

# Informe minería de datos

## Target: Partido político «*Ciudadanos, Partido de la ciudadanía*»

### A) Consideraciones Previas

A) Dicho informe pretende dar a conocer la infraestructura telemática presente en Internet del objetivo fijado por el cliente.

B) Para la realización de éste informe no se ha realizado ningún ataque de fuerza bruta a ninguno de los servidores que aparecen en el informe.

c) Las herramientas usadas han sido principalmente mtr, ping, whois, nslookup y dig.

d) Se omite el análisis exhaustivo en servidores compartidos.

### B) Recolección de datos

Se analiza el dominio ciudadanos-cs.org a partir de éste se encuentran otros dominios (análisis de subdominios en páginas posteriores):

**[1] ciudadanos-cs.org (164.138.208.214 - ES) - OK - REDIRECT <https://www.ciudadanos-cs.org> (54.230.15.75 -USA)**

[2] ciudatans-cs.org (62.82.134.146 -ES) - KO

[3] mejorunidos.com (164.138.208.214 -ES) - REDIRECT 1

[4] mejorunidos.org (164.138.208.214 -ES) - REDIRECT 1

[5] mejorunidos.net (164.138.208.214 -ES) - REDIRECT 1

[6] mejorunidos.es (164.138.208.214 -ES) - REDIRECT 1

[7] mejorunidos.cat (164.138.208.214 -ES) - REDIRECT 1

[8] mejorunidos.eu (164.138.208.214 -ES) - REDIRECT 1

[9] millorjunts.com (164.138.208.214 -ES) - REDIRECT 1

[10] millorjunts.org (164.138.208.214 -ES) - REDIRECT 1

[11] millorjunts.net (164.138.208.214 -ES) - REDIRECT 1

[12] millorjunts.es (164.138.208.214 -ES) - REDIRECT 1

[13] millorjunts.eu (164.138.208.214 -ES) - REDIRECT 1

[14] blog-cs.com (164.138.208.214 -ES) - 403

[15] blog-cs.org (164.138.208.214 -ES) - directadmin (web control panel)

[16] europa-cs.org (xxx) - ya no pertenece a ciudadanos

[17] cs-elecciones2011.com - no operativo, registrado por Blanco Estudio Creativo - BOLD, S.C.P.

[18] vota-cs.com - no operativo, registrado por Blanco Estudio Creativo - BOLD, S.C.P.

[19] albertrivera.info (46.105.122.74 -FR) - operativo - registrado por Blanco Estudio Creativo - BOLD, S.C.P.

[20] diadaasantjordi.info (62.82.134.146 - ES) - no operativo - registrado por Matias Alonso de Pedro - Ciudadanos-Partido de la Ciudadania - secretario.general@ciudadanos-cs.org

[21] redciudadana.net (62.82.134.146 -ES) - no operativo - registrado por Luis Folgoso - Ciudadanos-Partido de la Ciudadania - luis.folgoso@gmail.com

[22] vamosacontardiadas.com (64.34.68.40) - ??? - PABLO ORESTE (Buenos Aires)

[23] noismos.com (ko) - no operativo - registrado por Luis Folgoso - Ciudadanos-Partido de la Ciudadania - luis.folgoso@gmail.com

