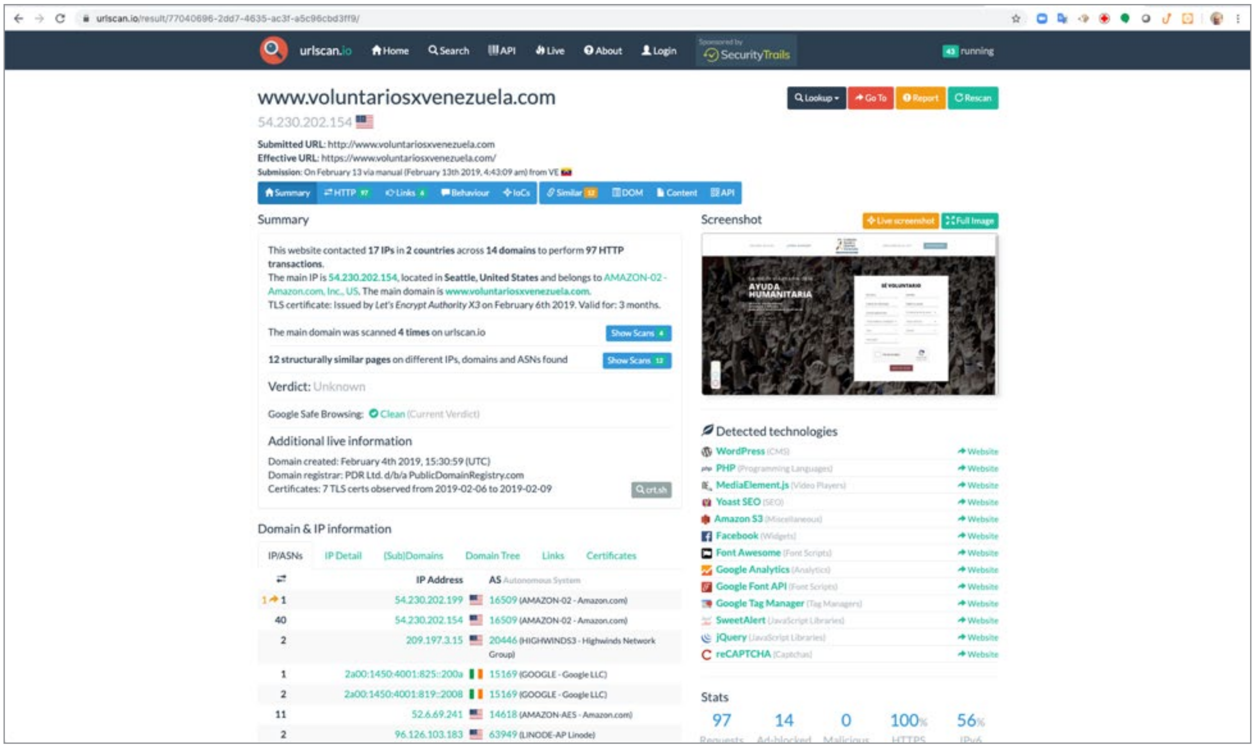
www.voluntariosxvenezuela.com

Search results (4 / 4, sorted by date)

	URL	Submitted	Size	⇄	IPs	⚑	⌂
1 □	**URL:** www.voluntariosxvenezuela.com/ **IP:** 13.35.253.46 - **PTR:** server-13-35-253-46.fra6.r.cloudfront.net - **Server:** AmazonS3 **GeoIP:** Seattle,US - AS16509 (AMAZON-02 - Amazon.com, Inc., US)	3 hours ago **Via:** manual	7 MB	79	15	6	
2 □	**URL:** www.voluntariosxvenezuela.com/ **IP:** 13.35.253.123 - **PTR:** server-13-35-253-123.fra6.r.cloudfront.net - **Server:** AmazonS3 **GeoIP:** Seattle,US - AS16509 (AMAZON-02 - Amazon.com, Inc., US)	7 hours ago **Via:** manual	7 MB	79	15	6	
3 □	**URL:** www.voluntariosxvenezuela.com/ **IP:** 54.230.93.129 - **PTR:** server-54-230-93-129.fra2.r.cloudfront.net - **Server:** AmazonS3 **GeoIP:** Seattle,US - AS16509 (AMAZON-02 - Amazon.com, Inc., US)	6 months ago **Via:** manual	5 MB	97	17	2	
4 □	**URL:** www.voluntariosxvenezuela.com/ **IP:** 54.230.202.154 - **PTR:** server-54-230-202-154.fra50.r.cloudfront.net - **Server:** AmazonS3 **GeoIP:** Seattle,US - AS16509 (AMAZON-02 - Amazon.com, Inc., US)	6 months ago **Via:** manual	5 MB	97	17	2	

(4 results in total, 4 shown)

Click on the one with IP 54[.]230[.]22[.]154. https://urlscan.io/result/77040696-2dd7-4635-ac3f-a5c96cbd3ff9/



www.voluntariosxvenezuela.com

54.230.202.154

Submitted URL: http://www.voluntariosxvenezuela.com
Effective URL: https://www.voluntariosxvenezuela.com/
Submission: On February 13 via manual (February 13th 2019, 4:43:09 am) from VE

Summary

This website contacted **17 IPs** in **2 countries** across **14 domains** to perform **97 HTTP transactions**.
The main IP is 54.230.202.154, located in **Seattle, United States** and belongs to AMAZON-02 - Amazon.com, Inc., US. The main domain is www.voluntariosxvenezuela.com.
TLS certificate: Issued by *Let's Encrypt Authority X3* on February 6th 2019. Valid for: 3 months.

The main domain was scanned **4 times** on urlscan.io

12 structurally similar pages on different IPs, domains and ASNs found

Verdict: Unknown

Google Safe Browsing: Clean (Current Verdict)

Additional live information

Domain created: February 4th 2019, 15:30:59 (UTC)
Domain registrar: PDR Ltd. d/b/a PublicDomainRegistry.com
Certificates: 7 TLS certs observed from 2019-02-06 to 2019-02-09

Domain & IP information

⇄	IP Address	AS Autonomous System
1 ➔ 1	54.230.202.199	16509 (AMAZON-02 - Amazon.com)
40	54.230.202.154	16509 (AMAZON-02 - Amazon.com)
2	209.197.3.15	20446 (HIGHWINDS3 - Highwinds Network Group)
1	2a00:1450:4001:825::200a	15169 (GOOGLE - Google LLC)
2	2a00:1450:4001:819::2008	15169 (GOOGLE - Google LLC)
11	52.6.69.241	16509 (AMAZON-AES - Amazon.com)
2	96.126.103.183	63949 (LINODE-AP Linode)

Screenshot

Detected technologies

WordPress (CMS)	Website
PHP (Programming Languages)	Website
MediaElement.js (Video Players)	Website
Yoast SEO (SEO)	Website
Amazon S3 (Miscellaneous)	Website
Facebook (Widgets)	Website
Font Awesome (Font Scripts)	Website
Google Analytics (Analytics)	Website
Google Font API (Font Scripts)	Website
Google Tag Manager (Tag Managers)	Website
SweetAlert (JavaScript Libraries)	Website
jQuery (JavaScript Libraries)	Website
reCAPTCHA (Captchas)	Website

