

VE SIN FILTRO

Internet Censorship, DNS poisoning and Phishing in Venezuela

Measuring from censorship to
state-sponsored attacks



Noticias Reporta Test Evade los bloqueos Todas las guías

VESINFILTRO
Infórmate sobre el estado de internet en Venezuela

Internet en Vzla **Regular**

The State of Internet Censorship in Venezuela.

August 16, 2018

Autor: Andrés Azpúrua (Venezuela Inteligente / VEsinfiltro), Mariengracia Chirinos (IPYS Venezuela), Leonid Evdokimov (OONI), Maria Xynou (OONI)

The grid of images includes: 1. A town with blue network lines overlaid on the landscape. 2. A grey square with a small icon of a document and a network symbol. 3. A man with a blacked-out mouth holding a white sign that says 'YO DECIDO QUE DECIR'. 4. A mountain landscape with blue network lines overlaid. 5. A man sitting at a computer monitor. 6. A protest sign that says 'YO DECIDO QUE OPINAR'. 7. A woman's face in a close-up shot.

Thread

VE sin Filtro
@vesinfiltro

El bloqueo a [@youtube](#) parece haber sido levantado a las 2:42:20 (hora de Venezuela) [#5Jul](#) [#DiaDeLaIndependencia](#)

El Incidente duró 1hora 36 mintos, únicamente en [#CANTV](#), el principal proveedor de [#internetVE](#) y empresa estatal [#Venezuela](#) [#keepItOn](#)

Translate Tweet

inicio 2019-07-05 2019-07-05 fin

Youtube
Durante protestas en contra de las violaciones de Derechos Humanos en el día de la independencia
Afecta: Servicios de Google y Bing

Bloqueado

CANTV Metodo TCP block

VESINFILTRO @VEsinfiltro vesinfiltro.com



VENEZUELAN
CONTEXT

Critical failure of public services



<https://rpp.pe/mundo/actualidad/venezuela-venezolanos-recogen-agua-del-contaminado-rio-guaire-debido-a-la-escasez-por-apagon-caracas-noticia-1185399>

The state of the internet in Venezuela

- State ISP dominant share of residential internet access
- Decreasing residential internet penetration
- Three mobile operators
- Average download speeds:
 - 2.8 Mbps – SpeedTest
 - 1.5 Mbps – M_Lab
- ~46% have residential internet access (OVSP)
- Fragile infrastructure and frequent blackouts

INTERNET CENSORSHIP

Clarifications

Case

One or more related sites or service being blocked for a specific reason

Event

Continuous block of a target by an ISP



Indefinite Blocks

Long lasting, some 6+ years

Telecom regulator orders

On all/most major ISPs

Big and small sites

No clear end

Indefinite Blocks

Long lasting, some 6+ years

Telecom regulator orders

On all/most major ISPs

Big and small sites

No clear end

Tactical Blocks

As short as possible

Just in time to silence an event

**Tries to balance the political cost
of blocking high-traffic sites and services**

Seen only at state ISP CANTV,

How we measure

A mixture of:

- **Off the shell probes with custom settings**
 - **OONI (legacy CLI)**
 - **Custom scripts**
- **OONI-run links with custom links**
- **Occasionally RIPE ATLAS**

run.ooni.io links

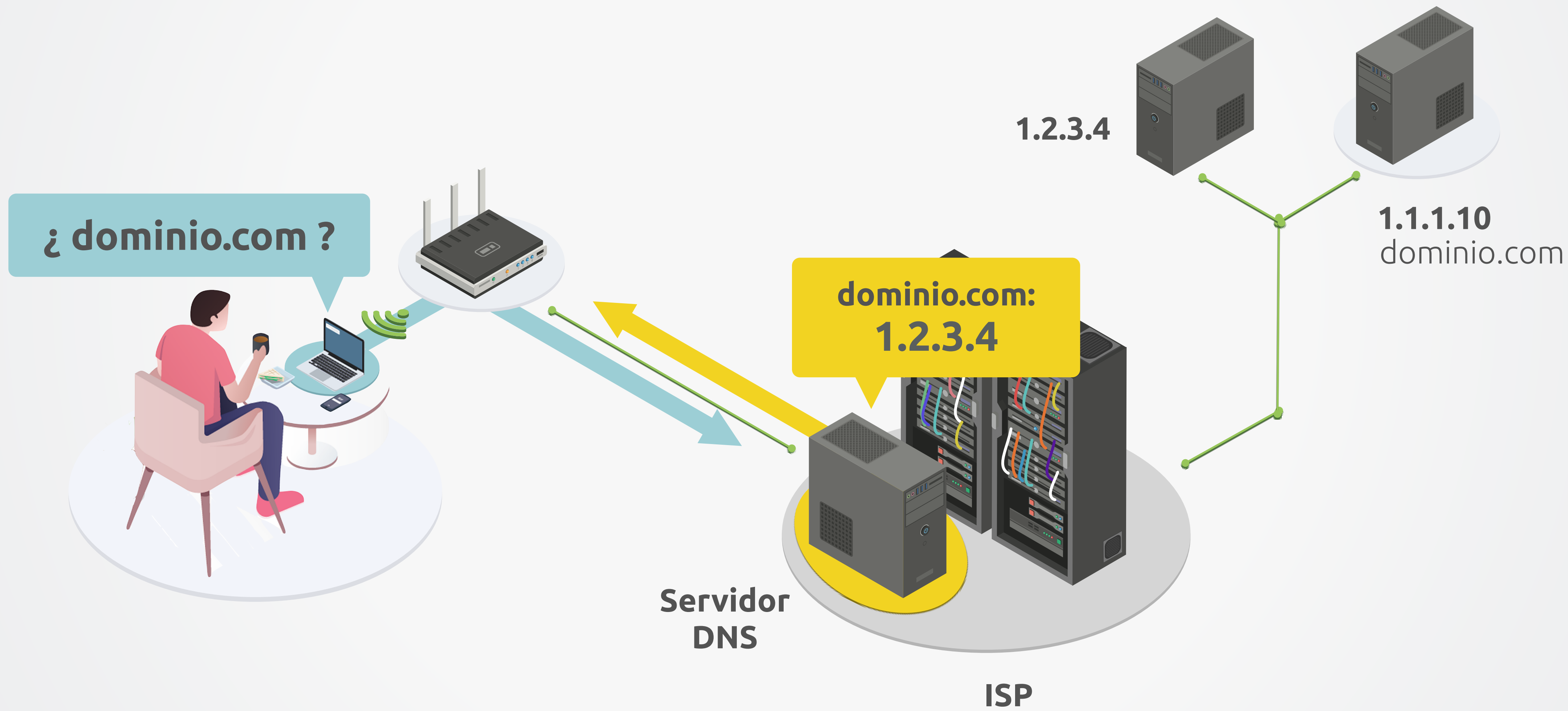
- Fundamental to quickly get multiple measurements fast
- Critical for unexpected incidents
- Key to bridge any gaps
- Faster turnaround of measurements

Measuring probes

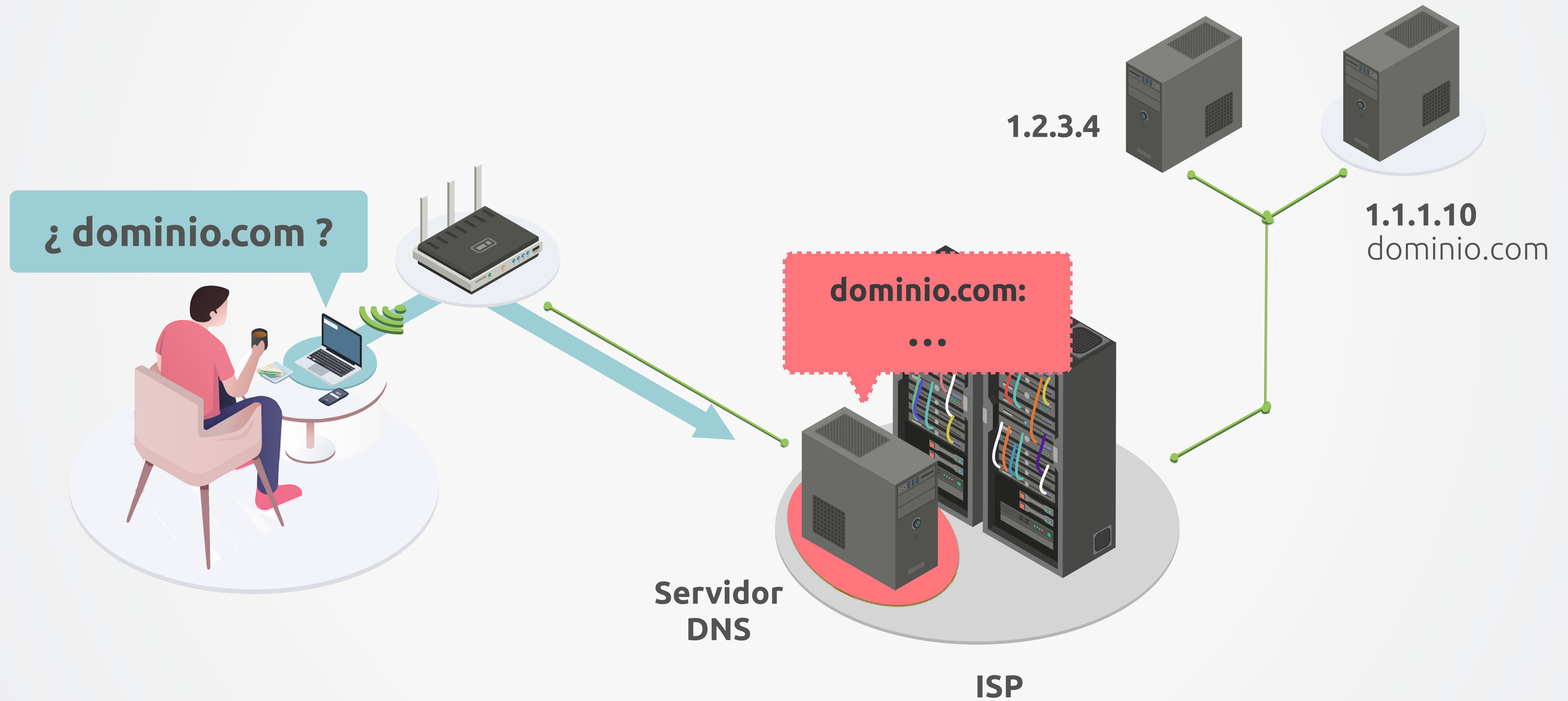
- Guaranteed more data points of whole list
- Increased test frequency based on URL importance
- Alternative tests:
 - High intensity dns, tcp, filtering by http host and SNI
 - Block rate when needed
- Currently migrating versions, to be released

