

VE SIN FILTRO

Andrés E. Azpúrua

#imv2020

Venezuela
►inteligente

Internet Censorship, DNS poisoning and Phishing in Venezuela

Measuring from censorship to
state-sponsored attacks

Andrés E. Azpúrua

#imv2020



VEsinFiltro.com

@VEsinFiltro

The screenshot shows a dark-themed web browser window for vesinfiltro.com/noticias/state_of_internet_c. The main heading is "The State of Internet Censorship in Venezuela." Below it is the date "August 16, 2018" and author information: "Autor: Andrés Azpúrua (Venezuela Inteligente / VEsinFiltro), Mariengracia Chirinos (IPYS Venezuela), Leonid Evdokimov (OONI), Maria Xynou (OONI)". A large orange circular overlay is positioned in the top right corner of the page content area.

VE SIN FILTRO
Infórmate sobre el estado de internet en Venezuela

Noticias Reporta Test Evade los bloqueos Todas las guías 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 screenshot shows a dark-themed Twitter thread from the account [@VEsinFiltro](https://twitter.com/vesinfiltro/status/114811111111111111). The first tweet discusses the removal of a YouTube block. Subsequent tweets provide details about the duration of the incident and its impact on CANTV, #internetVE, and #Venezuela. A screenshot of a VEsinFiltro dashboard is also shown, indicating a YouTube block by CANTV using a TCP block method.

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 1 hora 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 Método TCP block

VE SIN FILTRO @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-apagón-caracas-
noticia-1185399](https://rpp.pe/mundo/actualidad/venezuela-venezolanos-recogen-agua-del-contaminado-rio-guaire-debido-a-la-escasez-por-apagón-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

Persecution of online speech



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.oni.io links

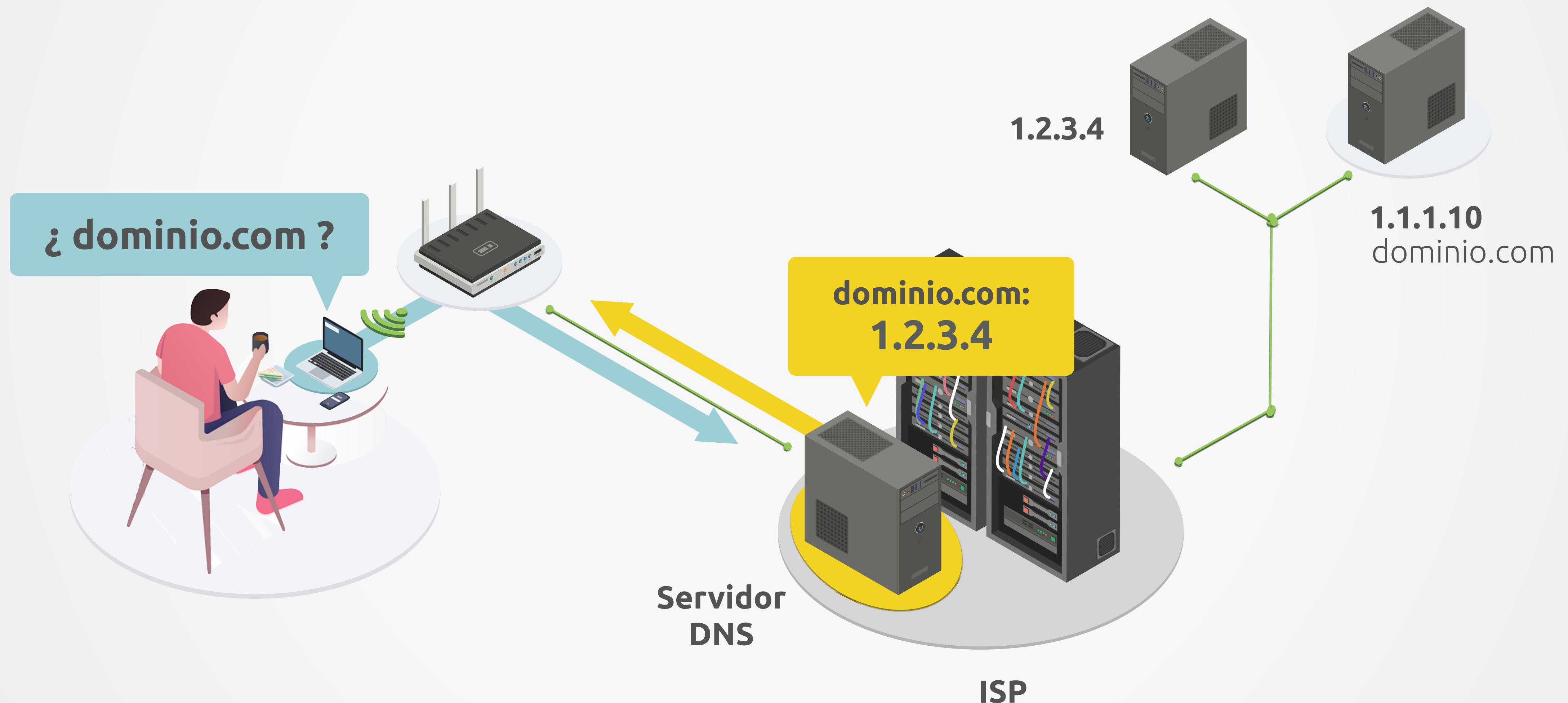
- Fundamental to quickly get multiple measurements fast
- Critical for unexpected incidents
- Key to bridge any gaps
- Faster turnaround of measurements

Measuring probes

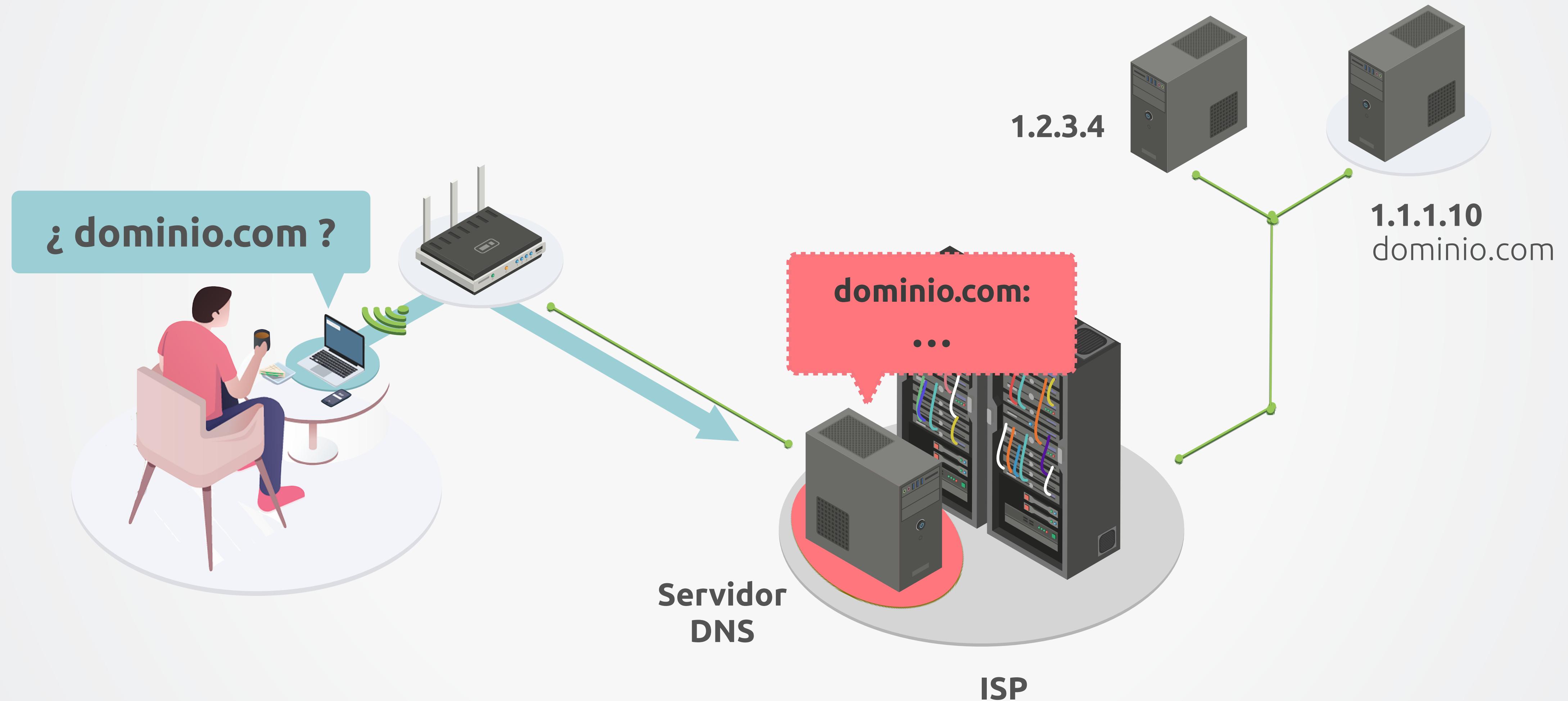
- Guaranteed more data points of whole list
- Increased test frequency based on URL importance
- Alternative tests:
 - High intensity dns, tcp, filtering by http host and SNI
 - Block rate when needed
- Currently migrating versions, to be released