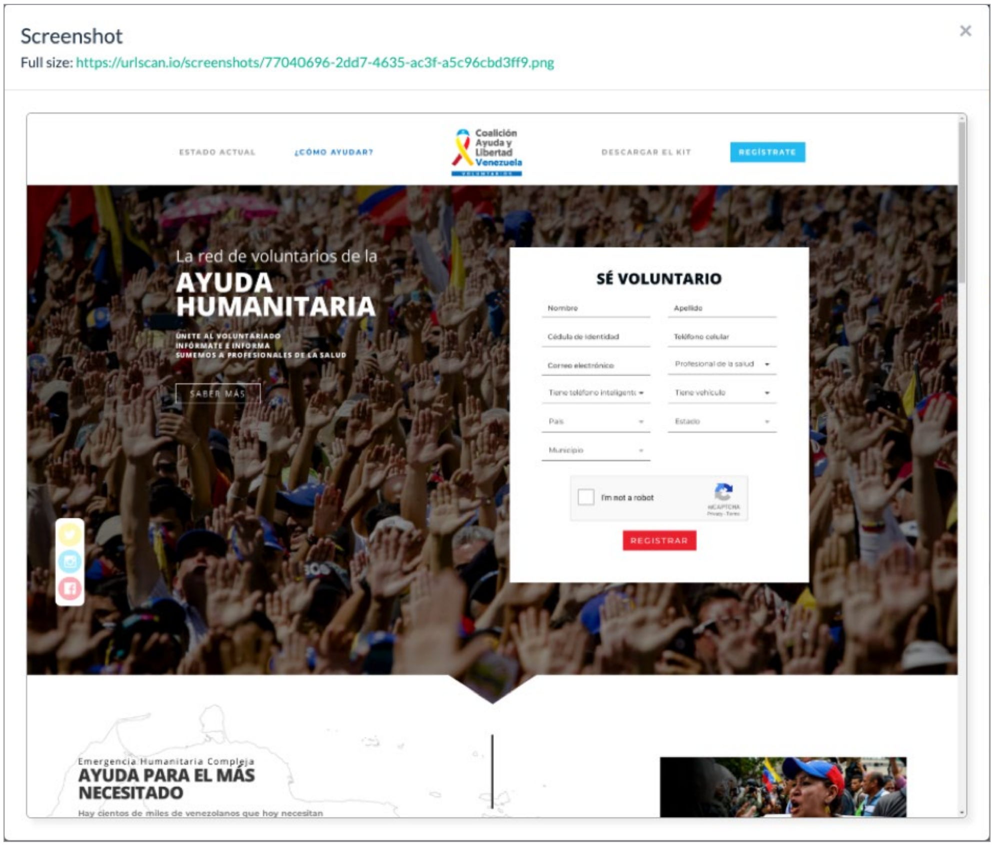
Stats

97	14	0	100%	56%
Requests	Ad-blocked	Malicious	HTTPS	IPv6

The legitimate and fraudulent domain screenshots appear to be identical.

Legitimate domain www[.]voluntariosxvenezuela[.]com

https://urlscan.io/screenshots/77040696-2dd7-4635-ac3f-a5c96cbd3ff9.png



Screenshot
Full size: https://urlscan.io/screenshots/77040696-2dd7-4635-ac3f-a5c96cbd3ff9.png

La red de voluntarios de la
AYUDA HUMANITARIA

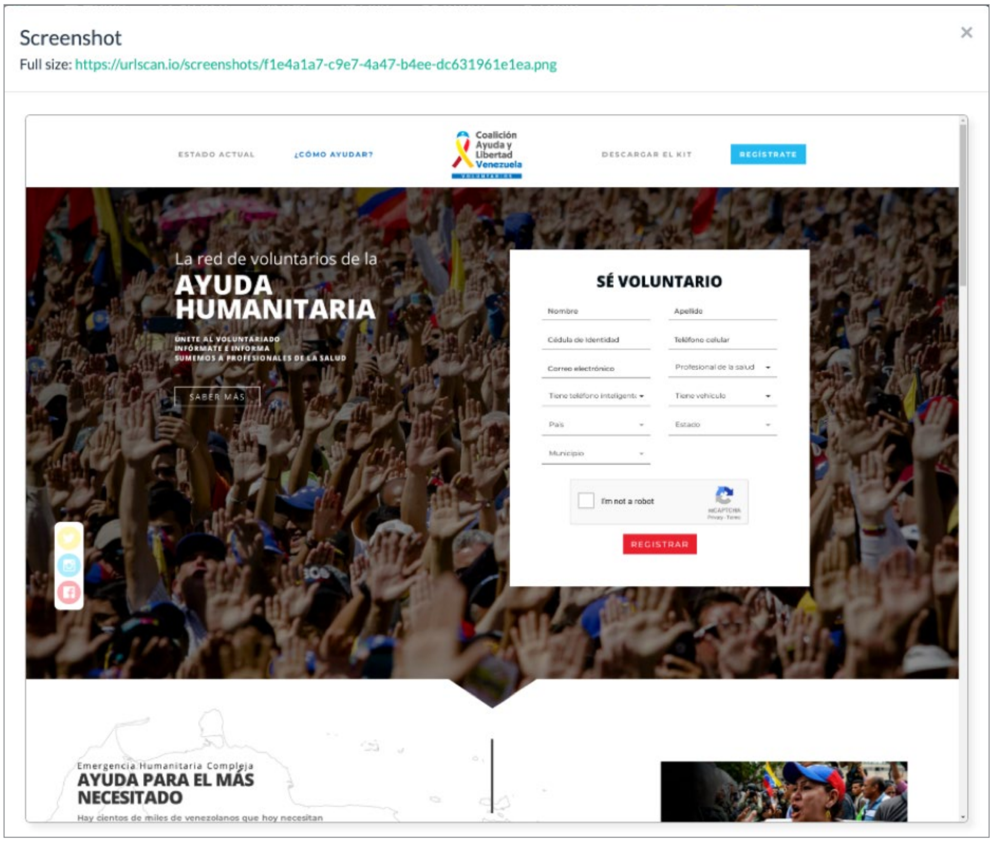
ÚNETE AL VOLUNTARIADO
INFÓRMATE E INFORMA
SUMEMOS A PROFESIONALES DE LA SALUD

SÉ VOLUNTARIO

Nombre
Apellido
Cédula de identidad
Teléfono celular
Correo electrónico
Profesional de la salud
Tiene teléfono inteligente
Tiene vehículo
País
Estado
Municipio

Emergencia Humanitaria Compleja
AYUDA PARA EL MÁS NECESITADO
Hay cientos de miles de venezolanos que hoy necesitan

Potential fraudulent domain www[.]voluntariosxxvenezuela[.]com
https://urlscan.io/screenshots/f1e4a1a7-c9e7-4a47-b4ee-dc631961e1ea.png



Screenshot

Full size: https://urlscan.io/screenshots/f1e4a1a7-c9e7-4a47-b4ee-dc631961e1ea.png

Now that we have determined that the potential fraudulent domain is using cookies and trackers from the real domain and appears to have an identical screenshot, we will now investigate it in PassiveTotal.

The website www[.]voluntariovenezuela[.]com was infringing on the real domain and the video showed that the DNS cache redirected ther real domain to this infringing domain. This could happen because of DNS spoofing was reported and we observed it in the video .

According to Wikipedia
https://en.wikipedia.org/wiki/DNS_spoofing

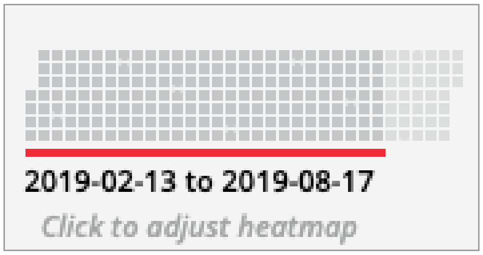
DNS spoofing, also referred to as DNS cache poisoning, is a form of computer security hacking in which corrupt Domain Name System data is introduced into the DNS resolver's cache, causing the name server to return an incorrect result record, e.g. an IP address. This results in traffic being diverted to the attacker's computer (or any other computer).

That means if a person was in Venezuela and using the DNS servers in Venezuela a poison cache entry could be entered in and force users to be redirected to a fraudulent IP address. So, if the DNS server entry for www[.]voluntariosxvenezuela[.]com was changed to point to a different IP address in the cache then all users typing in that real domain would do a lookup of the IP address in the DNS server. The DNS server would respond with the cached entry which could have been poisoned with a back IP address. This appears to be what happened from the twitter posts we were given.