ATLAS probes

- Alternative way to get different kinds of measurements
- Record changes



DNS Blocks

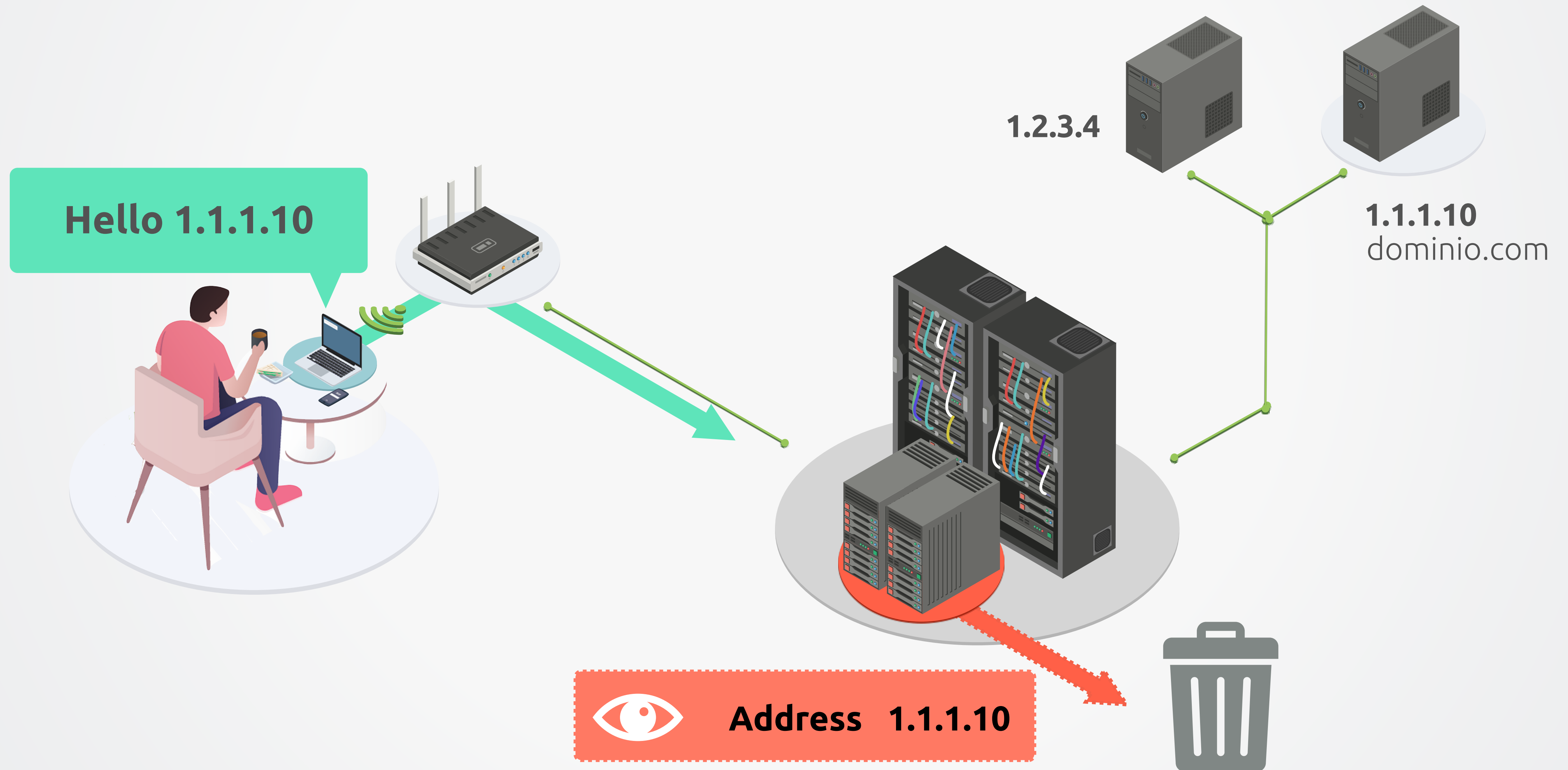


DNS Blocks

On all mainstream ISPs

| Domain | Typical awnser | CANTV, supercable, Digitel, Movistar | Inter |
|-----------|-----------------------------|---|-----------|
| ntn24.com | 104.28.8.75, 104.28.9.75 | no answer (server failure) | 127.0.0.1 |

TCP blocks

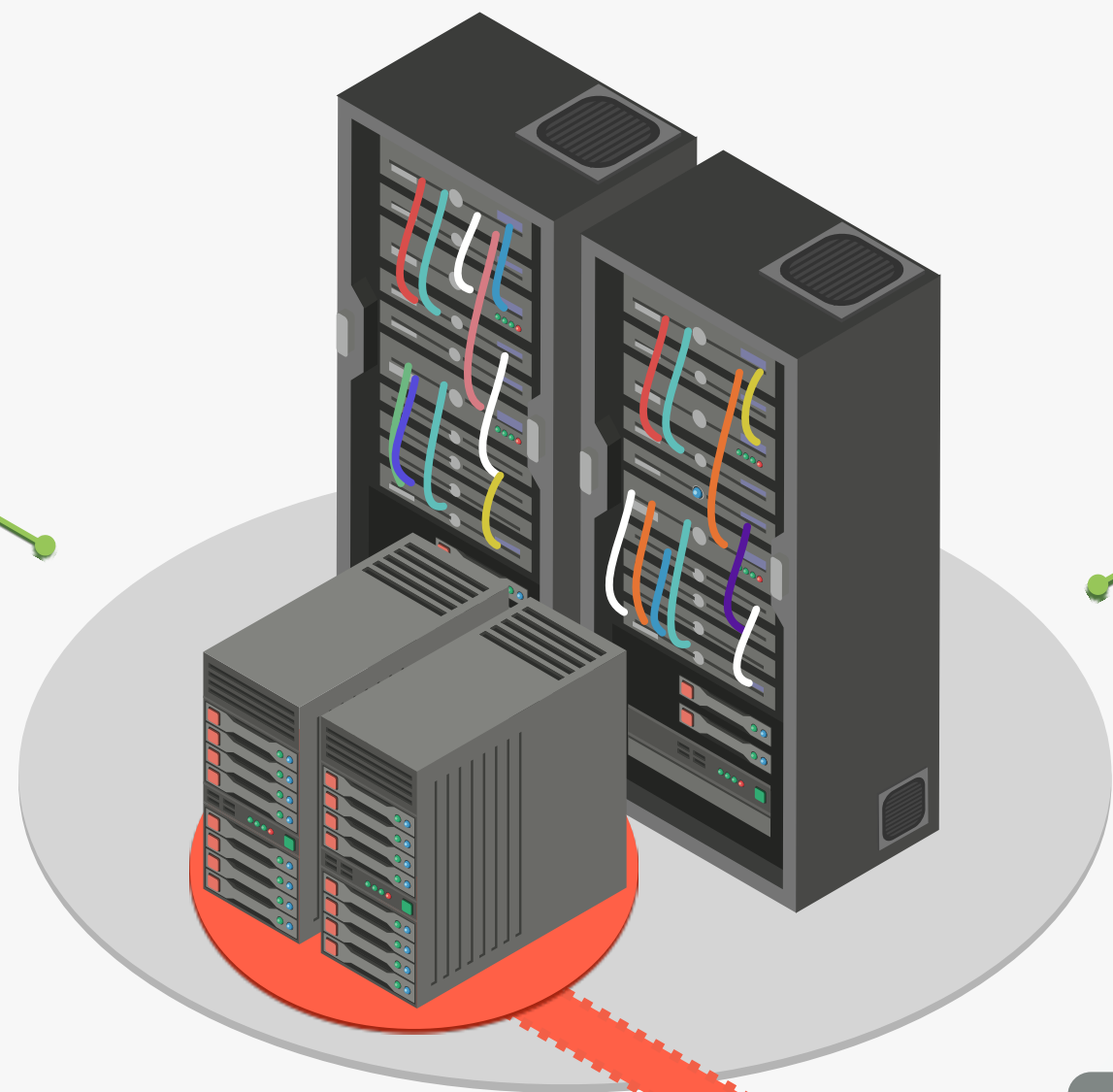


TCP blocks

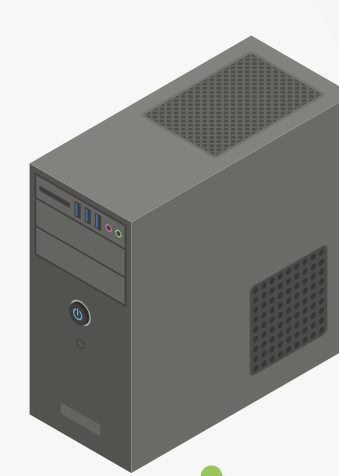
- Was largely deprecated until 2019
- Mostly used to block Youtube
- Evidence of misconfiguration

HTTP blocks

Hello 1.1.1.10 :
I want dominio.com



1.2.3.4




1.1.1.10
dominio.com

 Asking for domonio.com



HTTP blocks (http host and SNI filtering)

- Higher value sites with indefinite blocks
- Social media and streaming platforms
except YouTube most of the time
- Mostly used by CANTV