[24] albertrivera.es (46.105.122.74 -FR) - operativo

**La práctica totalidad de las webs operativas se redireccionan a <https://www.ciudadanos-cs.org> (54.230.15.75 -USA)**

## c) Minería de datos con cada uno de los dominios/IPs

### ciudadanos-cs.org

#### WHOIS

\$ whois ciudadanos-cs.org  
Domain Name: CIUDADANOS-CS.ORG  
Domain ID: D150745802-LROR  
WHOIS Server:  
Referral URL: http://www.godaddy.com  
Updated Date: 2016-06-07T11:18:14Z  
Creation Date: 2008-01-25T12:10:06Z  
Registry Expiry Date: 2025-01-25T12:10:06Z  
[...]  
Registrant ID: CR34829544  
Registrant Name: Ciudadanos - Partido de la Ciudadania  
Registrant Organization: Ciudadanos-Partido de la Ciudadania  
Registrant Street: Plaza Urquinaona N. 6, piso 16 B  
Registrant City: Barcelona  
Registrant State/Province: Barcelona  
Registrant Postal Code: 08010  
Registrant Country: ES  
Registrant Phone: +93.3429436  
Registrant Phone Ext:  
Registrant Fax:  
Registrant Fax Ext:  
Registrant Email: dominios@silicontower.net  
ns1.silicontower.net 93.189.92.100  
ns2.silicontower.net 93.189.93.100

#### REVERSE DNS

server.ciudadanos-cs.org

#### OTRAS BÚSQEDAS QUE RELACIONEN OTROS DNS CON LA IP O DNS

##### PTR of the IP addresses of ciudadanos-cs.org (2 shown)

hospedado-en.cyberneticos.com  
webchile1.cyberneticos.com

##### Names pointing to same IP address as ciudadanos-cs.org (42 shown)

Which hostnames and domains point to the same IP address as ciudadanos-cs.org?

mejorunidos.cat	millorjunts.com	mejorunidos.es
blog-cs.com	noismos.com	millorjunts.es
cs-elecciones2011.com	vamosacontardiadas.com	mejorunidos.eu
mejorunidos.com	vota-cs.com	millorjunts.eu

albertrivera.info  
diadaasantjordi.info  
mejorunidos.net  
millorjunts.net  
redciudadana.net  
blog-cs.org  
ciudadanos-cs.org  
ciudadans-cs.org  
europa-cs.org  
mejorunidos.org

millorjunts.org  
mail.mejorunidos.cat  
mail.blog-cs.com  
ns1.blog-cs.com  
mail.cs-elecciones2011.com  
mail.mejorunidos.com  
mail.millorjunts.com  
mail.vamosacontardiadas.com  
mail.vota-cs.com  
mail.mejorunidos.es

mail.millorjunts.es  
mail.mejorunidos.eu  
mail.millorjunts.eu  
mail.albertrivera.info  
mail.mejorunidos.net  
mail.millorjunts.net  
mail.blog-cs.org  
mail.europa-cs.org  
mail.mejorunidos.org  
mail.millorjunts.org

Names of the name servers of ciudadanos-cs.org (23 shown)

dbfgs.com  
wienerheurige.net  
ns1.siliconhosting.com  
ns2.siliconhosting.com  
dns1.yopigest.com  
dns2.yopigest.com  
ns5.arditec.es  
ns6.arditec.es

ns1.asistech.es  
ns2.asistech.es  
ns1.asistech.net  
ns1.dadko.net  
ns2.dadko.net  
ns1.dns-raiz.net  
ns2.dns-raiz.net  
ns1.infokode.net

ns2.infokode.net  
ns1.silicontower.net  
ns2.silicontower.net  
ns1.mancomunidad.org  
ns2.mancomunidad.org  
ns1.solmarina.org  
ns2.solmarina.org

### **ALOJAMIENTO**

siliconhosting.com (Barcelona)  
panel.silicontower.net

### **CORREO ELECTRÓNICO**

El correo electrónico para éste dominio se encuentra alojado en google

aspmx2.googlemail.com  
aspmx3.googlemail.com  
aspmx4.googlemail.com  
aspmx5.googlemail.com  
aspmx.l.google.com  
alt1.aspmx.l.google.com  
alt2.aspmx.l.google.com

PTR of the IP addresses of ciudadanos-cs.org

hospedado-en.cyberneticos.com  
webchile1.cyberneticos.com

### **OTROS DOMINIOS REFERIDOS EN ns1.silicontower.net**

Al tratarse de un servicio de DNS de una empresa de hosting no implica que todas las webs sean referidas al target indicado. Ésta información es simplemente informativa y se incluye

como parte de la minería de datos.

