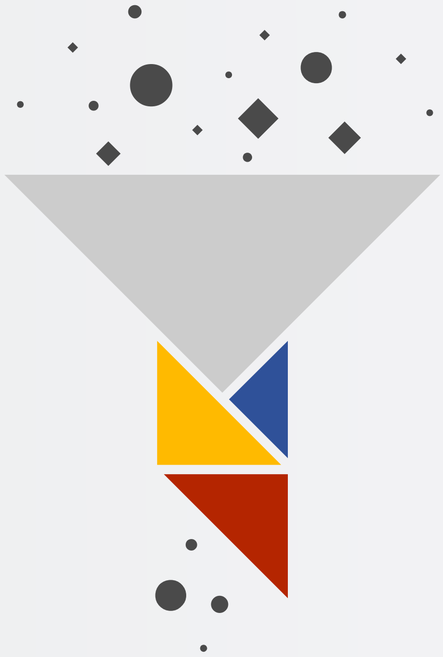


# VE SIN FILTRO

Andrés E. Azpúrua

#imv2020

Venezuela inteligente

# Internet Censorship, DNS poisoning and Phishing in Venezuela

## Measuring from censorship to state-sponsored attacks

VE SIN FILTRO

Venezuela inteligente

Andrés E. Azpúrua

#imv2020

VEsinFiltro.com

@VEsinFiltro

vesinfiltro.com/noticias/state_of_internet_c

Noticias Reporta Test Evade los bloqueos Todas las guías

VESINFILTRO

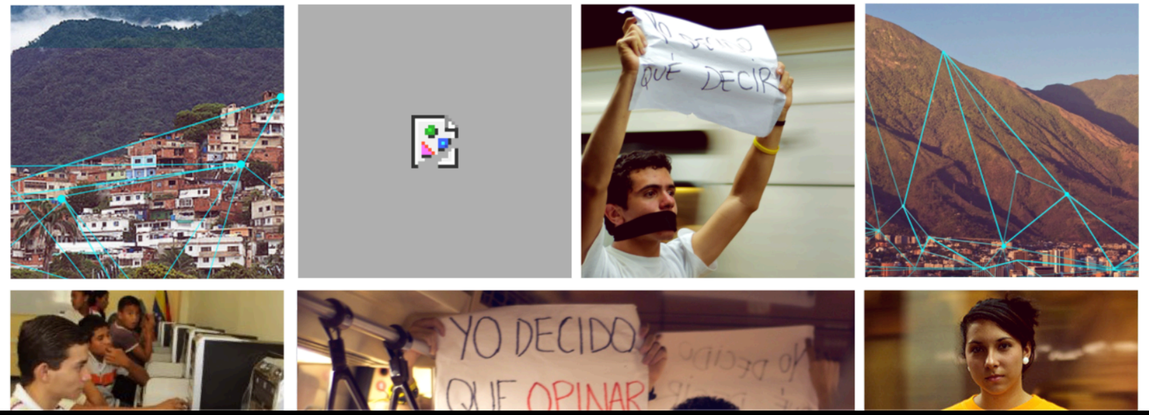
*Infórmate sobre el estado de internet en Venezuela*

*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)




twitter.com/vesinfiltro/stat

**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

# 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

# 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 mayor ISPs

Big and small sites

No clear end

# Indefinite Blocks

Long lasting, some 6+ years

Telecom regulator orders

On all/most mayor 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

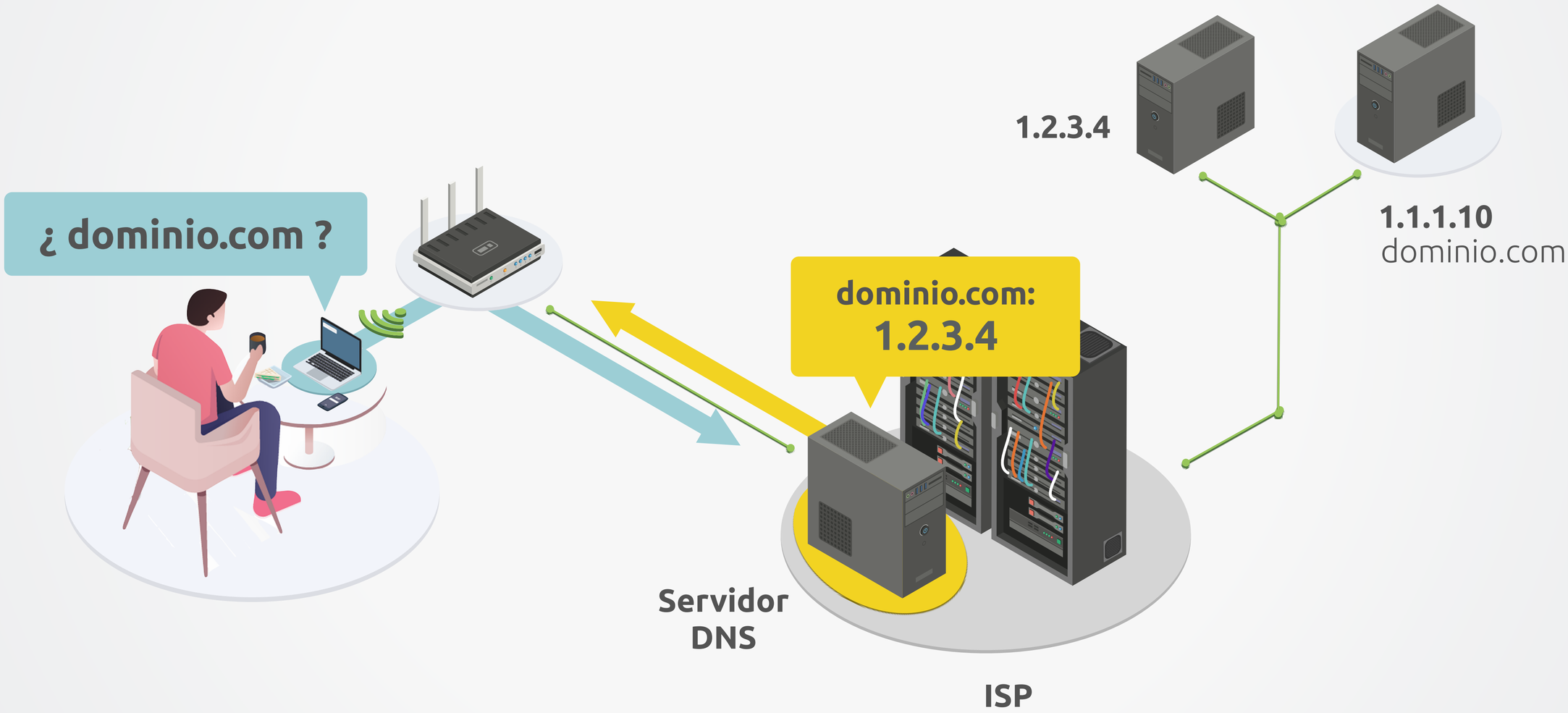
- Fundamental to quickly get multiple measurements fast
- Critical for unexpected incidents
- Key to bridge any gaps
- Faster turnaround of measurements

