



CAZANDO GAMUSINOS

TÉCNICAS OSINT

PARA DESCUBRIR

LO QUE SE CUECE

DETRÁS DE LAS

FALSAS WEBS

gamusino

1. *m. Esp.* Animal imaginario, cuyo nombre se usa para dar bromas a los cazadores novatos.

Sevilla, 6-7 de febrero de 2020



```
# whoami
```

José Luis Navarro Adam

Técnico Superior de Seguridad Informática

Perito Judicial de Seguridad Informática

Director de Proyectos e I+D Girsanet (<https://girsanet.com>)

Consultor Ciberseguridad en Zinetik Consultores (<https://zinetik.com>)

```
# cat /home/jlnavarro/.profile
```

"Constructor de Murallas". Apasionado de la seguridad informática y la privacidad en Internet. Creador del firewall CDC-data y fan de Raspberry PI
#PurpleTeam

Email: jlnavarro@girsanet.com y jlnavarro@zinetik.com

Twitter: @JLNavarroAdam

Linkedin: <https://www.linkedin.com/in/jlnavarroadam/>



```
# ./charla.sh
```

Continuamente nos llegan ofertas de muerte de artículos muy buscados con precios irresistibles. A veces como anuncios en webs o redes sociales, y otras por correos electrónicos. Con el auge de los black fridays, singles days, rebajas, navidades, continuamente nos inundan de chollos irresistibles. Y por desgracia muchas veces son fraudes.

Objetivo: emplear técnicas OSINT para descubrir qué hay detrás de esas webs falsas, qué patrones siguen, cómo identificarlas, cómo dejarlas fuera de juego, y emplearlas como herramientas de detección de IoC en investigaciones forenses y policiales



1. EMPIEZA LA CAZA: El ofertón del Black Friday!!!



GALEO

CARRITO DE COMPRAS (0)

BUSCAR

ENTRAR/REGISTRARSE

Accesorios para calzado, relojes y joyería

Actividades creativas

Aire libre y deportes

Animales y figuras

Más ▾

Accesorios para calzado, relojes y joyería



www.galeonvigo.es

JINXIAOXIAO Caja de Almacenamiento de cosméticos

€19.53

€11.25

Ahorre: 42% descuento



www.galeonvigo.es

Correa de Repuesto Glowjoy Compatible con Fitbit

€19.45

€11.06

Ahorre: 43% descuento



www.galeonvigo.es

S-tubit Joyas de Cuero Hechas a Mano y Hechas a Mano Rollos con

€38.09

€21.60

Ahorre: 43% descuento



www.galeonvigo.es

Caja De Exhibición De La Organización De La Pulsera De La

€92.89

€50.79

Ahorre: 45% descuento



1. EMPIEZA LA CAZA: La diferencia está en los detalles...

Browser window showing the website <https://www.galeonvigo.es/>. The page displays four products for sale, each with a price, discount, and rating.

Product	Price	Discount	Rating
Yyqthbc Scooter de Aluminio Plegable Kick Scooter Rueda de	€163.17 / €59.82	Ahorre: 63% descuento	★★★★★ (2023)
YBZS Pedal De Bicicleta De Montaña Ligero. Plataforma De	€36.33 / €20.92	Ahorre: 42% descuento	★★★★★ (3281)
WENZHEN Regalos de Scooter Scooter 3 en 1 para niños con	€168.56 / €59.82	Ahorre: 65% descuento	★★★★★ (2023)
Myself-Inflatable floating row Gigante piña Inflable	€70.60 / €40.66	Ahorre: 42% descuento	★★★★★ (3145)

Red arrows point to the following contact information:

- www.galeonvigo.es
- sales@customerservicesglobal.com
- Casa Contáctenos
- Envío y devoluciones Aviso de privacidad
- Síguenos (Social media icons: Twitter, Facebook, Pinterest, Instagram)



1. EMPIEZA LA CAZA: La diferencia está en los detalles...

https://www.galeonvigo.es/privacy.html

Buscar...

Archivo Edición Ver Favoritos Herramientas Ayuda

Información de mi Cuenta

Intimidad

¿Cuál es su política de privacidad?

Nos tomamos su privacidad muy en serio. Nunca alquilaremos ni venderemos su información a terceros, solo usaremos la información que recopilamos de usted para transmitir la información de su pedido, o para enviarle catálogos y correos electrónicos a petición suya.

Seguridad

¿Es seguro hacer un pedido en su sitio?

¡Absolutamente! Nos tomamos la seguridad muy en serio y hacemos todo lo que podemos para proteger los datos confidenciales de nuestros clientes. La información de la tarjeta de crédito para pedidos web está protegida de las siguientes maneras:

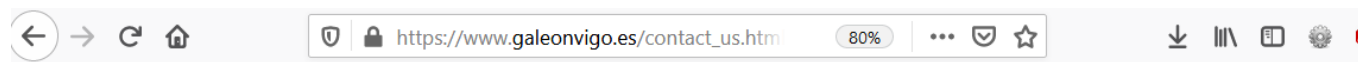
1. Cifrado SSL hacia y desde los servidores y el navegador web.
2. Los números de tarjeta de crédito no se almacenan en nuestra base de datos. Mantenemos en el archivo solo los últimos 4 dígitos en los casos donde necesitamos verificar la tarjeta que se usó.
3. Una vez que la información se transmite a nuestros servidores para su procesamiento, utilizamos un cifrado aún más fuerte en la parte posterior para transmitir la solicitud a nuestro procesador de pagos para verificar la tarjeta de crédito y colocar una autorización para el total del pedido.
4. Si la autorización, la verificación de dirección y la evaluación de riesgos están claras, se acepta el pedido y se asocia un único ID único con el pedido para fines de facturación de la autorización previa. Esta identificación no se puede usar para colocar más autorizaciones o facturar más que la autorización original. No contiene un enlace identificable al número de la tarjeta de crédito.
5. Una vez que la ID se ha utilizado para facturar la orden (lo que ocurre una vez que la orden comienza a enviarse), ya no es válida y no se puede usar para autorizar o facturar nuevamente.

ATRÁS

Bla bla bla...



1. EMPIEZA LA CAZA: La diferencia está en los detalles...



GALEO

CARRITO DE COMPRAS (0)

BUSCAR

ENTRAR/REGIS

Accesorios para calzado, relojes y joyería

Actividades creativas

Aire libre y deportes

Animales y figuras

Más ▾

INICIO > MI CUENTA

Información de mi Cuenta

Nota:

Si desea consultar información detallada sobre el producto, asegúrese de dejar el enlace del producto.

Por favor inicie sesión antes de enviar el mensaje, no podemos recibir ningún mensaje anónimo. Si necesita una respuesta más rápida, envíe un correo electrónico a sales@customerservicesglobal.com

* Información obligatoria

*Nombre:

*Dirección de email:

*Mensaje:



1. EMPIEZA LA CAZA: La diferencia está en los detalles...

Información de la página - https://www.galeonvigo.es/

General Medios Permisos Seguridad

Identidad del sitio web
Sitio web: www.galeonvigo.es
Propietario: Este sitio web no proporciona información sobre su dueño.
Verificado por: cPanel, Inc.
Expira el: lunes, 17 de febrero de 2020

Privacidad e historial
¿Se ha visitado este sitio web anteriormente?
¿Este sitio web almacena información?
¿Se han guardado contraseñas de este sitio web?

Detalles técnicos
Conexión cifrada (TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256)
La página que está viendo fue cifrada.
El cifrado dificulta que personas no autorizadas lean esta página mientras viajó por Internet.

Visor de certificados: "www.galeonvigo.es"

General Detalles

Este certificado ha sido verificado para los siguientes usos:

- Certificado del cliente SSL
- Certificado del servidor SSL

Emitido para

Nombre común (CN)	www.galeonvigo.es
Organización (O)	<No es parte de un certificado>
Unidad organizativa (OU)	<No es parte de un certificado>
Número de serie	00:CA:25:7D:F5:E3:13:5F:D3:2A:61:87:FC:C5:8D:7B:8A

Emitido por

Nombre común (CN)	cPanel, Inc. Certification Authority
Organización (O)	cPanel, Inc.
Unidad organizativa (OU)	<No es parte de un certificado>

Periodo de validez

Comienza el	lunes, 18 de noviembre de 2019
Caduca el	lunes, 17 de febrero de 2020

Huellas digitales

Huella digital SHA-256	06:FF:BB:A3:8B:D6:5E:FA:CB:4F:85:38:BB:AC:EE:1A:42:E9:F5:1E:63:D5:74:F5:DE:07:07:D5:0D:12:6A:8E
Huella digital SHA1	7B:48:C2:22:26:25:43:4E:C1:FE:60:17:E4:5A:0B:49:9D:53:3E:96

Cerrar



1. EMPIEZA LA CAZA: Por supuesto siempre ver el código html generado

<https://templates.net>



2. TIRANDO DE LOS HILOS: galeonvigo.es



GOBIERNO DE ESPAÑA MINISTERIO DE ECONOMÍA Y EMPRESA domini.es red.es @administración electrónica

Español | Català | Euskera | Galego | English

Seguinos en: RSS LinkedIn

Buscar...