Evolution

2013 - 2018

Censorship moving depending on the priorities of the moment

Focused on sites publishing black market exchange rates

And News media around specific events, specially protests

Few large scale network shutdowns

Evolution

2018

Start of DPI blocking

Major mainstream news targeted

Block of Tor

Evolution

2018

Start of significant
DPI blocking

Major mainstream
news targeted

Block of Tor

2019

**Dramatic increase of censorship to
news**

Widespread use of SNI-Filtering

Major internet platforms blocked

Start of Tactical blocks

Evolution

2018

Start of significant
DPI blocking

Major mainstream
news targeted

Block of Tor

2019

Dramatic increase of
censorship to news

Widespread use of SNI-Filtering

Major internet platforms
blocked

Start of Tactical blocks

2020

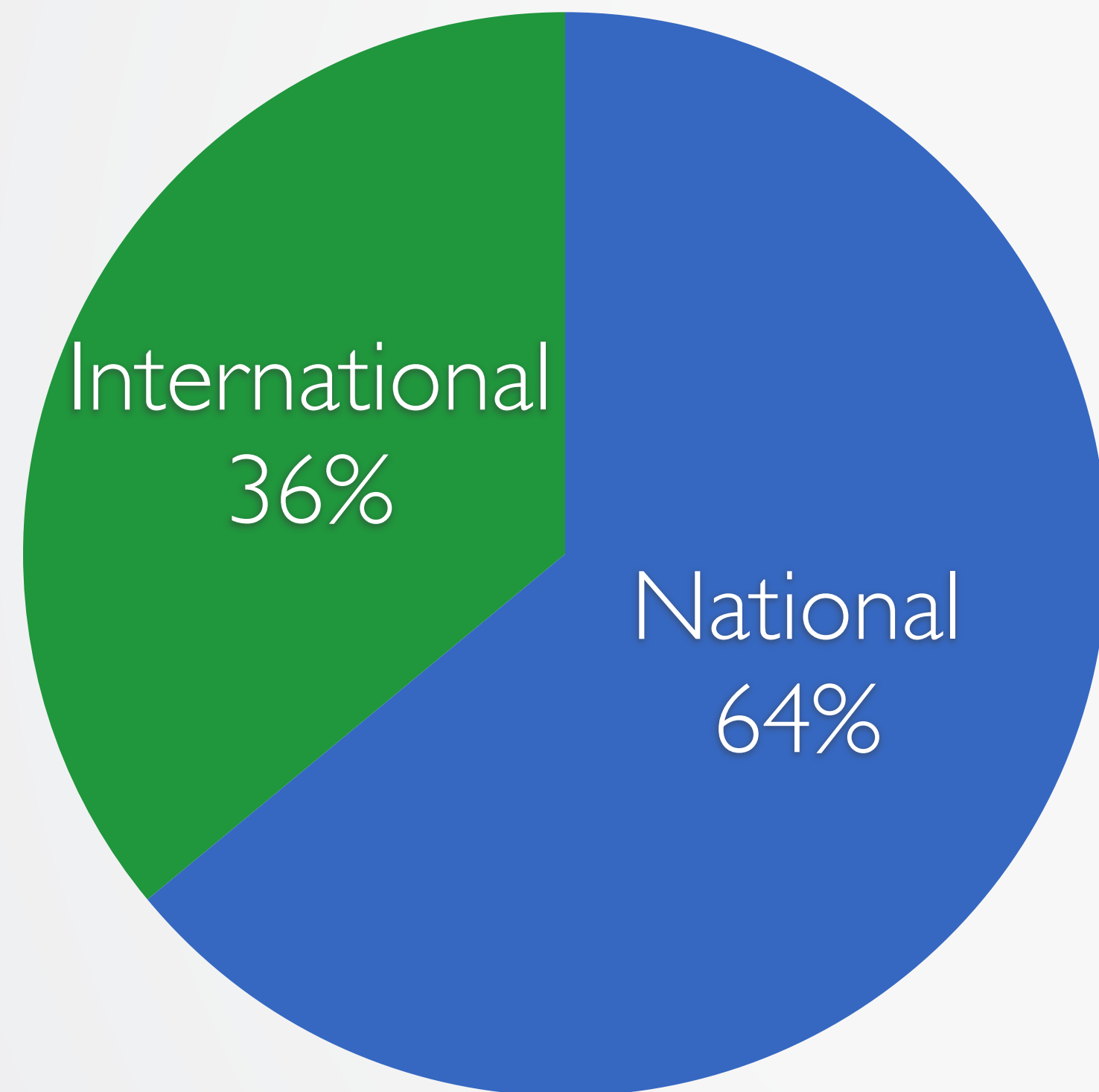
**Blocking of opposition
COVID-19 initiatives**

**Seemingly degraded DPI
blocking capacity**

**Continuation of Tactical
blocks of major social media**

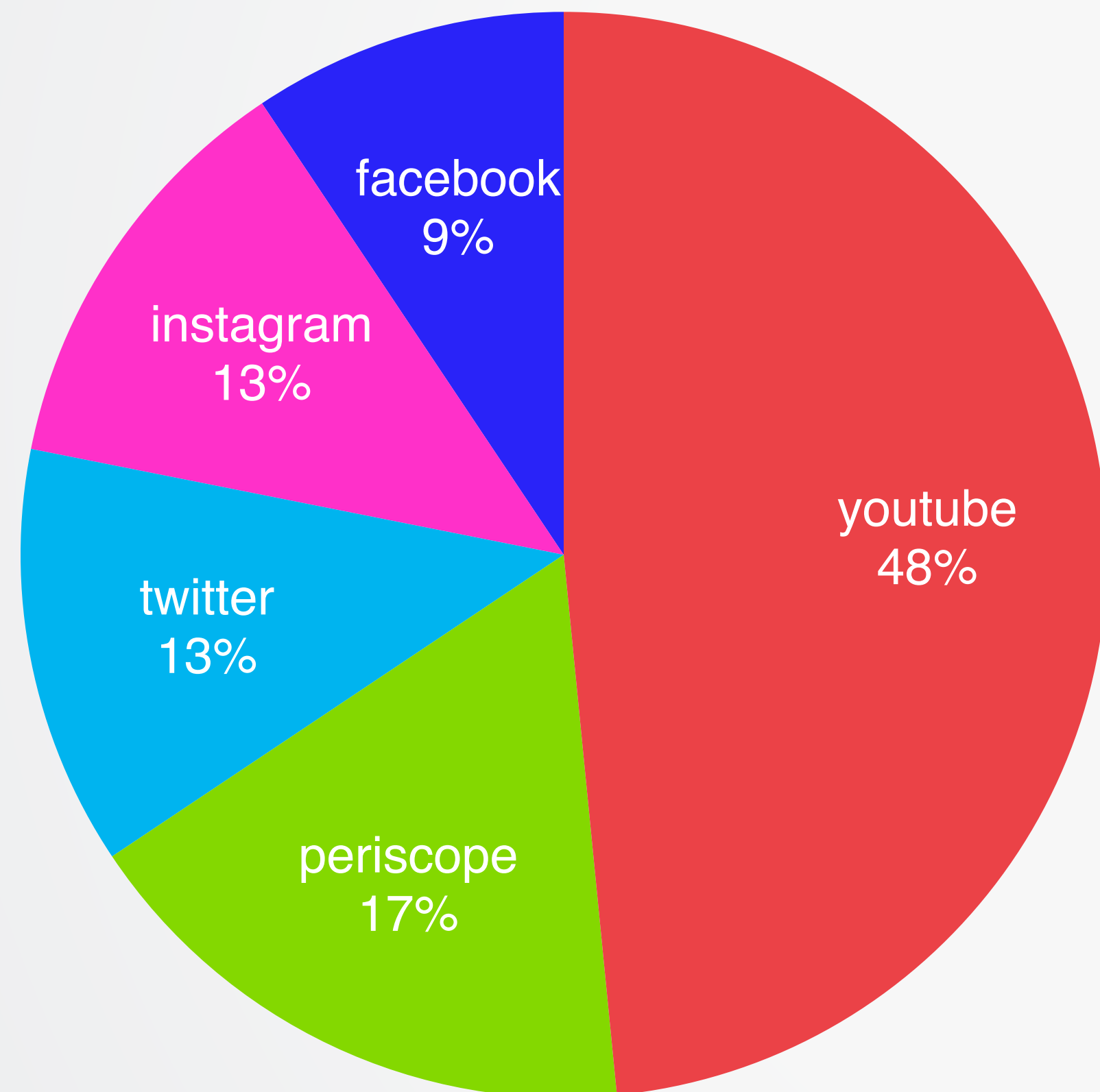
New blocks to news media

Censorship of news media



- 12 news media sites just in the first 3 months of 2019
- Over 25 news media sites blocked during 2019
- 4 News sites newly blocked in 2020
- **Severely limits access to information**

Tactical blocks in 2019



- At least 64 Tactical blocks events
- 31 for YouTube
- Some times more than one in a day
- AVG: 3h 08 min
MIN: 20min
MAX: 24h

¿Damaged capacity?

On 2020-04-06 a fire disrupted a CANTV facility in Caracas

- Multiple blocked sites became unblocked
- Later Tactical blocks used DNS



Covid-19 blocks

| Site | Dominio | CANTV | Movistar | Digitel | Supercable | Inter |
|----------------------------|--------------------------------|---------------|---------------|---------------|---------------|-------------|
| Coronavirus Venezuela | coronavirusvenezuela.info | ACCESIBLE | BLOQUEO DNS | BLOQUEO DNS | BLOQUEO DNS | ACCESIBLE |
| Heroes de la Salud | apoyosaludve.com | BLOQUEO DNS | BLOQUEO DNS | BLOQUEO DNS | BLOQUEO DNS | BLOQUEO DNS |
| Heroes de la Salud | heroesdesaludve.org | * BLOQUEO DNS | * BLOQUEO DNS | * BLOQUEO DNS | * BLOQUEO DNS | BLOQUEO DNS |
| Heroes de la Salud | heroesdesaludve.info | * BLOQUEO DNS | * BLOQUEO DNS | * BLOQUEO DNS | * BLOQUEO DNS | BLOQUEO DNS |
| Heroes de la Salud | porlasaludve.com | BLOQUEO DNS | BLOQUEO DNS | BLOQUEO DNS | BLOQUEO DNS | BLOQUEO DNS |
| Heroes de la Salud | saludvzla.com | * BLOQUEO DNS | * BLOQUEO DNS | * BLOQUEO DNS | BLOQUEO DNS | BLOQUEO DNS |
| Heroes de la Salud | apoyoheroesaludve.com | BLOQUEO DNS | BLOQUEO DNS | BLOQUEO DNS | BLOQUEO DNS | BLOQUEO DNS |
| Teleconsulta COVID-19 | teleconsulta.presidenciave.org | ACCESIBLE | BLOQUEO DNS | BLOQUEO DNS | ACCESIBLE | ACCESIBLE |
| Teleconsulta COVID-19 | medicos.presidenciave.or | ACCESIBLE | BLOQUEO DNS | ACCESIBLE | ACCESIBLE | ACCESIBLE |
| Presidencia VE (J. Guaidó) | presidenciave.com | ACCESIBLE | BLOQUEO DNS | BLOQUEO DNS | BLOQUEO DNS | BLOQUEO DNS |
| Presidencia VE (J. Guaidó) | presidenciave.org | ACCESIBLE | BLOQUEO DNS | BLOQUEO DNS | BLOQUEO DNS | BLOQUEO DNS |
| Presidencia VE (J. Guaidó) | pvenezuela.com | BLOQUEO DNS | BLOQUEO DNS | BLOQUEO DNS | BLOQUEO DNS | BLOQUEO DNS |
| Presidencia VE (J. Guaidó) | vepresidencia.com | BLOQUEO DNS | BLOQUEO DNS | BLOQUEO DNS | BLOQUEO DNS | BLOQUEO DNS |

Not current snapshot

**DNS MANIPULATION
AND STATE-SPONSORED
PHISHING**

Case: VoluntariosxVenezuela.com

The screenshot shows a web browser window with the URL www.voluntariosxvenezuela.com. The page features a navigation bar with the following elements:

- ESTADO ACTUAL
- ¿CÓMO AYUDAR?
- Logo: Coalición Ayuda y Libertad Venezuela VOLUNTARIOS
- DESCARGAR EL KIT
- REGÍSTRATE (button)

The main content area has a background image of a crowd with raised hands. On the left, there is a call to action:

La red de voluntarios de la
AYUDA HUMANITARIA
ÚNETE AL VOLUNTARIADO
INFÓRMATE E INFORMA
SUMEMOS A PROFESIONALES DE LA SALUD

Social media icons for Twitter, Instagram, and Facebook are visible. A "SABER MÁS" button is located below the text.

