CyberSquatting dot es

Wiktor Nykiel
Iván Portillo

GOBIERNO DE ESPAÑA
MINISTERIO DE ENERGÍA, TURISMO Y AGENDA DIGITAL

incibe_
TRABAJANDO POR LA CONFIANZA DIGITAL

CyberCamp.es

Índice general

Quiénes somos

Conceptos básicos

Cyber ocupación

Dominios.es

Herramientas

Comunicación

Canal de Telegram

https://telegram.me/CyberSquatting

Hashtag

#CyberSquattingDotES

Quiénes somos

Wiktor Nykiel

Cyber Intelligence & Security Expert
Senior Manager - EY

wiktornykiel wiktornykiel email@wiktornykiel.com

Actualmente es **Senior Manager del servicio de Inteligencia** en EY para la región de EMEIA, especializado en servicios financieros.

Anteriormente fue **Responsable Global del Servicio de Ciber Inteligencia** en Prosegur.

También fue el **Fundador de Hackdoor**, una startup tecnológica enfocada a la innovación dentro del área de Ciber Inteligencia.

Ha sido **profesor en cursos de ciberseguridad** en la Universidad de Alcalá de Henares, habiendo sido investigador de la misma Universidad.

La pasión por la tecnología y la seguridad le motivan a investigar y aprender día a día.

Quiénes somos

Iván Portillo

Cyberintelligence Expert
Senior Analyst - EY

ivanportillomorales

ivanPorMor

Actualmente es **Analista Senior** dentro del servicio de Inteligencia para el sector financiero dentro de EY.

Anteriormente ha desempeñado funciones de analista de **Ciber Inteligencia** en diferentes **SOCs** (Centros de Operaciones de Seguridad) de grandes multinacionales.

Co-fundador de Hackdoor, startup finalista del programa CyberVentures cuyo foco principal fue la innovación dentro del área de Ciber Inteligencia.

Siempre enfocado a las investigaciones innovadoras entrelazando la seguridad con las nuevas tecnologías.

Quiénes somos

Gonzalo Espinosa

Software developer
Cibersecurity R&D

gonzaloespinosa

Actualmente es **Investigador de Ciberseguridad** en la **Universidad de Alcalá** (Madrid) y especializado en la planificación y ejecución de proyectos de Ciber inteligencia y Seguridad lógica.

Anteriormente ha desempeñado funciones de desarrollador software especializado en sistemas web en diferentes empresas con más de 5 años de experiencia.

Co-fundador de Hackdoor, startup finalista del programa CyberVentures cuyo foco principal fue la innovación dentro del área de Ciber Inteligencia.

Matricula de Honor por el TFG: Aplicación web para análisis, detección, evaluación y alerta de riesgos asociados a amenazas de Cybersquatting, Typosquatting e IDN Homograph

Conceptos básicos

Esta presentación

Contexto

CyberSquatting con ejemplos

Entidades reguladoras

IDNs

Introducción / esta presentación

En la presentación se pretende exponer los riesgos de la ciberocupación y maneras de detectarlas antes de que pueda suponer una amenaza hacia cualquier marca o entidad.

1 Se mostrarán en qué consisten los diferentes tipos de técnicas como typosquatting, bitsquatting o IDN Homograph entre otras, así como herramientas OpenSource genéricas que permiten detectar estos ataques.

2 Una vez introducido el contexto se presentará la idea del estudio sobre dominios con TLD .es para obtener los datos sobre los que trabajar de fuentes abiertas, para posteriormente analizarlos y realizar una herramienta que permita automatizar el trabajo.

3 Una vez desarrollada la presentación, se mostrará la efectividad de la misma, así como su funcionamiento, intentando detectar amenazas reales en este campo.

Introducción / contexto

294.000.000 dominios registrados en el año **2015**

1.800.000 dominios registrados con extensión o **TLD .es**

Los registros legítimos conllevan otros dominios registrados para suplantar la marca original, mandar **phishing**, **spam**, generan **estafas online**, etc.

"**Facebook** indemnizado con $2.800.000 por daños debidos a TypoSquatting, devolviéndoles 100 dominios que utilizaban variaciones para lucrarse".