INICIO BUSCA Y REGISTRA TU DOMINIO AGENTES REGISTRADORES TODO LO QUE NECESITAS SABER **GESTIONA TU DOMINIO** ACTUALIDAD Y NOTICIAS SOBRE NOSOTROS

Información de Dominio

Volver

Los datos de contacto de este dominio están ocultos. Si desea comunicarse con el Titular y el PCA pulse [aquí](#)

DATOS DEL TITULAR	
Nombre del Dominio	galeonvigo.es
Estado	Activado
Identificador	12C3B2E-ESNIC-F5
Titular	spaghetti proclamation
Fecha de Alta	03-09-2019
Fecha de Caducidad	03-09-2020
Agente Registrador	REGISTRAR.EU

PERSONA DE CONTACTO ADMINISTRATIVO	
Identificador	12C3B2F-ESNIC-F5
Nombre	spaghetti proclamation

PERSONA DE CONTACTO TECNICO	
Identificador	12C3B2F-ESNIC-F5
Nombre	spaghetti proclamation

SERVIDORES DNS	
Nombre Servidor	IP
hcns3.dz8.org	
hcns4.dz8.org	



2. TIRANDO DE LOS HILOS: dz8.org

Site Info **new** Who Is Trace Route RBL Check What's My IP? Web Search

Enter Web Site URL Address:
dz8.org **Query**



大理折客网 大理打折网:最新最快最全的同城打折信息。

Description: 大理折客网- (dz8.org) 打折是一种生活方式, 生活是一门艺术, 没有完美的艺术, 只有更好的生活。从现在开始就成为一名时尚“折客”, 相信你的选择一定没问题, 大声叫出来我是一名”折客, 我就要打折”。

Keywords: 大理,大理市,打折网,折客网,大理折客网,大理打折,大理促销,大理下关,大理旅游,大理州,大理促销海报,大理网站,大理酒店,大理打折机票, 打折促销知识

Tags: [dz8](#), [大理折客网](#), [最新最快最全的同城打折信息](#), [大理打折网](#), [节能汽车推广目录](#), [折扣促销](#), [大理打折网广告位](#), [政府补贴](#), [分类信息](#), [发布信息需知](#), [节日促销](#), [第一批](#), [第二批](#), [开业促销](#), [org](#), [优惠券](#), [大理州](#), [大理市](#), [我就要打折](#), [打折是一种生活方式](#), [生活是一门艺术](#), [相信你的选择一定没问题](#), [大声叫出来我是一名](#), [只有更好的生活](#), [没有完美的艺术](#), [从现在开始就成为一名时尚](#), [欧普照明龙山市场专卖店开始试营业了](#), [诚征各地区站管理员](#), [博物馆陈列馆纪念馆规划设计场馆设](#), [款雅阁](#), [中升丰田限时抢购第二轮激情绽放](#), [欢迎你的加入](#), [种优惠](#), [第三批](#), [古宅古镇故居祠堂故里规划规划设计](#), [暂无本类信息](#), [网络广告策划过程](#), [大理洁净洗涤](#), [把本站设为首页](#), [更多>>](#),

Dz8.org

Content Revalency: Title: 0.00% Description: 8.33% Keywords: 0.00% | Document size: 57,656 bytes
More info: [Whois](#) - [Trace Route](#) - [RBL Check](#)

DZ8.ORG - Site Location

Country/Flag	Hong Kong
City/Region/Zip Code	Tsuen Wan, 00,
Organization	AS Data(Hong Kong)Limited
Internet Service Provider	AS Data(Hong Kong)Limited

DZ8.ORG - Domain Information

Domain	DZ8.ORG [Traceroute RBL/DNSBL lookup]
Whois server	whois.pir.org





2. TIRANDO DE LOS HILOS: hcns3.dns.org

Archivo Editar Ver Historial Marcadores Herramientas Ayuda

insite Bu site: OS Inform Regist CQ 52. X Servid CQ 51. la V OP Open VirusT ia.51. la

Enter Domain Name or IP Address:
52.214.115.96 Whois

52.214.115.96 - Geo Information

IP Address	52.214.115.96
Host	ec2-52-214-115-96.eu-west-1.compute.amazonaws.com
Location	IE, Ireland
City	Dublin, 07 D02
Organization	Amazon Technologies
ISP	Amazon Technologies
AS Number	AS16509 Amazon.com, Inc.
Latitude	53°33'31" North
Longitude	6°24'89" West
Distance	2472.70 km (1536.46 miles)

Map Location new

World Map Google Maps Yahoo

C:\WINDOWS\system32\nslookup.exe

Servidor predeterminado: UnKnown
Address: 192.168.10.1

> hcns3.dz8.org
Servidor: UnKnown
Address: 192.168.10.1

Respuesta no autoritativa:
Nombre: hcns3.dz8.org
Address: 52.57.114.204

> hcns4.dz8.org
Servidor: UnKnown
Address: 192.168.10.1

Respuesta no autoritativa:
Nombre: hcns4.dz8.org
Address: 52.214.115.96

> _



2. TIRANDO DE LOS HILOS: registrar.eu

Archivo Editar Ver Historial Marcadores Herramientas Ayuda

ar des Veeam Email ¿Qué Toolbo insite:

https://registrar.eu

Registrar.eu

For more information, please contact your hosting provider.
 Pour plus d'informations, vous contactez votre hosting provider.
 Für weitere Informationen kontaktieren Sie bitte Ihren Hosting Provider.
 Voor meer informatie, neem contact op met uw hosting provider.
 Para más información, por favor contacte con su proveedor de hosting.
 Для получения дополнительной информации свяжитесь с вашим.
 详情请联系您的域名注册商。

© Registrar.eu 2017

Archivo Editar Ver Historial Marcadores Herramientas Ayuda

¿Qué Toolbo insite: Bu site:ga .es Inform Regist CQ Rel X CQ Openp op Openp

cqcounter.com/w/

Site Info **new** Who Is Trace Route RBL Check What's My IP? Web Search

Enter Domain Name or IP Address:

registrar.eu **Whois**

REGISTRAR.EU - Geo Information

IP Address	185.87.187.6 Whois Trace Route DNSBL lookup
Host	registrar.eu
Location	NL, Netherlands
City	-,
Organization	PCextreme B.V.
ISP	PCextreme B.V.
AS Number	AS48635 Astralus B.V.
Latitude	52° 38'24" North
Longitude	4° 89'95" East
Distance	1744.92 km (1084.24 miles)



2. TIRANDO DE LOS HILOS: openprovider.com

Archivo Editar Ver Historial Marcadores Herramientas Ayuda

¿Qué? Toolbr insite: Bu site:ga .es Inform Regist

← → ↻ 🏠 🔒 🔍 ⋮ ⭐

cqcounter.com/wi

% and explicit permission by EURid, nor in any attempt hereof, to ap
% automated, electronic processes to EURid (or its systems).
%
% You agree that any reproduction and/or transmission of data for
% commercial purposes will always be considered as the extraction of
% substantial part of the content of the WHOIS database.
%
% By submitting the query you agree to abide by this policy and acce
% that EURid can take measures to limit the use of its WHOIS service
% in order to protect the privacy of its registrants or the integrit
% of the database.
%
% The EURid WHOIS service on port 43 (textual whois) never
% discloses any information concerning the registrant.
% Registrant and on-site contact information can be obtained through
% webbased WHOIS service available from the EURid website www.eurid.
%
% WHOIS registrar.eu
Domain: registrar.eu
Script: LATIN

Registrant:
NOT DISCLOSED!
Visit www.eurid.eu for webbased WHOIS.

On-site(s):
NOT DISCLOSED!
Visit www.eurid.eu for webbased WHOIS.

Registrar:
Name: Registrar.eu
Website: https://www.openprovider.com

Name servers:
ns-eu-west-2.openprovider.eu
ns-eu-west-1.openprovider.eu
ns-eu-central-1.openprovider.eu

Please visit www.eurid.eu for more info.

Archivo Editar Ver Historial Marcadores Herramientas Ayuda

¿Qué? Toolbr insite: Bu site:ga .es Inform Regist CQ Regist CQ Op X op Open

← → ↻ 🏠 🔒 🔍 ⋮ ⭐

cqcounter.com/wi

Site Info new Who Is Trace Route RBL Check What's My IP? Web Search

Enter Domain Name or IP Address:
openprovider.com Whois

OPENPROVIDER.COM - Domain Information new

Domain	OPENPROVIDER.COM [Site Info Traceroute RBL/DNSBL lookup]
Registrar	Hosting Concepts B.V. d/b/a Openprovider Hosting Concepts B.V. d/b/a Openprovider
Whois server	whois.verisign-grs.com
Created	04-Feb-2000
Updated	07-Jun-2019
Expires	04-Feb-2024
Time Left	1464 days 15 hours 28 minutes
Status	clientTransferProhibited https://icann.org/epp#clientTransferProhibited clientTransferProhibited https://icann.org/epp#clientTransferProhibited
DNS servers	NS-EU-CENTRAL-1.OPENPROVIDER.EU 18.194.228.62 NS-EU-WEST-1.OPENPROVIDER.EU 52.19.66.106 NS-EU-WEST-2.OPENPROVIDER.EU 52.56.180.255 ns-eu-central-1.openprovider.eu 18.194.228.62 ns-eu-west-1.openprovider.eu 52.19.66.106 ns-eu-west-2.openprovider.eu 52.56.180.255

OPENPROVIDER.COM - Geo Information

IP Address	185.87.187.6 Whois Trace Route DNSBL lookup
Host	openprovider.com
Location	🇳🇱 NL, Netherlands
City	-