ATLAS probes

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



DNS Blocks

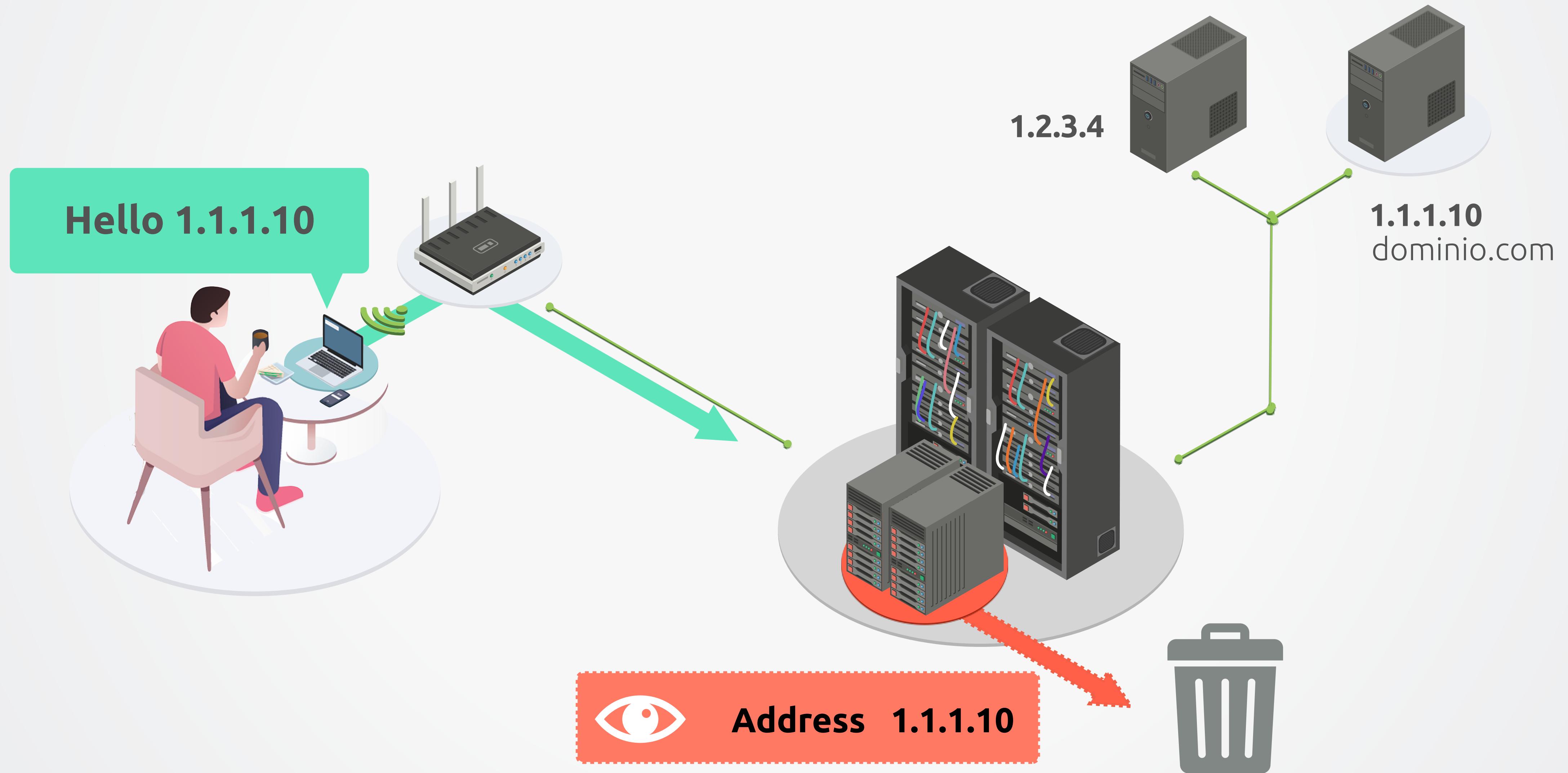


DNS Blocks

On all mainstream ISPs

Domain	Typical answer	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

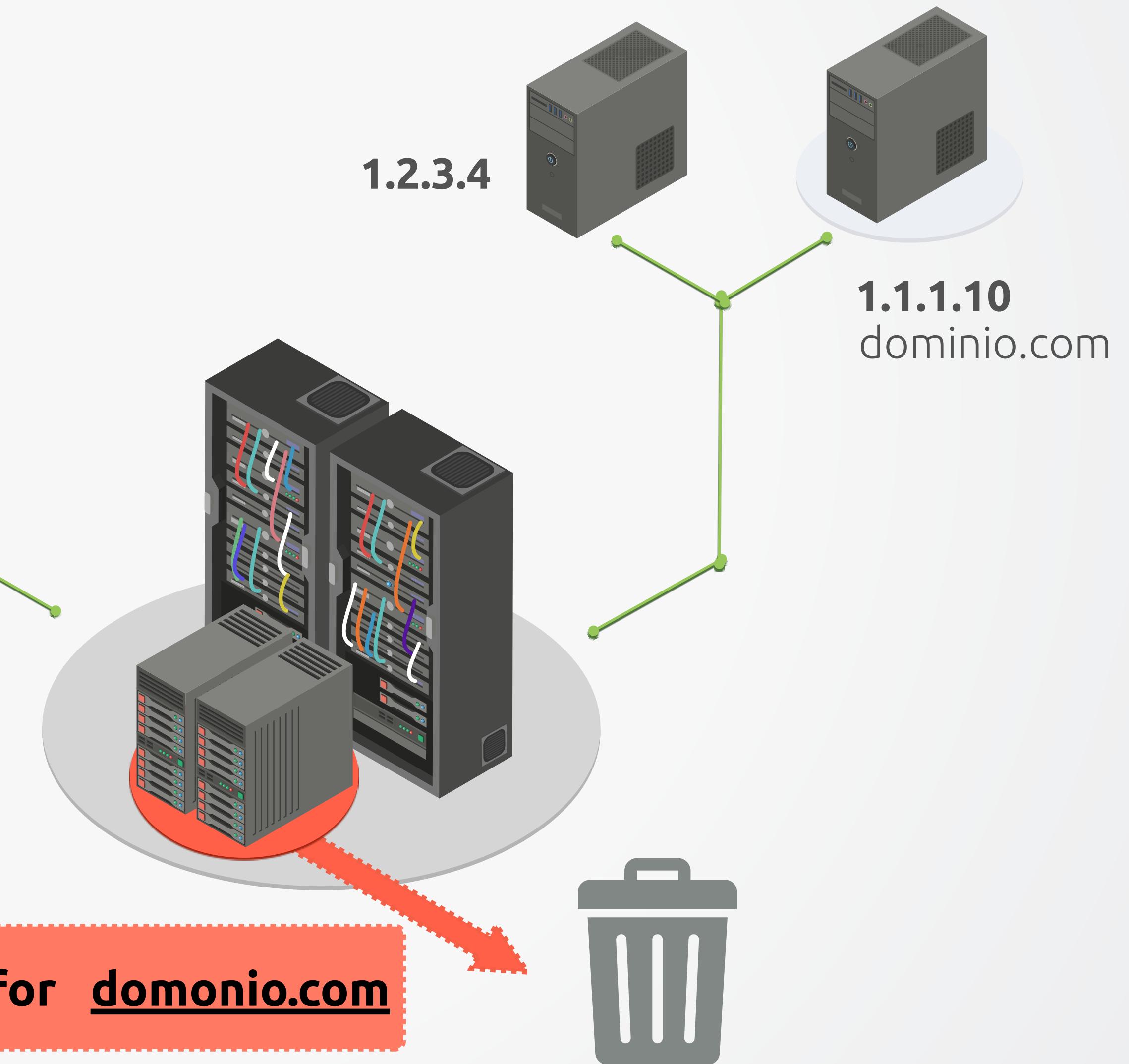


TCP blocks

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

HTTP blocks

Hello 1.1.1.10:
I want dominio.com



👁 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

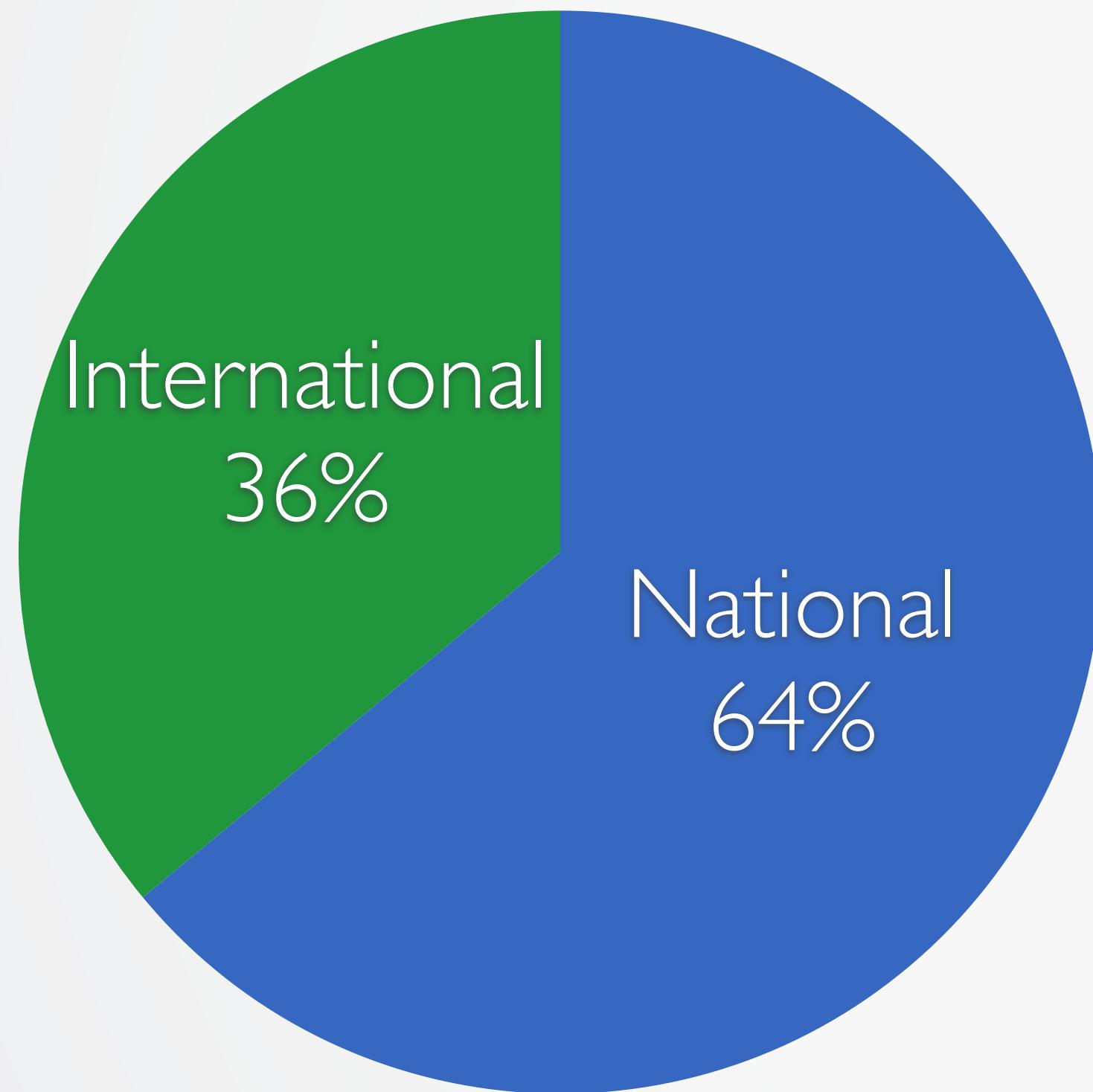
**Blocking of opposition
COVID-19 initiatives**

**Seemingly degraded DPI
blocking capacity**

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

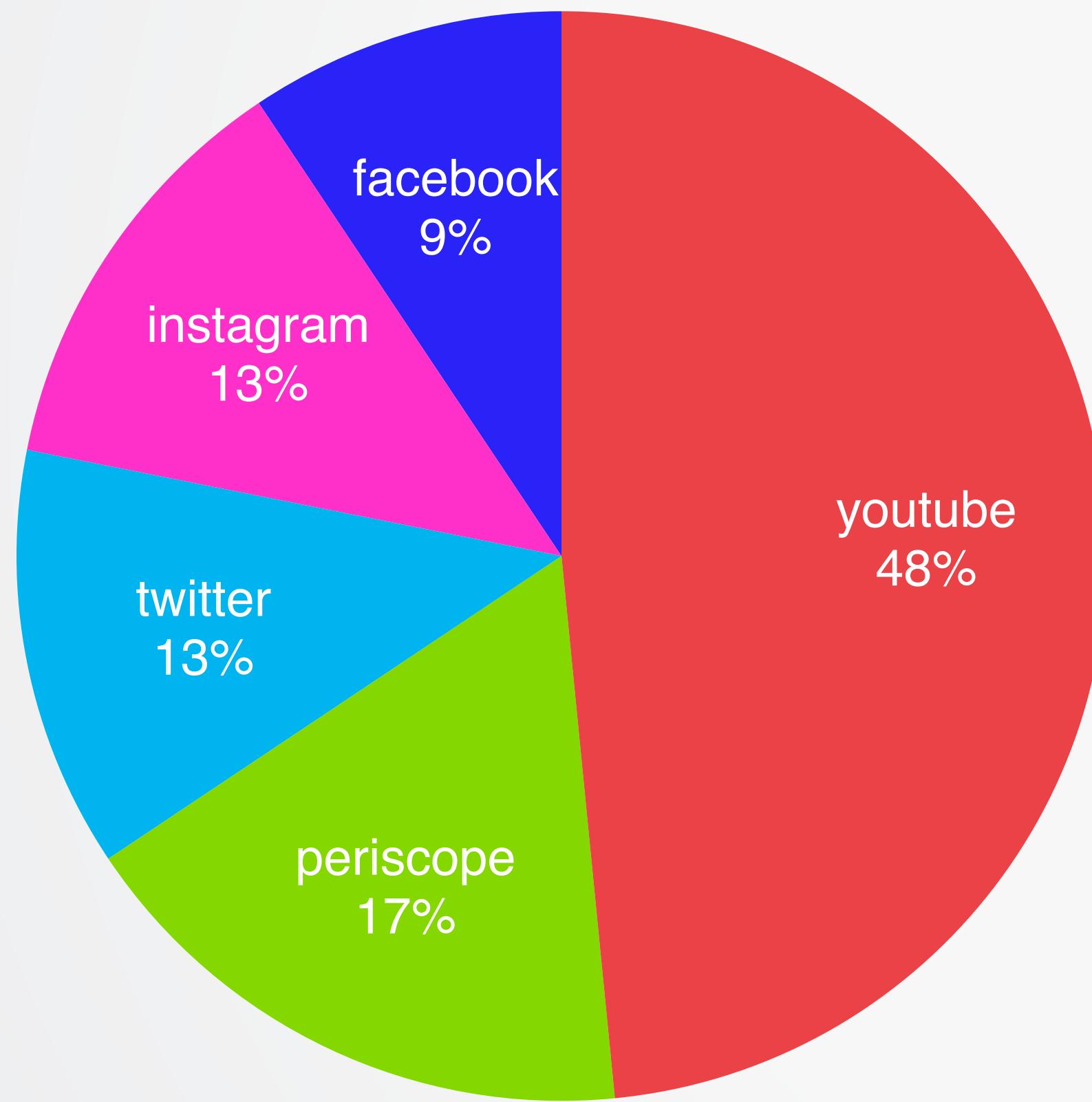
New blocks to news media

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 displaying the website www.voluntariosxvenezuela.com. The page features a large background image of many hands raised, symbolizing volunteerism. On the left side, there is a sidebar with social media links for Twitter, Instagram, and Facebook, and a "SABER MÁS" button. The main navigation menu includes "ESTADO ACTUAL", "¿CÓMO AYUDAR?", the logo