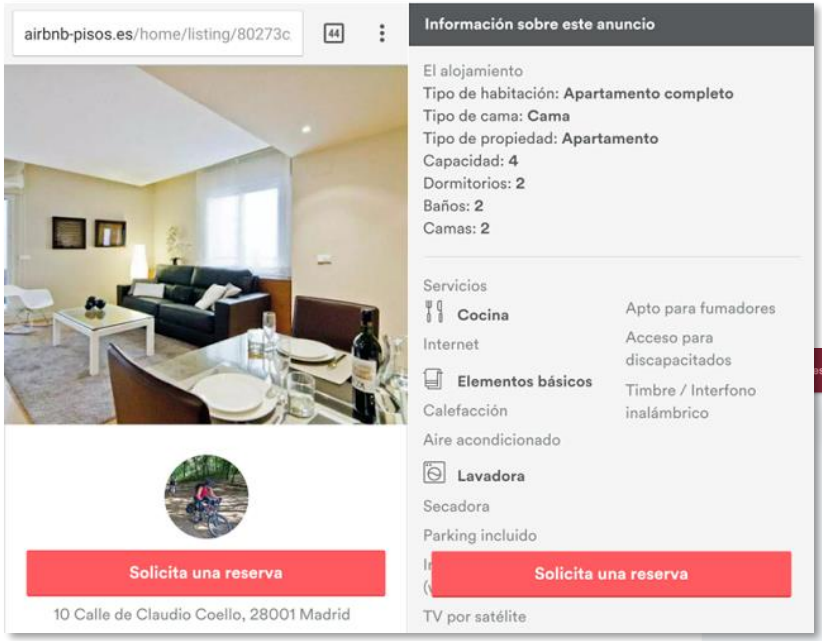
CyberSquatting / ¿Qué es?

Cybersquatting (denominado también **ocupación de dominio** o *Domain Grabbing*) es definido como el registro, tráfico o uso de un nombre de dominio de Internet con intención de mala fe, para la obtención y provecho de la buena voluntad asociada a una marca comercial, empresa o persona perteneciente a un tercero.

Si la finalidad última es la transferencia, subasta o extorsión con fines económicos, es denominado *Domain Dealing*.

El término es derivado del término anglosajón "**squatting**", que es el acto de ocupación o allanamiento de un espacio o edificio abandonado o desocupado, del cual el ocupante no es propietario, arrendatario, o carece de permiso para su utilización.

CyberSquatting / ejemplo práctico

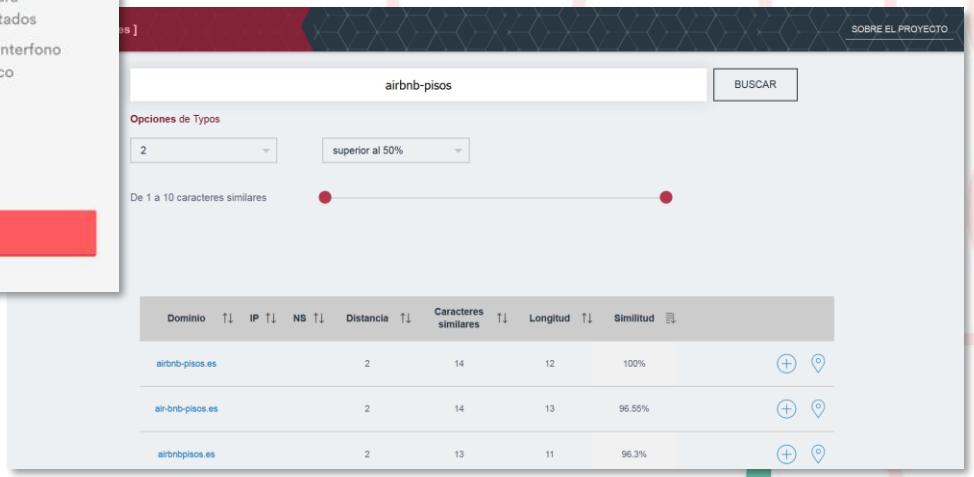


airbnb-pisos.es

air-bnb-pisos.es

airbnbpisos.es

airbnb.nom.es



Fuente http://www.elladodelmal.com/2016/08/como-te-estafan-1282-por-un-falso-piso.html