2. TIRANDO DE LOS HILOS: src://galeonvigo.es -> js.users.51.la

```
www.galeonvigo.es - Herramientas de desarrollo F12
F12  Explorador DOM  Consola  Depurador  Red  Rendimiento

www.galeonvigo.es X

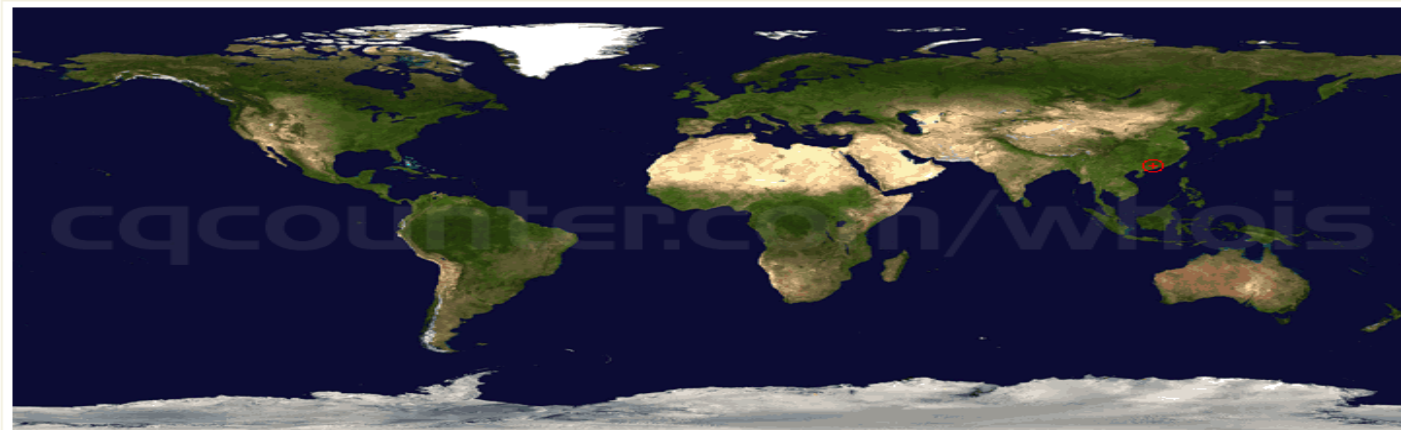
type="text/javascript"></script>
470 <script src="includes/templates/47frocks/js/plugins.js"
type="text/javascript"></script>
471 <script src="includes/templates/47frocks/js/site.js"
type="text/javascript"></script>
472 </body><script>
473   var colForms = document.getElementsByTagName('form');
474   for (let i = 0; i < colForms.length; i++)
475   {
476     var action = colForms[i].getAttribute('action');
477     if(action.indexOf('advanced_search_result') > 0)
478       colForms[i].setAttribute('action', '//www.for-searchs.com
479   }
480 </script>
481 <div style='display:none'><script
src='https://js.users.51.la/19830179.js'></script></div>
482
483
484
485
486
487
488 </html>
489
490
```

51.LA - Geo Information

IP Address	14.17.102.104	Whois	Trace Route	DNSBL lookup
Host	51.la			
Location	🇨🇳 CN, China			
City	Guangzhou, 30			
Organization	China Telecom Guangdong			
ISP	China Telecom Guangdong			
AS Number	AS134764 CHINANET Guangdong province network			
Latitude	23°11'67" North			
Longitude	113°25'00" East			
Distance	8285.52 km (5148.38 miles)			

Map Location

☒ World Map ☐ Google Maps ☐ Yahoo Maps ☐ Microsoft Live Maps



51.LA - Whois Information

Domain Name: [51.LA](#)
Registry Domain ID: D473296-LANIC
Registrar WHOIS Server:
Registrar URL:
Updated Date: 2019-03-25T13:22:06.0Z
Creation Date: 2005-01-17T01:00:00.0Z
Registry Expiry Date: 2023-01-17T23:59:59.0Z
Registrar: Key-Systems GmbH
Registrar IANA ID:



2. TIRANDO DE LOS HILOS: cdnhwc1.com & wsdvs.com

220.242.140.187 - Whois Information

```
% [whois.apnic.net]
% Whois data copyright terms    http://www.apnic.net/db/dbcopyright.html

% Information related to '220.242.0.0 - 220.242.255.255'

% Abuse contact for '220.242.0.0 - 220.242.255.255' is 'ipas@cnnic.cn'

inetnum:        220.242.0.0 - 220.242.255.255
netname:        CHINANETCENTER
descr:          ChinaNetCenter Ltd.
admin-c:        ZM1723-AP
tech-c:         ZM1723-AP
country:        CN
mnt-by:         MAINT-CNNIC-AP
mnt-irt:        IRT-CNNIC-CN
status:         ALLOCATED PORTABLE
last-modified:  2016-11-01T06:12:03Z
source:         APNIC

irt:            IRT-CNNIC-CN
address:        Beijing, China
e-mail:         ipas@cnnic.cn
abuse-mailbox:  ipas@cnnic.cn
admin-c:        IP50-AP
tech-c:         IP50-AP
auth:           # Filtered
remarks:        Please note that CNNIC is not an ISP and is not
remarks:        empowered to investigate complaints of network abuse.
remarks:        Please contact the tech-c or admin-c of the network.
mnt-by:         MAINT-CNNIC-AP
last-modified:  2017-11-01T08:57:39Z
source:         APNIC

person:         Zhong Xing
address:        4G Guomen Building, Sanyuan Bridge Dongsanhuan, Beijing
country:        CN
phone:          +86-010-84519900
e-mail:         zhongx@wangsu.com
nic-hdl:        ZM1723-AP
mnt-by:         MAINT-CNNIC-AP
```

C:\WINDOWS\system32\cmd.exe - nslookup

Microsoft Windows [Versión 10.0.18362.592]
(c) 2019 Microsoft Corporation. Todos los derechos reservados.

C:\Users\JLNAVARRO>nslookup
Servidor predeterminado: UnKnown
Address: 192.168.10.1

> js.users.51.la
Servidor: UnKnown
Address: 192.168.10.1

Respuesta no autoritativa:
Nombre: js.users.51.la.wsdvs.com
Addresses: 163.171.128.16

220.242.140.187
220.242.182.12
220.242.139.165

Aliases: js.users.51.la
js.users.51.la.c.cdnhwc1.com



2. TIRANDO DE LOS HILOS: cdnhwc1.com & wsdvs.com

```
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 56241
;; flags: qr rd ra; QUERY: 1, ANSWER: 5, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;js.users.51.la.c.cdnhwc1.com. IN A

;; ANSWER SECTION:
js.users.51.la.c.cdnhwc1.com. 7 IN CNAME js.us
js.users.51.la.wsdvs.com. 7 IN A 220.2
js.users.51.la.wsdvs.com. 7 IN A 220.2
js.users.51.la.wsdvs.com. 7 IN A 163.1
js.users.51.la.wsdvs.com. 7 IN A 220.2

;; Query time: 0 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Mon Feb 03 10:04:12 CET 2020
;; MSG SIZE rcvd: 159
```

Domain Name: [wsdvs.com](https://www.wsdvs.com)
Registry Domain ID: 1864059889_DOMAIN_COM-VRSN
Registrar WHOIS Server: grs-whois.hichina.com
Registrar URL: <http://whois.aliyun.com>
Updated Date: 2019-07-30T07:52:39Z
Creation Date: 2014-06-24T06:27:42Z
Registrar Registration Expiration Date: 2020-06-24T06:27:42Z
Registrar: Alibaba Cloud Computing (Beijing) Co., Ltd.
Registrar IANA ID: 420
Reseller:
Domain Status: ok <https://icann.org/epp#ok>
Registrant City:
Registrant State/Province: shang hai
Registrant Country: CN
Registrant Email: <https://whois.aliyun.com/whois/whoisForm>
Registry Registrant ID: Not Available From Registry
Name Server: DNS1.[WSDVS.ORG](https://www.wsdvs.org)
Name Server: DNS2.[WSDVS.INFO](https://www.wsdvs.info)
Name Server: DNS3.[WSDVS.ORG](https://www.wsdvs.org)
Name Server: DNS4.[WSDVS.INFO](https://www.wsdvs.info)
Name Server: DNS5.[CDN30.ORG](https://www.cdn30.org)
DNSSEC: unsigned
Registrar Abuse Contact Email: DomainAbuse@service.aliyun.com
Registrar Abuse Contact Phone: +86.95187
URL of the ICANN WHOIS Data Problem Reporting System: <http://>
>>>Last update of WHOIS database: 2020-02-03T09:04:44Z <<<

For more information on Whois status codes, please visit <http://>

Important Reminder: Per ICANN 2013RAA's request, Hichina has

ALIYUN.COM [[Site Info](#) [Traceroute](#) [RBL/DNSBL lookup](#)]
Alibaba Cloud Computing (Beijing) Co., Ltd. Alibaba Cloud Computing (Beijing) Co., Ltd.
whois.verisign-grs.com
28-Sep-2007
03-Jan-2019
28-Sep-2021
602 days 14 hours 54 minutes
clientTransferProhibited <https://icann.org/epp#clientTransferProhibited> serverDeleteProhibited
NS3.ALIYUN.COM [115.124.17.155](https://www.115.124.17.155)
NS4.ALIYUN.COM [110.75.20.27](https://www.110.75.20.27)
NS5.ALIYUN.COM [110.75.38.28](https://www.110.75.38.28)

IP Address	Whois	Trace Route	DNSBL lookup
140.205.135.3	Whois	Trace Route	DNSBL lookup
140.205.60.46	Whois	Trace Route	DNSBL lookup
106.11.253.86	Whois	Trace Route	DNSBL lookup
106.11.253.83	Whois	Trace Route	DNSBL lookup
106.11.249.99	Whois	Trace Route	DNSBL lookup
106.11.248.146	Whois	Trace Route	DNSBL lookup
106.11.248.144	Whois	Trace Route	DNSBL lookup
106.11.172.56	Whois	Trace Route	DNSBL lookup
106.11.172.55	Whois	Trace Route	DNSBL lookup
106.11.172.51	Whois	Trace Route	DNSBL lookup
106.11.172.9	Whois	Trace Route	DNSBL lookup

[aliyun.com](https://www.aliyun.com)
CN, China
Hangzhou, 02
Hangzhou Alibaba Advertising Co.,Ltd.
Zhejiang Taobao Network Co.,Ltd
AS37963 Hangzhou Alibaba Advertising Co.,Ltd.
30°29'36" North



2. TIRANDO DE LOS HILOS: 19830179.js

[illegible]



2. TIRANDO DE LOS HILOS: for-searchs.com

Site Info **new** Who Is Trace Route RBL Check What's My IP? Web Search

Enter Domain Name or IP Address:

Whois

FOR-SEARCHS.COM - Domain Information **new**

Domain
Registrar
Whois server
Created
Updated
Expires
Time Left
Status
DNS servers