Step 17: Open a new tab and go the website https://community.riskiq.com and search for the domain www[.]voluntariovenezuela[.]com

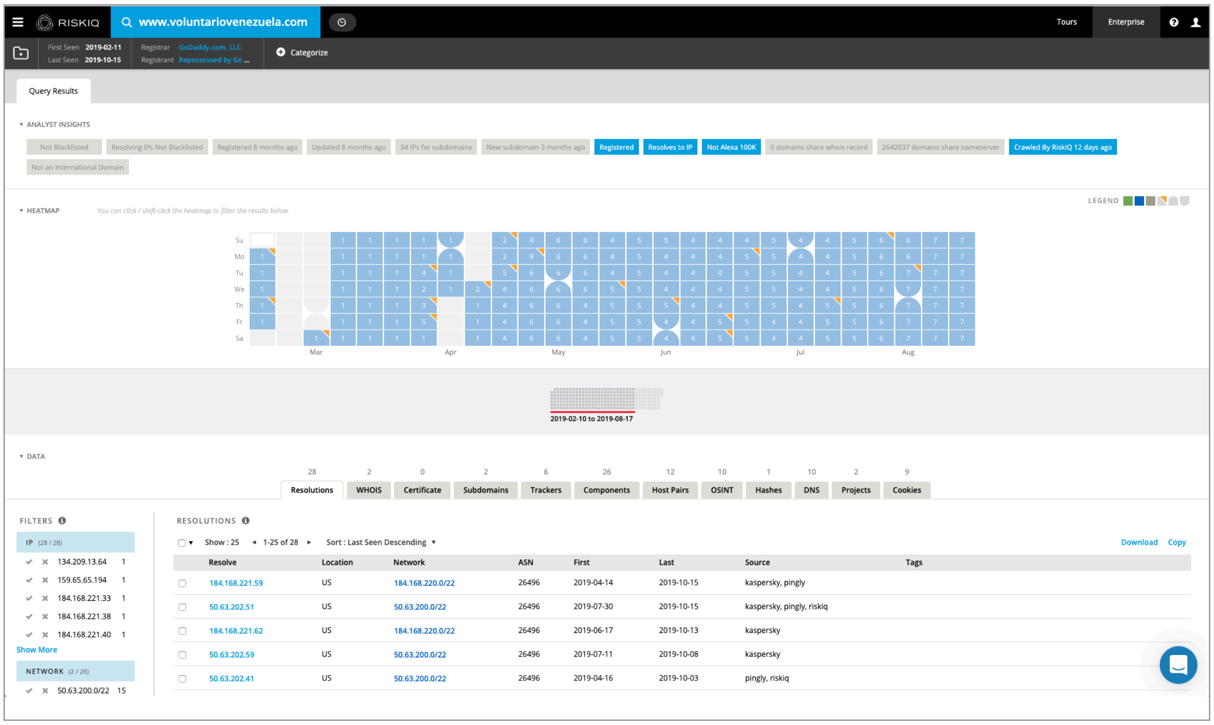
https://community.riskiq.com/search/www.voluntariovenezuela.com

Adjust the heatmap by clicking on the beginning of the timebar in order to filter the results to show you the beginning of February 2019. The heatmap only shows 6 months of results at a time. Since we are investigating an attack that is a little over 6 months, we have to click on the beginning of the timebar to see the results we are looking for.



2019-02-13 to 2019-08-17

Click to adjust heatmap



www.voluntariovenezuela.com

First Seen 2019-02-11
Last Seen 2019-10-15
Registrar GoDaddy.com, LLC
Registrant Repossessed by Go ...

▾ ANALYST INSIGHTS

Not Blacklisted | Resolving IPs Not Blacklisted | Registered 8 months ago | Updated 8 months ago | 34 IPs for subdomains | New subdomain 3 months ago | Registered | Resolves to IP | Not Alexa 100K | 0 domains share whois record | 2642037 domains share nameserver | Crawled By RiskIQ 12 days ago | Not an International Domain

▾ HEATMAP *You can click / shift-click the heatmap to filter the results below*

LEGEND

Su				1	1	1	1	1		2	4	6	6	4	5	5	4	4	4	5	4	4	5	6	6	7	7
Mo	1			1	1	1	1	1		2	9	6	6	4	5	4	4	4	5	5	4	4	5	6	6	7	7
Tu	1			1	1	1	4	1		5	6	6	6	4	5	4	4	4	5	5	4	4	5	6	7	7	7
We	1			1	1	1	2	1	2	4	6	6	6	5	5	4	4	4	5	5	4	4	5	6	7	7	7
Th	1			1	1	1	3		1	4	6	6	4	5	5	5	4	4	5	5	4	5	5	6	7	7	7
Fr	1			1	1	1	5		1	4	6	6	4	5	5	4	4	5	5	4	4	5	5	6	7	7	7
Sa			1	1	1	1	1		1	4	6	6	4	5	5	4	4	5	5	4	4	5	5	6	7	7	7
			Mar					Apr				May				Jun					Jul				Aug		

2019-02-10 to 2019-08-17

▾ DATA

28	2	0	2	6	26	12	10	1	10	2	9
Resolutions	WHOIS	Certificate	Subdomains	Trackers	Components	Host Pairs	OSINT	Hashes	DNS	Projects	Cookies

FILTERS

IP (28 / 28)

✓	✕	134.209.13.64	1
✓	✕	159.65.65.194	1
✓	✕	184.168.221.33	1
✓	✕	184.168.221.38	1
✓	✕	184.168.221.40	1

Show More

NETWORK (2 / 26)

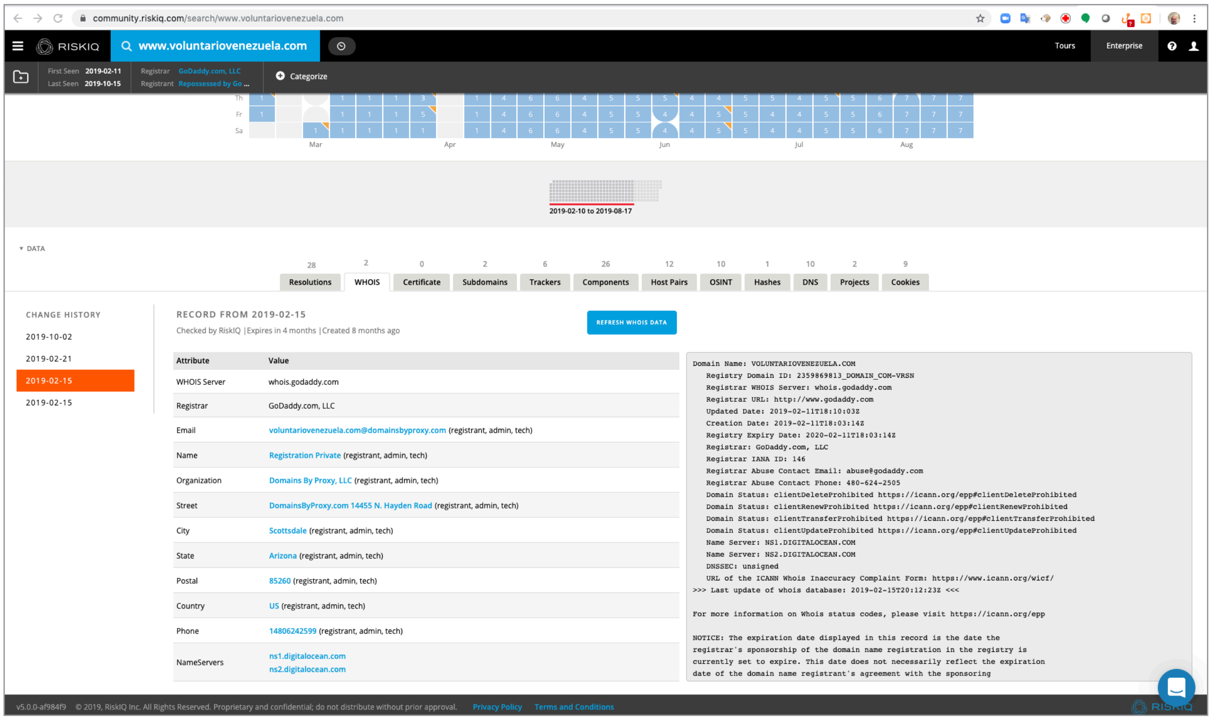
✓	✕	50.63.200.0/22	15

RESOLUTIONS

□ ▾ Show : 25 ◂ 1-25 of 28 ▸ Sort : Last Seen Descending ▾ Download Copy

	Resolve	Location	Network	ASN	First	Last	Source	Tags
□	184.168.221.59	US	184.168.220.0/22	26496	2019-04-14	2019-10-15	kaspersky, pingly	
□	50.63.202.51	US	50.63.200.0/22	26496	2019-07-30	2019-10-15	kaspersky, pingly, riskiq	
□	184.168.221.62	US	184.168.220.0/22	26496	2019-06-17	2019-10-13	kaspersky	
□	50.63.202.59	US	50.63.200.0/22	26496	2019-07-11	2019-10-08	kaspersky	
□	50.63.202.41	US	50.63.200.0/22	26496	2019-04-16	2019-10-03	pingly, riskiq	

Step 18: Click on the WHOIS tab.