CyberSquatting / otros casos

Nombre de dominio	Entidad afectada o reclamadora	Fecha de resolución
hillaryclinton.net	Hillary Diane Rodham Clinton	Mayo 2015
facebookghana.com	Facebook, Inc.	Agosto 2015
pepsix.com pepsixxx.com	PepsiCo, Inc	2003
pfiezer.com pfzerforliving.com	Pfizer Inc.	Agosto 2000
wwwdinersclub.com	Diners Club International Ltd.	Julio 2003
chatyahoo.com yahoonews.com yahow.com	Yahoo! Inc.	Octubre 2000
googleglass.es	Google Inc.	Abril 2014
googblog.com	Google Inc.	Marzo 2009
twitter.co.kr	Twitter Inc.	Febrero 2014
mikerowesoft.com	Microsoft Corporation	Enero 2004
atleticodemadrid.com	Club Atlético de Madrid S.A.D.	Diciembre 2015
i-tune.com itunes.net	Apple, Inc.	Junio 2012
allianz-es.com	Allianz, Compañía de Seguros y Reaseguros S.A	Septiembre 2009
bbvaneet.com	Banco Bilbao Vizcaya Argentaria. S.A	Diciembre 2005

TypoSquatting / ¿Qué es?

Typosquatting (denominado también **URL Hijacking**) es un comportamiento especulativo y de mala fe, consistente en el registro y/o uso, de nombres de dominios de internet, similares tipográficamente a nombres de dominios ya registrados, cuyas diferencias se basan en las faltas ortográficas o errores de escritura comunes de los usuarios al escribir el dominio legítimo.

Es considerado una variante del Cybersquatting.

El término es derivado del término anglosajón "typo" (error tipográfico) y "squatting", que es el acto de ocupación o allanamiento de un espacio o edificio abandonado o desocupado.

***Término** 1998 - R. C. Cumbow.*

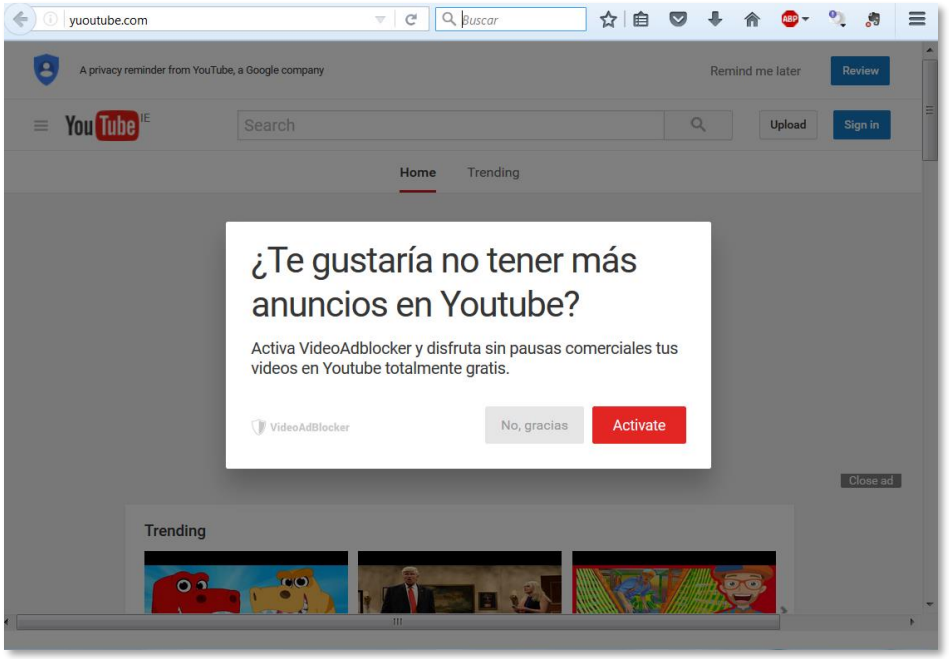
TypoSquatting / clasificación

- Omisión de caracteres
- Repetición de caracteres
- Intercambio de caracteres adyacentes
- Reemplazo de caracteres adyacentes
- Doble sustitución de caracteres
- Inserción de caracteres adyacentes
- Omisión de punto
- Omisión de guiones
- Singular o plural
- Faltas ortográficas comunes
- Intercambio de vocales
- Homófonos (Soundsquatting)
- Homoglifos (Homoglyphs – homográfos)
- Modificación de TLD –SLD
- Modificación de Bit (Bitflipping o Bitsquatting)