FOR-SEARCHS.COM - Whois Information

Domain Name: [FOR-SEARCHS.COM](https://www.for-searchs.com)
Registry Domain ID: 2358796364_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.name.com
Registrar URL: <http://www.name.com>
Updated Date: 2019-02-07T08:48:06Z
Creation Date: 2019-02-07T08:48:06Z
Registry Expiry Date: 2020-02-07T08:48:06Z
Registrar: Name.com, Inc.
Registrar IANA ID: 625
Registrar Abuse Contact Email: abuse@name.com
Registrar Abuse Contact Phone: 7202492374
Domain Status: clientTransferProhibited <https://icann.org/epp#clientTransferProhibited>

```
mc [root@cdcddata.girsanet.com]:/home/cedece
root@cdcddata:/home/cedece# dig www.for-searchs.com

; <<>> DiG 9.10.3-P4-Debian <<>> www.for-searchs.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 45296
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;www.for-searchs.com.      IN      A

;; ANSWER SECTION:
www.for-searchs.com.      299     IN      A      204.12.221.58

;; Query time: 3
;; SERVER: 127.0.0.1
```

204.12.221.58 - Geo Information

IP Address	204.12.221.58
Host	204.12.221.58
Location	US, United States
City	Kansas City, MO 64106
Organization	WholeSale Internet
ISP	WholeSale Internet
AS Number	AS32097 WholeSale Internet, Inc.
Latitude	39°10'68" North
Longitude	94°56'60" West
Distance	8977.81 km (5578.55 miles)



2. TIRANDO DE LOS HILOS: for-searchs.com

https://tools.dnsstuff.com/#dnsReport ty		
SOA		
Status	Test Name	Information
PASS	SOA record check	All nameservers provided a SOA record for the zone. This is good because your nameservers should be configured in a master slave relationship, which allows uniform updates and agreement of resource record data. The SOA records provided are: Primary nameserver: ns1cnb.name.com. Hostmaster E-mail address: support@name.com. Serial #: 1580342400 Refresh: 10800 Retry: 3600 Expire: 604800 Minimum: 3600
PASS	SOA serial agreement	All nameserver SOAs agree on the serial number. This means that your nameservers are using the same data (unless you have different sets of data with the same serial number, which would be very bad)!
WARN	SOA field check	One or more SOA fields are outside recommended ranges. Values that are out of specifications could cause delays in record updates or unnecessary network traffic. The SOA fields out of range are: serial 1580342400 SERIAL - we check that your serial number matches the recommended format found in RFC1912 section 2.2. expire 604800 EXPIRE - RFC1912 suggests a value between 1209600 to 2419200.
MX		
Status	Test Name	Information
FAIL	MX records check	No MX records exist within the zone. This is legal, but if you want to receive E-mail on this domain, you should have MX record(s). The program can't continue in a case like this, so we are assuming you don't receive mail on this domain.
WWW		
Status	Test Name	Information
PASS	WWW record check	Domain has a WWW hostname. www.for-searchs.com. 204.12.221.58 300
INFO	Domain record	The domain literal has no address records.
PASS	IP Address(es) valid	All addresses are public. If there were any private IPs, they would not be reachable, causing problems reaching your web site.
FAIL	WWW enabled	We were unable to connect to any of your WWW addresses listed. Users will be unable to access your site until this is resolved. 204.12.221.58 : server timeout
INFO	SSL enabled	SSL is not enabled. This is ok, but if your website offers online shopping or other private services, you should acquire an SSL cert and enable SSL. SSL will encrypt the data communication between your site and customers, helping to prevent private data from being intercepted and read.



2. TIRANDO DE LOS HILOS: @customerservicesglobal.com

Site Info **new** Who Is Trace Route RBL Check What's My IP? Web Search

Enter Domain Name or IP Address:

customerservicesglobal.com

Whois

CUSTOMERSERVICESGLOBAL.COM - Domain Information **new**

Domain	CUSTOMERSERVICESGLOBAL.COM [Site Info Traceroute RBL/DNSBL lookup]
Registrar	Gransy, s.r.o. GRANSY S.R.O D/B/A SUBREG.CZ
Whois server	whois.verisign-grs.com
Created	04-Jun-2019
Updated	08-Nov-2019
Expires	04-Jun-2020
Time Left	184 days 11 hours 33 minutes
Status	ok https://icann.org/epp#ok ok https://www.icann.org/epp#ok
DNS servers	DNS1.YANDEX.NET 213.180.204.213 DNS2.YANDEX.NET 93.158.134.213 dns1.yandex.net 213.180.204.213 dns2.yandex.net 93.158.134.213

CUSTOMERSERVICESGLOBAL.COM - Geo Information

IP Address	104.160.6.132 Whois Trace Route DNSBL lookup
Host	customerservicesglobal.com
Location	US, United States
City	Wilmington, DE 19803
Organization	CachedNet LLC
ISP	CachedNet LLC

customerservicesglobal.com

Domain Name: customerservicesglobal.com

Registry Domain ID: 2398442893_DOMAIN_COM-VRSN

Registrar WHOIS Server: whois.regtons.com

Registrar URL: http://regtons.com

Updated Date: 2019-11-08T00:00:00Z

Creation Date: 2019-06-04T00:00:00Z

Registrar Registration Expiration Date: 2020-06-04T00:00:00Z

Registrar: GRANSY S.R.O D/B/A SUBREG.CZ

Registrar IANA ID: 1505

Registrar Abuse Contact Email: abuse@regtons.com

Registrar Abuse Contact Phone: +420.734463373

Reseller: liu cheng

Domain Status: ok https://www.icann.org/epp#ok

Registry Registrant ID: G-1157143

Registrant Name: Domain Admin

Registrant Organization: Whois protection, this company does not own this domain name s.r.o.

Registrant Street: Jaurisova 515/4

Registrant City: Praha 4

Registrant State/Province:

Registrant Postal Code: 14000

Registrant Country: CZ



2. TIRANDO DE LOS HILOS: Liu Cheng

Google

liu cheng

Todo Imágenes Noticias Shopping Videos Más Configuración Herramientas

Aproximadamente 181.000.000 resultados (0,43 segundos)

Liu Cheng (bádminton) - Wikipedia, la enciclopedia libre
[https://es.wikipedia.org/wiki/Liu_Cheng_\(bádminton\)](https://es.wikipedia.org/wiki/Liu_Cheng_(bádminton))
Liu Cheng (Sanming, Fujian; 4 de julio de 1992) es un jugador profesional de bádminton chino, ganador del Campeonato Mundial de Bádminton en Glasgow ...

Liu Cheng (badminton) - Wikipedia
[https://en.wikipedia.org/wiki/Liu_Cheng_\(badmint...\)](https://en.wikipedia.org/wiki/Liu_Cheng_(badmint...)) Traducir esta página
Liu Cheng is a Chinese badminton player. He was the men's doubles World Champion in 2017 partnered with Zhang Nan, also the mixed doubles World and ...

Current ranking: 28 (MD 5 November 2019) **Height:** 1.84 m (6 ft 0 in)
Highest ranking: 2 (MD 21 June 2018); 2 (XD 3 ...
Achievements · BWF World ... · BWF World Tour (1 ...

LIU Cheng | Profile - BWF Fansite
<https://bwfbadminton.com/player/liu-cheng>
Q & A. Any previous Olympics Games competed in and results? "none". When and where you began playing, and why this sport? "9 years old, because nobody ...
LIU Cheng | TOURNAMENT ... · LIU Cheng | HEAD TO HEAD ... · Ranking history

Imágenes de liu cheng

Más imágenes de liu cheng

Denunciar imágenes

Liu Cheng
Jugador de bádminton

Liu Cheng es un jugador profesional de bádminton chino, ganador del Campeonato Mundial de Bádminton en Glasgow en 2017, en la modalidad de parejas masculinas junto a Zhang Nan. [Wikipedia](#)

Fecha de nacimiento: 4 de enero de 1992 (edad 27 años), Sanming, República Popular China

Estatura: 1,84 m
Peso: 82 kg
Posición actual: 28 (MD 5 November 2019)
Clasificación más alta: 2

Otras personas también buscan

Ver otros 10

Liu Yuchen Li Junhui Bao Yixin Huang Kaixiang Tang Jinhua

Sugerencias

Registrarse como responsable de este panel de información

**LIU CHENG = PACO GARCÍA
(en chino)**

Liu Cheng en Amazon.es: Libros y Ebooks de Liu Cheng

<https://www.amazon.es/Liu-Cheng>



2. TIRANDO DE LOS HILOS: regtons.com

REGTONS.COM - Domain Information ^{new}	
Domain	REGTONS.COM [Site Info Traceroute RBL/DNSBL lookup]
Registrar	Gransy, s.r.o. GRANSY S.R.O D/B/A SUBREG.CZ
Whois server	whois.verisign-grs.com
Created	02-Apr-2007
Updated	19-Dec-2016
Expires	02-Apr-2023
Time Left	1216 days 7 hours 10 minutes
Status	clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited clientTransferProhibited https://icann.org/epp#clientTransferProhibited clientDeleteProhibited https://www.icann.org/epp#clientDeleteProhibited Domain Status: clienttransferprohibited
DNS servers	NS.GRANSY.COM 82.208.29.194 NS2.GRANSY.COM 89.187.130.100 NS3.GRANSY.COM 72.26.225.234 NS4.GRANSY.COM 85.25.73.97 NS5.GRANSY.COM 79.172.193.112 ns.gransy.com 82.208.29.194 ns2.gransy.com 89.187.130.100 ns3.gransy.com 72.26.225.234 ns4.gransy.com 85.25.73.97 ns5.gransy.com 79.172.193.112
REGTONS.COM - Geo Information	
IP Address	77.78.104.200 Whois Trace Route DNSBL lookup
Host	regtons.com
Location	CZ, Czech Republic
City	-
Organization	Casablanca INT
ISP	Casablanca INT

insite:"casablanca int"

[Todo](#)[Maps](#)[Noticias](#)[Imágenes](#)[Shopping](#)[Más](#)[Configuración](#)

Aproximadamente 5 resultados (0,26 segundos)

ICT services | Casablanca.cz

<https://www.casablanca.cz> > ... [Traducir esta página](#)

We create services in the world of modern technology. We are a professional partner and guide in your world of telecommunications and ICT services.