On the right, a registration form titled "SÉ VOLUNTARIO" contains the following fields:

| | |
|------------------------------|---------------------------|
| Nombre | Apellido |
| Cédula de Identidad | Teléfono celular |
| Correo electrónico | Profesional de la salud ▼ |
| Tiene teléfono inteligente ▼ | Tiene vehículo ▼ |
| Pais ▼ | Estado ▼ |
| Municipio ▼ | |

ESTADO ACTUAL

INTERNACIONAL



DESCARGAR EL KIT

REGÍSTRATE

La red de voluntarios de la

AYUDA HUMANITARIA



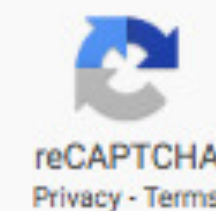
ÚNETE AL VOLUNTARIADO
INFÓRMATE E INFORMA
SUMEMOS A PROFESIONALES DE LA SALUD

SABER MÁS

SÉ VOLUNTARIO

| | |
|----------------------|----------------------|
| <input type="text"/> | <input type="text"/> |
| <input type="text"/> | <input type="text"/> |
| <input type="text"/> | <input type="text"/> |
| <input type="text"/> | <input type="text"/> |
| <input type="text"/> | <input type="text"/> |
| <input type="text"/> | <input type="text"/> |
| <input type="text"/> | <input type="text"/> |
| <input type="text"/> | <input type="text"/> |

I'm not a robot



REGISTRAR

Vectors

- Malicious links to voluntariovenezuela.com
- Visits to voluntariosxvenezuela.com
**With poisoned / manipulated
DNS responses**

First iteration

Original: **voluntariosxvenezuela.com**
AWS
Dominio en PublicDomainRegistry

Malicioso: **voluntariovenezuela.com**
159.65.65.194
Digital Ocean
Dominio registrado en GoDaddy

Malicious links

- **Twitter:** Links to fake domain being shared since 2019-02-11
- **Fake twitter accounts Twitter:**
[@voluntariosvene](#),
vs [@voluntariosxve](#)
- Other channels

Malicious links

← ⋮

Top Latest People Photos Videos

 **Mir(E)angelaRondon** ∞. @Mireangelar_ · Feb 11

Juntos podemos sumar esfuerzos para ayudar a salvar la vida de cientos de miles de venezolanos que hoy necesitan de todos nosotros para construir la Venezuela que queremos. #YoSoyVoluntario @VoluntariosxVe