# Measuring probes

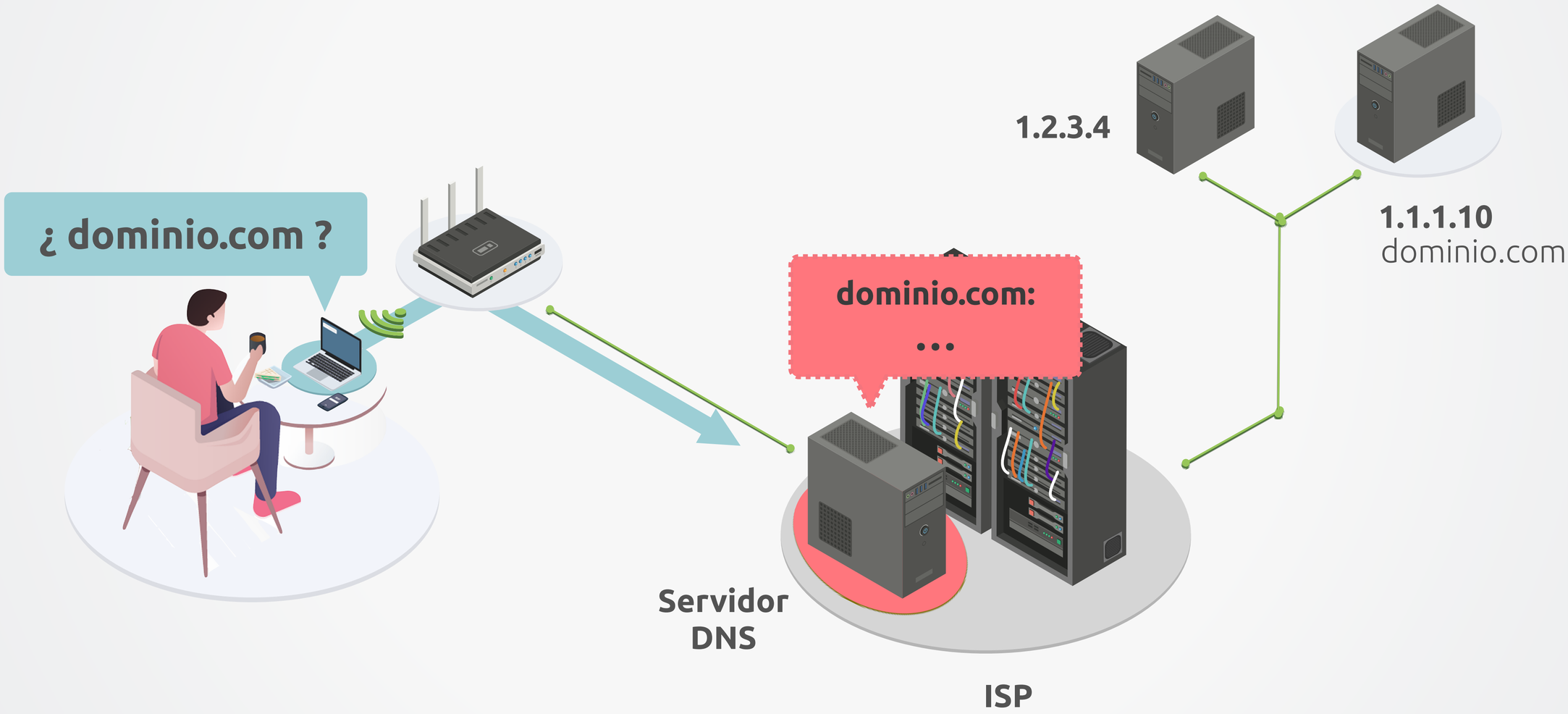
- Guaranteed more data points of whole list
- Increased test frequency based on URL importance
- Alternative tests:
    - High intensity dns, tcp, filtering by http host and SNI
    - Block rate when needed
- Currently migrating versions, to be released

# ATLAS probes

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


¿ dominio.com ?
dominio.com:
1.2.3.4
1.2.3.4
1.1.1.10
dominio.com
Servidor
DNS
ISP