Falta: insite:casablancaint"

Contact | Casablanca.cz

<https://www.casablanca.cz> > [contact](#) > [Traducir esta página](#)

Want to join forces? Do you need our help or do you have an enquiry? Feel free to contact us – together, we will try to find a solution. If you like to follow current ...

Falta: insite:casablancaint"

CASABLANCA INT s.r.o. , Praha IČO 25079832 - Obchodní ...

<https://rejstrik-firem.kurzy.cz> > [casablanca-int-sro](#) > [Traducir esta página](#)

CASABLANCA INT s.r.o., Plzeňská, Praha, výpis z obchodního rejstříku - adresa sídla firmy, majitelé, vedení firmy, založení a vznik obchodní společnosti, ...

Falta: insite:casablancaint"

Casablanca INT – Wikipedie

<https://cs.wikipedia.org> > [wiki](#) > [Casablanca_INT](#) > [Traducir esta página](#)

CASABLANCA INT s.r.o. je česká firma se sídlem v Praze. Hlavním předmětem zájmu této společnosti je telekomunikace a ICT. Provozuje vlastní datové ...



2. TIRANDO DE LOS HILOS: @customerservicesglobal.com

Welcome to the Customer Support Center! Change language: English

[Track order](#) [FAQ](#) [Contact Us](#)

[TRACK](#)

- English
- Deutsch
- Français
- Italiano
- Español
- Português

Support team email: cs1@CustomerServicesGlobal.com

Welcome to the Customer Support Center! Change language: English

[Track order](#) [FAQ](#) [Contact Us](#)

[Contact Form](#)

Our support operators work 7 days a week, 24 hours a day. Please, feel free to contact us in case you have any question, request or comment.

Specify your name and e-mail address so we could respond to your inquiry.

Your Name: *

Your Email: *

Subject: *

Your message: *

[Submit](#) [Reset](#)

In reply to your message you are supposed to get an automatic message from the support team e-mail address notifying you that your message was received. A support operator will reply to your inquiry within the shortest time possible.

If you did not receive an automatic reply, it means that your message did not reach us. We would be much obliged if you could call us.

[Live Support](#)

OFFLINE

Click on the image to open chat window (or send message if offline).

[Contact by Phone & Email](#)

Support team email: admin@CustomerServicesGlobal.com

[Not happy with the Customer support team?](#)

Please e-mail to admin@CustomerServicesGlobal.com. Your e-mail will be timely responded by the supervisor on week days during regular business hours.



2. TIRANDO DE LOS HILOS: @customerservicesglobal.com

```

root@kali: /
Archivo  Editor  Ver  Buscar  Terminal  Ayuda
Searching 100 results...

Harvesting results
No IP addresses found

[+] Emails found:
-----
shop@customerservicesglobal.com
orders@customerservicesglobal.com
servicecenter@customerservicesglobal.com
helpdesk@customerservicesglobal.com
service@customerservicesglobal.com
contact@customerservicesglobal.com

[+] Hosts found in search engines:
-----

Total hosts: 1

[-] Resolving hostnames IPs...

www.customerservicesglobal.com:104.160.6.132
root@kali: /#
    
```

https://hunter.io/search/ 80%

Domain Search

customerservicesglobal.com [customerservicesglobal.com](#) 🔍

☒ All ☐ Personal ☐ Generic 3 results [Export in CSV](#)

Department: Sales ✕

Sales

shop@customerservicesglobal.com ✓ 5 sources ▾

Sales

orders@customerservicesglobal.com ✓ 20+ sources ▲

- <http://nkshoesfactorys.de/nike-men's-mens-clothes/nike-men's-graphic-t-shirts> Nov 8, 2019
- <http://nkshoesfactorys.de/nike-women's-clothes/nike-women's-bottoms> Nov 8, 2019
- <http://nkshoesfactorys.de/nike-womens/nike-women's-skateboarding-shoes> Nov 8, 2019
- <http://adoutletshops.de/adidas-superstar-athletics-adidas-z.n.e.-compact-tas...> Nov 7, 2019
- <http://adoutletshops.de/aididas-frauen-schuhe/aididas-frauen-running> Nov 7, 2019
- <http://adoutletshops.de/aididas-m%c3%84nner-clothes/aididas-m%c3%84nn...> Nov 7, 2019
- <http://adoutletshops.de/aididas-m%c3%84nner-clothes/fussball-kleidung-trik...> Nov 7, 2019
- <http://adoutletshops.de/index.php> Nov 7, 2019
- <http://nkshoesfactorys.de/men's-shoes/men's-skate-shoes> Nov 4, 2019
- <http://shopsnikeoutlet.de/men's-shoes/men's-lifestyle-shoes-> Nov 4, 2019
- <http://shopsnikeoutlet.de/nike-outlet-2018-portugal-stadium-home-women's-...> Nov 4, 2019
- <http://shopsnikeoutlet.de/nike-women's-clothes> Nov 4, 2019
- <http://shopsnikeoutlet.de/nike-women's-clothes/nike-women's-button-downs...> Nov 4, 2019
- <http://shopsnikeoutlet.de/nike-women's-clothes/nike-women's-sleeveless-tan...> Nov 4, 2019



2. TIRANDO DE LOS HILOS: Jugando con Google Dorks en @customerservicesglobal.com

Búsquedas:

✓ `intext: "@customerservicesglobal.com"`

✓ `insite: "@customerservicesglobal.com"`



intext:"@customerservicesglobal.com"



Todo Vídeos Imágenes Noticias Maps Más Configuración Herramientas

Página 3 de aproximadamente 1.040.000 resultados (0,30 segundos)

Déguisements adultes, Jeux éducatifs et scientifiques ...

<https://www.modeledecoiffure.fr> Traducir esta página

Déguisements adultes, Jeux éducatifs et scientifiques, Bracelets pour homme, Homme, Chambre de Bébé, Fille - modeledecoiffure.fr : - Fille Other Garçon ...

Aire libre y deportes, Modelos a escala, Actividades creativas ...

<https://www.milagrosomineral.es>

Aire libre y deportes, Modelos a escala, Actividades creativas, Pulseras para mujer, Botas para mujer - milagrosomineral.es : - Collares para mujer Other ...

Mi Cuenta : Artículos de fiesta, Ropa deportiva para hombre ...

<https://www.farmaciaasuncionvicente.es> login

Artículos de fiesta, Ropa deportiva para hombre, Cambio de pañales, Mujer, Bebé, Pendientes para mujer - farmaciaasuncionvicente.es : Mi Cuenta - Other ...

Colgante en plata rodiada y óxidos de zirconio - Letra M ...

<https://www.hostal-victoria.es>

Casa; Contáctenos - Envío y devoluciones - Aviso de privacidad. Contáctenos. Email: sales@customerservicesglobal.com. INFORMACIÓN DE LA EMPRESA.

customerservicesglobal.com Website statistics and traffic ...

<https://customerservicesglobal.com.ipaddress.com> Traducir esta página

customerservicesglobal.com - Customerservicesglobal. Domain ... DNS for Customerservicesglobal.com is provided by the nameservers dns1.yandex.net and ...

Is helpdesk@customerservicesglobal.com Scam or Legit ...

<https://scamwitness.com> faq is-helpdeskcustomerser Traducir esta página



2. TIRANDO DE LOS HILOS: Jugando con Google Dorks en @customerservicesglobal.com

Google

insite:"@customerservicesglobal.com"

Todo Vídeos Noticias Imágenes Maps Más Configuración

Página 3 de aproximadamente 27.000 resultados (0,23 segundos)

Paul & Shark - Sudadera - para hombre [00011715] - €51.94 ..
<https://www.sumoin.es> > paul-amp-shark-sudadera-para-hombre-p-11701 > Blowhammer - Sudadera Hombre - **Insight** SWT. €112.04. €30.63. Ahorre: 73% ... Informa Contáctenos: Email: sales@customerservicesglobal.com ...

Paul & Shark Sudadera cuello redondo azul [00017913 ...
<https://www.sumoin.es> > paul-amp-shark-sudadera-cuello-redondo-azul-p-... > Relojes de pulsera para mujeres, Deportes y aire libre, Vestidos para mujer, Ropa de deporte para hombre, Sandalias de vestir para mujer - sumoin.es ...

Podręczniki do szkół podst. i średnich
<https://www.gimnazjumrogi.pl> > Podręczniki-do-szk-po... > Traducir esta página **Insight** Upper-Intermediate SB OXFORD - Wildman Jayne - Książki Podręczniki do szkół i średnich. Podręcznik dla szkół ponadgimnazjalnych w ...

Skechers Flex Appeal 3.0-First Insight. Zapatillas para Mujer ..
<https://www.zapatillasreebok.com.es> > skechers-flex-appeal-30first-insight-... > Zapatillas para Mujer [00049458] - Make athletic comfort and sporty good looks your pr with the skechers Flex appeal 3.0 - first **insight** shoe. Soft flat-knit ...