for "Coalición Ayuda y Libertad Venezuela VOLUNTARIOS", "DESCARGAR EL KIT", and a prominent blue "REGÍSTRATE" button. To the right of the registration form, there is a dropdown menu for "Profesional de la salud".

ESTADO ACTUAL ¿CÓMO AYUDAR?

Coalición
Ayuda y
Libertad
Venezuela
VOLUNTARIOS

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

Nombre _____ Apellido _____

Cédula de Identidad _____ Teléfono celular _____

Correo electrónico _____ Profesional de la salud ▾

Tiene teléfono inteligente ▾ Tiene vehículo ▾

País ▾ Estado ▾

Municipio ▾

ESTADO ACTUAL

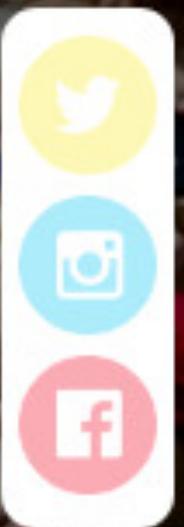
INTERNACIONAL



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

Nombre _____

Apellido _____

Cédula de Identidad _____

Teléfono celular _____

Correo electrónico _____

Profesional de la: _____

Tiene teléfono int. _____

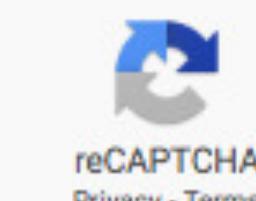
Tiene vehículo _____

País _____

Estado _____

Municipio _____

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](https://twitter.com/voluntariosvene),
vs [@voluntariosxve](https://twitter.com/voluntariosxve)
- Other channels