cnn.com 01100011 01101110 01101110 0101110 01100011 01101111 01101101

con.com 01100011 01101111 01101110 0101110 01100011 01101111 01101101

TypoSquatting / ejemplo práctico

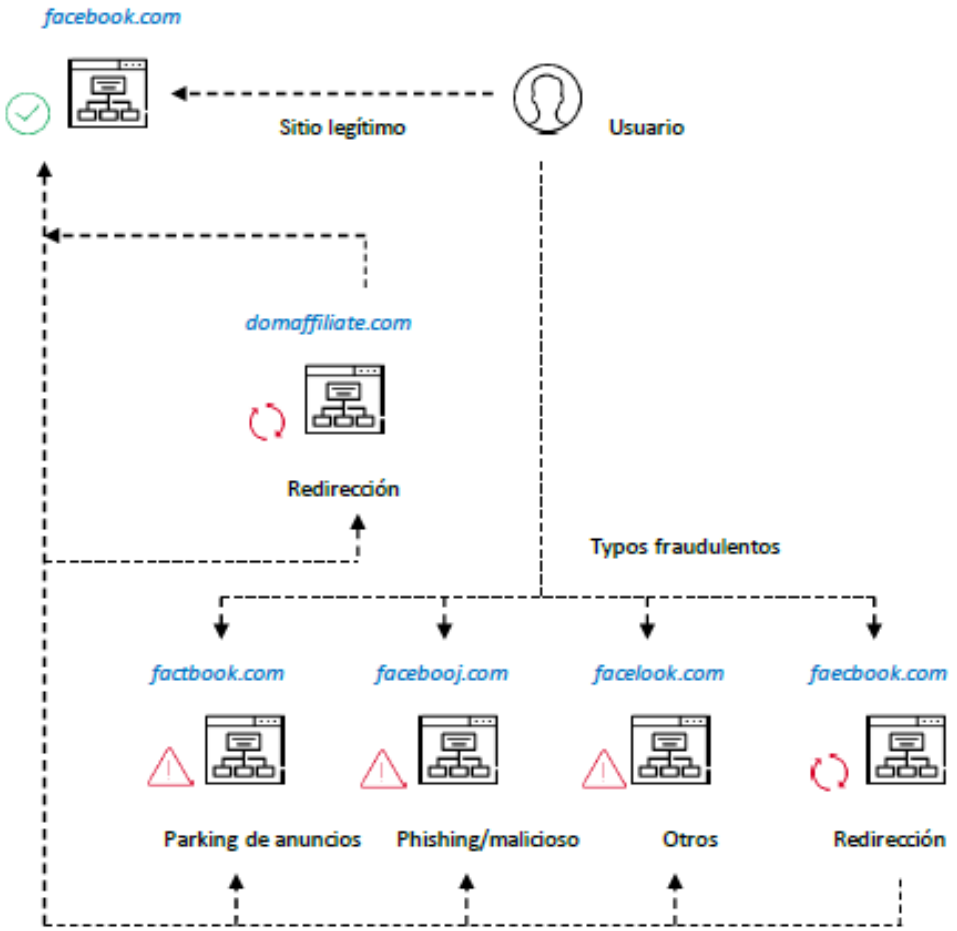


yuoutube.com, yutuve.com
wikipwdia.com, en.wikiedia.org
geogle.es, googls.com
craigslit.com, twitterz.com
victoriesecrets.com
gmnail.com, gmaio.com
linkedid.com