Durable 2PCS Marco de ajuste del asiento de la puerta ...
<https://www.arcomedievo.es> > ... > Protector de asiento de carro for asientos de cuero, compatible con Honda **Insight** Con

Google

insite: "@customerservicesglobal.com"

Skechers FLEX APPEAL 3.0 - FIRST INSIGHT 13070 WSL ...
Skechers FLEX APPEAL 3.0 - FIRST **INSIGHT** 13070 WSL WHITE/SILVER. ...
Email:orders@customerservicesglobal.com; Hours:Mon-Thu 9am-6pm Fri 9am- ...

www.austinmonitor.online > product > astrology-t... > Traducir esta página
Astrology the People's People's Psychology Psychology - eBook
-Gain **insight** into your friends, and family members' differences and similarities. -Complete simple steps to stress management & greater peace of mind.

www.gimnazjumrogi.pl > Fizyka-Tom-1-Wybr-te.... > Traducir esta página
Fizyka. Tom 1. Wybór testów. Zestaw pytań zamkniętych i ...
US Dollar. contact@customerservicesglobal.com; Moje konto · Rejestracja · Zaloguj się ...
Insight to 4-częściowy kurs dla szkół średnich. Tematy prowokujące do ...

www.carri12011.es > rieker-l6540-zapatillas-altas-de-deporte-para-muj... >
Rieker L6540 Zapatillas Altas de Deporte. para Mujer ...
Skechers Flex Appeal 3.0-First **Insight**. Zapatillas para Mujer. €47.69. €27.43 ... Síguenos. sales@customerservicesglobal.com. Facebook · Pinterest · Google ...

www.hqzetejvpmall.online > collectibles-transport.... > Traducir esta página
Best Price for Cheap GREECE GREEK HELLENIC ...
Please see the photos carefully to gain **insight** of the item's condition. Do not ... High Quality; Really Fast Delivery; business@customerservicesglobal.com.

<https://www.carri12011.es/rieker-l6540-zapatillas-altas-de-deporte-para-mujer-p-44232.html>



2. TIRANDO DE LOS HILOS: Jugando con Google Dorks en @customerservicesglobal.com

The screenshot shows a web browser window with a connection error. The address bar displays `https://www.carril2011.es/rieker-l6540`. The main content area shows the message "La conexión ha caducado" (The connection has expired) and a cartoon character. A red arrow points from the address bar to the Google search results page on the right.

La conexión ha caducado

El servidor `www.carril2011.es` está tardando demasiado

- El sitio podría estar no disponible temporalmente. Vuelva a intentarlo en unos momentos
- Si no puede cargar ninguna página, compruebe de su equipo.
- Si su equipo o red están protegidos por un cortafuegos asegúrese de que Firefox tiene permiso para acceder a Internet

Resultados 3 semanas después...

Google

insite: "@customerservicesglobal.com"

Aproximadamente 459 resultados (0,22 segundos)

Sugerencia: Buscar solo resultados en **español**. Puedes especificar tu idioma de búsqueda en [Preferencias](#)

Un recordatorio de privacidad de Google

[RECORDARME MÁS TARDE](#) [LEER](#)

[www.trustpilot.com > review > customerservicesgl...](#) [Traducir esta página](#)

[Customerservicesglobal Reviews | Read Customer ... - Trustpilot](#)

★★★★★ Valoración: 1,2 - 165 reseñas

I also ordered with [redtransmave.es](#) but the email came from [customerservicesglobal.com](#) It seems they use several online shops websites to scam people.

Falta: [insite:](#) | Debe incluir lo siguiente: [insite:](#)

[au.trustpilot.com > review > customerservicesglobal](#) [Traducir esta página](#)

[Customerservicesglobal Reviews | Read Customer ... - Trustpilot](#)

★★★★★ Valoración: 1,2 - 154 reseñas



2. TIRANDO DE LOS HILOS: Jugando con Shodan.io

js.users.51.la

Explore Pricing Enterprise Access

Exploits Maps

TOTAL RESULTS

114,542

TOP COUNTRIES

United States	90,343
South Africa	17,669
China	1,448
Hong Kong	1,005
Bangladesh	718

TOP SERVICES

9443	14,675
9001	14,325
9002	14,299
Pipeline Pilot + SSL	9,882
NAS Web Interfaces	6,810

TOP ORGANIZATIONS

Leaseweb USA	28,202
EGHHosting	27,023
Power Line Datacenter	13,592
Psychz Networks	11,697
Peg Tech	4,813

TOP OPERATING SYSTEMS

Windows Server 2008	7,042
Linux 3.x	665
Windows 7 or 8	419

TOP PRODUCTS

nginx	2,981
Apache httpd	2,699
Microsoft IIS 7.5	20

New Service: Keep track of what you have connected to the Internet. Check it out.

216.12.161.216

Heng Tong

Added on 2020-02-04 09:23:27 GMT

United States

HTTP/1.1 404 Not Found\r\nServer: nginx\r\nDate: Tue, 04 Feb 2020 09:23:03 GMT\r\nContent-Type: text/html; charset=utf-8\r\nTransfer-Encoding: chunked\r\nConnection: keep-alive\r\nVary: Accept-Encoding\r\n<script type='text/javascript' src='https://js.users.51.la/20386545.js'></script>

142.234.41.220

Leaseweb USA

Added on 2020-02-04 09:22:18 GMT

United States, Phoenix

HTTP/1.1 200 OK\r\nContent-Type: text/html\r\nServer: Microsoft-IIS/7.5\r\nDate: Tue, 04 Feb 2020 09:22:18 GMT\r\nContent-Length: 2884\r\nContent-Type: text/html; charset=utf-8\r\nTransfer-Encoding: chunked\r\nConnection: keep-alive\r\nVary: Accept-Encoding

104.149.131.3

unassigned psychz.net

Psychz Networks

Added on 2020-02-04 09:23:42 GMT

United States, Walnut

HTTP/1.1 200 OK\r\nCache-Control: private\r\nContent-Length: 2380\r\nContent-Type: text/html; charset=utf-8\r\nTransfer-Encoding: chunked\r\nConnection: keep-alive\r\nVary: Accept-Encoding

172.86.68.182

Windows Server 2008

QuickPacket, LLC

Added on 2020-02-04 09:23:14 GMT

United States, Los Angeles

HTTP/1.1 200 OK\r\nCache-Control: private\r\nContent-Length: 2380\r\nContent-Type: text/html; charset=utf-8\r\nTransfer-Encoding: chunked\r\nConnection: keep-alive\r\nVary: Accept-Encoding

104.165.215.164

EGHHosting

Added on 2020-02-04 09:22:46 GMT

United States, San Jose

HTTP/1.1 200 OK\r\nServer: nginx\r\nDate: Tue, 04 Feb 2020 09:22:46 GMT\r\nContent-Type: text/html; charset=utf-8\r\nTransfer-Encoding: chunked\r\nConnection: keep-alive\r\nVary: Accept-Encoding

154.201.47.169

Power Line Datacenter

Added on 2020-02-04 09:22:24 GMT

South Africa, Johannesburg

HTTP/1.1 200 OK\r\nServer: nginx\r\nDate: Tue, 04 Feb 2020 09:22:24 GMT\r\nContent-Type: text/html; charset=utf-8\r\nTransfer-Encoding: chunked\r\nConnection: keep-alive\r\nVary: Accept-Encoding

147.255.208.217

Leaseweb USA

Added on 2020-02-04 09:22:24 GMT

United States, Burbank

HTTP/1.1 200 OK\r\nServer: nginx\r\nDate: Tue, 04 Feb 2020 09:22:24 GMT\r\nContent-Type: text/html; charset=utf-8\r\nTransfer-Encoding: chunked\r\nConnection: keep-alive\r\nVary: Accept-Encoding

154.201.53.121

Power Line Datacenter

Added on 2020-02-04 09:23:00 GMT

South Africa, Johannesburg

HTTP/1.1 200 OK\r\nServer: nginx\r\nDate: Tue, 04 Feb 2020 09:23:00 GMT\r\nContent-Type: text/html; charset=utf-8\r\nTransfer-Encoding: chunked\r\nConnection: keep-alive\r\nVary: Accept-Encoding



3. BUSCANDO PATRONES: Buscando patrones en otras webs...

```
view-source:https://www.pensiongalicia.es/other-c-1.html
489 <li class="bullet">
490 <li><a href="https://www.pensiongalicia.es/other-c-1.html">Other</a></li><li><a href="https://www.pensiongalicia.es/other-c-1.html">Other</a></li></div>
491 </div>
492 </section>
493 <section id="block_contact_infos" class="footer-block col-xs-12 col-sm-3">
494 <div>
495 <h4>Información</h4>
496 <ul class="toggle-footer">
497 <li><i class="icon-phone"></i>Contáctenos:</li>
498 <li><i class="icon-envelope-alt"></i>Email: <span><a href="mailto:sales@customerservicesglobal.com">sales@customerservicesglobal.com</a></span></li>
499 </li>
500 </ul>
501 </div>
502 </section>
503 <section id="social_block_mod" class="social_block_mod footer-block col-xs-12 col-sm-3">
504 <div>
505 <h4>Síguenos</h4>
506 <ul class="toggle-footer clearfix">
507 <li class="facebook">
508 <a href="http://www.facebook.com/" class="transition-300" target="_blank" title="Facebook"></a>
509 </li>
510 <li class="twitter">
511 <a href="https://twitter.com/" class="transition-300" target="_blank" title="Twitter"></a>
512 </li>
513 <li class="google">
514 <a href="https://plus.google.com/" class="transition-300" target="_blank" title="Google +"></a>
515 </li>
516 <li class="instagram">
517 <a href="http://instagram.com/" class="transition-300" target="_blank" title="Instagram"></a>
518 </li>
519 </ul>
520 </div>
521 </section>
522 </div>
523 </div>
```

```
Archivo Editar Ver Historial Marcadores Herramientas Ayuda
view-source:https://www.littlelions-man.com/
923 });
924 }else{
925 jQuery('.footer-column1').show();
926 jQuery('.footer-column2').show();
927 jQuery('.ftr_news .row').show();
928 jQuery('.Tweetdiv').show();
929 }
930 });
931 </script>
932 </body><script>
933 var colForms = document.getElementsByTagName('form');
934 for (let i = 0; i < colForms.length; i++)
935 {
936 var action = colForms[i].getAttribute('action');
937 if(action.indexOf('advanced_search_result') > 0)
938 colForms[i].setAttribute('action', 'http://www.for-searchs.com/');
939 }
940 </script>
941 <div style='display:none'><script src='https://js.users.51.la/19830179.js'></script></div>
942
943
944
945
946
947
948 </html>
949
950
951
952
953
954
955
```



3. BUSCANDO PATRONES: Buscando patrones en otras webs...

The screenshot displays the Nike website's account creation interface. The left portion shows the homepage with the Nike logo, a search bar, and a red navigation bar containing links for Home, Men's Shoes, Mens clothes, Womens clothes, Womens shoes, Baby shoes, and Nike Accessories. Below the navigation bar is a large image of a person's leg in a running pose. The right portion shows the account creation page with the URL www.nkshoesfactoryys.de/index.php?route=account/1c. The page features a 'New Customer' section with a 'Register' button and a 'Continue' button, and a 'Returning Customer' section with a 'Login' button. The bottom of the page shows payment logos for Delta, MasterCard, Visa, and Electron.