RECORD FROM 2019-02-15

Checked by RiskIQ |Expires in 4 months |Created 8 months ago

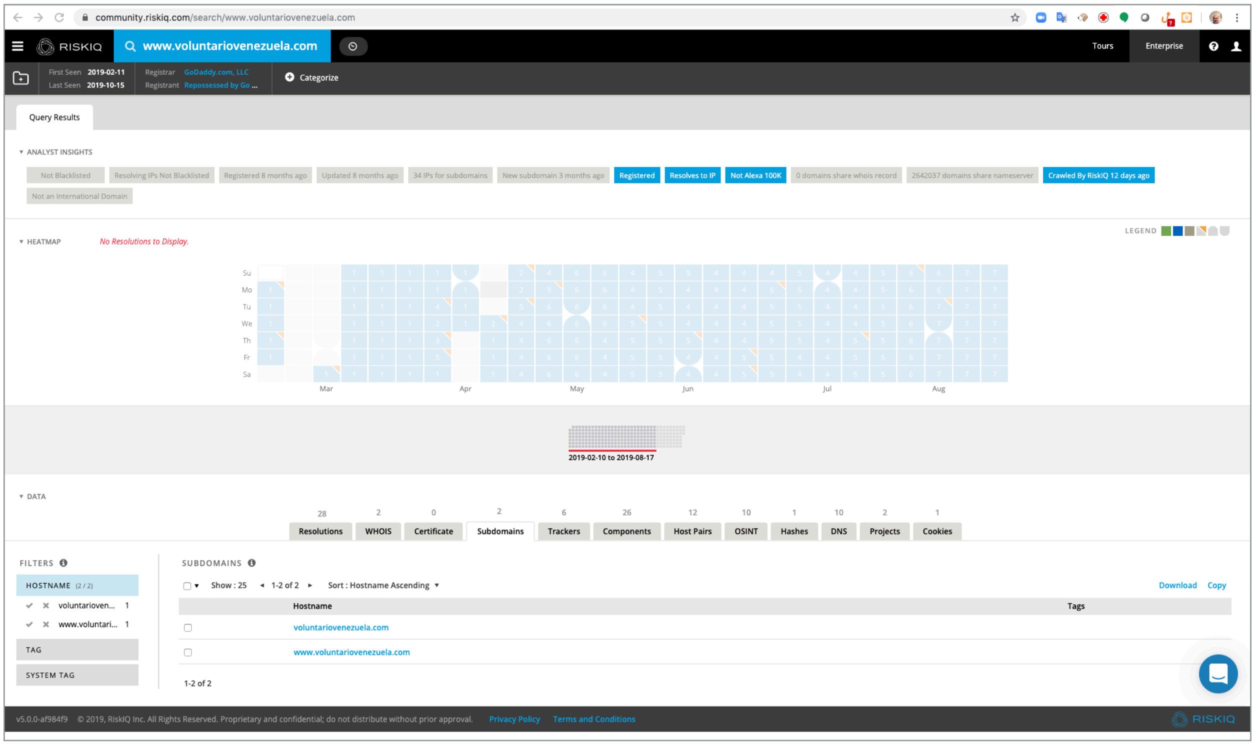
Attribute	Value
WHOIS Server	whois.godaddy.com
Registrar	GoDaddy.com, LLC
Email	voluntariovenezuela.com@domainsbyproxy.com (registrant, admin, tech)
Name	Registration Private (registrant, admin, tech)
Organization	Domains By Proxy, LLC (registrant, admin, tech)
Street	DomainsByProxy.com 14455 N. Hayden Road (registrant, admin, tech)
City	Scottsdale (registrant, admin, tech)
State	Arizona (registrant, admin, tech)
Postal	85260 (registrant, admin, tech)
Country	US (registrant, admin, tech)
Phone	14806242599 (registrant, admin, tech)
NameServers	ns1.digitalocean.com ns2.digitalocean.com

```
Domain Name: VOLUNTARIOVENEZUELA.COM
   Registry Domain ID: 2359869813_DOMAIN_COM-VRSN
   Registrar WHOIS Server: whois.godaddy.com
   Registrar URL: http://www.godaddy.com
   Updated Date: 2019-02-11T18:10:03Z
   Creation Date: 2019-02-11T18:03:14Z
   Registry Expiry Date: 2020-02-11T18:03:14Z
   Registrar: GoDaddy.com, LLC
   Registrar IANA ID: 146
   Registrar Abuse Contact Email: abuse@godaddy.com
   Registrar Abuse Contact Phone: 480-624-2505
   Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
   Domain Status: clientRenewProhibited https://icann.org/epp#clientRenewProhibited
   Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
   Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
   Name Server: NS1.DIGITALOCEAN.COM
   Name Server: NS2.DIGITALOCEAN.COM
   DNSSEC: unsigned
   URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2019-02-15T20:12:23Z <<<

For more information on Whois status codes, please visit https://icann.org/epp

NOTICE: The expiration date displayed in this record is the date the
registrar's sponsorship of the domain name registration in the registry is
currently set to expire. This date does not necessarily reflect the expiration
date of the domain name registrant's agreement with the sponsoring
```

The WHOIS information is privacy protected. No further avenues of investigation.

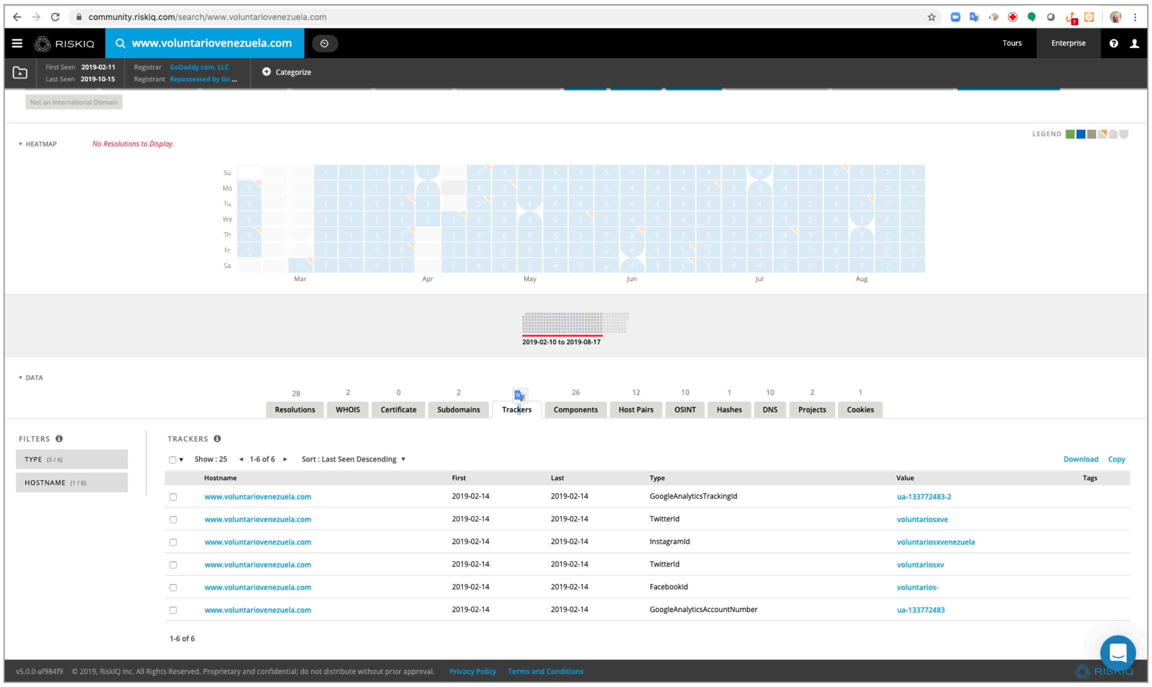
Step 19: Click on the subdomain tab

We only see two results for the domain. We will move on and come back to the subdomains if we need to further investigate them.