# DNS Blocks

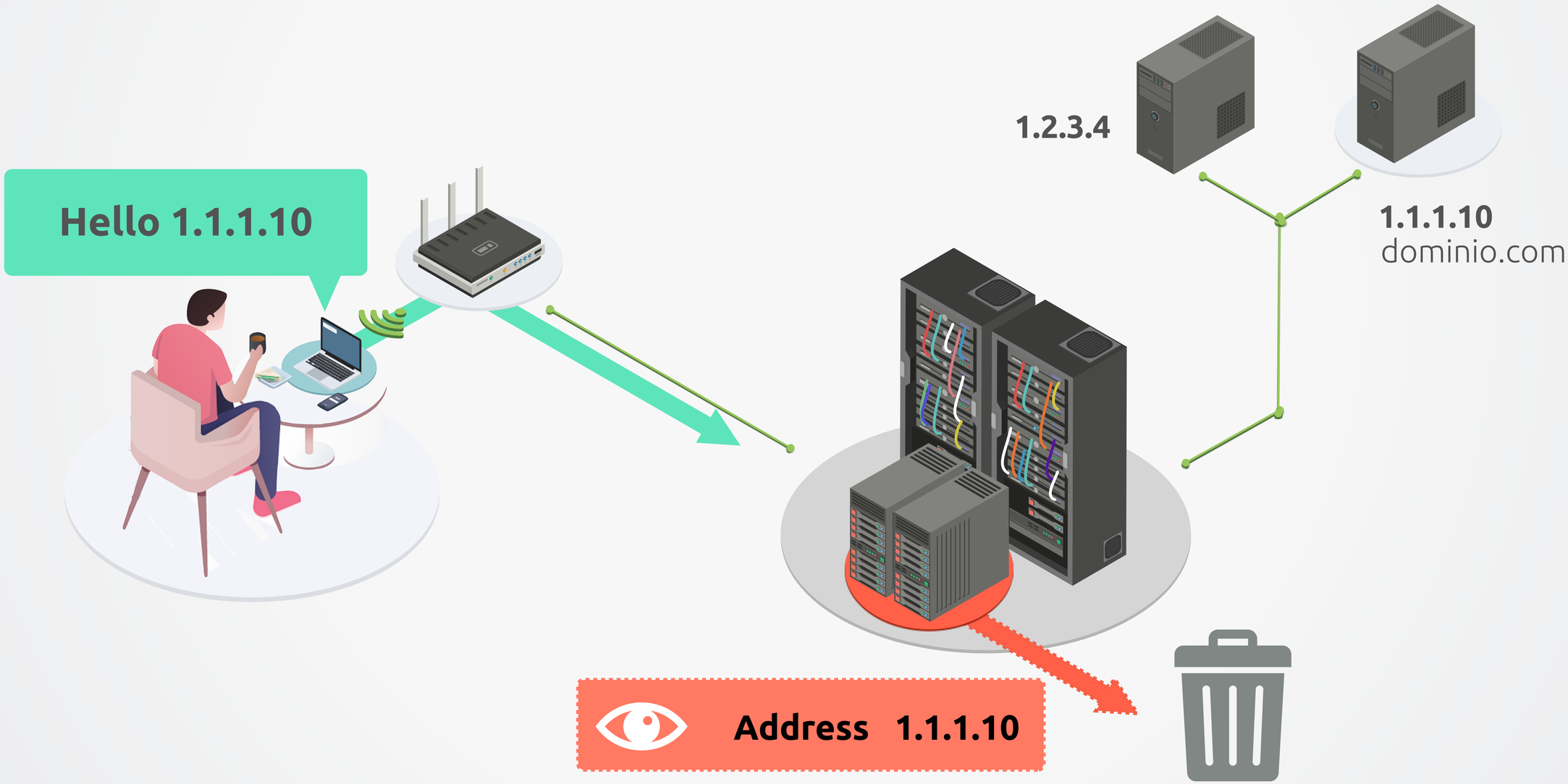

¿ dominio.com ?
dominio.com:
...
Servidor
DNS
ISP
1.2.3.4
1.1.1.10
dominio.com

# 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`** |

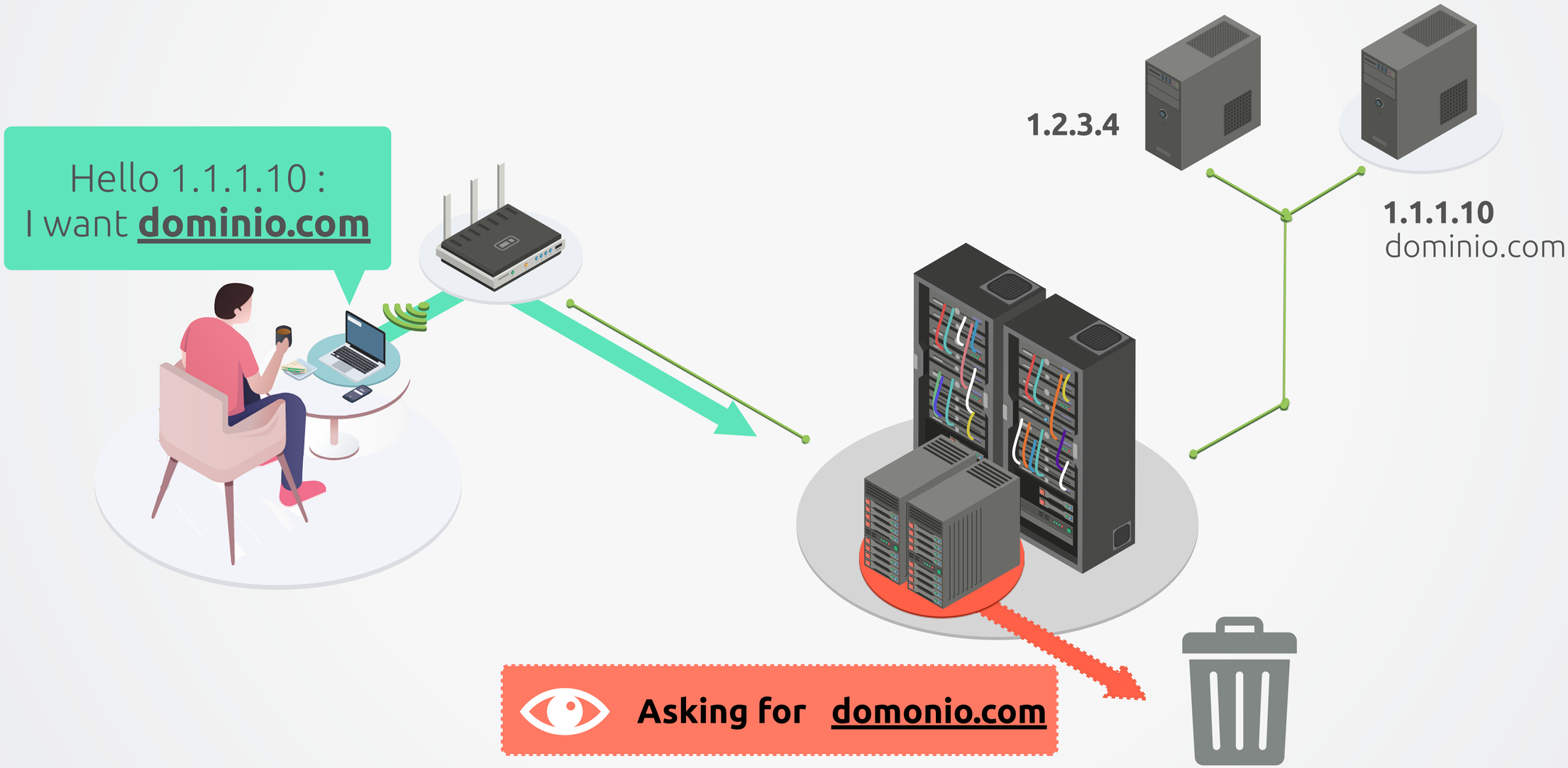
# TCP blocks



# 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 shudowns

# Evolution

## 2018

**Start of DPI blocking**

**Mayor mainstream news targeted**

**Block of Tor**

# Evolution

## 2018

Start of significant DPI blocking

Mayor mainstream news targeted

Block of Tor

## 2019

**Dramatic increase of censorship to news**

**Widespread use of SNI-Filtering**

**Mayor internet platforms blocked**

**Start of Tactical blocks**

# Evolution

## 2018

Start of significant DPI blocking

Mayor mainstream news targeted

Block of Tor

## 2019

Dramatic increase of censorship to news

Widespread use of SNI-Filtering

Mayor internet platforms blocked

Start of Tactical blocks

## 2020

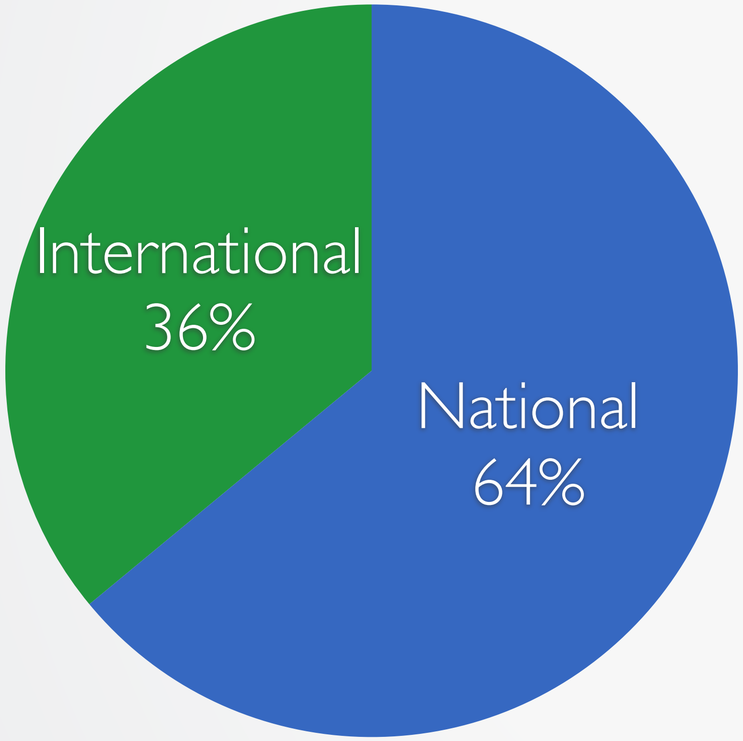
**Blocking of opposition COVID-19 initiatives**

**Seemingly degraded DPI blocking capacity**

**Continuation of Tactical blocks of mayor social media**

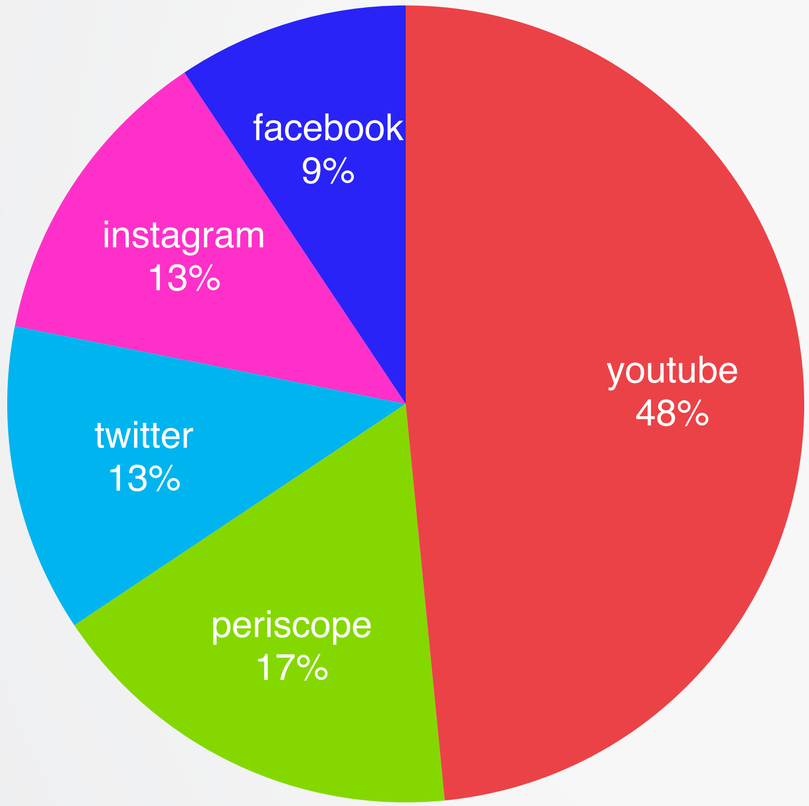
**New blocks to news media**

# 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




- Al 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

https://www.elnacional.com/venezuela/bomberos-controlaron-incendio-en-la-sede-de-cantv-del-municipio-chacao/