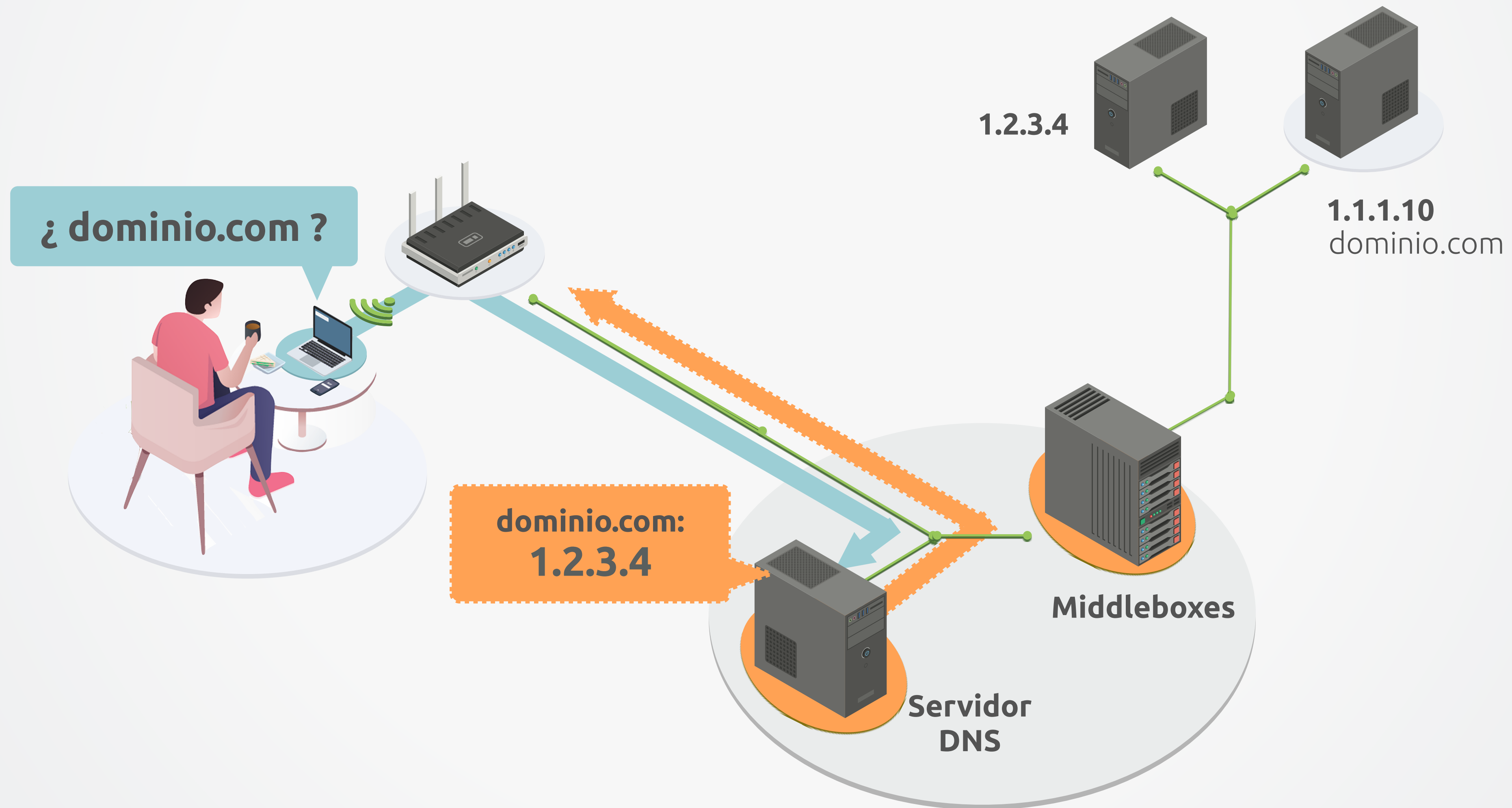
voluntariovenezuela.com



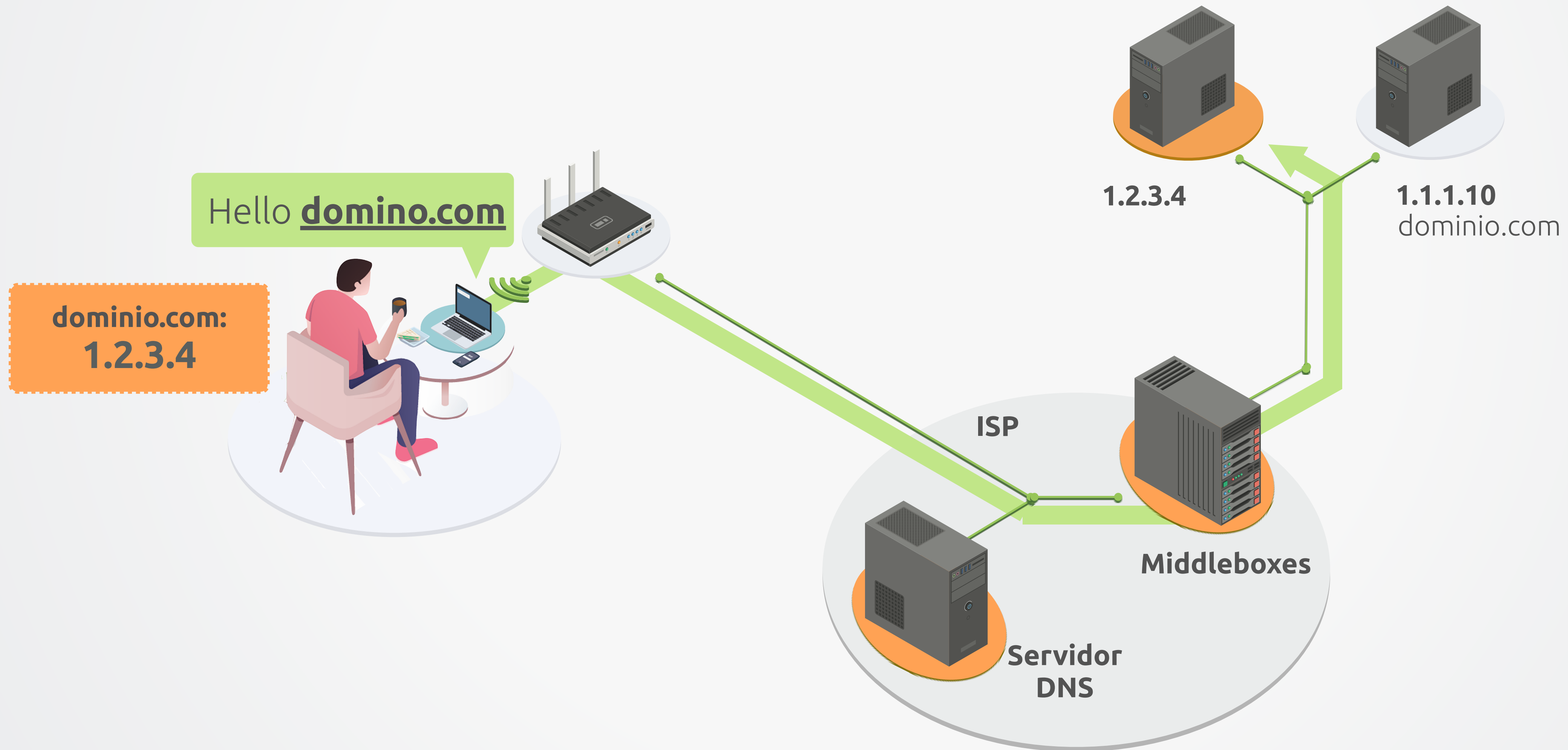
1 ↻ ♥ ↗

 **Alexander Rodriguez** @alerodriguez150 · Feb 11

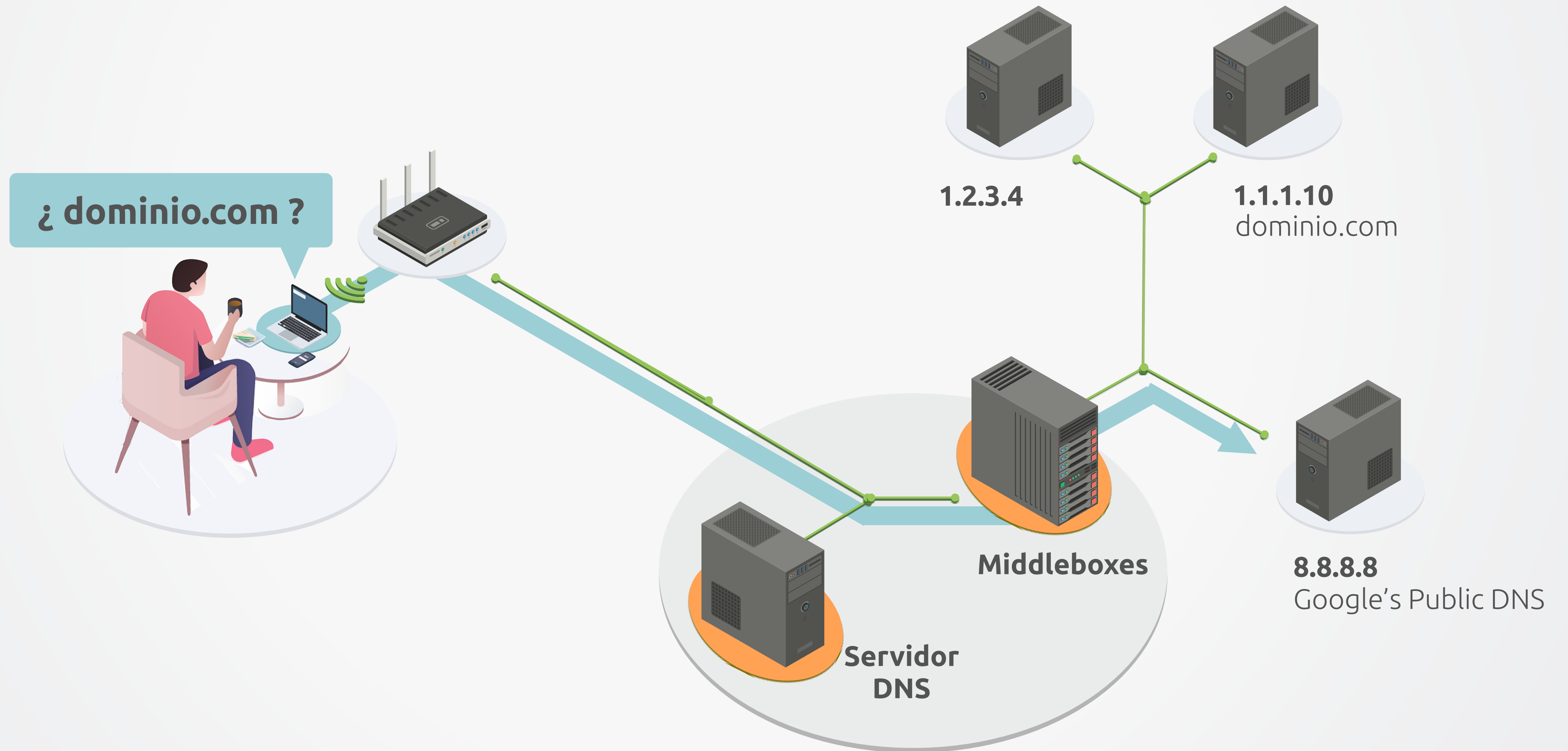
DNS manipulation



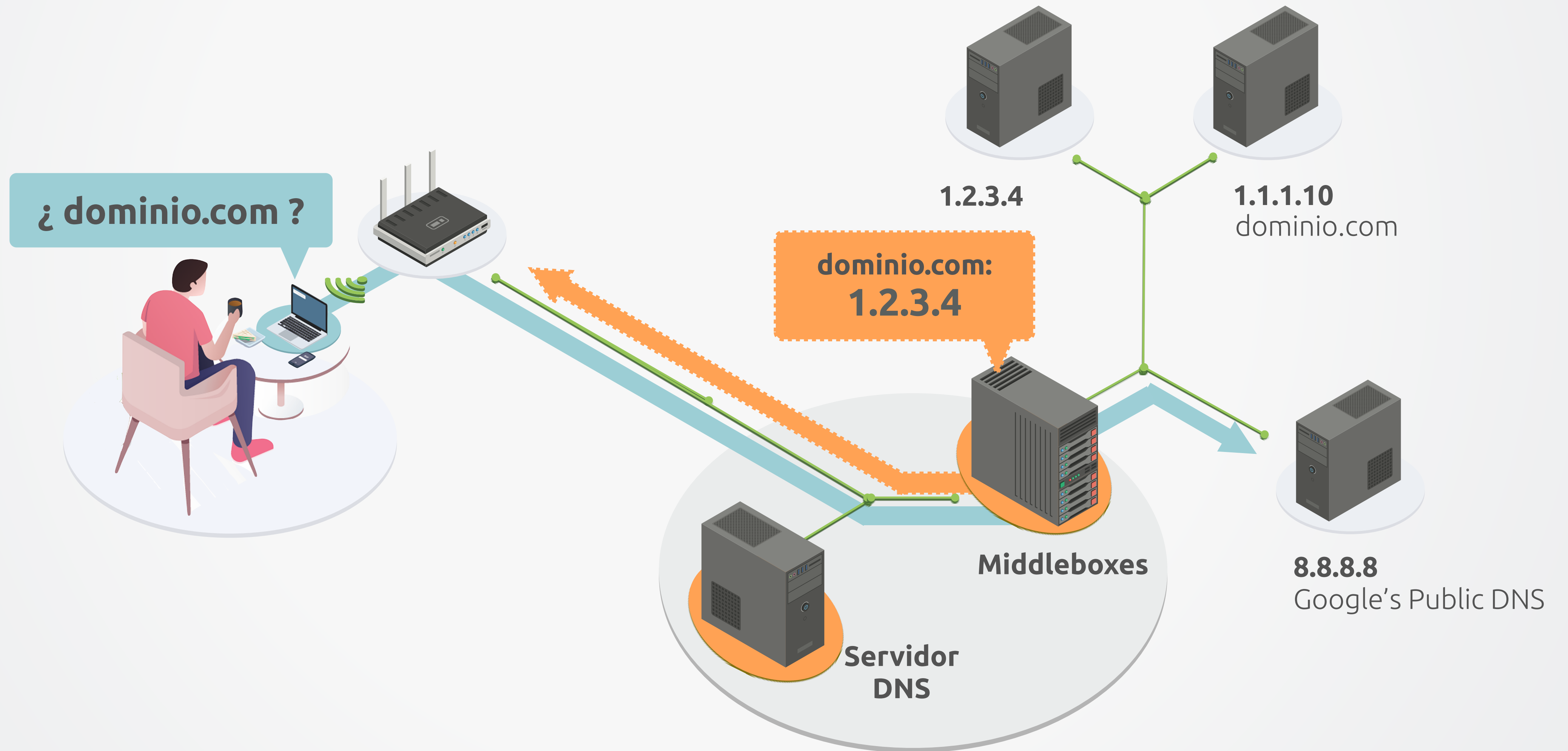
DNS manipulation



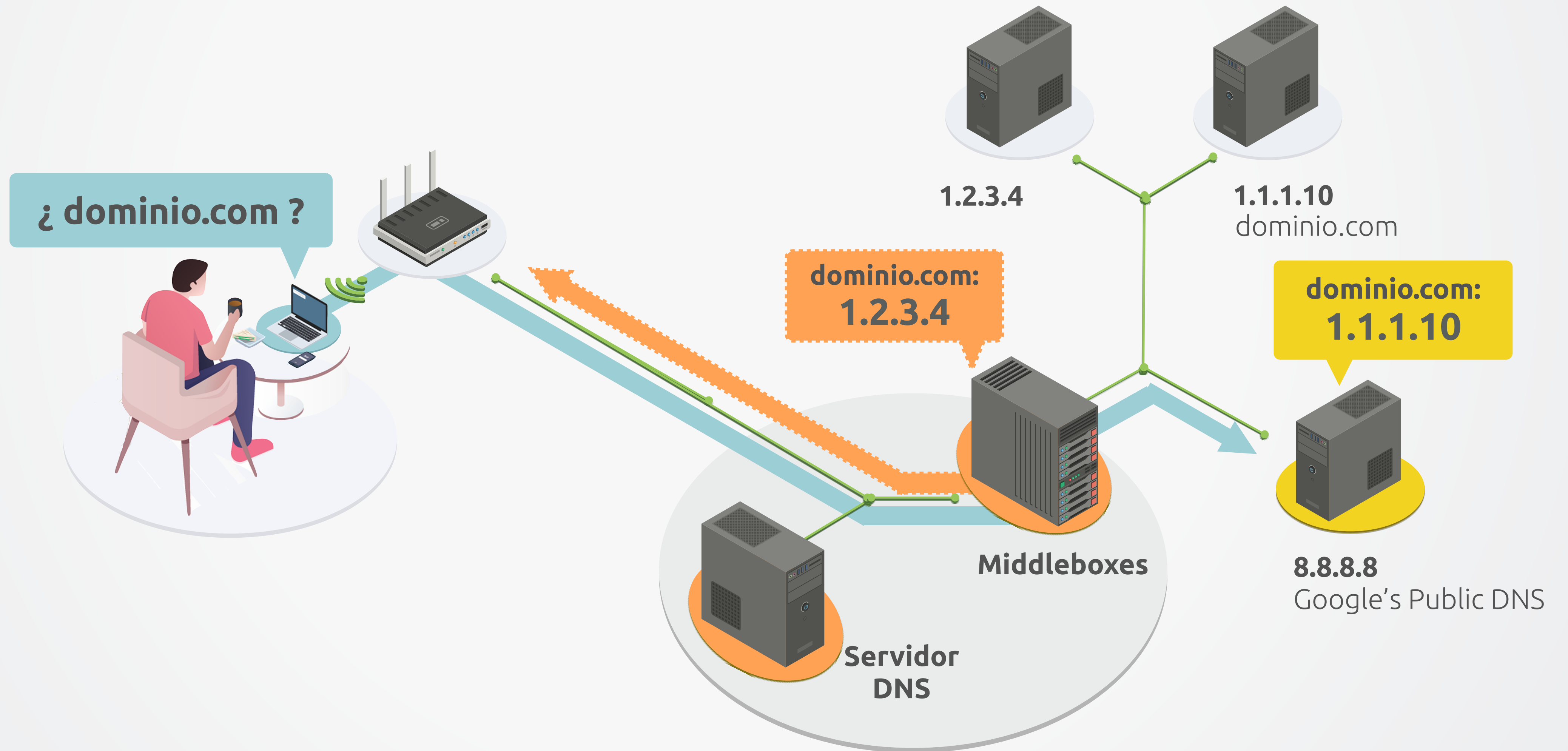
DNS manipulation



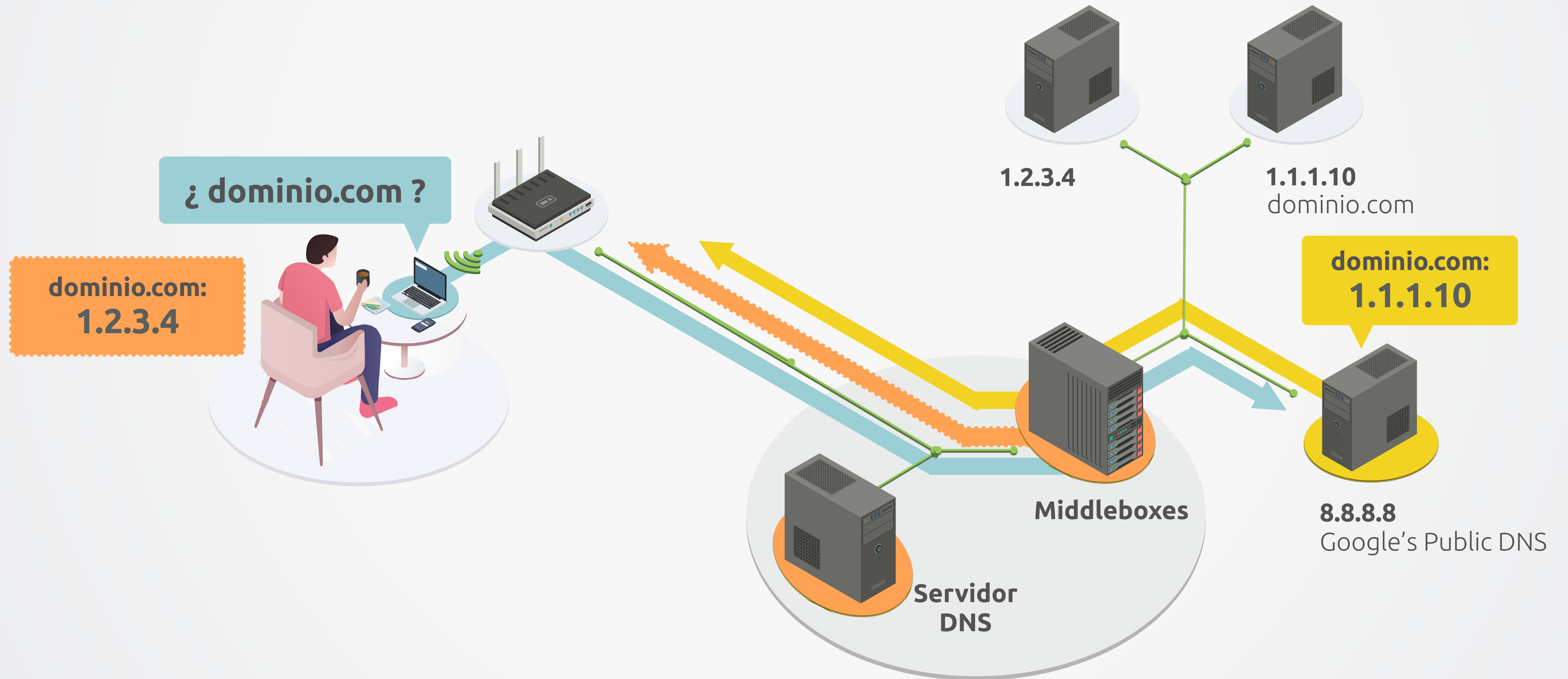
DNS manipulation



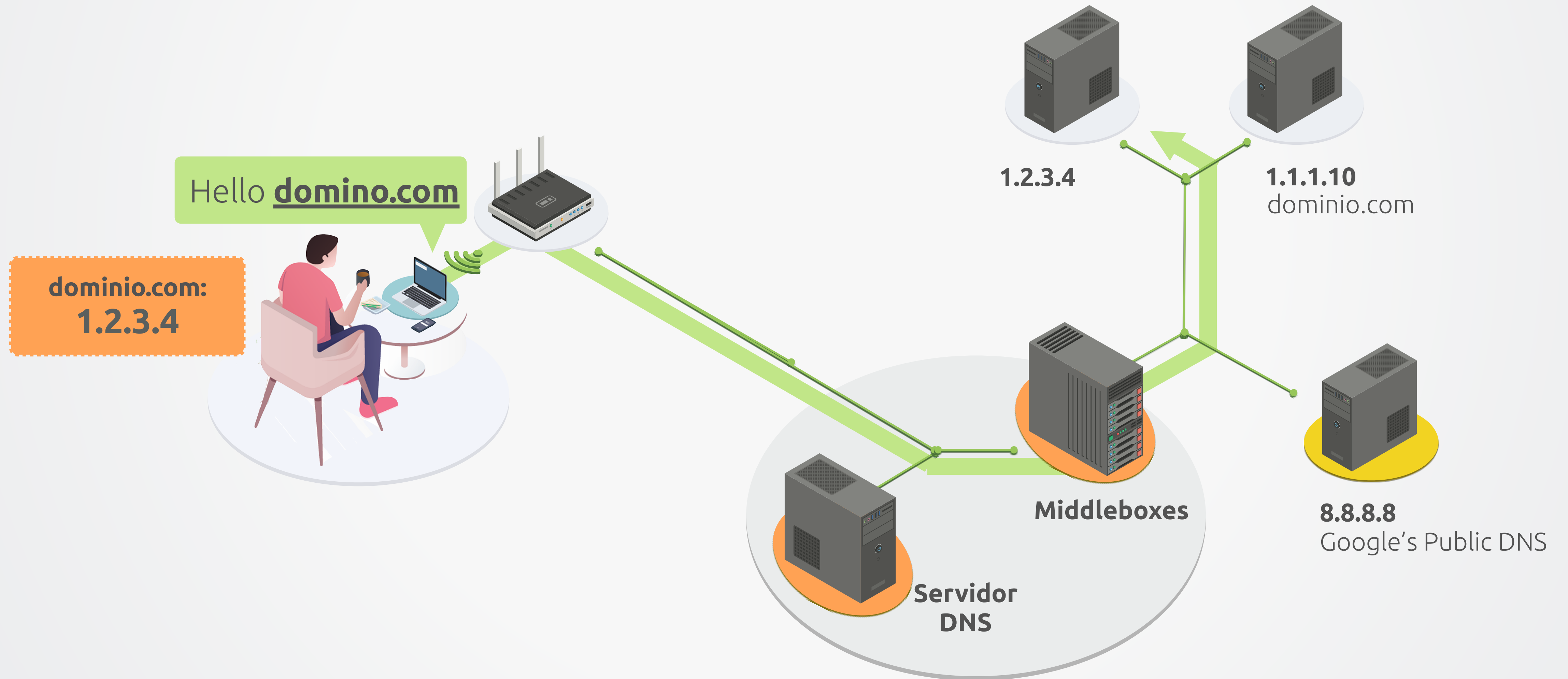
DNS manipulation



DNS manipulation



DNS manipulation



Fuel for fake news



Lechuginos 
@Lechuginos_com

Conozca aquí a Luis Carlos Diaz el nerd que aunque trate de ocultarle a sus aliados el gran error que cometió, jamás podrá negar que por de 10 MIL DOLARES vendió la base de datos de los inscritos en voluntariosxvenezuela.com

Muchas gracias @LuisCarlos ahora sabemos quién es quien

311 2:35 - 18 feb. 2019

947 personas están hablando de esto

fanbrg Retweeted

00x00 @The_00x00 · Feb 17

OJO las advertencias se hicieron en su debido momento hasta @jguaido lo sabía y también el ing @andresAzp pdte de @ISOC_Venezuela @LuisCarlos @joseluisrivas @phenobarbital todos especialistas en él área pero por razones desconocidas no atendieron nuestro llamado

Translate Tweet

Juan Guaidó @jguaido · 14 feb.

Ya estamos listos para comenzar la Conferencia Mundial de la Crisis Humanitaria en Venezuela. Vamos a articular un esfuerzo internacional sin precedentes para atender a los venezolanos.

Pueden seguir en vivo el evento en ayudahumanitariavenezuela.com
#AvalanchaHumanitaria

Inicio
En Venezuela se registra una emergencia humanitaria compleja en la que millones de personas no tienen acceso a comida, medicinas o insumos médicos. Debi...
ayudahumanitariavenezuela.com

211 4,7K 8,5K

yoel duran @yoel_duran28

En respuesta a @jguaido

Urgente mi presidente necesito notificarle vulnerabilidades detectadas en el servidor dónde está alojada la página de voluntarios x Venezuela

9:23 - 14 feb. 2019

Jesus Lara @phenobarbital · 14 feb.

Y lo sé, ya le voy a agradecer pero imagina que se te van a robar, entonces yo le cargo a tres a los malandros, los ahuyento, llamo a la policía, te doy la cola y presentas la denuncia y le regreso a tu casa. Personas como @josegarcia01 o @joseluisrivas merecen el agradecimiento

Jesus Lara @phenobarbital · 14 feb.