Malicious links

voluntariovenezuela.com since:2019-02-11 until:2019-02

Top Latest People Photos Videos

Mir(E)angelaRondonoo. @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

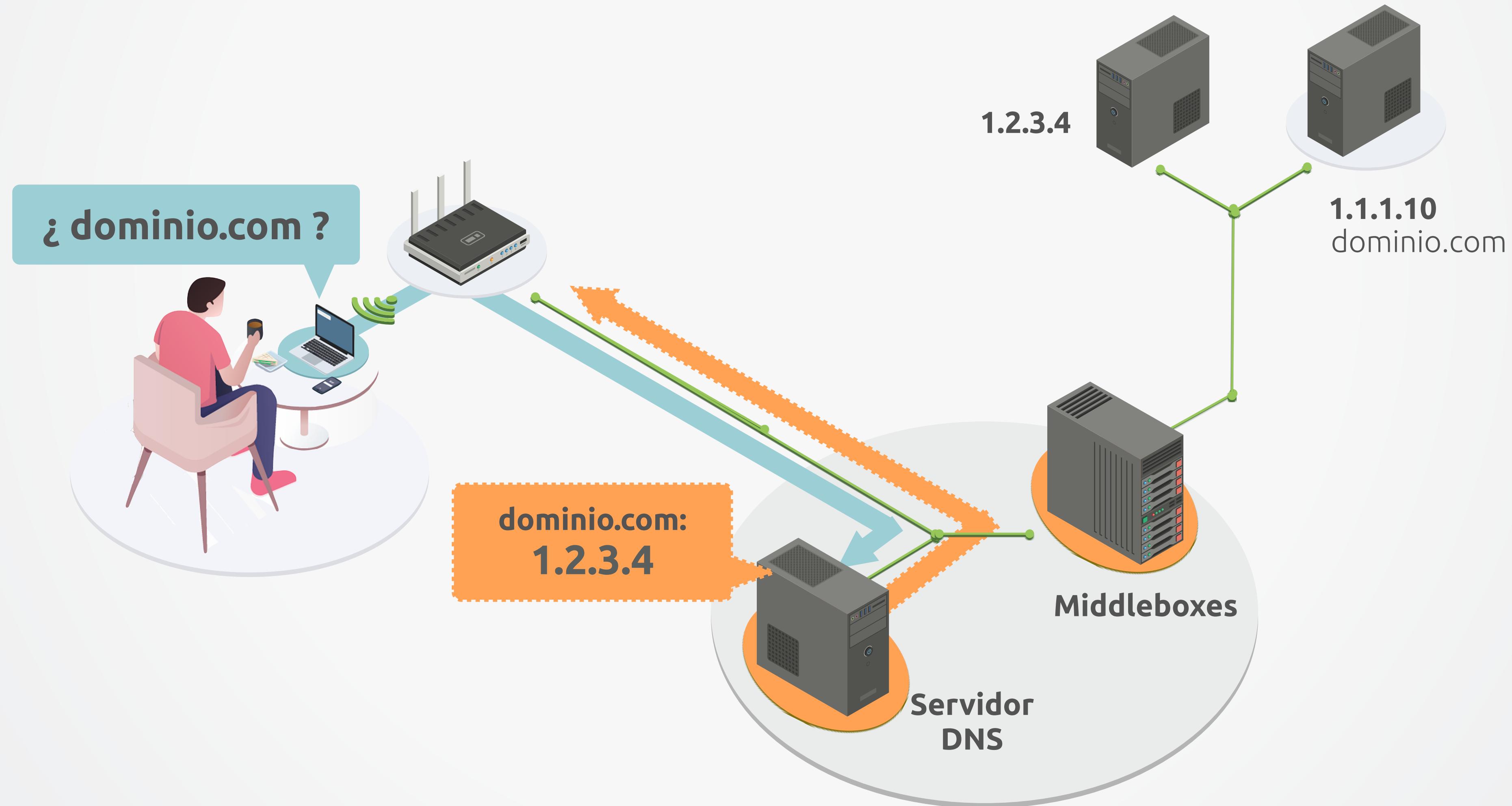
voluntariovenezuela.com

The image grid consists of four square photographs. The top-left photo shows a crowd of people with text overlay: '¿Qué es la ayuda humanitaria?' and 'Insumos médicos y alimenticios brindados a la población víctima de la emergencia humanitaria compleja?'. The top-right photo shows a woman and a child with text overlay: '¿Qué es la emergencia humanitaria compleja?' and 'Es un escenario de vulnerabilidad grave a causa de factores políticos: está en riesgo la vida, salud y mantenimiento de toda una población por factores como la pobreza'. The bottom-left photo shows a crowd with text overlay: '¿Qué es la ayuda humanitaria?'. The bottom-right photo shows a woman with text overlay: '¿Qué es la emergencia humanitaria compleja?'