Pointing to 93.189.92.100 (13 shown)

wienerheurige.net	ns1.asistech.es	ns1.silicontower.net
ns1.siliconhosting.com	ns1.asistech.net	ns1.mancomunidad.org
dns1.yopigest.com	ns1.dadko.net	ns1.solmarina.org
dns2.yopigest.com	ns1.dns-raiz.net	
ns5.arditec.es	ns1.infokode.net	

servers the PTR records of 93.189.92.100 (89 shown)

santurtzi.biz	masajeselixir.com	lleidaweb.net
3goprint.com	naturainmobiliaria.com	silicontower.net
agoradb.com	notariomarbella.com	spainon.net
agrestecaza.com	pastoresalemanesbiloba.com	wshop.net
altahogar.com	pequenova.com	ades-economia-social.org
breincoarchitecture.com	perfyde.com	arditec.org
campusbasketballstar.com	profinsaysuministros.com	discretia.org
cap-sailing.com	psicotecnicoeldoncel.com	esclat.org
clinicasanzaibiza.com	ropaantiestatica.com	globallogbook.org
condearanda.com	sarriadeter.com	myfarmacia.org
couple4you.com	sorteosanjorge.com	kitebuggy.tv
cubensisproject.com	tecmaserm.com	www.danielvalle.com
dormirenpedraza.com	transplast.com	www.donde-es.com
ejulianjimenez.com	amalau.es	www.garminbarcelonatriathlon.com
elnotariodigital.com	climaclick.es	www.guillemcarbonell.com
empresasagrupadasfavia.com	enriko.es	www.lurdenok.com
estevezminguez.com	espacioronda.es	*.micvweb.com
figuratmf.com	gaenfisioterapia.es	www.psdtdnn.com
forgam.com	kastwey.es	www.restaurantesdepdraza.com
globallogbook.com	kempa.es	m
hermandadsantacruz.com	lasliras.es	www.tot-hom.com
ibiza-tickets.com	multitrade-spain.es	www.city-hotels.es
kaiserindustrial.com	puertopesquero.es	www.kickboxing-fek.es
lacunza-gonzalez.com	silicontower.es	psk-php4-lnx-rh-01.dns-raiz.net
laflordejava.com	victortranslator.es	www.indagacionesaxiologicas.net
lasaladeta.com	bioelements.eu	jns.jnsoft.net
lascaidasdejesus.com	ciberespinal.eu	ajllagostera.siliconpeople.net
leznocar.com	multitradespain.info	
lleidaalquiler.com	cordoba.ms	
lucasinografia.com	ibizainlove.net	
luxurysuitesmadrid.com	inasasl.net	

**164.138.208.214**

Se identifica éste servidor como el servidor principal publicitario a internet, dicho servidor

aloja las principales webs del partido político además de que el mismo dispone de un servidor de correo electrónico para los dominios:

mail.albertrivera.info  
mail.blog-cs.org  
mail.blog-cs.com  
mail.mejorunidos.cat  
mail.mejorunidos.com

mail.millorjunts.com  
mail.mejorunidos.es  
mail.millorjunts.es  
mail.mejorunidos.eu  
mail.millorjunts.eu

mail.mejorunidos.net  
mail.millorjunts.net  
mail.mejorunidos.org  
mail.millorjunts.org

Se identifica también un servicio de nombres de dominio ns1.blog-cs.com

Dicho servidor nos revela 2 IPs 164.138.208.216 (servidor compartido) y 85.17.109.12 (servidor compartido contratado por cyberneticos Hosting -tiertary.cyberneticos.com).