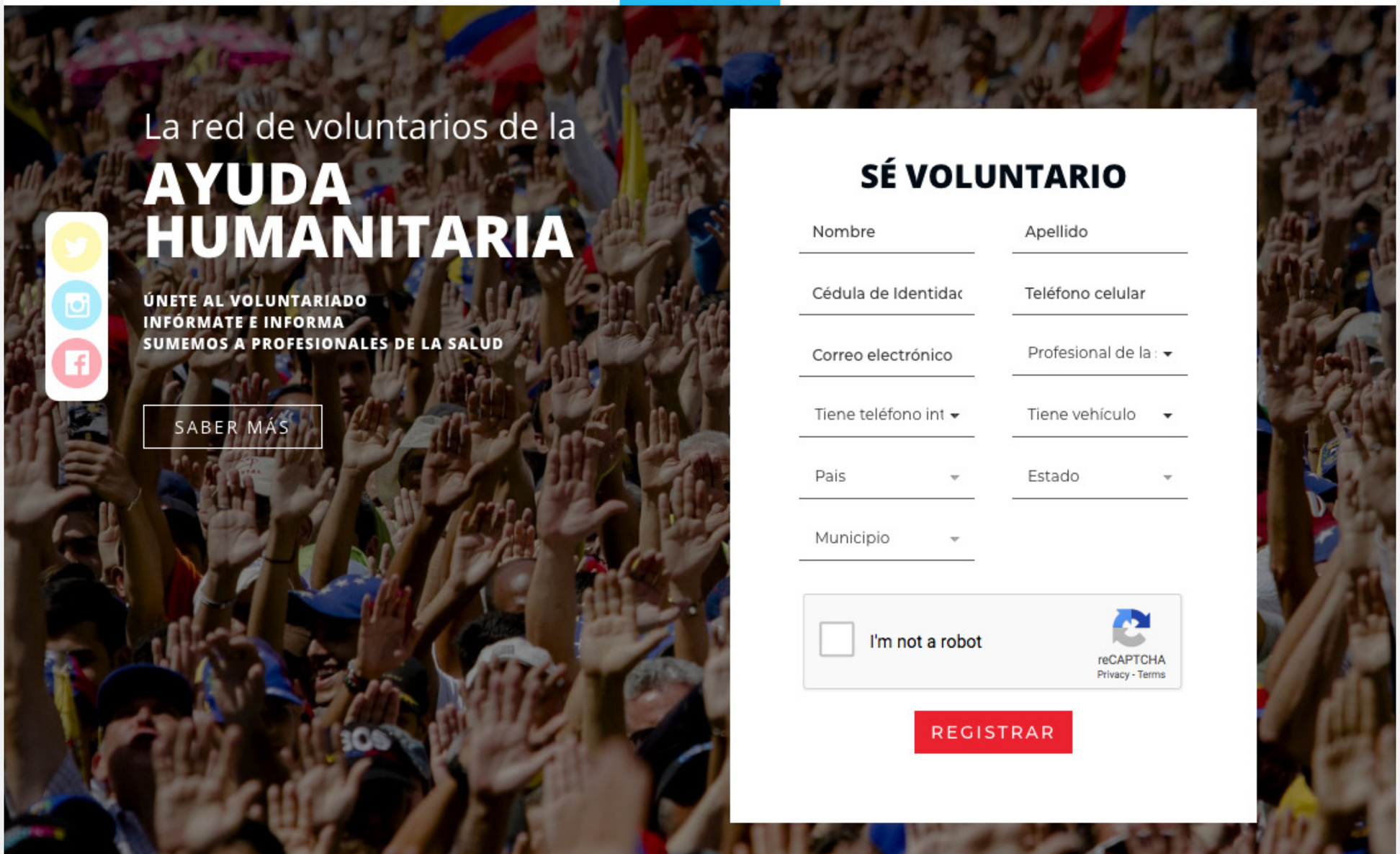
# Covid-19 blocks

| 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


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 Identidac
Teléfono celular
Correo electrónico
Profesional de la :
Tiene teléfono int
Tiene vehículo
Pais
Estado
Municipio
I'm not a robot
reCAPTCHA
Privacy - Terms
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

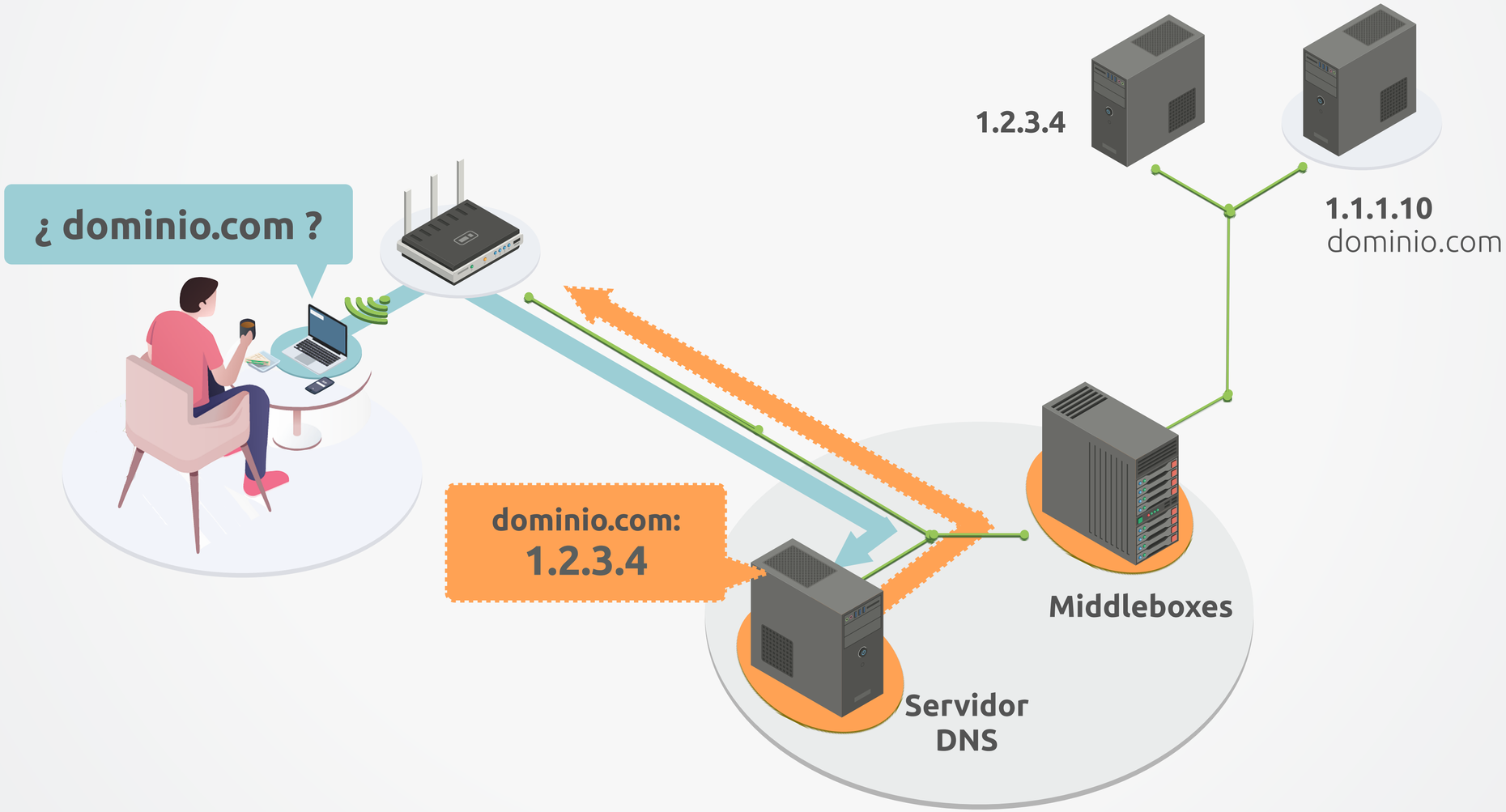
Malicioso: **voluntariovenezuela.com**
159.65.65.194
Digital Ocean
Dominio registrado en GoDaddy

# Malicious links

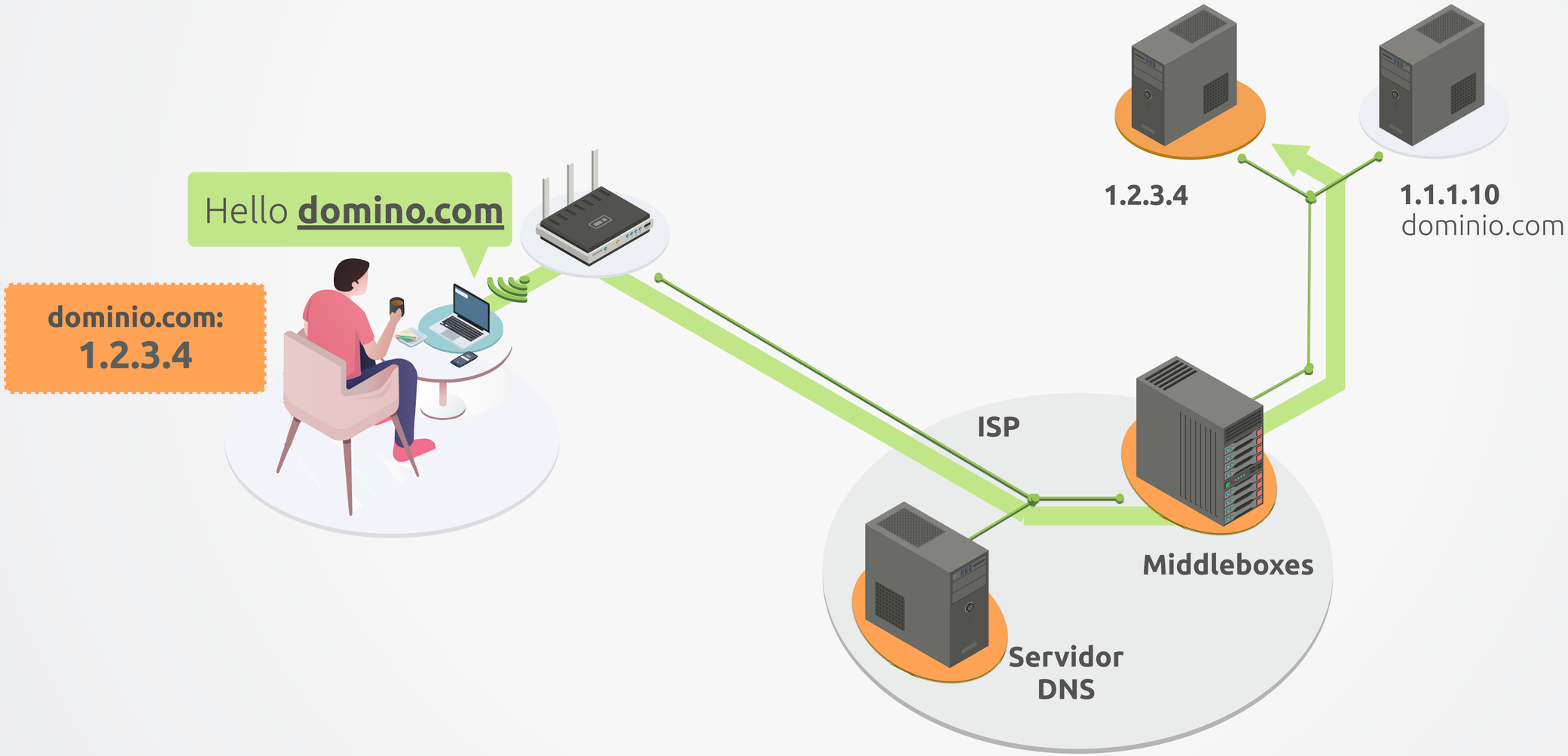
- **Twitter:** Links to fake domain being shared since 2019-02-11
- **Fake twitter accounts Twitter**: @voluntariosvene, vs @voluntariosxve
- Other channels