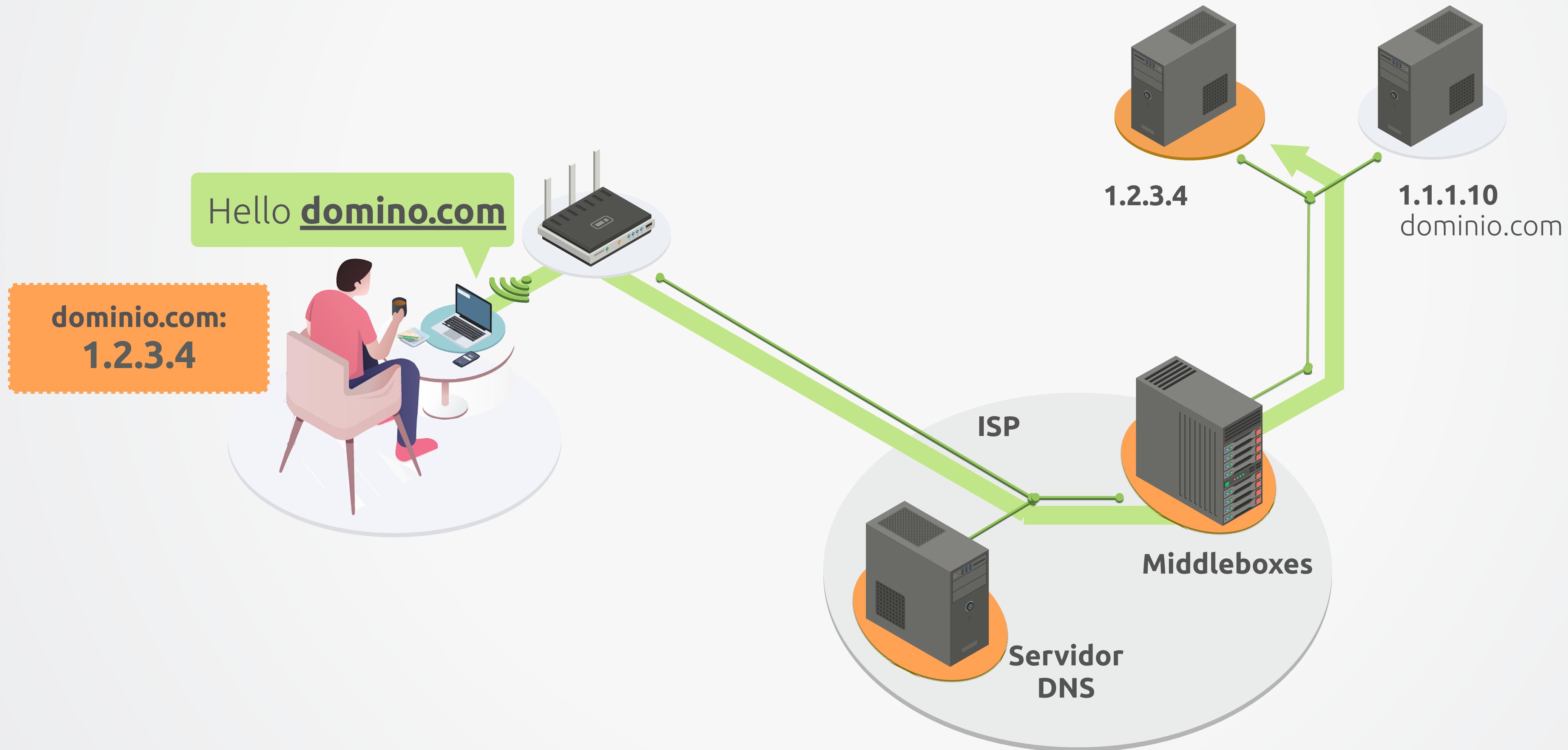
1 ↗ ❤ ↖

Alexander Rodriguez @alerodriguez150 · Feb 11

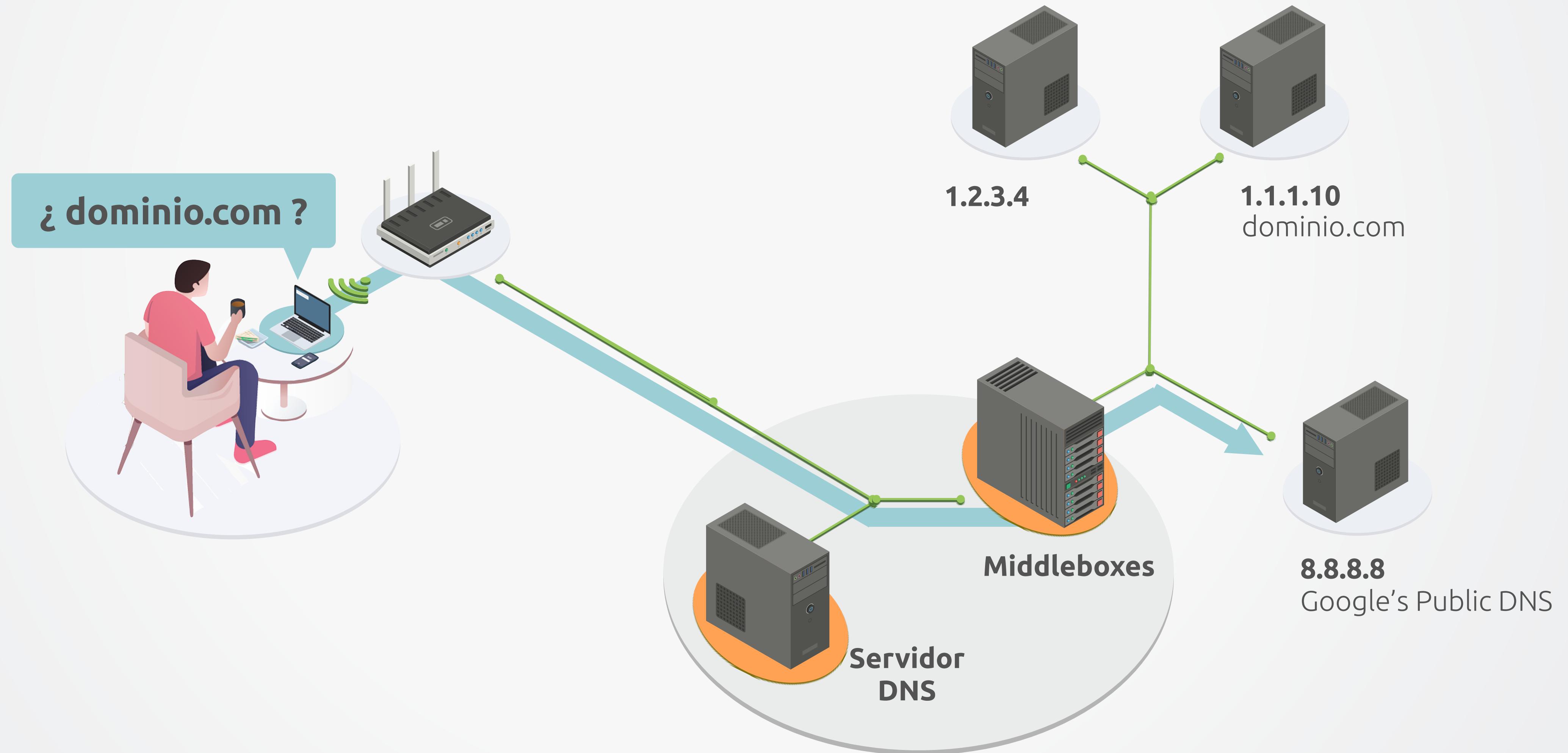
DNS manipulation



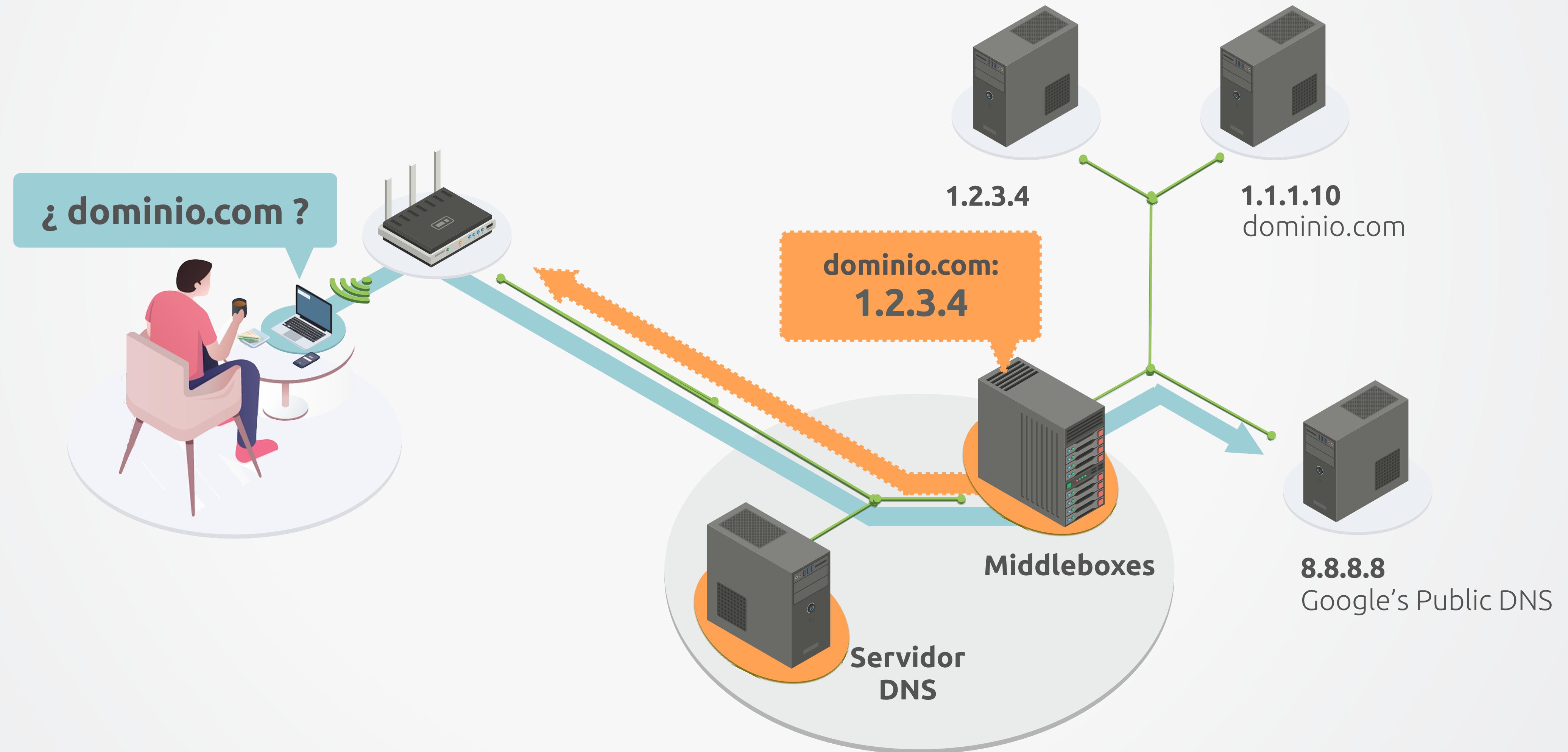
DNS manipulation



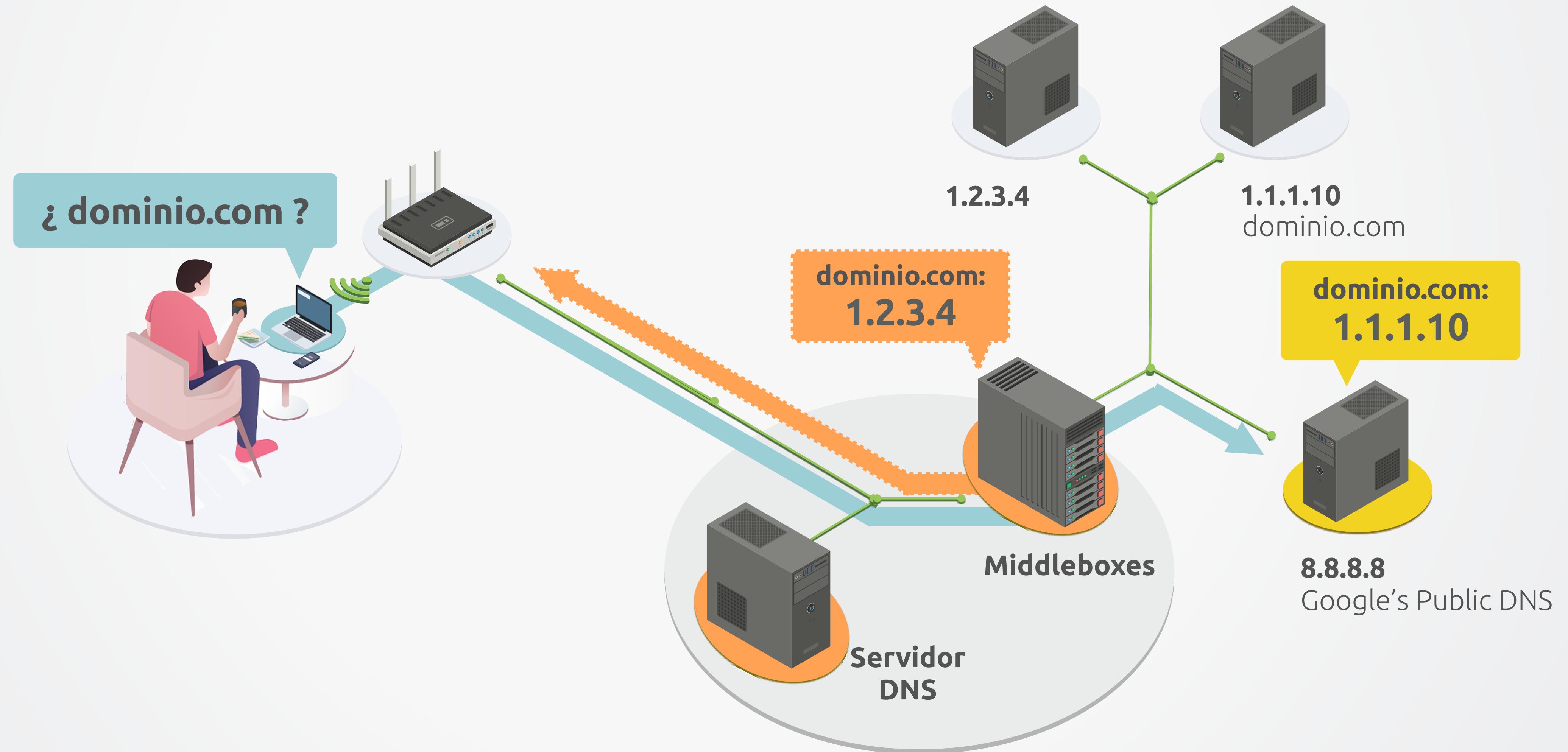
DNS manipulation



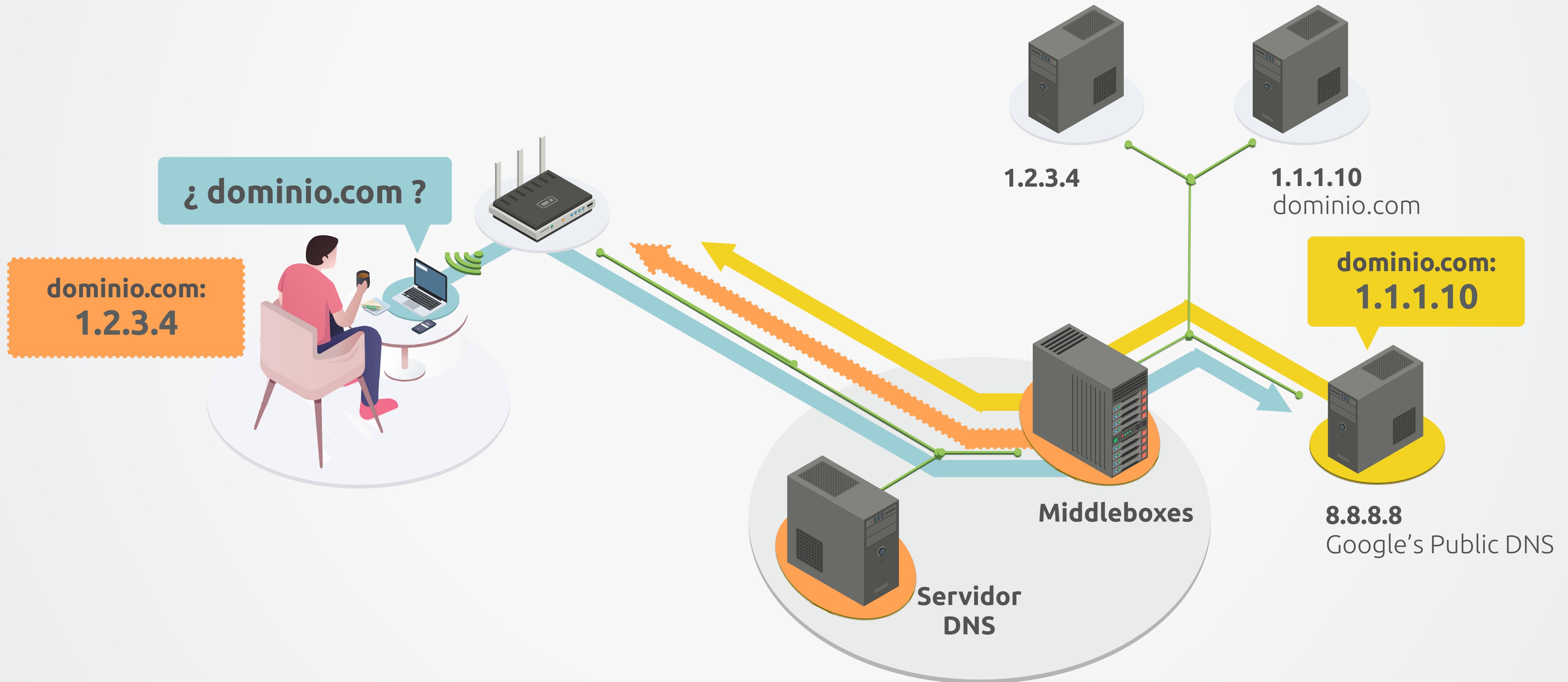
DNS manipulation



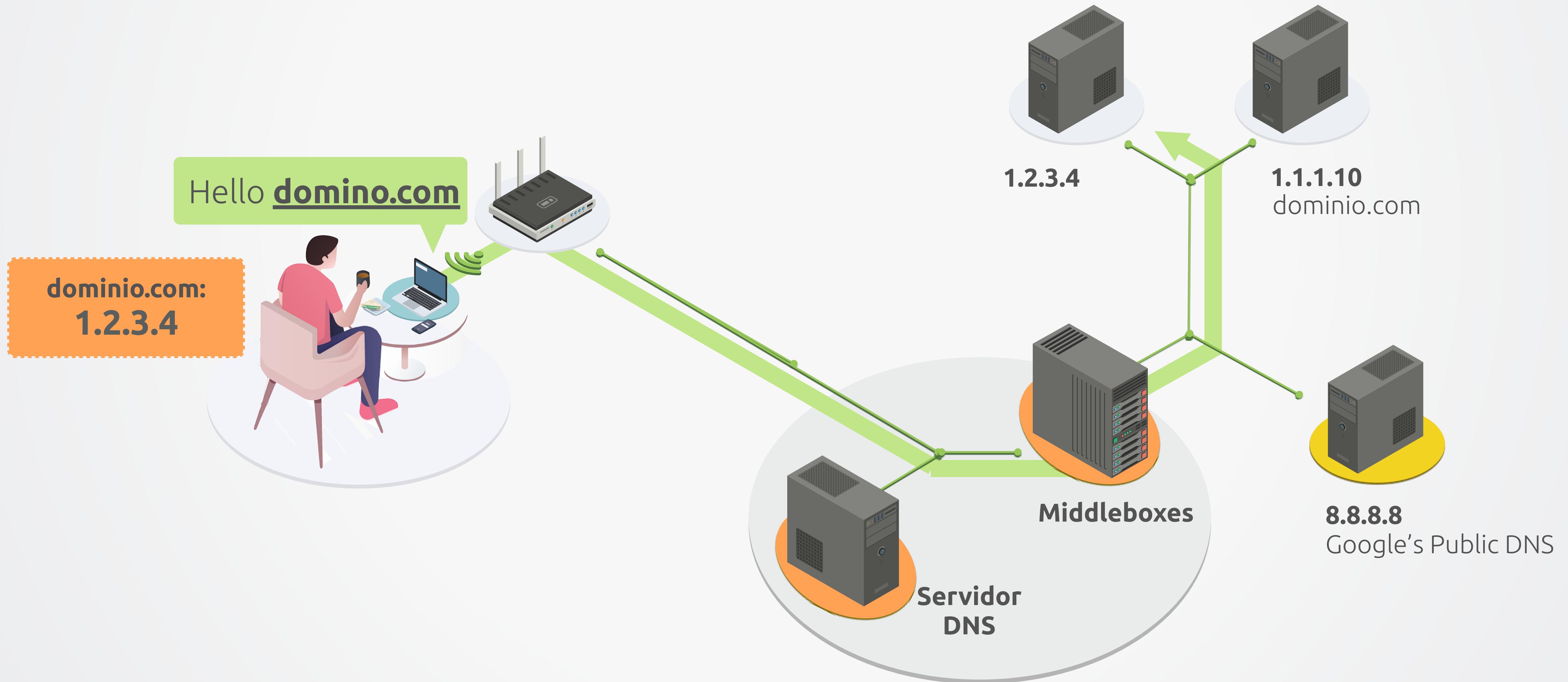
DNS manipulation



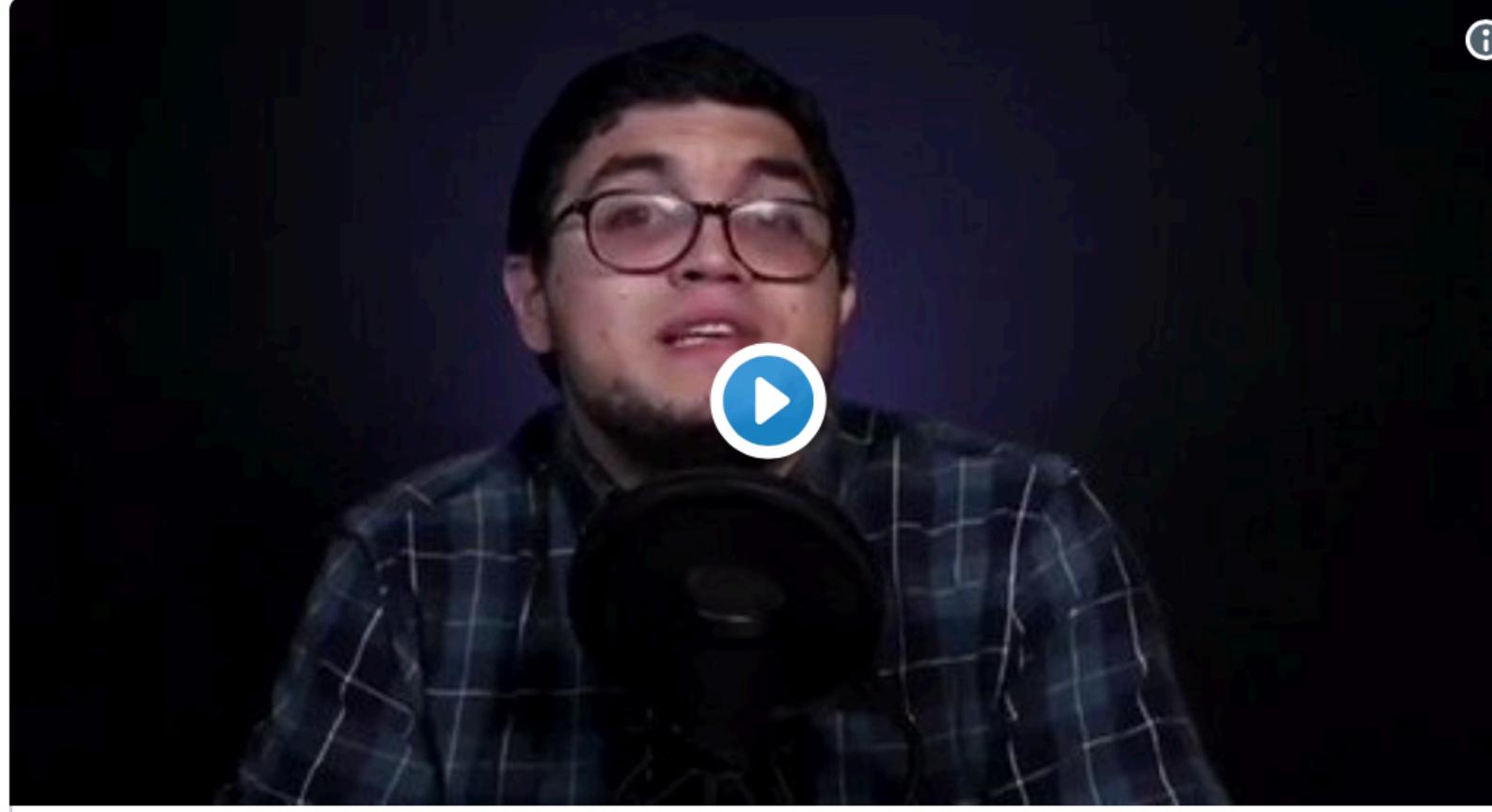
DNS manipulation



DNS manipulation



Fuel for fake news



Lechuguinos  [@Lechuguinos_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

conferencia M de la Crisis Hu n Venezuela

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](#)

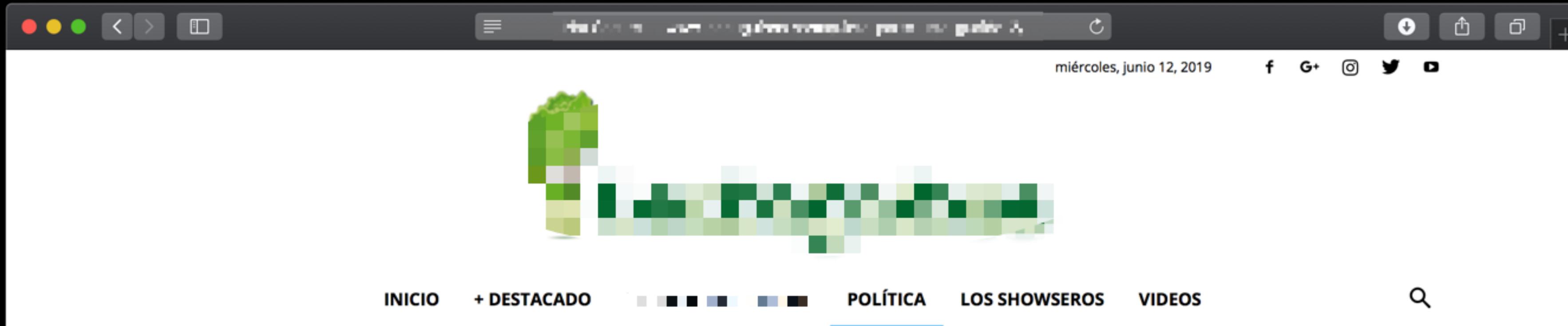
Urgente mi presidente necesito notificarle vulnerabilidades detectadas en el servidor dónde está alojada la página de voluntarios x Venezuela

9:23 - 14 feb. 2019

16 31 39

Show this thread

Personal information published



The screenshot shows a web browser window with a dark header bar. The address bar displays a URL starting with "http://www.lechuguinos.com/politica/". The date "miércoles, junio 12, 2019" is shown in the top right corner, along with social media sharing icons for Facebook, Google+, Instagram, Twitter, and YouTube.