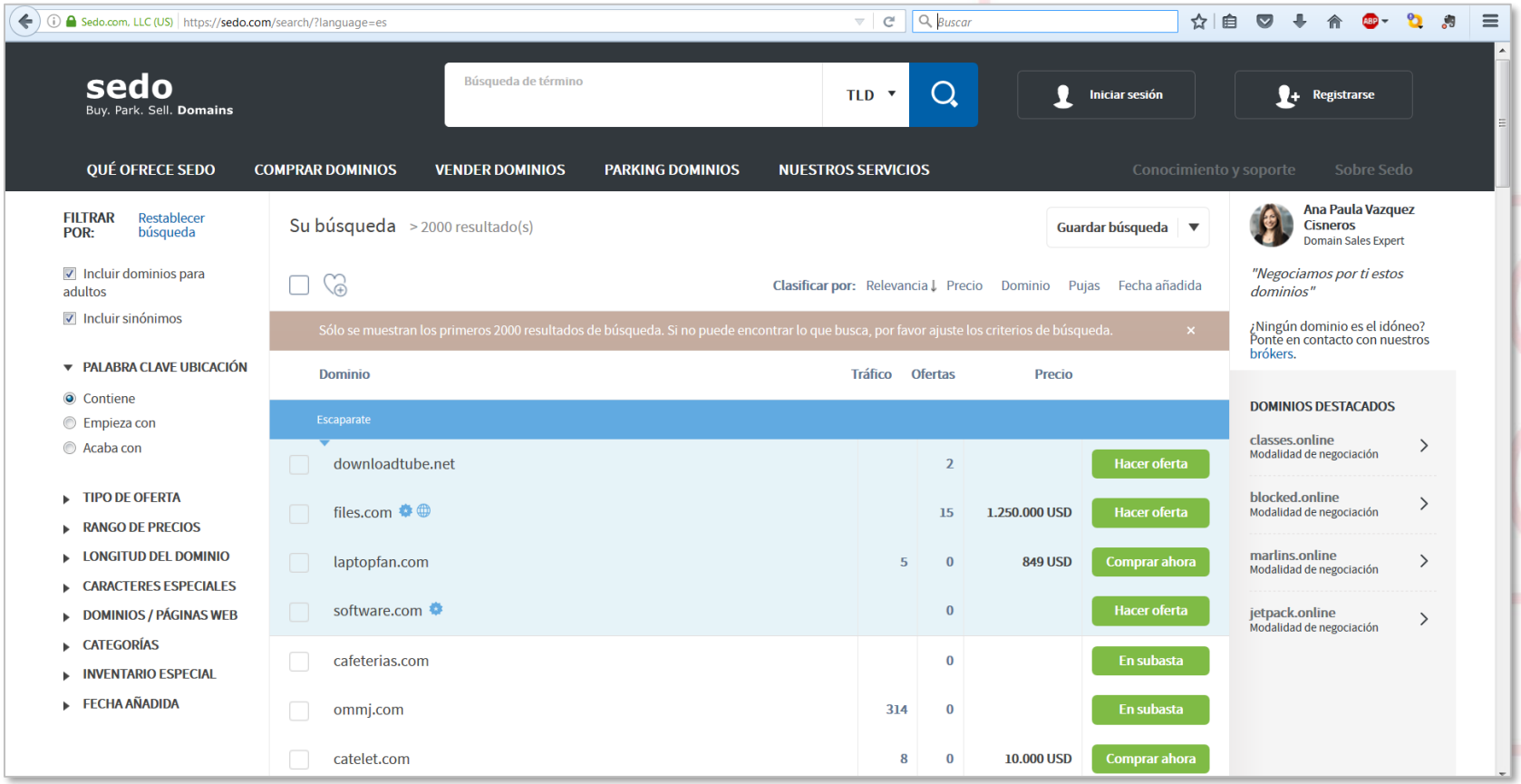
yuoutube.com
yutuve.com
yutube.com

¿ youtube.com ?

TypoSquatting / usos fraudulentos



Domain Dealing / Compra Venta de dominios



¿Quién regula?

El ICANN o *Internet Corporation for Assigned Names and Numbers*, es una organización pública de ámbito internacional, sin fines de lucro fundada en 1998 y responsable de:

- Protocolo de Internet (IP).
- Asignación de espacio de direcciones.
- Registradores e identificadores de protocolo y genéricos (gTLD).
- Códigos de países (ccTLD).
- La gestión de del sistema de nombres de dominios de nivel superior y funciones de gestión del sistema de servidores raíz.

¿Quién regula?

GOBIERNO DE ESPAÑA
MINISTERIO DE INDUSTRIA, ENERGÍA Y TURISMO

red.es

Red.es es la entidad pública empresarial española, adscrita al Ministerio de Industria, Energía y Turismo encargada de consolidar el desarrollo de la Sociedad de la Información en España y la gestión del registro de nombres de dominio bajo el código de país correspondiente a España (.es).

La actividad de Red.es se basa en cuatro ejes de trabajo principales:

- Gestión de los dominios ccTLD ".es".
- Servicios compartidos entre administraciones públicas.
- Colaboración público-privada.
- Internacionalización.