# Malicious links

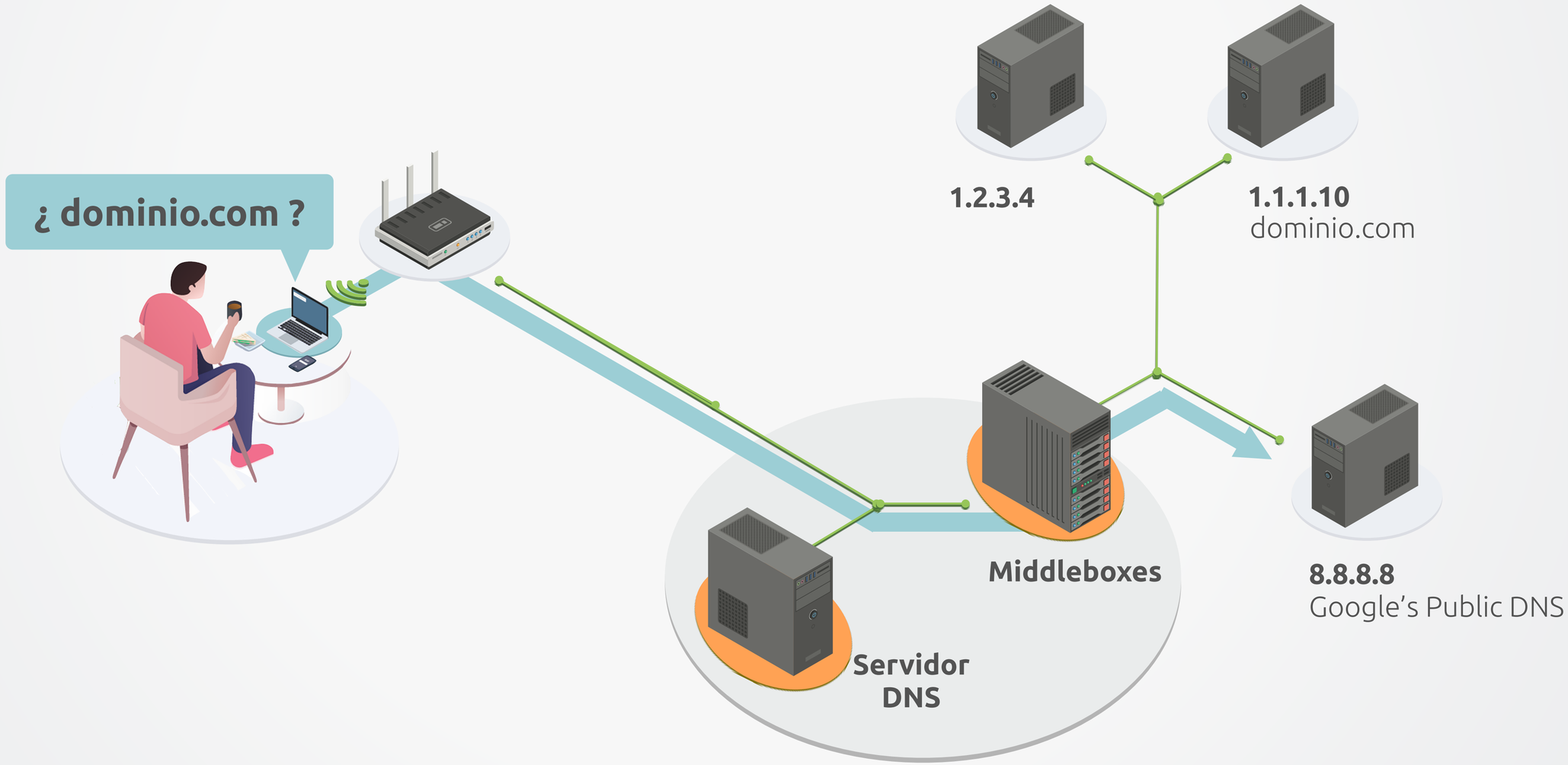
# DNS manipulation



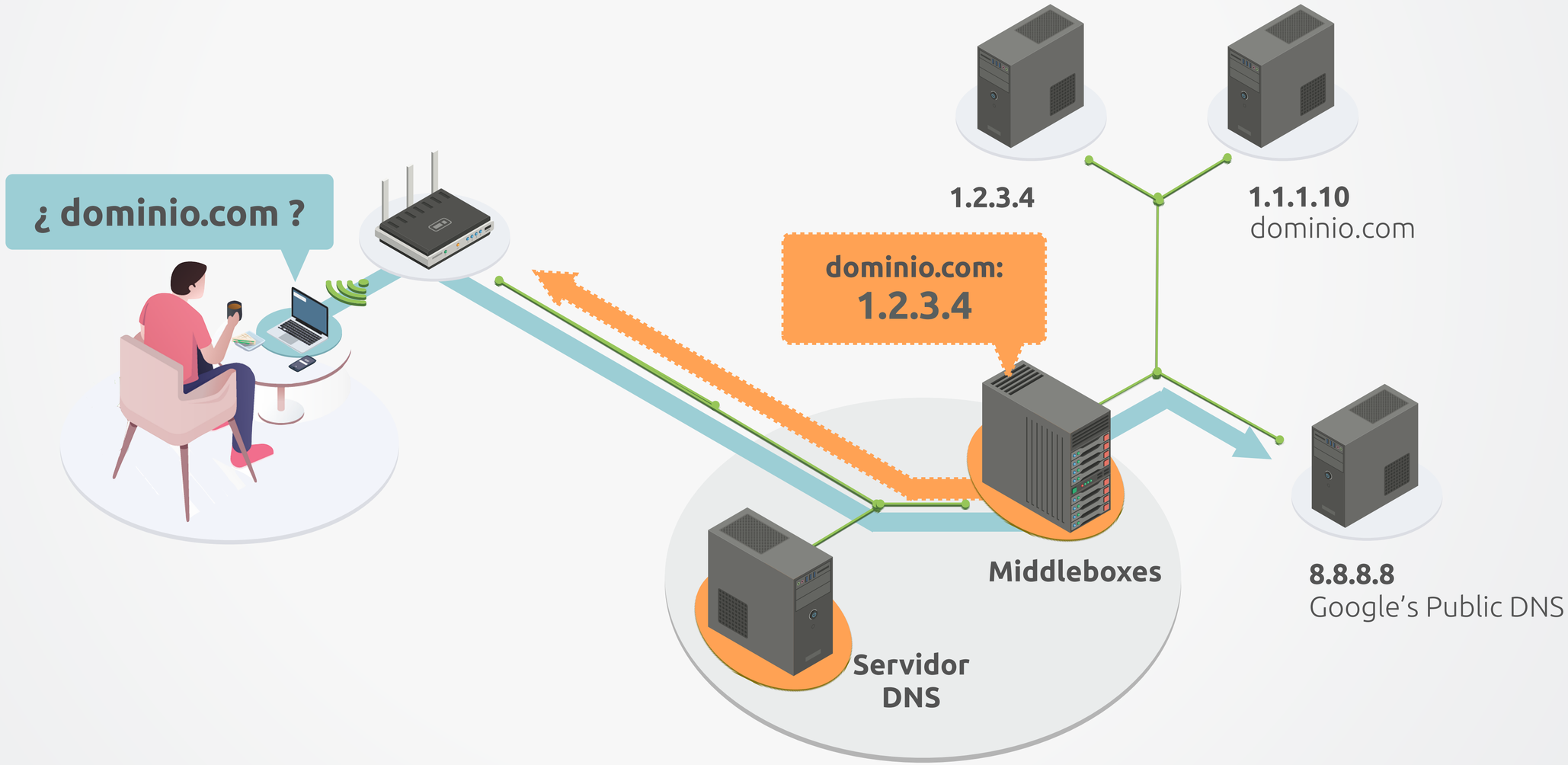
# DNS manipulation



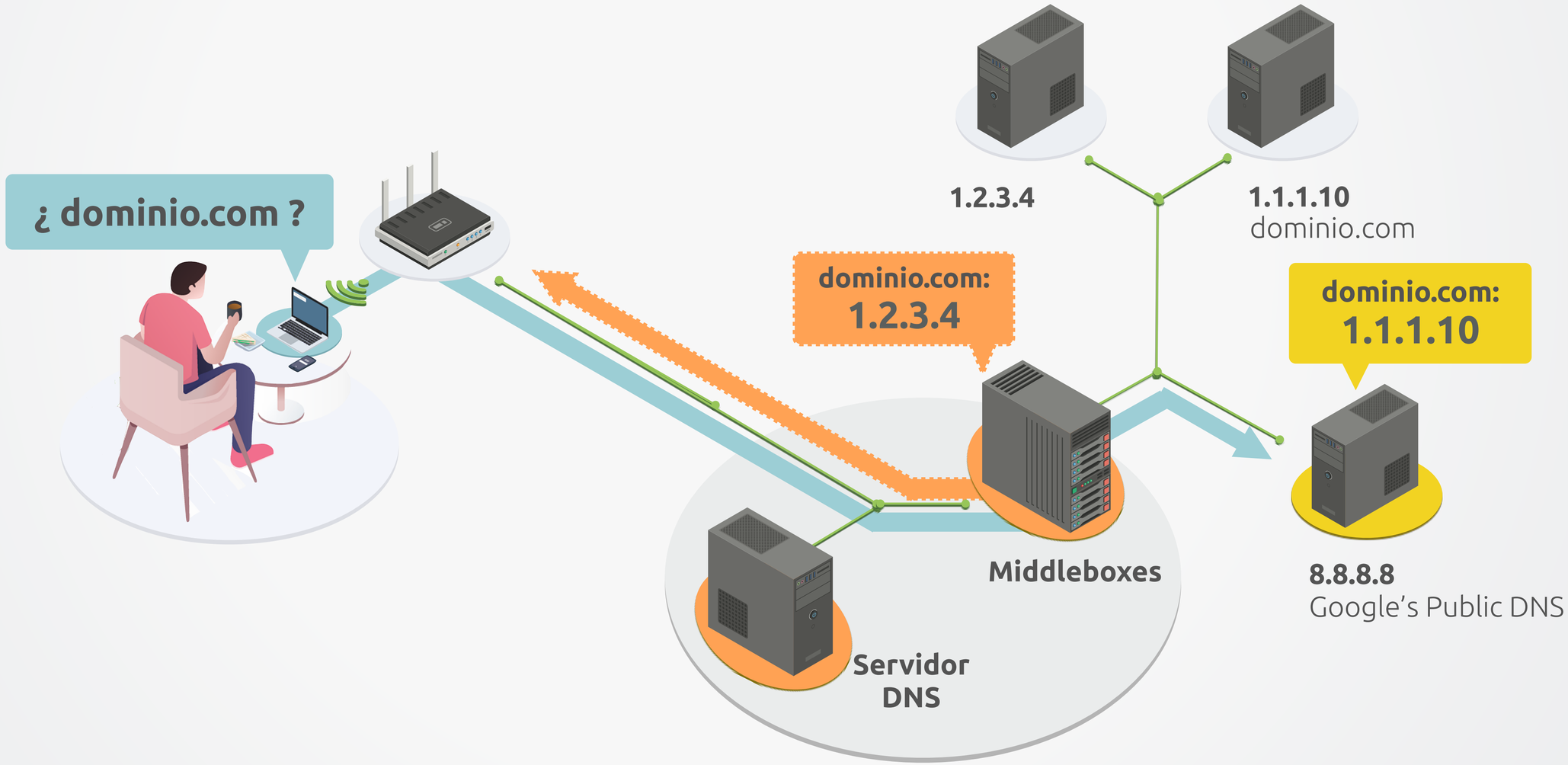
# DNS manipulation



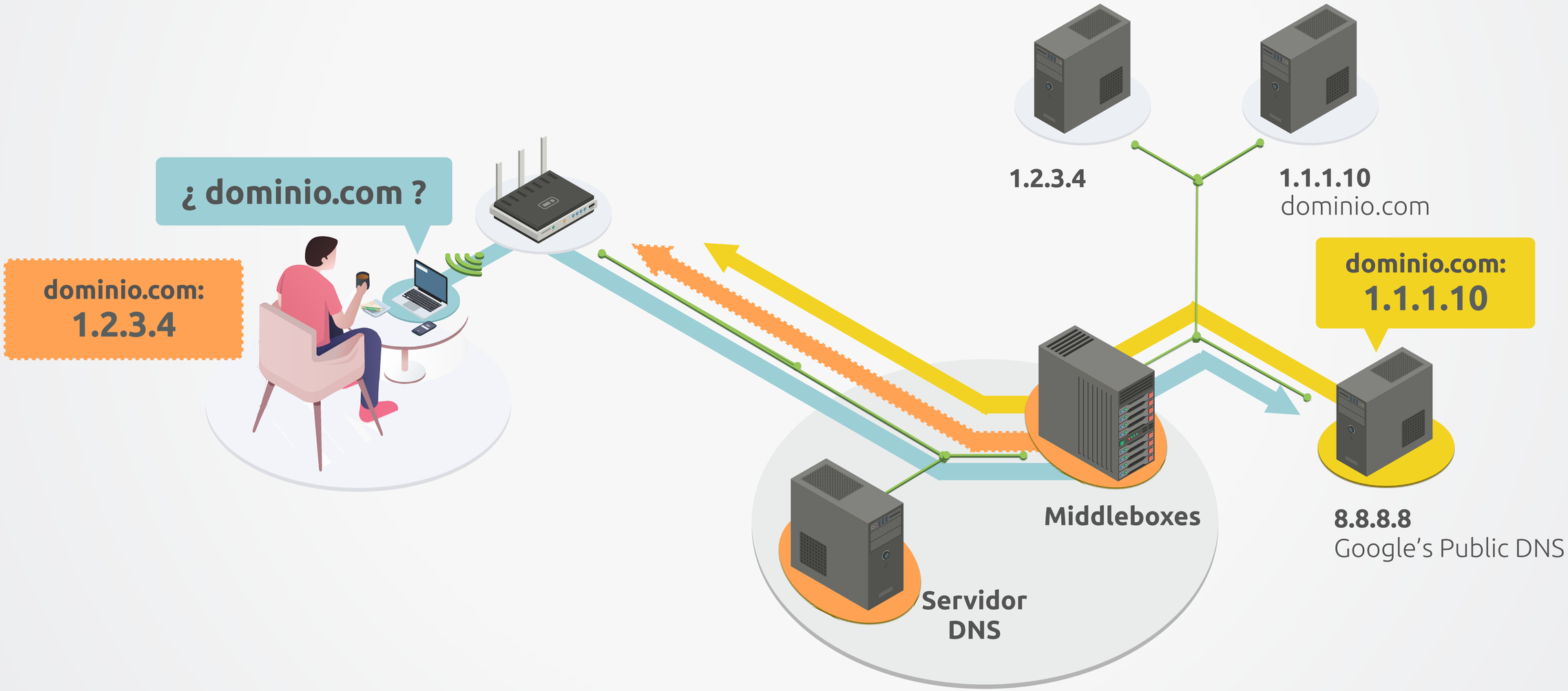
# DNS manipulation



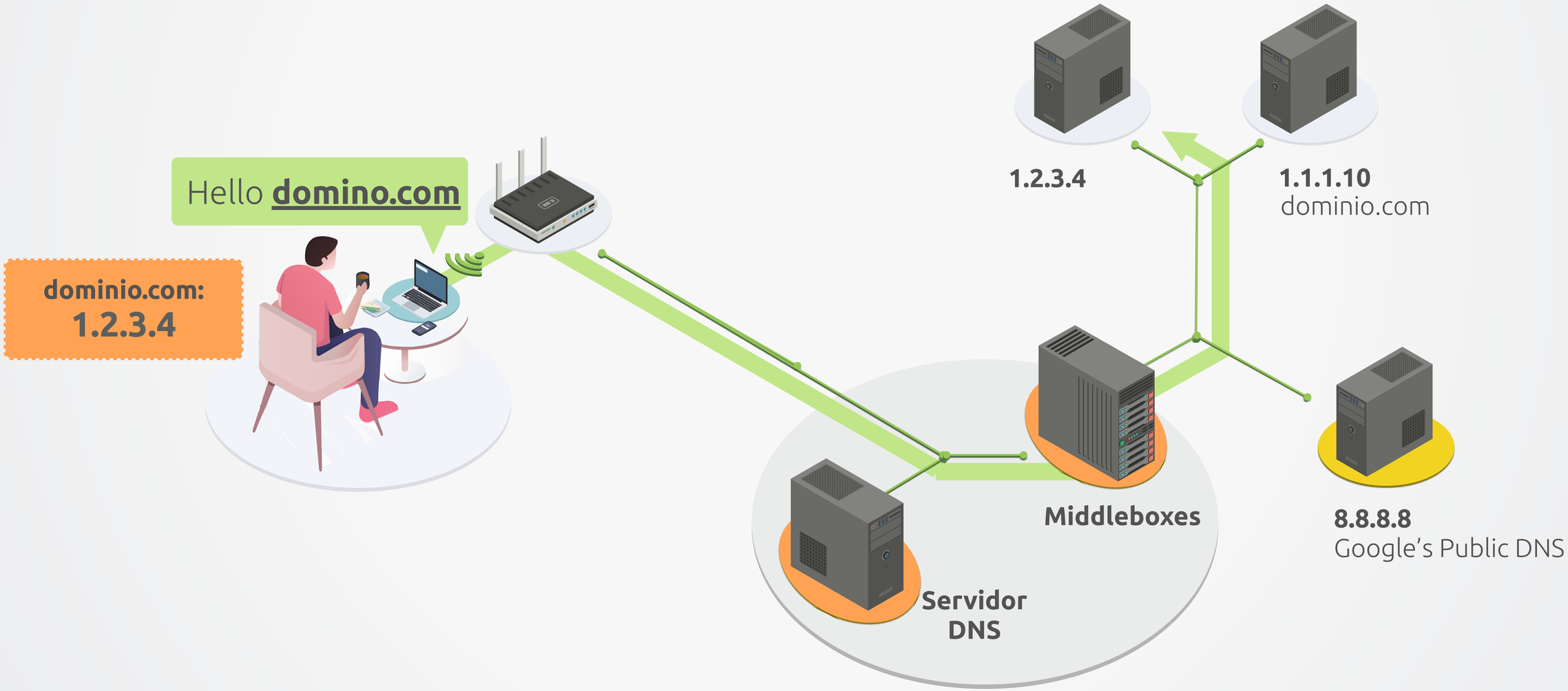
# DNS manipulation



# DNS manipulation



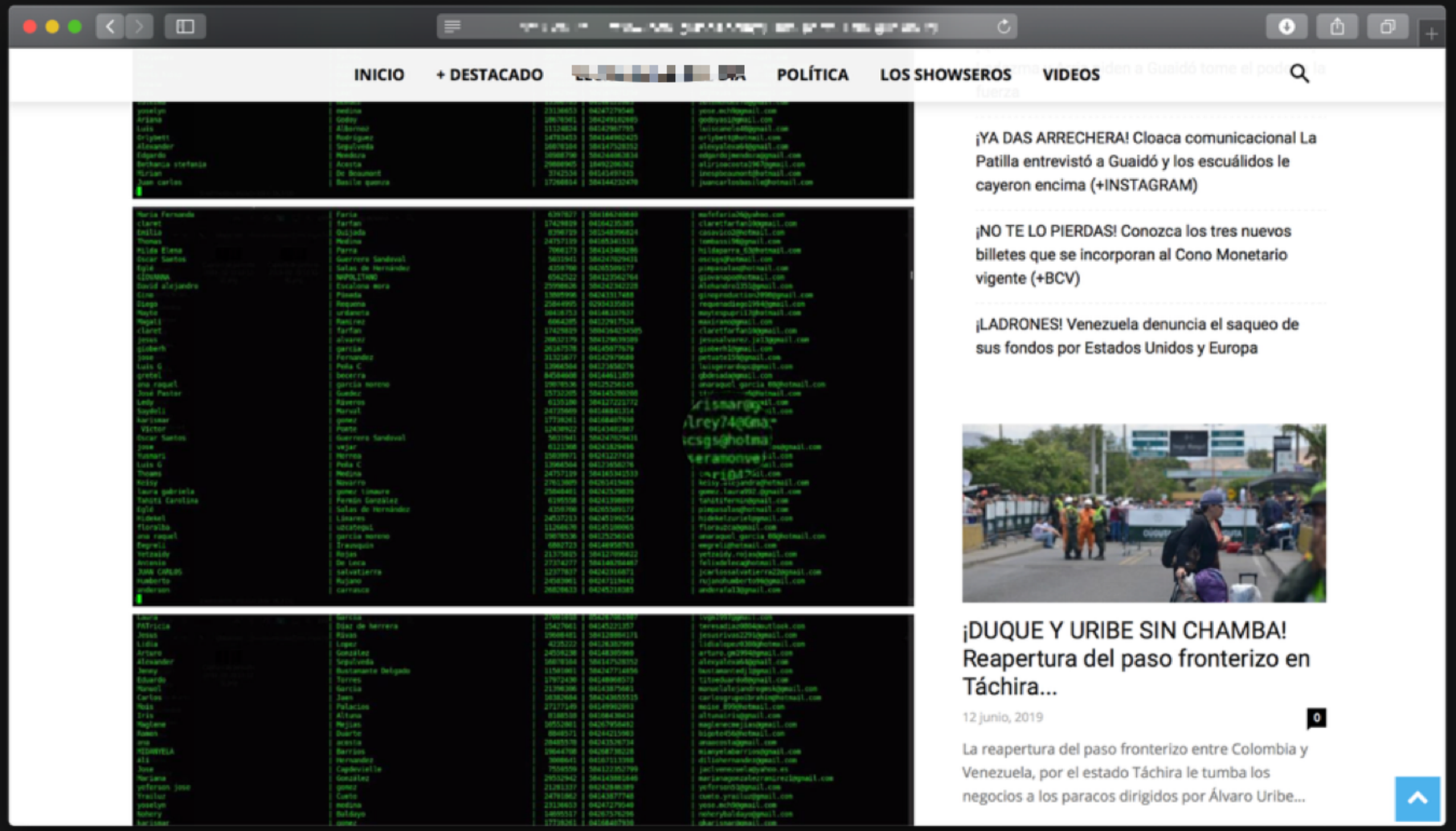