	Hostname	Tags
□	voluntariovenezuela.com	
□	www.voluntariovenezuela.com	

Step 20: Click on the trackers tab



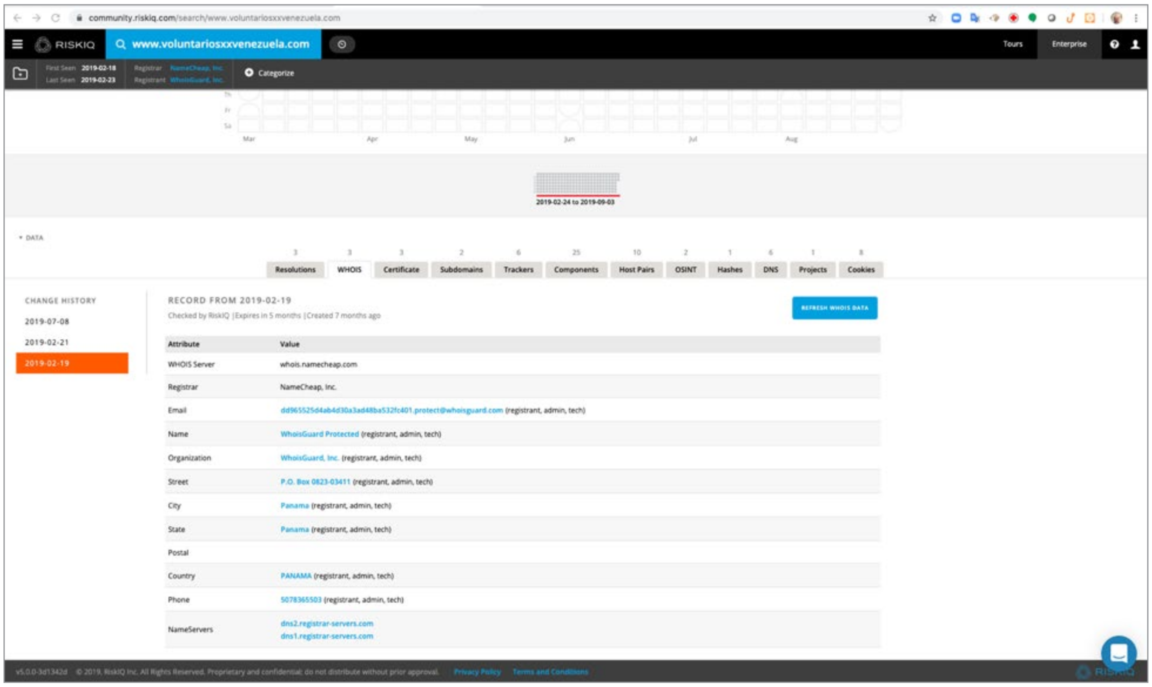
First Seen 2019-02-11
Last Seen 2019-10-15
Registrar GoDaddy.com, LLC
Registrant Repossessed by Go ...

Hostname	First	Last	Type	Value	Tags
www.voluntariovenezuela.com	2019-02-14	2019-02-14	GoogleAnalyticsTrackingId	ua-133772483-2	
www.voluntariovenezuela.com	2019-02-14	2019-02-14	TwitterId	voluntariosxve	
www.voluntariovenezuela.com	2019-02-14	2019-02-14	InstagramId	voluntariosxvenezuela	
www.voluntariovenezuela.com	2019-02-14	2019-02-14	TwitterId	voluntariosxv	
www.voluntariovenezuela.com	2019-02-14	2019-02-14	FacebookId	voluntarios-	
www.voluntariovenezuela.com	2019-02-14	2019-02-14	GoogleAnalyticsAccountNumber	ua-133772483	

The results show that the domain is utilizing all of the trackers from real domain www[.]voluntariosxvenezuela[.]com (Google, Twitter, Instagram, and Facebook). We witnessed in the twitter video the DNS poison attack redirection only within Venezuela. We need to find out more information about the IP address that the website was utilizing during this attack.

Step 21: Open a new tab to https://community.riskiq.com and search for the domain www[.]voluntariosxxvenezuela[.]com

https://community.riskiq.com/search/www.voluntariosxxvenezuela.com



First Seen 2019-02-18
Last Seen 2019-02-23
Registrar NameCheap, Inc.
Registrant WhoisGuard, Inc.

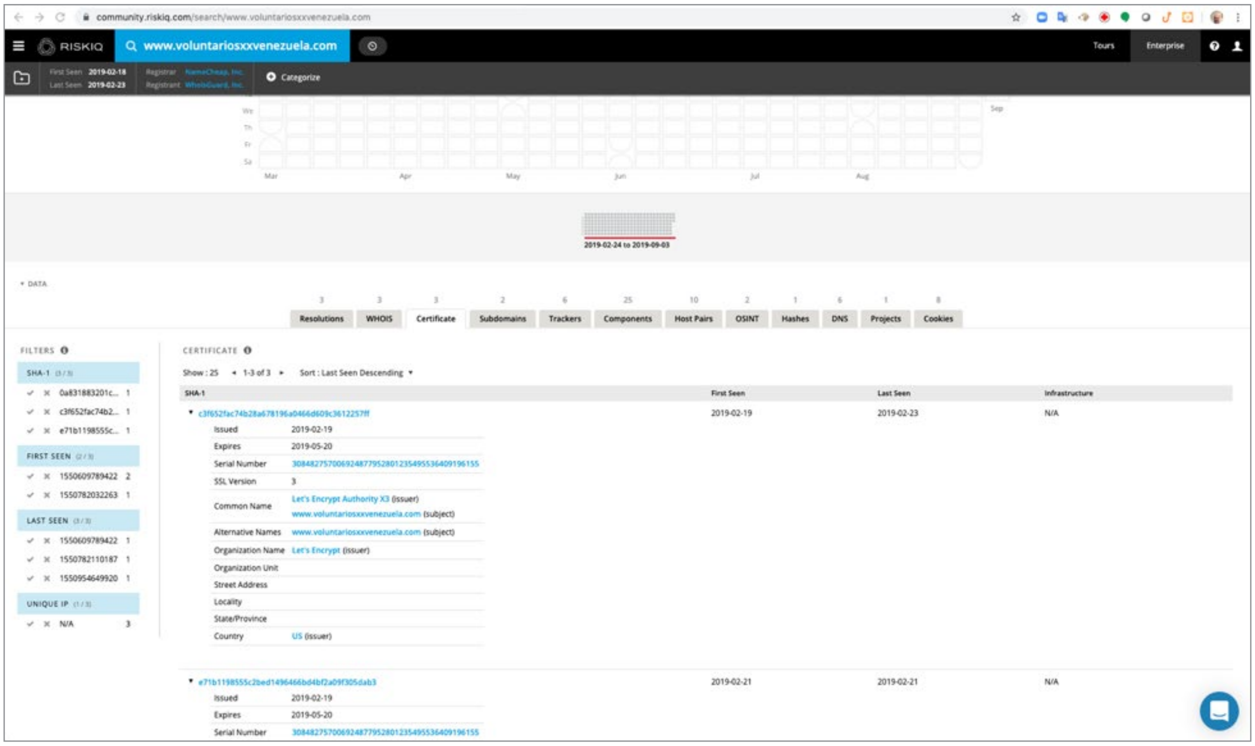
CHANGE HISTORY
2019-07-08
2019-02-21
2019-02-19

RECORD FROM 2019-02-19
Checked by RiskIQ |Expires in 5 months |Created 7 months ago

Attribute	Value
WHOIS Server	whois.namecheap.com
Registrar	NameCheap, Inc.
Email	dd965525d4ab4d30a3ad48ba532fc401.protect@whoisguard.com (registrant, admin, tech)
Name	WhoisGuard Protected (registrant, admin, tech)
Organization	WhoisGuard, Inc. (registrant, admin, tech)
Street	P.O. Box 0823-03411 (registrant, admin, tech)
City	Panama (registrant, admin, tech)
State	Panama (registrant, admin, tech)
Postal	
Country	PANAMA (registrant, admin, tech)
Phone	5078365503 (registrant, admin, tech)
NameServers	dns2.registrar-servers.com dns1.registrar-servers.com

The WHOIS information is privacy protected.