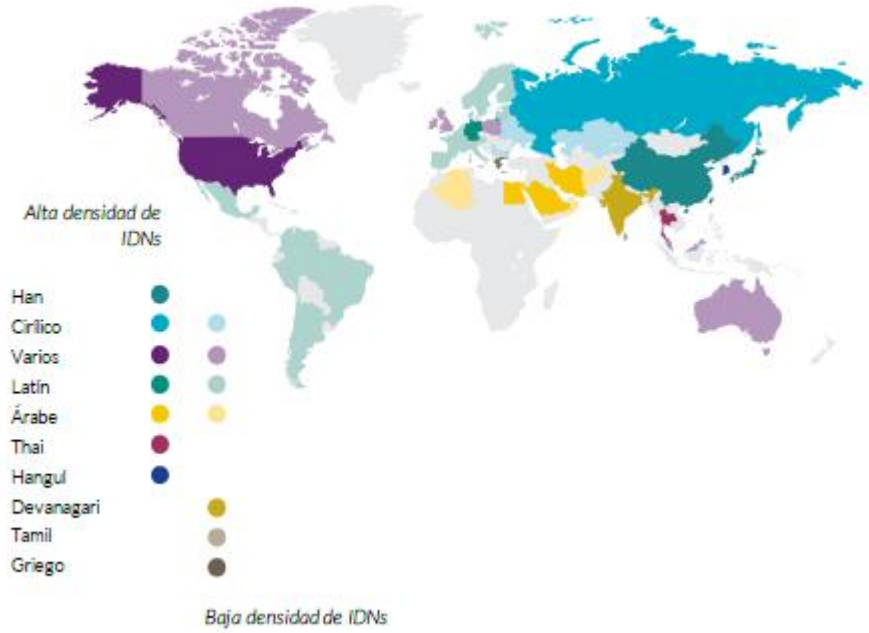
IDN / Internationalized Domain Name

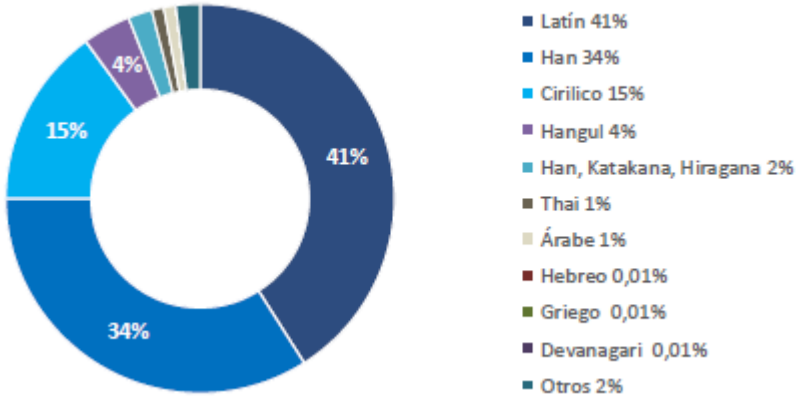
Los *Nombre de Dominio Internacionalizado* o IDN (Internationalized Domain Name) son nombres de dominio definidos bajo el protocolo IDNA, el cual permite codificación de caracteres internacionales o multilingües no codificados según el código ASCII en DNS.

Mediante tablas IDN (también denominadas "*tablas de variantes idiomáticas*", "*tablas de idioma*" o "*tablas de código de escritura*"), se enumeran y describen, por la IANA, los caracteres de un idioma específico con los que puede operar un determinado registro de TLD.

Idioma	Nombre de dominio en formato no ASCII
Español	eñe.es
Japonés	日本レジストリサービス.jp
Chino tradicional	中文.tw
Coreano	구글.kr
Alemán	stellenbörse.de
Árabe	عربي.com
Hebreo	ישראל.com
Ruso	доменные-имена.com

IDN / estadísticas de uso





IDN / Ataque IDN Homograph

IDN Homografos o *IDN Homoglyph*

Comportamiento especulativo y de mala fe, consistente en el registro y/o uso, de nombres de dominio internacionalizados o IDN, idénticos o muy similares tipográficamente a nombres de dominio ya registrados, pero con diferentes *Punycode A-label*, para lo cual se vale de caracteres semejantes en otros alfabetos.