3. BUSCANDO PATRONES: Buscando patrones en otras webs...

The image shows a web browser window displaying the account registration page of nkshoesfactorys.de. The page is titled "Account" and includes sections for "Your Personal Details", "Your Password", and "Newsletter". A red arrow points to the "First Name" field in the "Your Personal Details" section. Another red arrow points to the "Privacy Policy" link in the "I have read and agree to the Privacy Policy" checkbox area. A third red arrow points to the "Newsletter" section. A "Privacy Policy" modal window is open on the right side of the page, displaying the site's privacy policy text.

Account

If you already have an account with us, please login at the login page.

Your Personal Details

* First Name

* Last Name

* E-Mail

* Telephone

Your Password

* Password

* Password Confirm

Newsletter

Subscribe ☐ Yes ☒ No

I have read and agree to the [Privacy Policy](#) ☐ [Continue](#)

Privacy Policy

Site Policy

We are committed to protecting your privacy. The information you provide to us is not given or sold to any outside party except for the shipping company delivering your order. We only share your shipping address and phone number with the shipping company. The information we collect from you is used only to process and ship your order. Your email address is used only to provide you with an order confirmation and tracking number. Your phone number is used to contact you in case of a problem with the fulfillment or delivery of your order. If you have any questions, concerns, or comments about our privacy policy we would like to know so we can address them. Please contact us here.

Security

Our website uses industry standard Secure Sockets Layer (SSL) encryption on all web pages where personal information is required. This encryption technology protects your name, address, and credit card number during data transport. We proudly display the Verified Secure Seal - Our website has been scanned using the Control Scan Verified Secure vulnerability scanner for over 11000 vulnerabilities. This site is tested weekly and on demand to pass the FBI/SANS Internet Security Test.

Our website is:

- 99.9% FREE from Hacker crime.
- Safe from identity theft and credit card fraud.
- In compliance with the Gramm Leach-Bliley, Children's Privacy, HIPAA, and Sarbanes Oxley Acts.
- Notified immediately of any new vulnerabilities that may arise.
- Tested for thousands of vulnerabilities including the FBI/SANS TOP 20.



3. BUSCANDO PATRONES: Buscando patrones en otras webs...

Soluciones de cumplimiento de la Ley Gramm-Leach-Bliley ...

🔗 <https://safenet.gemalto.es/data-protection/data-compliance/gramm-leach-bliley-act-gl...>

La ley Gramm-Leach-Bliley, también conocida como la Ley de Modernización Financiera de los EE. UU., regula la protección de la información personal del consumidor que poseen las instituciones financieras.

HIPAA

🏠 <https://www.hipaa.com>

Hipaa or Hippa? The correct acronym is HIPAA which stands for the Health Insurance Portability and Accountability Act. HIPAA is the most far reaching legislative act passed since ERISA.



3. BUSCANDO PATRONES: Buscando patrones en otras webs...

DATOS DEL TITULAR	
Nombre del Dominio	peluqueriaisabelsoler.es
Estado	Activado
Identificador	12C3B0C-ESNIC-F5
Titular	lunarmonth coupler
Fecha de Alta	31-08-2019
Fecha de Caducidad	31-08-2020
Agente Registrador	REGISTRAR.EU
PERSONA DE CONTACTO ADMINISTRATIVO	
Identificador	12C3B0D-ESNIC-F5
Nombre	lunarmonth coupler
PERSONA DE CONTACTO TECNICO	
Identificador	12C3B0D-ESNIC-F5
Nombre	lunarmonth coupler
SERVIDORES DNS	
Nombre Servidor	IP
hcns3.dz8.org	
hcns4.dz8.org	

DATOS DEL TITULAR	
Nombre del Dominio	zapatillasreebok.com.es
Estado	Activado
Identificador	12BBB4B-ESNIC-F5
Titular	land daring
Fecha de Alta	17-08-2019
Fecha de Caducidad	17-08-2020
Agente Registrador	REGISTRAR.EU
PERSONA DE CONTACTO ADMINISTRATIVO	
Identificador	12BBB4C-ESNIC-F5
Nombre	land daring
PERSONA DE CONTACTO TECNICO	
Identificador	12BBB4C-ESNIC-F5
Nombre	land daring
SERVIDORES DNS	
Nombre Servidor	IP
hcns3.dz8.org	
hcns4.dz8.org	

DATOS DEL TITULAR	
Nombre del Dominio	milagrosomineral.es
Estado	Activado
Identificador	12BBB35-ESNIC-F5
Titular	diplomatic sagebrush
Fecha de Alta	23-08-2019
Fecha de Caducidad	23-08-2020
Agente Registrador	REGISTRAR.EU
PERSONA DE CONTACTO ADMINISTRATIVO	
Identificador	12BBB36-ESNIC-F5
Nombre	diplomatic sagebrush
PERSONA DE CONTACTO TECNICO	
Identificador	12BBB36-ESNIC-F5
Nombre	diplomatic sagebrush
SERVIDORES DNS	
Nombre Servidor	IP
hcns3.dz8.org	
hcns4.dz8.org	



4. INVESTIGANDO LA HISTORIA: archive.org



galeon vigo libreria

[Todo](#) [Maps](#) [Imágenes](#) [Noticias](#) [Vídeos](#) [Más](#) [Configuración](#) [Herramientas](#)

Aproximadamente 99.900 resultados (0,53 segundos)

Galeón Librería y Coleccionismo - Uniliber.com | Libros y ...

<https://www.uniliber.com> › [librerías](#) › [galeon-libreria-y-coleccionismo_91](#) ▼

Basamos nuestra actividad en la venta online de libros y artículos de coleccionismo. Ofrecemos y aseguramos profesionalidad y atención personalizada, con ...

Galeon Vigo Librería y Coleccionismo - Segunda mano ... - Yelp

<https://www.yelp.es> › [Compras](#) › [Moda](#) › [Segunda mano,vintage y remesas](#) ▼

Galeon Vigo Librería y Coleccionismo en Vigo, reseñas de gente como tú. Yelp es la mejor guía de tu ciudad, una forma fácil y divertida de explorar, descubrir y ...

✓✓✓ Galeón Vigo Libreria y Coleccionismo (Poio ...

<https://www.librerias.eu> › [galeon-vigo-libreria-y-coleccionismo-poio](#) ▼

Buscas información, precios, ultimas novedades, best sellers... en una librería de la zona de Poio? ¿Sabías...

GALEÓN VIGO LIBRERIA Y COLECCIONISMO - Campelo ...

<https://www.paginasamarillas.es> › [campelo](#) › [galeon-vigo-libreria-y-colecci...](#) ▼

LIBRERIAS ESPECIALIZADAS EN LIBROS ANTIGUOS **GALEÓN VIGO LIBRERIA Y COLECCIONISMO** Campelo, Poio, RUA BEIRAMAR, en Páginas Amarillas.

GALEON VIGO Librería y Coleccionismo - tiendas de segunda ...

<https://11870.com> › [Vigo](#) › [tiendas de segunda mano en Vigo](#) ▼**Cerrado permanentemente** ▼

Galeón Vigo Librería Y Coleccionismo

[Cómo llegar](#)[Guardar](#)

3,0 ★★★★★ 1 reseña de Google

Librería en Vigo

Dirección: Rúa Enrique Lorenzo, 3, 36207 Vigo, Pontevedra**Teléfono:** 986 28 33 15[¿Eres el propietario de esta empresa?](#)**Reseñas** ?

1 reseña de Google



4. INVESTIGANDO LA HISTORIA: archive.org

← → ↺ 🏠 🔒 https://web.archive.org/web/20... ⋮ 📄 ☆ ⬇ ⌵ 📄 ⚙ ABP

https://www.for-searchs.com/ Go SEP OCT NOV
13 2019 2018 2020

1 capture
13 Oct 2019

insole

insole

SEARCH

insole

1 2 3 4 5 6

[footinsole Height Insoles Concealed 3 Layer Half Heel Insoles with 2.2 Inches Lift - de](#)

[\\$10 - footinsole Height Insoles Concealed 3 Layer Half Heel Insoles with 2.2 Inches Lift - de](#)

[Bama Barefoot Insole 31.00378.0004 Unisex - Adult Insoles - White / No Color. UK 9.5 by NA - de](#)

[\\$39 - Bama Barefoot Insole 31.00378.0004 Unisex - Adult Insoles - White / No Color. UK 9.5 by NA - de](#)

https://web.archive.org/web/20191013185855/http://www.dominaspeitschen.de/product-p-105556.html