# DNS manipulation



# Fuel for fake news


# Personal information published

# Exposure for 5 thousand victims



# 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

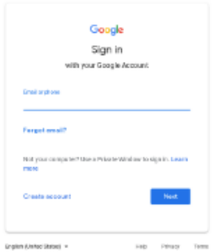
**Brand:** Google

**IP:** 159.65.65.194

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

Dispute Verdict

**Screenshot**

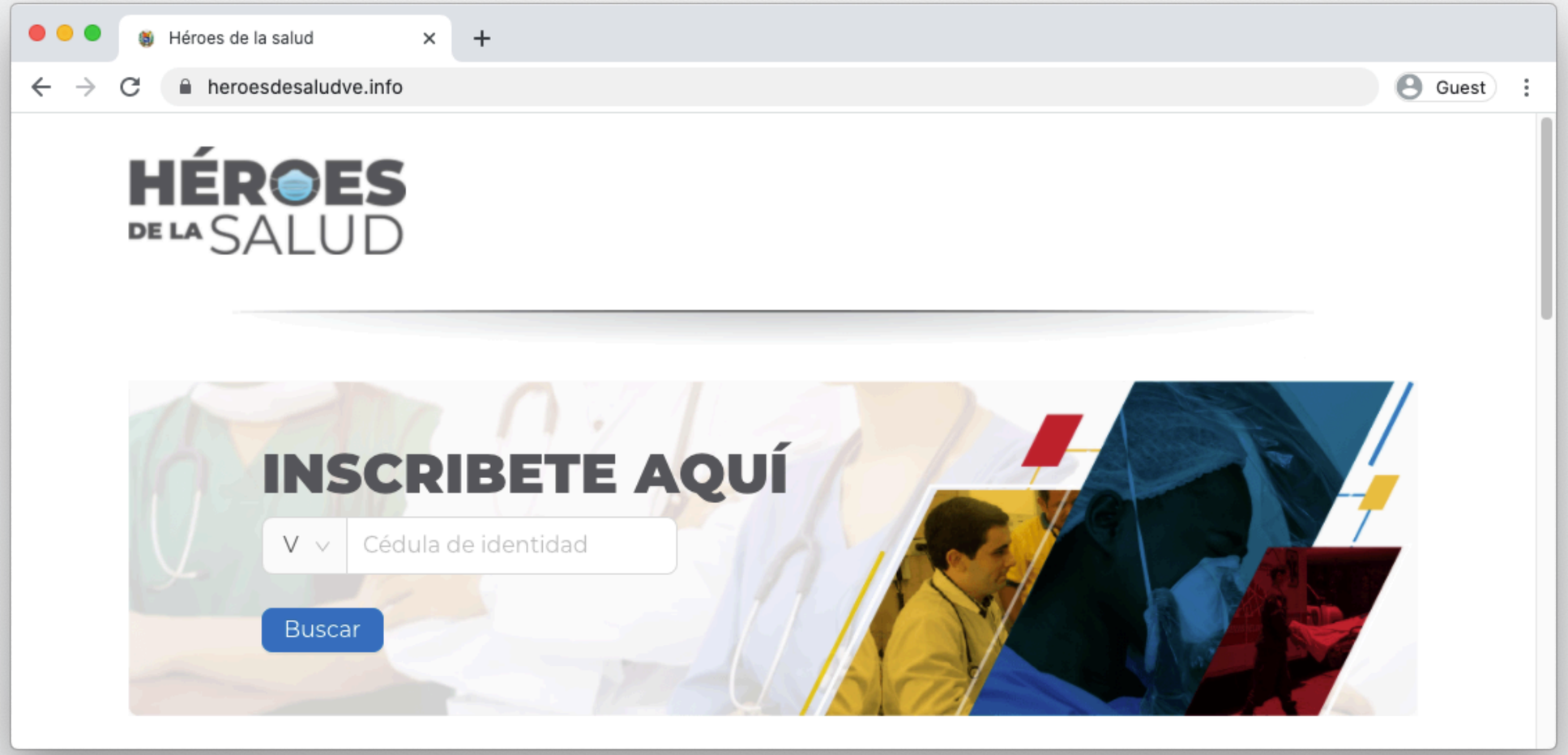