Step 22: Click on the Certificate tab.



First Seen 2019-02-18 | Last Seen 2019-02-23 | Registrar NameCheap, Inc. | Registrant WhoisGuard, Inc.

FILTERS

SHA-1 (3 / 3)
- 0a831883201c... 1
- c3f652fac74b2... 1
- e71b1198555c... 1

FIRST SEEN (2 / 3)
- 1550609789422 2
- 1550782032263 1

LAST SEEN (3 / 3)
- 1550609789422 1
- 1550782110187 1
- 1550954649920 1

UNIQUE IP (1 / 3)
- N/A 3

CERTIFICATE

Show : 25 ◂ 1-3 of 3 ▸ Sort : Last Seen Descending ▾

SHA-1	First Seen	Last Seen	Infrastructure
c3f652fac74b28a678196a0466d609c3612257ff	2019-02-19	2019-02-23	N/A
e71b1198555c2bed1496466bd4bf2a09f305dab3	2019-02-21	2019-02-21	N/A

c3f652fac74b28a678196a0466d609c3612257ff

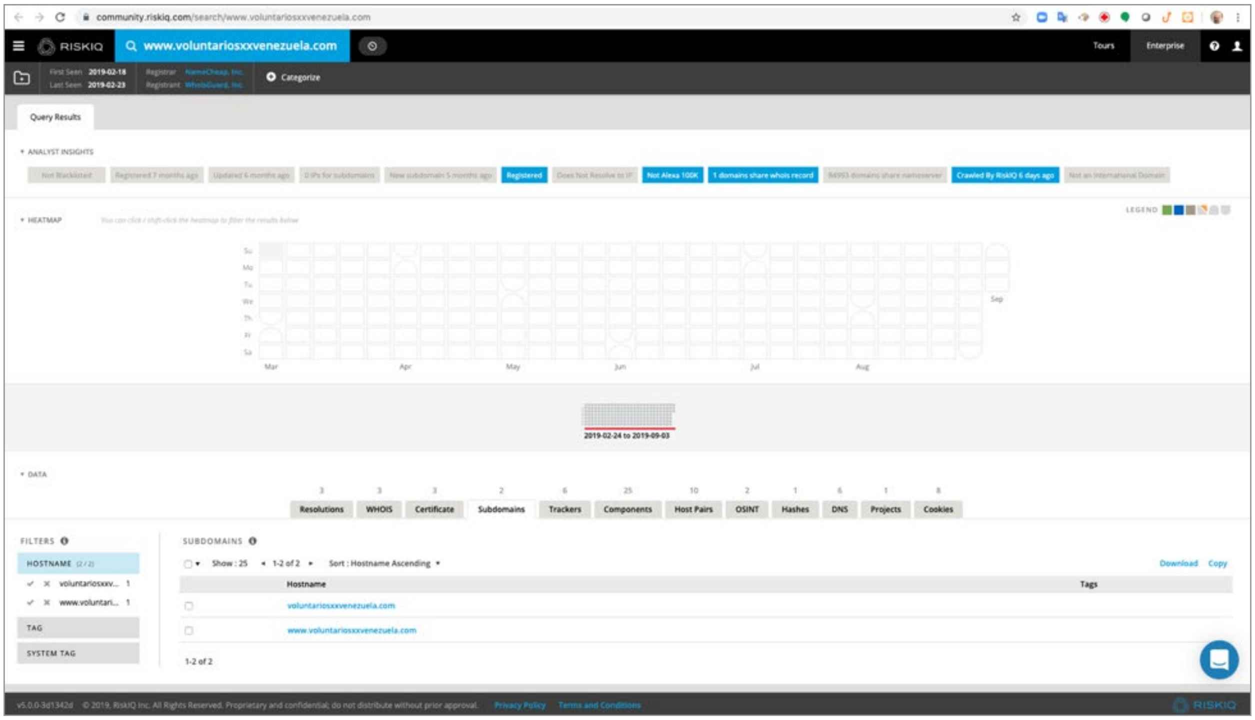
Issued	2019-02-19
Expires	2019-05-20
Serial Number	308482757006924877952801235495536409196155
SSL Version	3
Common Name	Let's Encrypt Authority X3 (issuer) www.voluntariosxxvenezuela.com (subject)
Alternative Names	www.voluntariosxxvenezuela.com (subject)
Organization Name	Let's Encrypt (issuer)
Organization Unit	
Street Address	
Locality	
State/Province	
Country	US (issuer)

e71b1198555c2bed1496466bd4bf2a09f305dab3

Issued	2019-02-19
Expires	2019-05-20
Serial Number	308482757006924877952801235495536409196155

In the results, if you expand the certificate information you can see that all of the certificates were free Let's Encrypt certificates. This can sometimes be an indicator of a fraudulent domain. Threat actors usually don't like to spend money of infrastructure or certificates.

Step 23: Click on the subdomains tab.



FILTERS

HOSTNAME (2 / 2)
- voluntariosxxv... 1
- www.voluntari... 1

TAG

SYSTEM TAG

SUBDOMAINS

□ ▾ Show : 25 ◂ 1-2 of 2 ▸ Sort : Hostname Ascending ▾

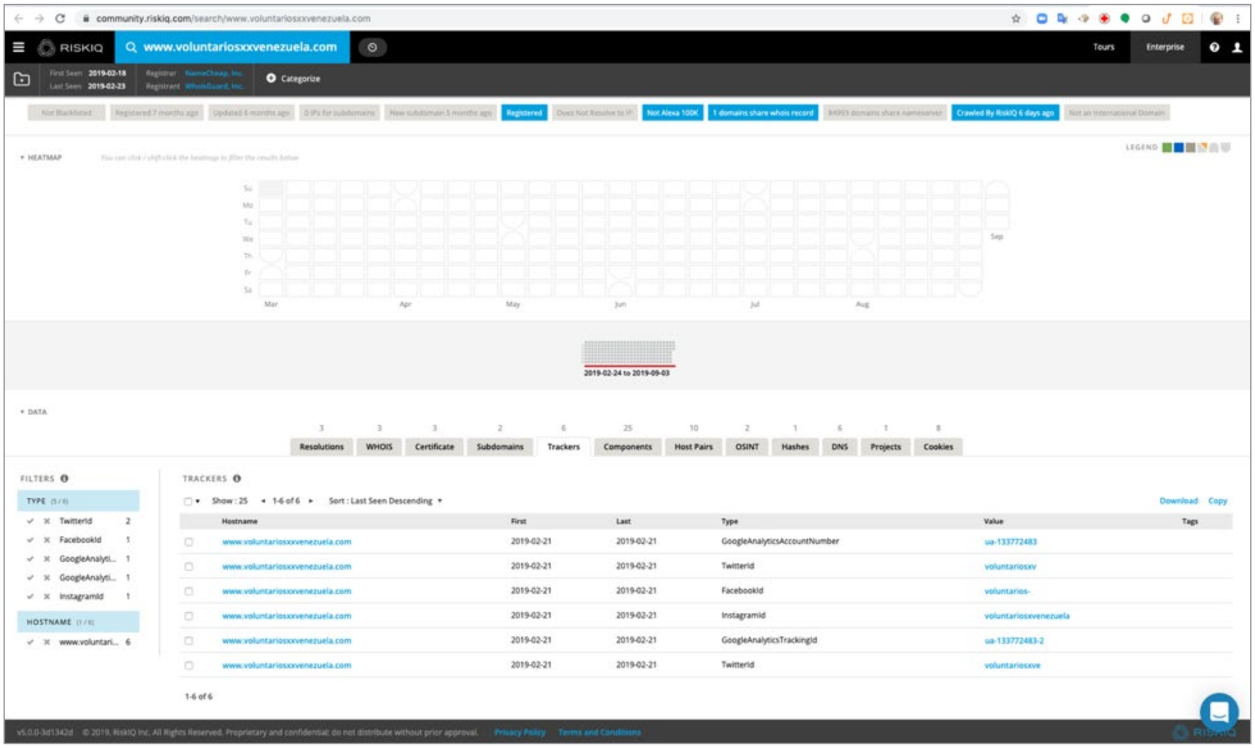
	Hostname	Tags
□	voluntariosxxvenezuela.com	
□	www.voluntariosxxvenezuela.com	

1-2 of 2

v5.0.0-3d1342d © 2019, RiskIQ Inc. All Rights Reserved. Proprietary and confidential; do not distribute without prior approval.