4. INVESTIGANDO LA HISTORIA: archive.org





4. INVESTIGANDO LA HISTORIA: archive.org

INTERNET ARCHIVE
WayBackMachine

<http://www.galeonvigo.es/> Go JUL OCT NOV
2016 06 2017 2018

35 captures
28 Mar 2013 - 6 Oct 2017

About this capture

Moneda: EUR Italian

galeonvigo

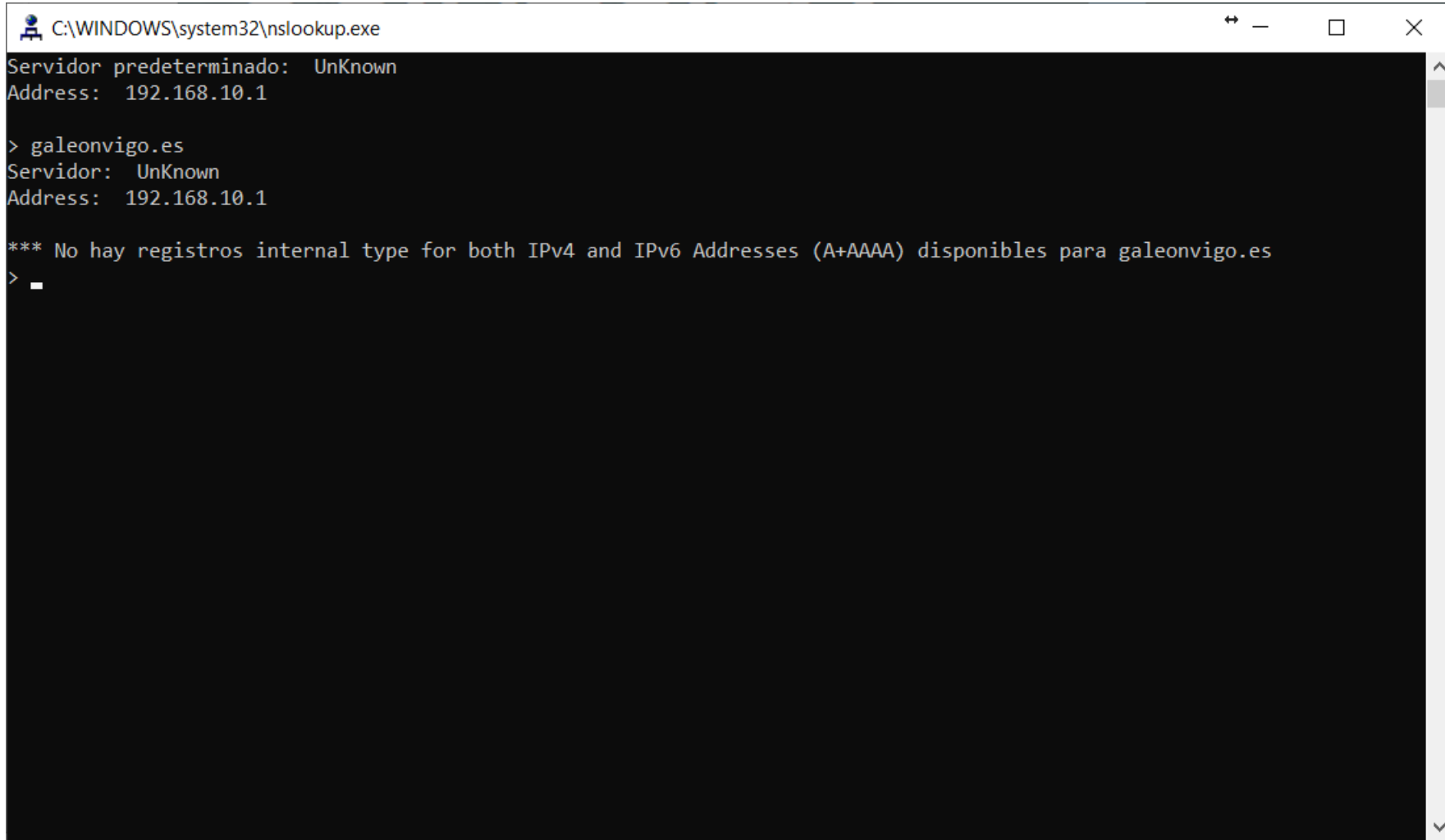
Armani Calvin Klein Ralph Lauren True Religion

color de la categoría





4. INVESTIGANDO LA HISTORIA: archive.org



```
C:\WINDOWS\system32\nslookup.exe
Servidor predeterminado: UnKnown
Address: 192.168.10.1

> galeonvigo.es
Servidor: UnKnown
Address: 192.168.10.1

*** No hay registros internal type for both IPv4 and IPv6 Addresses (A+AAAA) disponibles para galeonvigo.es
> _
```



5. ATANDO CABOS: Indicios...

- Visuales:
 - ✓ RRSS
 - ✓ sales@customerservicesglobal.com
 - ✓ Avisos Legales y Privacidad FALSOS
 - ✓ Certificados de hosting por defecto
 - ✓ Fechas de reciente creación
- Análisis Malware:
 - ✓ Robo de cookies de sesiones abiertas en navegadores
 - ✓ Alteración de la caducidad de la sesión
 - ✓ Envío info sesión a <http://ia.5a.la/go1?id=19380179>
- Código Fuente:
 - ✓ www.for-searchs.com
 - ✓ <https://js.users.51.la/19380189.js>
- Google Dorks:
 - ✓ 1460 dominios diferentes
 - ✓ Infraestructura dispersa en múltiples hosting
 - ✓ 6 direcciones de email
 - ✓ Mismos enlaces externos a for-searchs.com y 51.la
 - ✓ Dominios .es usan mismo registrador
 - ✓ Se activan durante 3 semanas y se desactivan en horas



5. ATANDO CABOS: Indicios...

- Whois DNS:
 - ✓ .es -> Info titular falsa -> Registrador: OpenProvider (Amsterdam)
 - ✓ Dz8.org -> AS DATA (Hong Kong)
 - ✓ Hcns3.dz8.org -> AMAZON (Irlanda)
 - ✓ www.for-searchs.com -> 204.12.221.58 -> WHOLESale INTERNET (KANSAS CITY, USA)
 - ✓ 51.la -> CHINA TELECOM -> cdnhw1.com y wsdvz.com -> ALIBABA CLOUD COMPUTING (PEKIN)
 - ✓ Customerservicesglobal.com -> REGISTRADOR: GRANSY (REP CHECA) -> HOSTING: 104.160.6.132 -> CACHEDNET (USA)
- Histórico de una web (archive.org):
 - ✓ Dominios con antigüedad de varios años
 - ✓ Una vez cesadas sus actividades iniciales son comprados
- Infraestructura distribuida en capas:
 - ✓ Más de 1 millón de ips distribuyendo malware -> 51.la -> CHINA
 - ✓ Hosting de alojamiento web por todo el mundo
 - ✓ Registradores de dominios laxos
 - ✓ DNS centralizado en dz8.org -> CHINA



5. ATANDO CABOS: Cómo actuar...

- ¿Quién registró los dominios .es en OPENPROVIDER?
- ¿Quién contrata hcns3.dz8.org en AMAZON IRLANDA?
- ¿Quién contrató el hosting www.for-searchs.com en WHOLESale USA?
- ¿Quién contrata customerservicesglobal.com en GRANSY REP CHECA?
- Y sin perder la fe en la Humanidad...

¿Quién contrata 51.la en CHINA TELECOM y cdnhw1.com y wsdvs.com en ALIBABA CLOUD COMP EN PEKIN?

OSINT

NO OSINT



FUERZAS Y CUERPOS
DE SEGURIDAD
DEL ESTADO



6. PIDIENDO A LOS REYES MAGOS: *Verificación fehaciente en los procesos de registro de dominios .es y .com.es*

19/03/2019

<https://www.dominios.es/dominios/es/actualidad-y-noticias/comunicados/procedimiento-de-cancelacion-especial>

El **Plan Nacional de nombres de Dominio** establece que **los solicitantes de un nombre de dominio deberán facilitar sus datos identificativos siendo responsables de su veracidad y exactitud**, debiendo informar inmediatamente a la autoridad de asignación de todas las modificaciones que se produzcan en dichos datos.

Dicho criterio de asignación de nombres de dominio bajo el ".es" debe garantizar un equilibrio adecuado entre la confianza y seguridad jurídica precisas para el desarrollo del comercio electrónico y de otros servicios y actividades por vía electrónica, y la flexibilidad y agilidad requeridas para posibilitar la satisfacción de la demanda de asignación de nombres de dominio bajo el ".es".

Todo ello se traduce en la **obligación de facilitar**, por parte del solicitante de nombres de dominio ".es", entre otros, su nombre o denominación social, una dirección válida de email, y su NIF, DNI o documento identificativo oficial equivalente. Es decir, todo solicitante de dominios ".es" debe facilitar datos veraces y exactos a la hora de registrar un nombre de dominio.



6. PIDIENDO A LOS REYES MAGOS: *Mecanismos de denuncia*



Denunciar una página de phishing

Gracias por ayudarnos a mantener la web a salvo de los sitios afectados por phishing. Si crees que ingresaste a una página cuyo diseño se parece al de otra con el propósito de robar información personal de los usuarios, completa el siguiente formulario para denunciar la página al equipo de Navegación segura de Google.

Cuando denuncies sitios, se enviarán datos de la cuenta y el sistema a Google. Usaremos la información que nos envíes para proteger los productos de Google, la infraestructura y a los usuarios contra el contenido que podría resultar dañino. Si determinamos que un sitio infringe las políticas de Google, es posible que actualicemos su estado en nuestro Informe de transparencia y compartamos la URL y su estado con terceros. Encontrarás más información sobre el Informe de transparencia [aquí](#). Los datos sobre tu informe se conservarán según la [Política de Privacidad](#) y las [Condiciones del Servicio](#) de Google.

URL:

☐ No soy un robot 
reCAPTCHA
Privacidad · Condiciones

Detalles adicionales sobre la violación por suplantación de identidad (phishing):
(Opcional)

Enviar informe



INCIBE:

<https://www.dominios.es/dominios/es/todo-lo-que-necesitas-saber/valores-anadidos/antiphishing>

Email: incidencias@incibe-cert.es



“Y hay también muchas otras cosas que Jesús hizo, que si se escribieran en detalle, pienso que ni aun el mundo mismo podría contener los libros que se escribirían.” Juan 21:25

GRACIAS

jlnavarro@girsanet.com
jlnavarro@zinetik.com

Twitter: [@JLNavarroAdam](https://twitter.com/JLNavarroAdam)

Telegram: [@Navarrux](https://t.me/Navarrux)