Dicho servidor está alojado por la empresa  
Cyberneticos Hosting S.L.  
CIF: B91647842  
Calle Varadero 3 PL 1. Parque Industrial "El Palmar"  
11500 - El Puerto de Santa María, Cádiz

### **82.98.160.143**

Se trata de un wordpress multisite

TODO

<https://www.robtex.com/?dns=82.98.160.143>

#### **Expanding search with DNS enumeration...**

Searching vhosts for domain: fic3.eu  
Searching vhosts for domain: miramecuandotehablo.com  
Searching vhosts for domain: lariadearosa.com  
Searching vhosts for domain: federacioncaza.com  
Searching vhosts for domain: aefcft.com  
Searching vhosts for domain: minercat.com  
Searching vhosts for domain: compacthabit.com  
Searching vhosts for domain: age.gal  
Searching vhosts for domain: lasermedicalrent.com  
Searching vhosts for domain: labroma.org  
Searching vhosts for domain: qode.pro  
Searching vhosts for domain: conmoitamiga.org  
Searching vhosts for domain: adelantosdigital.com  
Searching vhosts for domain: ciudadanos-cs.org  
Searching vhosts for domain: dinaserver.com  
jovenes.ciudadanos-cs.org

<https://www.robtex.com/?dns=213.192.233.202>

## **mejorunidos.com**

se aplica también a mejorunidos.cat, mejorunidos.org, mejorunidos.eu, mejorunidos.net, mejorunidos.es, millorjunts.com, millorjunts.net, millorjunts.eu, millorjunts.org, millorjunts.es, blog-cs.com, blog-cs.org, albertrivera.info.

Parece que el dominio estuvo alojado en algún momento bajo la IP 62.82.134.146 (hospedado-en.cyberneticos.com AUNA TLC)

## **D) OTROS SERVIDORES A DESTACAR**

### **albertrivera.info**

Se ha encontrado alojado en algún momento en el servidor compartido de OVH  
ks384293.kimsufi.com

### **albertrivera.es**

El dominio está alojado en el servidor compartido de OVH ks384293.kimsufi.com



## E) Estudio de los subdominios

Hasta el momento se han analizado simplemente los nombres de los dominios, en esta sección nos adentramos a analizar los subdominios que están albergados en algunos de los dominios previamente analizados.

### ciudadanos-cs.org

Subdomain	IP address	Country (whois)
webadmin.ciudadanos-cs.org	?	?
webcache.ciudadanos-cs.org	?	?
www1.ciudadanos-cs.org	?	?
pop3.ciudadanos-cs.org	213.192.233.202	ES (silicontower)
www0.ciudadanos-cs.org	?	?
lists.ciudadanos-cs.org	213.192.233.202	ES (silicontower)
web.ciudadanos-cs.org	?	?
web1.ciudadanos-cs.org	?	?
web0.ciudadanos-cs.org	?	?
www-dev.ciudadanos-cs.org	?	?
ftp.ciudadanos-cs.org	164.138.208.214	ES (cyberneticos)
murcia.ciudadanos-cs.org	82.98.160.143	ES (dinahosting)
homedir.ciudadanos-cs.org	?	?
malaga.ciudadanos-cs.org	82.98.160.143	ES (dinahosting)
webguide.ciudadanos-cs.org	?	?
home.ciudadanos-cs.org	?	?
mysql.ciudadanos-cs.org	?	?
webaccess.ciudadanos-cs.org	?	?
avila.ciudadanos-cs.org	82.98.160.143	ES (dinahosting)
majadahonda.ciudadanos-cs.org	82.98.160.143	ES (dinahosting)
test.ciudadanos-cs.org	54.230.197.230	USA (amazon)
www2.ciudadanos-cs.org	?	?
search.ciudadanos-cs.org	?	?
wwwwww.ciudadanos-cs.org	?	?
app.ciudadanos-cs.org	82.98.160.143	ES (dinahosting)
secure.ciudadanos-cs.org	151.80.35.228	?
https.ciudadanos-cs.org	?	?
webmail.ciudadanos-cs.org	213.192.233.202	ES (silicontower)
mail.ciudadanos-cs.org	213.192.233.202	ES (silicontower)
almeria.ciudadanos-cs.org	82.98.160.143	ES (dinahosting)
httpd.ciudadanos-cs.org	?	?
portavoz.ciudadanos-cs.org	164.138.208.214	ES (cyberneticos)
my.ciudadanos-cs.org	?	?
webdev.ciudadanos-cs.org	?	?
webinterface.ciudadanos-cs.org	?	?
dev.ciudadanos-cs.org	82.98.160.143	ES (dinahosting)