Hasta las Gm estuve con los otros panas revisando las redes, que no levantarán otro droplet, que no volverán a contaminar los DNS, haciendo denuncias en Godaddy, contactando a los de ESET, Kaspersky y al sol de hoy ni nos escribieron, ¿nos quedaran ganas? Pues sí.

yoel duran @yoel_duran28

En respuesta a @phenobarbital @gonzalob y a 7 más

Has probado la seguridad del certificado SSL de la página oficial de voluntariosxvenezuela es vulnerable si no lo sabian

17:46 - 14 feb. 2019

yoel duran @yoel_duran28 · 3d

Así es amigo eso puede provocar que un atacante tome el control del servidor y robar la información y que este expuesto a publicar eso

Jose-Luis Rivas @joseluisr... · 1d

Ya va: cómo.

16 31 39

Show this thread

Personal information published

miércoles, junio 12, 2019

INICIO + DESTACADO POLÍTICA LOS SHOWSERS VIDEOS

Inicio > Destacado > ¡DESTAPANDO LA OLLA! Salíó la quinta parte de los nombres de «voluntarios»...

Destacado Lechuguino del día Lechuguinos Política

¡DESTAPANDO LA OLLA! Salíó la quinta parte de los nombres de «voluntarios»... nombres de «voluntarios»... aut... la Guaidó»

22 febrero, 2019

Destacados

¡DIQUE Y LIBRE SIN CHAMBA!

Open "www.lechuguinos.com/politica/" in a new tab

Exposure for 5 thousand victims


INICIO + DESTACADO POLÍTICA LOS SHOWS VIDEOS

| | | | | |
|-------------------|---------------|----------|--------------|----------------------------|
| medina | medina | 23136653 | 04247279540 | yene.mcd@gmail.com |
| joselyn | medina | 23136653 | 04247279540 | yene.mcd@gmail.com |
| ariana | sobry | 28678361 | 286249102480 | gobrya1@gmail.com |
| luis | albernoz | 11124824 | 04247967795 | luciano14@gmail.com |
| crispin | rodriguez | 14792453 | 286144802425 | crispinrodriguez@gmail.com |
| alexander | teguinde | 28678361 | 286147528252 | alexander14@gmail.com |
| edgardo | medina | 28688796 | 286244662834 | edgardo14@gmail.com |
| terhania stefania | acosta | 28688945 | 2862286242 | terhania2019@gmail.com |
| marian | de boumont | 2742534 | 04241497435 | marianaboumont@gmail.com |
| juan carlos | basile guerra | 17288824 | 286144232470 | juancarlosbasile@gmail.com |

¡YA DAS ARRECHERA! Cloaca comunicacional La Patilla entrevistó a Guaidó y los escuálidos le cayeron encima (+INSTAGRAM)

¡NO TE LO PIERDAS! Conozca los tres nuevos billetes que se incorporan al Cono Monetario vigente (+BCV)

¡LADRONES! Venezuela denuncia el saqueo de sus fondos por Estados Unidos y Europa



¡DUQUE Y URIBE SIN CHAMBA! Reapertura del paso fronterizo en Táchira...

12 junio, 2019

La reapertura del paso fronterizo entre Colombia y Venezuela, por el estado Táchira le tumba los negocios a los paracos dirigidos por Álvaro Uribe...



More domains

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

Example: accounts.gmail.com

accounts.gmail.web.ve

Sign in - Google Accounts

URL <http://accounts.gmail.web.ve/>

Redirected URL: <https://accounts.gmail.web.ve/signin/v2/identifier?passive=1209600&continue=https%3A%2F%2Faccounts.google.com%2FManageAccount&followup=https%3A%2F%2Faccounts.google.com%2FManageAccount&flowName=GlifWebSignIn&flowEntry=ServiceLogin>

Disposition: phish

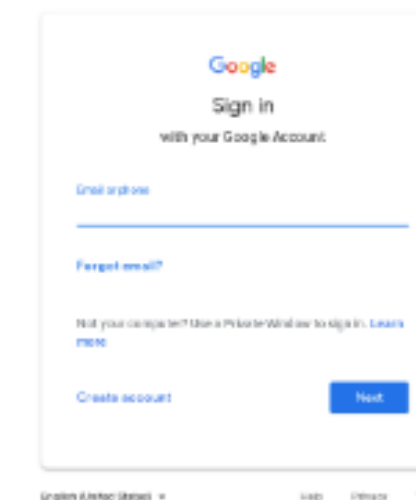
Brand: [Google](#)

IP: [159.65.65.194](#)

Scan Time: Aug 16, 2018, 6:33:52 AM

[Dispute Verdict](#)

Screenshot



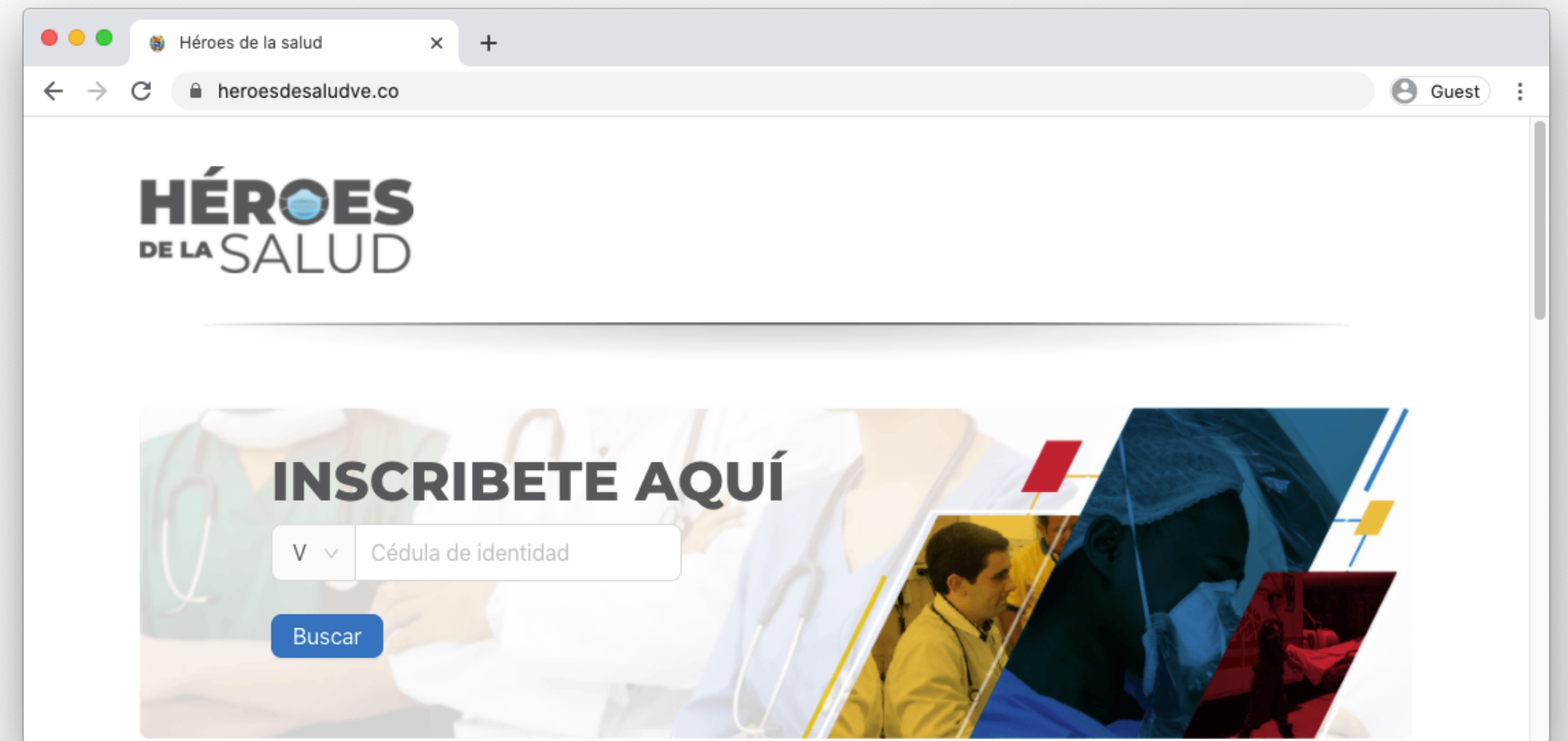
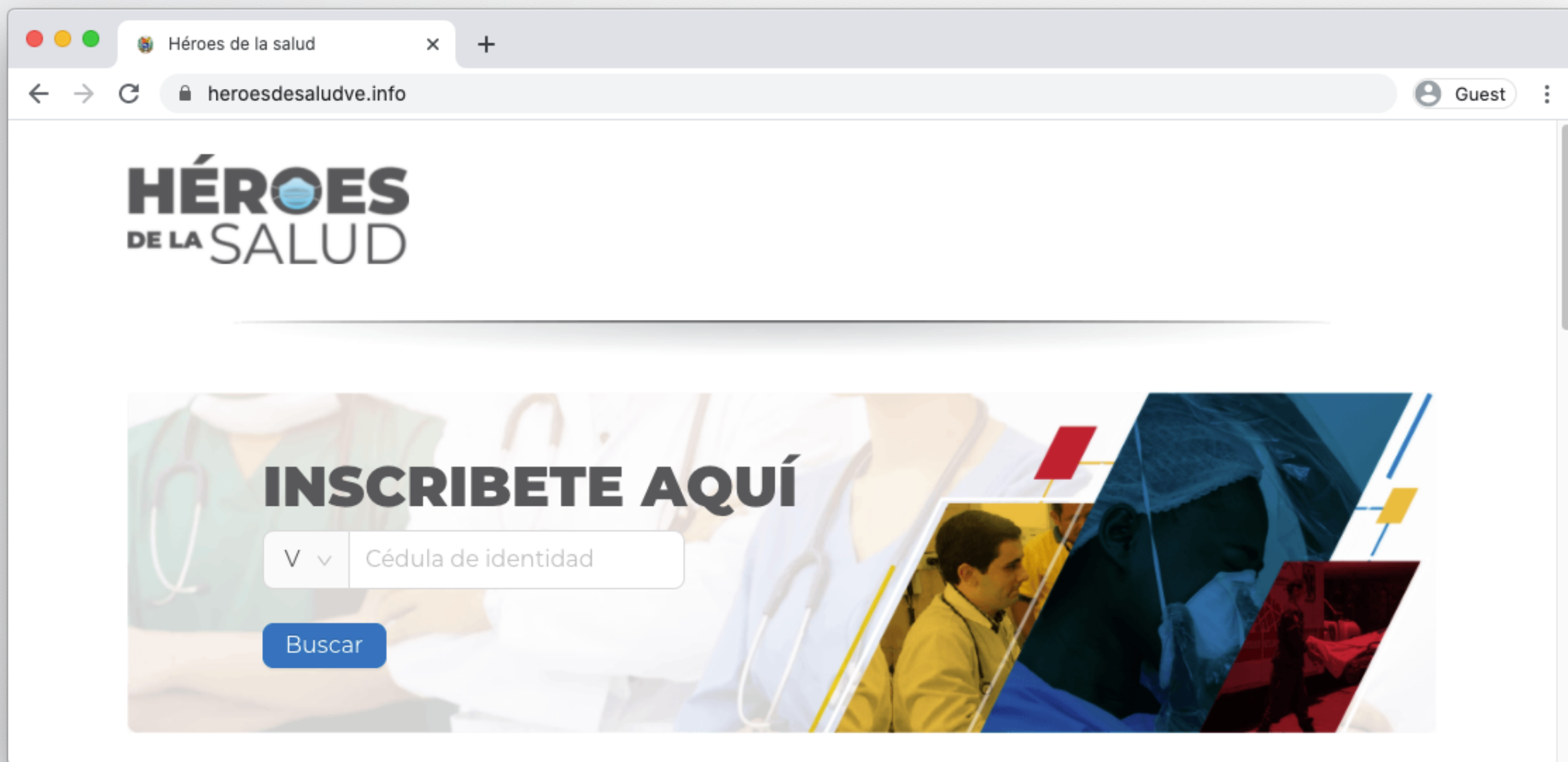
Inconsistent DNS responses documented