source: checkphish.ai

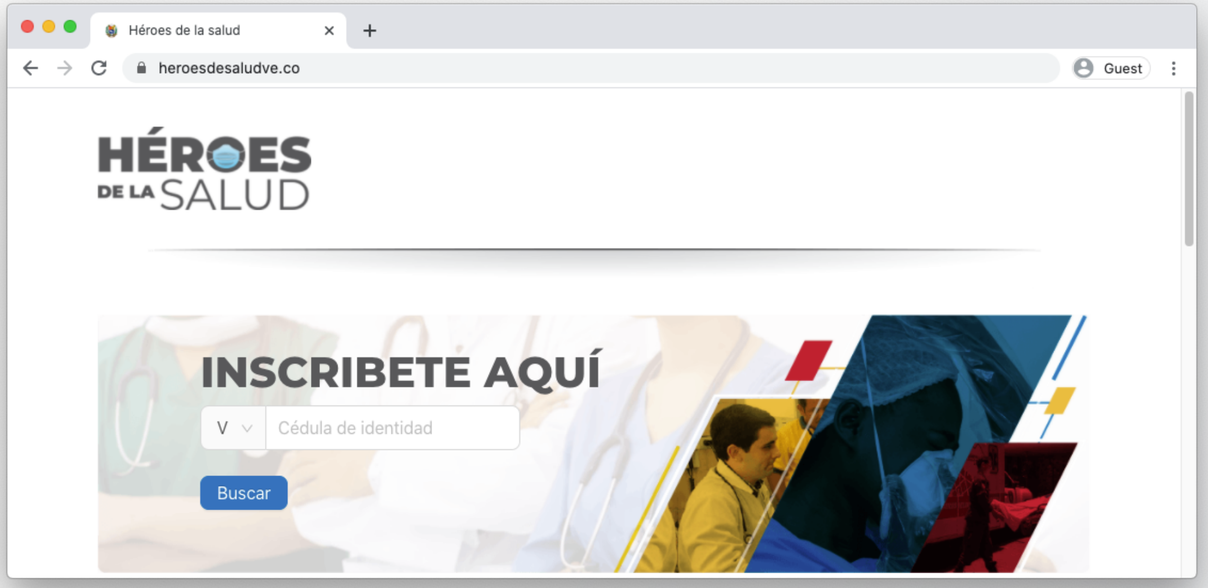
# Inconsistent DNS responses documented

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

# Case: Héroes de la salud



# Case: Héroes de la salud

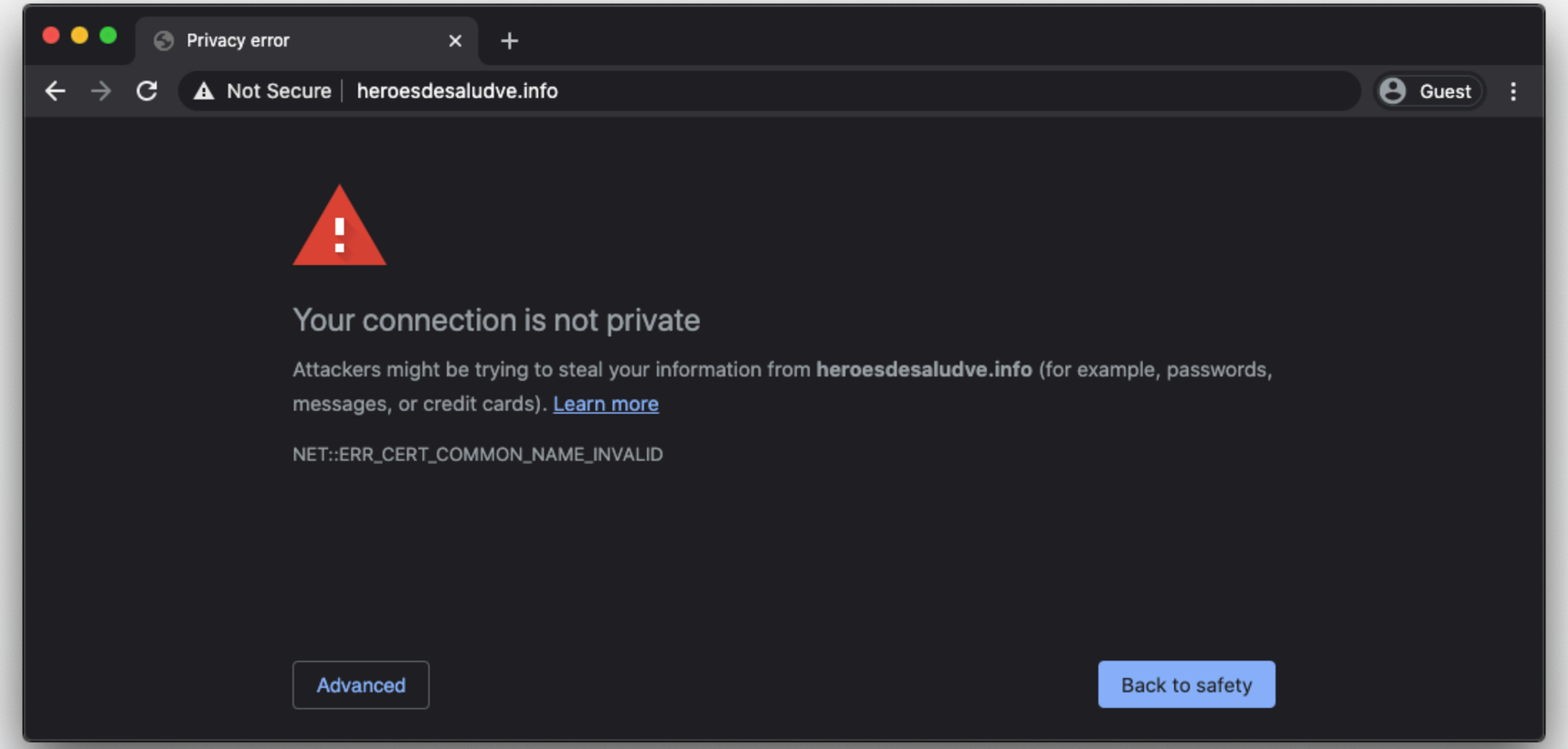



# Selectively (not) blocking

| 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://vepresidencia.com/ | BLOQUEO DNS | ACCESIBLE | ACCESIBLE | ACCESIBLE | ACCESIBLE |

2020-04-30

# Similar M.O.


Privacy error
Not Secure | heroesdesaludve.info
Guest
Your connection is not private
Attackers might be trying to steal your information from heroesdesaludve.info (for example, passwords, messages, or credit cards). Learn more
NET::ERR_CERT_COMMON_NAME_INVALID
Advanced
Back to safety

# 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