ww3.ciudadanos-cs.org	164.138.208.216	ES (cyberneticos)
smtp.ciudadanos-cs.org	213.192.233.202	ES (silicontower)
lasrozas.ciudadanos-cs.org	82.98.160.143	ES (dinahosting)
wwwroot.ciudadanos-cs.org	?	?
web2.ciudadanos-cs.org	?	?
http.ciudadanos-cs.org	?	?
madrid.ciudadanos-cs.org	82.98.160.143	ES (dinahosting)
www.ciudadanos-cs.org	54.230.11.24	USA (amazon)
ayuntamiento-madrid.ciudadanos-cs.org	46.105.122.74	FR (ovh)
guadalajara.ciudadanos-cs.org	82.98.160.143	ES (dinahosting)
valencia.ciudadanos-cs.org	82.98.160.143	ES (dinahosting)
aragon.ciudadanos-cs.org	82.98.160.143	ES (dinahosting)
digital.ciudadanos-cs.org	164.138.208.214	ES (cyberneticos)
ww.ciudadanos-cs.org	?	?
baleares.ciudadanos-cs.org	82.98.160.143	ES (dinahosting)
websurveys.ciudadanos-cs.org	?	?
website.ciudadanos-cs.org	?	?
pozuelo.ciudadanos-cs.org	82.98.160.143	ES (dinahosting)
navarra.ciudadanos-cs.org	82.98.160.143	ES (dinahosting)
revista.ciudadanos-cs.org	46.105.122.74	FR (ovh)
webserver.ciudadanos-cs.org	?	?
weblog.ciudadanos-cs.org	?	?

**- www.ciudadanos-cs.org (54.230.11.24 )Dicha web con certificado ssl habilitado está alojado en los servidores de Amazon en EEUU.**

Subdomain	IP address	Country (whois)
my.ciudadans-cs.org	?	?
www.ciudadans-cs.org	62.82.134.146	ES (cyberneticos)
weblog.ciudadans-cs.org	?	?
web1.ciudadans-cs.org	?	?
webguide.ciudadans-cs.org	?	?
home.ciudadans-cs.org	?	?
webadmin.ciudadans-cs.org	?	?
https.ciudadans-cs.org	?	?
webserver.ciudadans-cs.org	?	?
search.ciudadans-cs.org	?	?
ftp.ciudadans-cs.org	62.82.134.146	ES (cyberneticos)
http.ciudadans-cs.org	?	?
homedir.ciudadans-cs.org	?	?
ww.ciudadans-cs.org	?	?
websurveys.ciudadans-cs.org	?	?
webaccess.ciudadans-cs.org	?	?
www-dev.ciudadans-cs.org	?	?

wwwroot.ciudadans-cs.org	?	?
www.ciudadans-cs.org	?	?
www1.ciudadans-cs.org	?	?
web.ciudadans-cs.org	?	?
webmail.ciudadans-cs.org	?	?
www0.ciudadans-cs.org	?	?
httpd.ciudadans-cs.org	?	?
webcache.ciudadans-cs.org	?	?
webinterface.ciudadans-cs.org	?	?
website.ciudadans-cs.org	?	?
web0.ciudadans-cs.org	?	?
webdev.ciudadans-cs.org	?	?
web2.ciudadans-cs.org	?	?
mysql.ciudadans-cs.org	?	?
www2.ciudadans-cs.org	?	?