We see that there is a subdomain for www[.]voluntariosxxvenezuela[.]com and voluntariosxxvenezuela[.]com.

Step 24: Click on the Trackers tab.

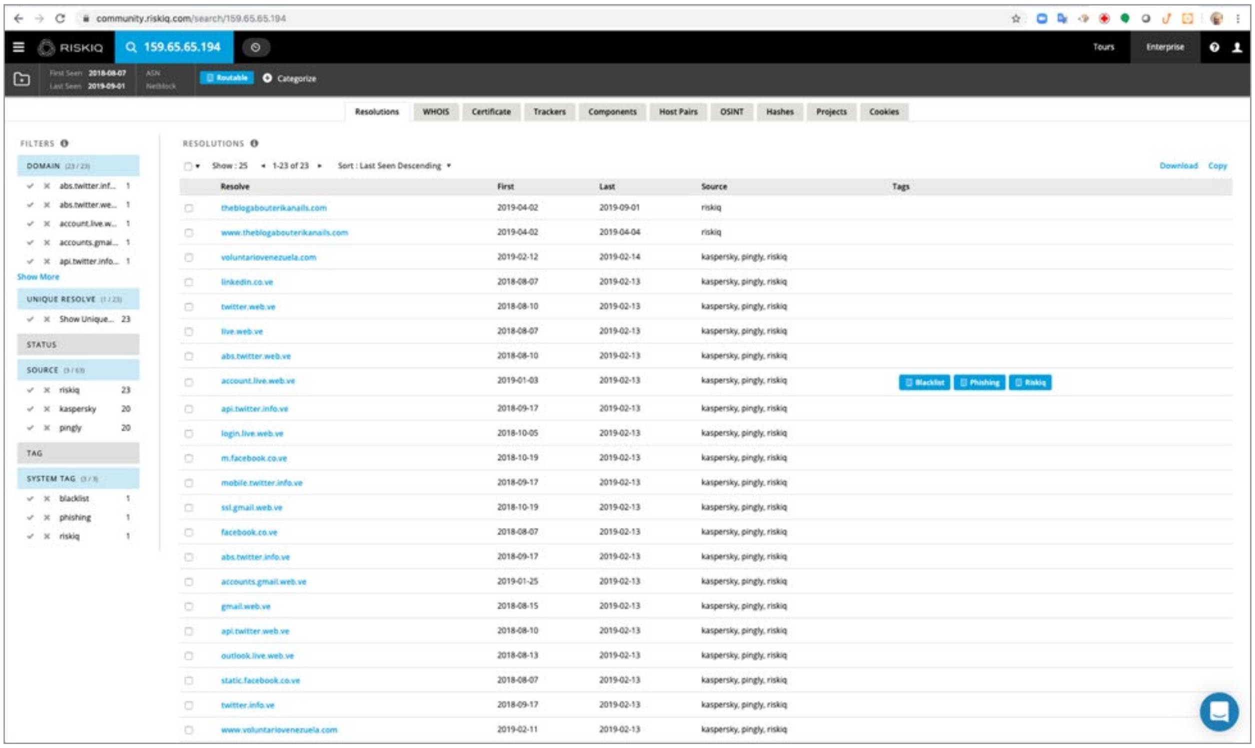


Hostname	First	Last	Type	Value	Tags
www.voluntariosxxvenezuela.com	2019-02-21	2019-02-21	GoogleAnalyticsAccountNumber	ua-133772483	
www.voluntariosxxvenezuela.com	2019-02-21	2019-02-21	TwitterId	voluntariosxv	
www.voluntariosxxvenezuela.com	2019-02-21	2019-02-21	FacebookId	voluntarios-	
www.voluntariosxxvenezuela.com	2019-02-21	2019-02-21	InstagramId	voluntariosxvenezuela	
www.voluntariosxxvenezuela.com	2019-02-21	2019-02-21	GoogleAnalyticsTrackingId	ua-133772483-2	
www.voluntariosxxvenezuela.com	2019-02-21	2019-02-21	TwitterId	voluntariosxve	

We see the google analytics tracking ID, twitter, Facebook and Instagram ids from the legitimate domain vountariosxvenezuela[.]com

Step 25: In a new tab we will now investigate the IP address 159[.]65[.]65[.]194 that appeared in the twitter post.

https://community.riskiq.com/search/159.65.65.194



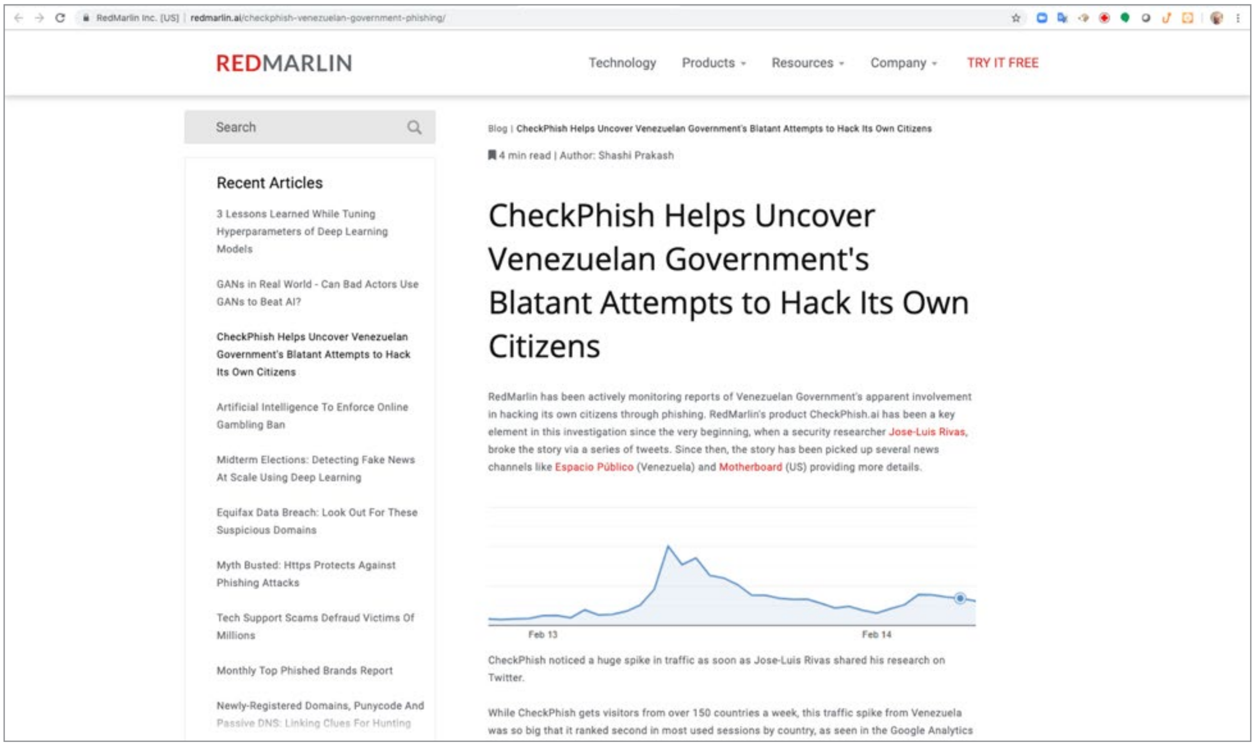
Resolve	First	Last	Source	Tags
theblogabouterikanails.com	2019-04-02	2019-09-01	riskiq	
www.theblogabouterikanails.com	2019-04-02	2019-04-04	riskiq	
voluntariovenezuela.com	2019-02-12	2019-02-14	kaspersky, pingly, riskiq	
linkedin.co.ve	2018-08-07	2019-02-13	kaspersky, pingly, riskiq	
twitter.web.ve	2018-08-10	2019-02-13	kaspersky, pingly, riskiq	
live.web.ve	2018-08-07	2019-02-13	kaspersky, pingly, riskiq	
abs.twitter.web.ve	2018-08-10	2019-02-13	kaspersky, pingly, riskiq	
account.live.web.ve	2019-01-03	2019-02-13	kaspersky, pingly, riskiq	Blacklist Phishing Riskiq
api.twitter.info.ve	2018-09-17	2019-02-13	kaspersky, pingly, riskiq	
login.live.web.ve	2018-10-05	2019-02-13	kaspersky, pingly, riskiq	
m.facebook.co.ve	2018-10-19	2019-02-13	kaspersky, pingly, riskiq	
mobile.twitter.info.ve	2018-09-17	2019-02-13	kaspersky, pingly, riskiq	
ssl.gmail.web.ve	2018-10-19	2019-02-13	kaspersky, pingly, riskiq	
facebook.co.ve	2018-08-07	2019-02-13	kaspersky, pingly, riskiq	
abs.twitter.info.ve	2018-09-17	2019-02-13	kaspersky, pingly, riskiq	
accounts.gmail.web.ve	2019-01-25	2019-02-13	kaspersky, pingly, riskiq	
gmail.web.ve	2018-08-15	2019-02-13	kaspersky, pingly, riskiq	
api.twitter.web.ve	2018-08-10	2019-02-13	kaspersky, pingly, riskiq	
outlook.live.web.ve	2018-08-13	2019-02-13	kaspersky, pingly, riskiq	
static.facebook.co.ve	2018-08-07	2019-02-13	kaspersky, pingly, riskiq	
twitter.info.ve	2018-09-17	2019-02-13	kaspersky, pingly, riskiq	
www.voluntariovenezuela.com	2019-02-11	2019-02-13	kaspersky, pingly, riskiq	