- OONI mobile app
run.ooni.io
- Package capture of manual experiments

Case: Héroes de la salud



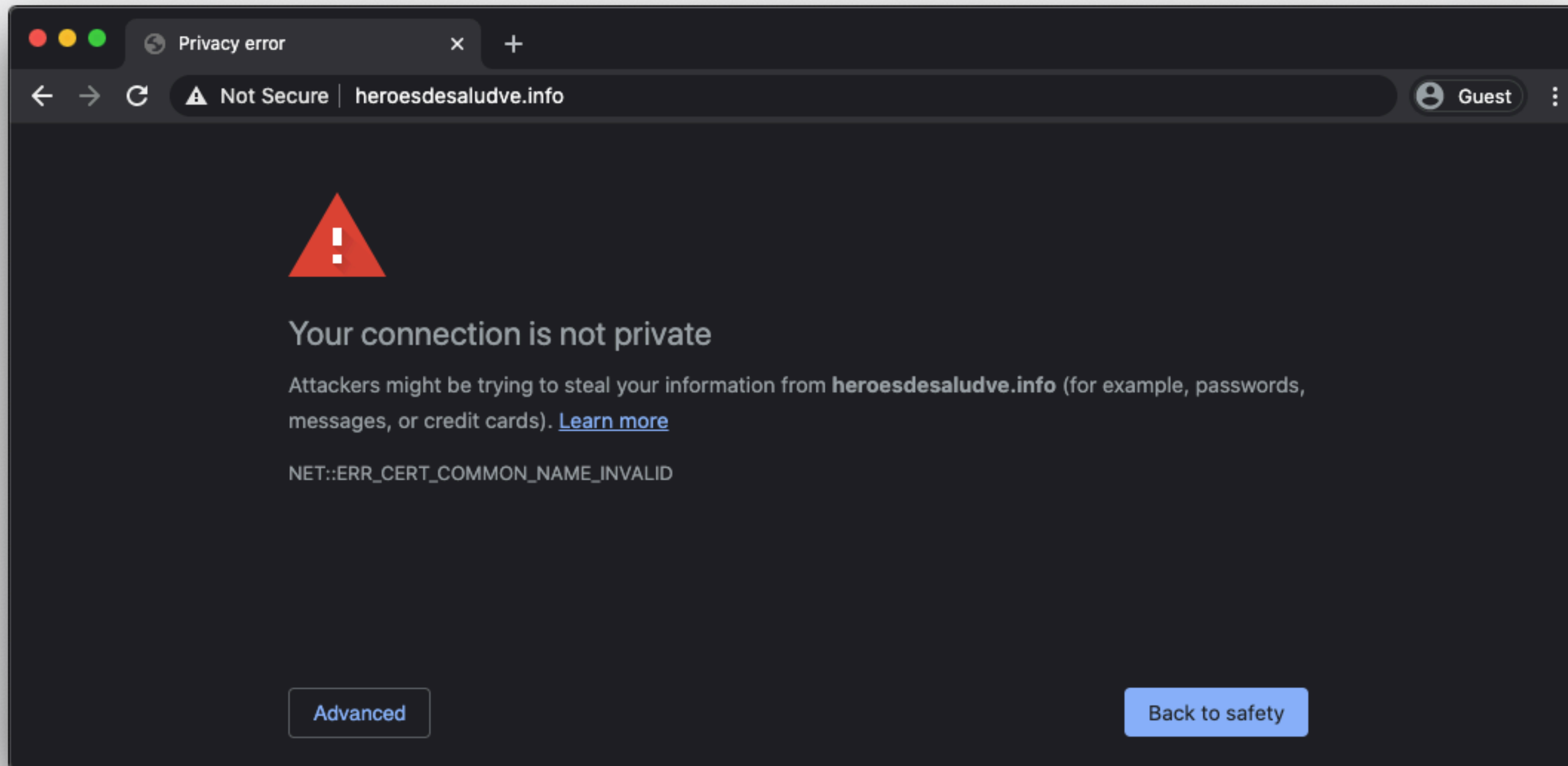
Case: Héroes de la salud



Selectively (not) blocking

| Sitio | URL | CANTV | Movistar | Digitel | Inter | Supercable |
|-------------------------------------|---|-----------------|-------------|-------------|-------------|-------------|
| Coronavirus Venezuela | http://coronavirusvenezuela.info | BLOQUEO DNS * | BLOQUEO DNS | BLOQUEO DNS | ACCESIBLE | ACCESIBLE |
| Heroes de la Salud, apoyo acovid-19 | https://apoyosaludve.com/ | BLOQUEO DNS | BLOQUEO DNS | BLOQUEO DNS | BLOQUEO DNS | BLOQUEO DNS |
| Heroes de la Salud, apoyo covid-19 | https://heroesdesaludve.org/ | BLOQUEO DNS | BLOQUEO DNS | BLOQUEO DNS | BLOQUEO DNS | N /A |
| Heroes de la Salud, apoyo covid-19 | https://heroesdesaludve.info/ | DNS POSONING | BLOQUEO DNS | BLOQUEO DNS | BLOQUEO DNS | N /A |
| Teleconsulta COVID-19 | https://teleconsulta.presidenciave.org/ | ACCESIBLE | BLOQUEO DNS | ACCESIBLE | ACCESIBLE | ACCESIBLE |
| Teleconsulta COVID-19 | https://medicos.presidenciave.org | ACCESIBLE | BLOQUEO DNS | ACCESIBLE | ACCESIBLE | ACCESIBLE |
| Presidencia VE (J. Guaidó) | https://presidenciave.com/ | ACCESIBLE | BLOQUEO DNS | BLOQUEO DNS | BLOQUEO DNS | BLOQUEO DNS |
| Presidencia VE (J. Guaidó) | http://presidenciave.org | ACCESIBLE | BLOQUEO DNS | BLOQUEO DNS | BLOQUEO DNS | BLOQUEO DNS |
| Presidencia VE (J. Guaidó) | https://pvenezuela.com/ | BLOQUEO DNS | ACCESIBLE | ACCESIBLE | ACCESIBLE | ACCESIBLE |
| Presidencia VE (J. Guaidó) | http://vepresidencia.com/ | BLOQUEO DNS | ACCESIBLE | ACCESIBLE | ACCESIBLE | ACCESIBLE |

Similar M.O.



After server was disabled

| Site | Dominio | CANTV | Movistar | Digitel | Supercable | Inter |
|----------------------------|--------------------------------|---------------|---------------|---------------|---------------|-------------|
| Coronavirus Venezuela | coronavirusvenezuela.info | ACCESIBLE | BLOQUEO DNS | BLOQUEO DNS | BLOQUEO DNS | ACCESIBLE |
| Heroes de la Salud | apoyosaludve.com | BLOQUEO DNS | BLOQUEO DNS | BLOQUEO DNS | BLOQUEO DNS | BLOQUEO DNS |
| Heroes de la Salud | heroesdesaludve.org | * BLOQUEO DNS | * BLOQUEO DNS | * BLOQUEO DNS | * BLOQUEO DNS | BLOQUEO DNS |
| Heroes de la Salud | heroesdesaludve.info | * BLOQUEO DNS | * BLOQUEO DNS | * BLOQUEO DNS | * BLOQUEO DNS | BLOQUEO DNS |
| Heroes de la Salud | porlasaludve.com | BLOQUEO DNS | BLOQUEO DNS | BLOQUEO DNS | BLOQUEO DNS | BLOQUEO DNS |
| Heroes de la Salud | saludvzla.com | * BLOQUEO DNS | * BLOQUEO DNS | * BLOQUEO DNS | BLOQUEO DNS | BLOQUEO DNS |
| Heroes de la Salud | apoyoheroesaludve.com | BLOQUEO DNS | BLOQUEO DNS | BLOQUEO DNS | BLOQUEO DNS | BLOQUEO DNS |
| Teleconsulta COVID-19 | teleconsulta.presidenciave.org | ACCESIBLE | BLOQUEO DNS | BLOQUEO DNS | ACCESIBLE | ACCESIBLE |
| Teleconsulta COVID-19 | medicos.presidenciave.or | ACCESIBLE | BLOQUEO DNS | ACCESIBLE | ACCESIBLE | ACCESIBLE |
| Presidencia VE (J. Guaidó) | presidenciave.com | ACCESIBLE | BLOQUEO DNS | BLOQUEO DNS | BLOQUEO DNS | BLOQUEO DNS |
| Presidencia VE (J. Guaidó) | presidenciave.org | ACCESIBLE | BLOQUEO DNS | BLOQUEO DNS | BLOQUEO DNS | BLOQUEO DNS |
| Presidencia VE (J. Guaidó) | pvenezuela.com | BLOQUEO DNS | BLOQUEO DNS | BLOQUEO DNS | BLOQUEO DNS | BLOQUEO DNS |
| Presidencia VE (J. Guaidó) | vepresidencia.com | BLOQUEO DNS | BLOQUEO DNS | BLOQUEO DNS | BLOQUEO DNS | BLOQUEO DNS |

Not current snapshot

Inconsistent DNS responses documented

- OONI mobile app
run.ooni.io
- Package capture of manual experiments
- RIPE Atlas