Subdomain	IP address	Country (whois)
www2.albertrivera.info	?	?
mail.albertrivera.info	164.138.208.214	ES (cyberneticos)
web.albertrivera.info	?	?
web0.albertrivera.info	?	?
wwwroot.albertrivera.info	?	?
webcache.albertrivera.info	?	?

**www.albertrivera.info** **46.105.122.74** **FR**  
**(ovh)**

webmail.albertrivera.info	164.138.208.214	ES (cyberneticos)
www0.albertrivera.info	?	?
mysql.albertrivera.info	?	?
my.albertrivera.info	?	?
https.albertrivera.info	?	?
webguide.albertrivera.info	?	?
www-dev.albertrivera.info	?	?
smtp.albertrivera.info	164.138.208.214	ES (cyberneticos)
httpd.albertrivera.info	?	?
localhost.albertrivera.info	127.0.0.1	?
webserver.albertrivera.info	?	?
webdev.albertrivera.info	?	?
weblog.albertrivera.info	?	?
webaccess.albertrivera.info	?	?
www.albertrivera.info	?	?
webinterface.albertrivera.info	?	?
website.albertrivera.info	?	?
web1.albertrivera.info	?	?
http.albertrivera.info	?	?
webadmin.albertrivera.info	?	?
pop.albertrivera.info	164.138.208.214	ES (cyberneticos)

ww.albertrivera.info	?	?
homedir.albertrivera.info	?	?
web2.albertrivera.info	?	?
home.albertrivera.info	?	?
ftp.albertrivera.info	164.138.208.214	ES (cyberneticos)
websurveys.albertrivera.info	?	?
search.albertrivera.info	?	?
www1.albertrivera.info	?	?

Subdomain	IP address	Country (whois)
webdev.mejorunidos.com	?	?
web2.mejorunidos.com	?	?
homedir.mejorunidos.com	?	?
webinterface.mejorunidos.com	?	?
www-dev.mejorunidos.com	?	?
ftp.mejorunidos.com	164.138.208.214	ES (cyberneticos)
httpd.mejorunidos.com	?	?
webmail.mejorunidos.com	164.138.208.214	ES (cyberneticos)
mail.mejorunidos.com	164.138.208.214	ES (cyberneticos)
webaccess.mejorunidos.com	?	?
web0.mejorunidos.com	?	?
http.mejorunidos.com	?	?
weblog.mejorunidos.com	?	?
www0.mejorunidos.com	?	?
pop.mejorunidos.com	164.138.208.214	ES (cyberneticos)
localhost.mejorunidos.com	127.0.0.1	?
websurveys.mejorunidos.com	?	?
ww.mejorunidos.com	?	?
webcache.mejorunidos.com	?	?
website.mejorunidos.com	?	?
webserver.mejorunidos.com	?	?
web.mejorunidos.com	?	?
search.mejorunidos.com	?	?
webadmin.mejorunidos.com	?	?
www1.mejorunidos.com	?	?
web1.mejorunidos.com	?	?
www2.mejorunidos.com	?	?
wwwroot.mejorunidos.com	?	?
wwwwww.mejorunidos.com	?	?
https.mejorunidos.com	?	?
smtp.mejorunidos.com	164.138.208.214	ES (cyberneticos)
www.mejorunidos.com	164.138.208.214	ES (cyberneticos)
home.mejorunidos.com	?	?
my.mejorunidos.com	?	?
mysql.mejorunidos.com	?	?
webguide.mejorunidos.com	?	?

## **F) Google Analytics:**

Las herramientas de Google analytics de Ciudadanos analizaron como webs propias las siguientes webs

Egara civitas(?) - blog a blogspot <http://egara-civitas.blogspot.com.es/>  
<http://movciudadano.es/> (82.98.160.221)

Deciudadanoaciudadano.org

ciudadans.org (galicia)

csalmeria.org

elcambio.es (politica y porno???) (el mismo google analytics)

societatcivilcatalana.org (el mismo google analytics)

<http://www.ciudadanosbormujos.es/>