The main content area features a large, pixelated green and white graphic resembling a lechuga (lettuce) on the left. Below it is a navigation menu with tabs: "INICIO", "+ DESTACADO", a series of colored squares, "POLÍTICA" (which is underlined in blue), "LOS SHOWSEROS", "VIDEOS", and a search icon. A small "Q" icon is also present.

The breadcrumb navigation shows the path: "Inicio > Destacado > ¡DESTAPANDO LA OLLA! Salío la quinta parte de los nombres de «voluntarios»..."

Below the breadcrumb, there is a row of category tags: "Destacado", "Lechuguino del día", "Lechuguinos", and "Política".

¡DESTAPANDO LA OLLA! Salío la quinta parte de los nombres de «voluntarios» invitados por la autócrata Línea a la Guaidó»

22 febrero, 2019

A small image of a person's face is visible at the bottom left, partially obscured by binary code. At the bottom right, there is a "Destacados" section with a link to "DUQUE Y URIBE SIN CHAMPA".

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

Exposure for 5 thousand victims

The screenshot shows a news website with a dark header. The header includes navigation icons (back, forward, search, etc.) and a menu bar with categories like 'INICIO', '+ DESTACADO', 'POLÍTICA', 'LOS SHOWSEROS', 'VIDEOS', and a search icon. Below the header is a large list of names and numbers, likely a database dump or a list of contacts. To the right of this list are several news articles with titles and images. One article features a photo of people at a border crossing. Another article discusses the reopening of a border crossing between Colombia and Venezuela.



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.google.com/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

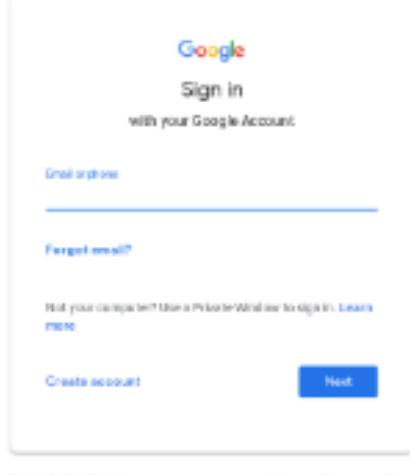
Brand: [Google](#)

IP: [159.65.65.194](#)

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

[Dispute Verdict](#)

Screenshot



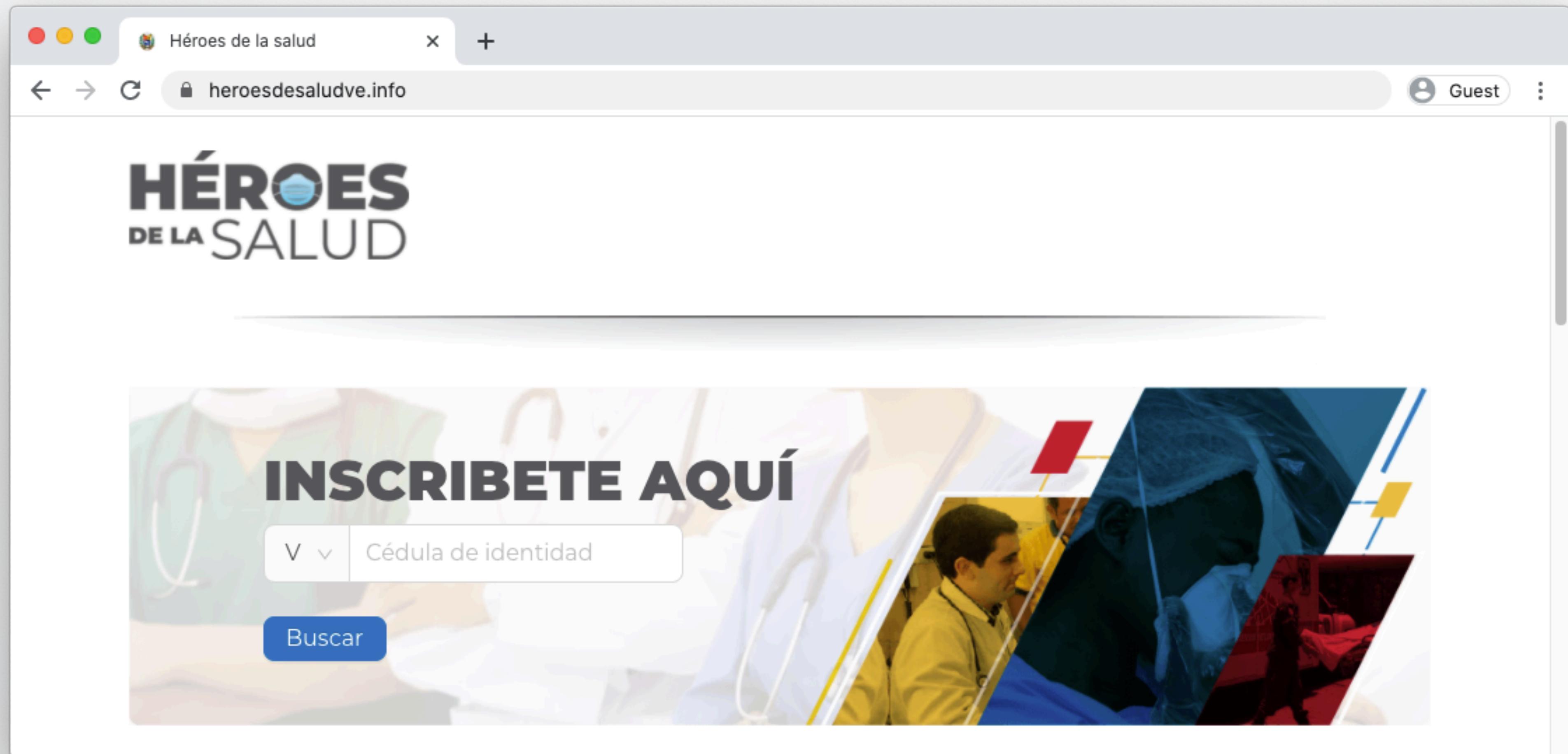
The screenshot shows a Google sign-in page with the heading "Sign in with your Google Account". It features fields for "Email or phone" and "Password", along with links for "Forgot email?" and "Not your computer? Use a PIN or token to sign in. Learn more". Below the form are "Create account" and "Next" buttons. At the bottom, there's a link for "Google Account Settings" and icons for "Help", "Privacy", and "Terms".