If you examine the list of domains. We see many popular domains LinkedIn, Twitter, Microsoft login account[.]live, Facebook, Outlook, Gmail. But all of the domains end in .ve. That means that these domains are controlled by the TLD for the Venezuelan government. The fraudulent domain voluntariovenezuela[.]com also appears. All of these domains seem to have end all around the same time when the attack stopped on February 13, 2019.

Step 26: Click on the OSINT tab.

Click on the link for the source www[.]redmarlin.ai

https://www.redmarlin.ai/checkphish-venezuelan-government-phishing/



RedMarlin Inc. [US] | redmarlin.ai/checkphish-venezuelan-government-phishing/

REDMARLIN

Technology Products Resources Company TRY IT FREE

Search

Recent Articles

3 Lessons Learned While Tuning Hyperparameters of Deep Learning Models

GANs in Real World - Can Bad Actors Use GANs to Beat AI?

CheckPhish Helps Uncover Venezuelan Government's Blatant Attempts to Hack Its Own Citizens

Artificial Intelligence To Enforce Online Gambling Ban

Midterm Elections: Detecting Fake News At Scale Using Deep Learning

Equifax Data Breach: Look Out For These Suspicious Domains

Myth Busted: Https Protects Against Phishing Attacks

Tech Support Scams Defraud Victims Of Millions

Monthly Top Phished Brands Report

Newly-Registered Domains, Punycode And Passive DNS: Linking Clues For Hunting

Blog | CheckPhish Helps Uncover Venezuelan Government's Blatant Attempts to Hack Its Own Citizens

4 min read | Author: Shashi Prakash

CheckPhish Helps Uncover Venezuelan Government's Blatant Attempts to Hack Its Own Citizens

RedMarlin has been actively monitoring reports of Venezuelan Government's apparent involvement in hacking its own citizens through phishing. RedMarlin's product CheckPhish.ai has been a key element in this investigation since the very beginning, when a security researcher Jose-Luis Rivas, broke the story via a series of tweets. Since then, the story has been picked up several news channels like Espacio Público (Venezuela) and Motherboard (US) providing more details.

CheckPhish noticed a huge spike in traffic as soon as Jose-Luis Rivas shared his research on Twitter.

While CheckPhish gets visitors from over 150 countries a week, this traffic spike from Venezuela was so big that it ranked second in most used sessions by country, as seen in the Google Analytics

This OSINT article describes how the Venezuelan Government attempted to hack its own citizens.

Conclusion:

1. Is www[.]voluntariovenezuela[.]com fraudulent?
   Yes, we determined that www[.]voluntariovenezuela[.]com is fraudulent and was infringing on the legitimate domain. Utilizing urlscan.io we could saw the fraudulent domain had the same webpage as the legitimate domain. PassiveTotal exposed www[.]voluntariovenezuela[.]com was utilizing the same trackers and cookies from the legitimate domain www[.]voluntariosxvenzuela[.]com. Which meant it was copied from the legitimate domain. Redirections were seen only within Venezuela as demonstrated from the video posted to twitter. Use of a different DNS server not controlled by the TLD .ve worked correctly. This demonstrated that DNS poisoning occurred. The poisoned DNS cache pointed users within Venezuela to the fraudulent domain www[.]voluntariovenezuela[.]com at IP address 159[.]65[.]65[.]194. This IP address hosted other domains that were solely controlled by the TLD .ve.

2. Are any other websites also infringing on the real website www[.]voluntariosxvenezuela[.]com
   Yes, www[.]voluntariosxxvenezuela[.]com, voluntariosxxvenezuela[.]com, www[.]voluntariovenezuela[.]com, voluntariovenezuela[.] were also infringing on the legitimate website.

3. Can you determine or infer who is behind this domain infringing DNS poison attack?
   Since the TLD was controlled by the Venezuelan government we can highly speculate that the attack was carried out by them. Many OSINT reports concluded they were responsible for the attack against their Citizens

4. Are there any other websites that the threat actor is currently using or has used in attacks?
   Below is a list of the domains that were used in the attack in February 2019. Each one could be investigated to get the full understanding of the attack.

   theblogabouterikanails[.]com
   www[.]theblogabouterikanails[.]com
   voluntariovenezuela[.]com
   linkedin[.]co[.]ve
   twitter[.]web[.]ve
   live[.]web[.]ve
   abs[.]twitter[.]web[.]ve
   account[.]live[.]web[.]ve
   api[.]twitter[.]info[.]ve
   login[.]live[.]web[.]ve
   m[.]facebook[.]co[.]ve
   mobile[.]twitter[.]info[.]ve
   ssl[.]gmail[.]web[.]ve
   facebook[.]co[.]ve
   abs[.]twitter[.]info[.]ve
   accounts[.]gmail[.]web[.]ve
   gmail[.]web[.]ve
   api[.]twitter[.]web[.]ve
   outlook[.]live[.]web[.]ve
   static[.]facebook[.]co[.]ve
   twitter[.]info[.]ve
   www[.]voluntariovenezuela[.]com
   mobile[.]twitter[.]web[.]ve

5. What are some ways people can to do to be protect against DNS spoofing?
   If users manually set their DNS server to a known good DNS server this could prevent DNS poison attacks. For example, you could set your DNS servers to Google's DNS servers 8[.]8[.]8[.]8 and 8[.]8[.]4[.]4

RiskIQ, Inc.
22 Battery Street, 10th Floor
San Francisco, CA. 94111

sales@riskiq.net
1 888.415.4447

Learn more at riskiq.com