source: checkphish.ai

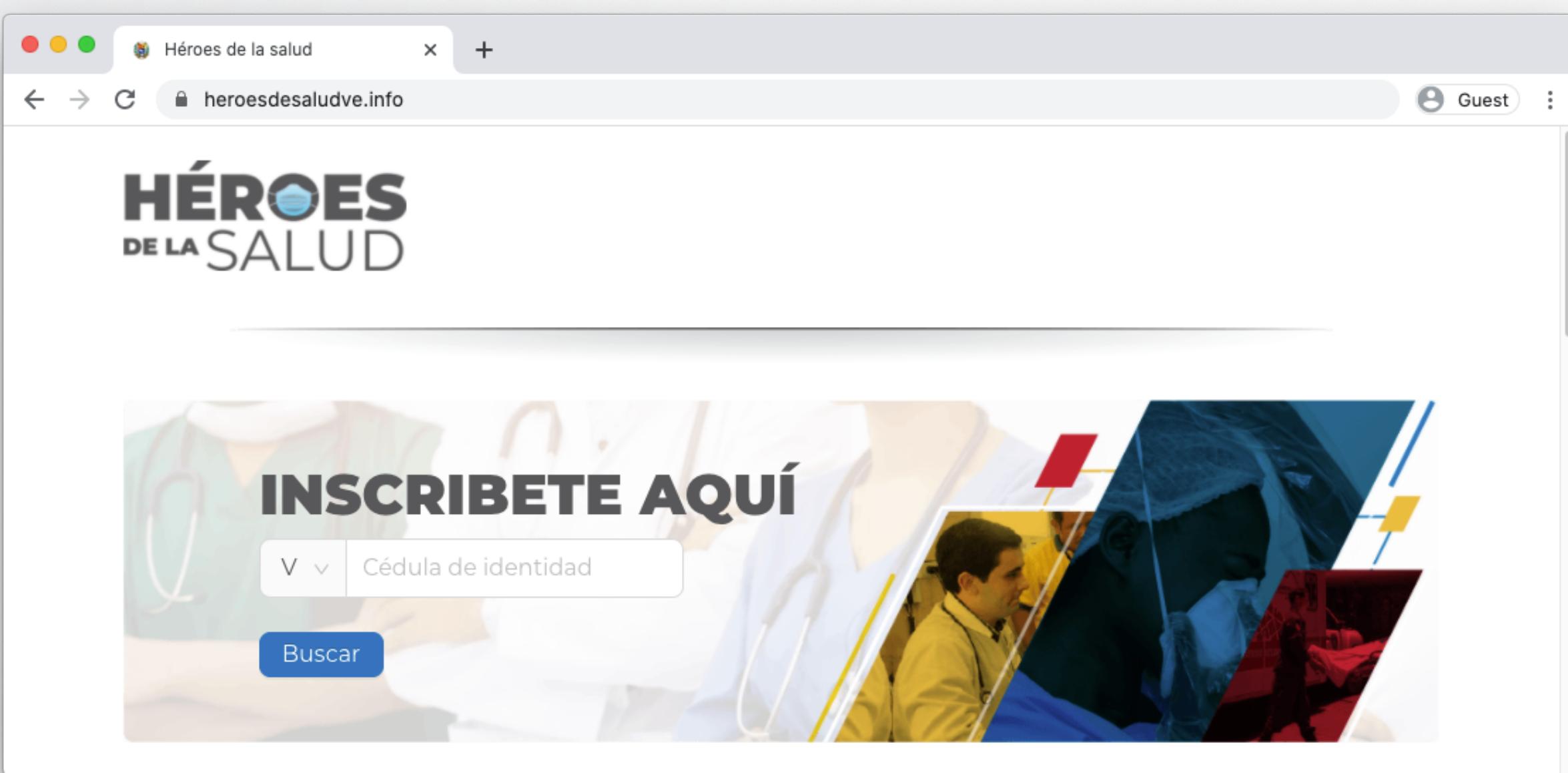
Inconsistent DNS responses documented

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

Case: Héroes de la salud



Case: Héroes de la salud

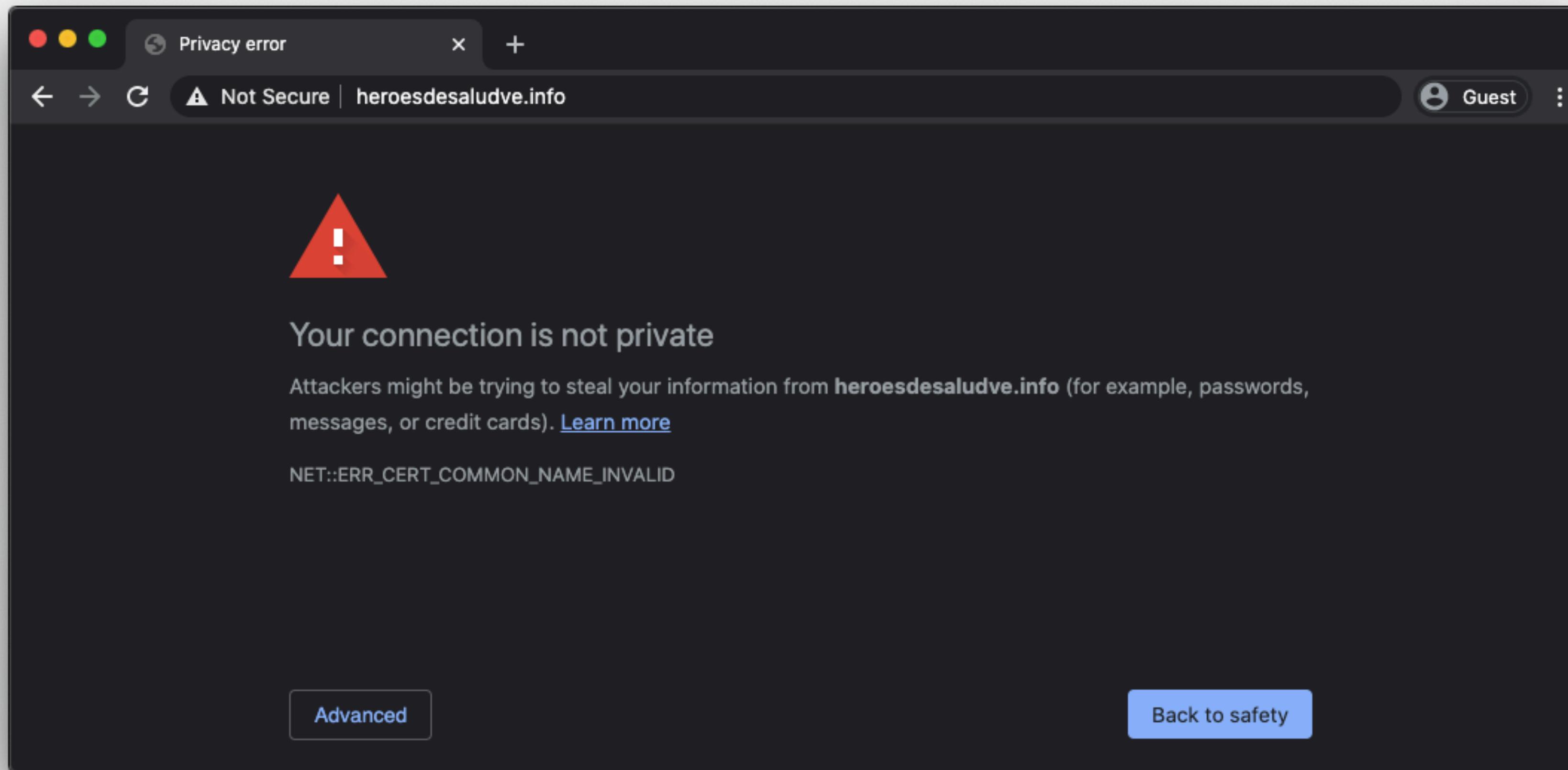


Selectively (not) blocking

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://vrepresidencia.com/	BLOQUEO DNS	ACCESIBLE	ACCESIBLE	ACCESIBLE	ACCESIBLE

2020-04-30

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