- Adición de **subdominios con barra** (slash): www.microsoft.com/index.html.win-azure.com/
- Intercambio de caracteres **idénticos**: ebay.com (vocal "a" corresponde al cirílico U+0430).
- Intercambio de caracteres **semejantes**:
  τoshiba.com "τ" (vocal tau, U+03C4) por (consonante latina t, U+0074).
- **Punycode Spoofing:** transformación del A-label desde U-label
  https://岍岊岊岅岉岉.com --> https://xn--citibank.com

IDN / Homograph en acción…

Alfabeto	IDN Unicode (U-Label)	Punycode ASCII (A-Label)	Código Unicode
Griego	gοogle.uk	xn--gogle-rce.uk	U+0067 U+03BF U+006F U+0067 U+006C U+0065 U+002E U+0075 U+006B
Latín	google.uk	*No necesario (ASCII)*	U+0067 U+006F U+006F U+0067 U+006C U+0065 U+002E U+0075 U+006B
Cirílico	νodafone.uk	xn--odafone-rof.uk	U+03BD U+006F U+0064 U+0061 U+0066 U+006F U+006E U+0065 U+002E U+0075 U+006B
Latín	vodafone.com	*No necesario (ASCII)*	U+0076 U+006F U+0064 U+0061 U+0066 U+006F U+006E U+0065 U+002E U+0075 U+006B

Nuestro caso / Spain is different !

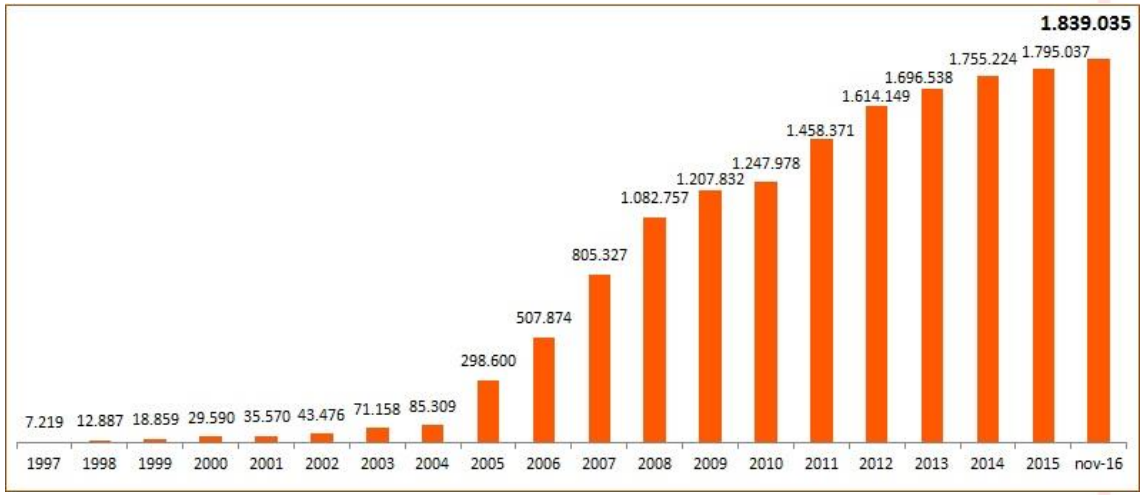
- Registrador: Red.es.
- Extracción de información.

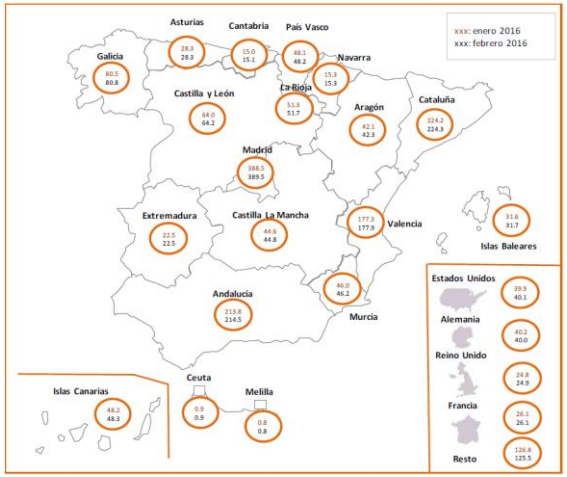
  - Manual
  - Whois43 dominios es
  - RISP datos.gob.es reutiliza la información pública

- Tratamiento de la información: ¿Qué hemos conseguido?.

Dominios.es / Made In Spain

Dominios.es / estadísticas





ÚLTIMOS INFORMES PUBLICADOS

INFORMES	PERIODICIDAD	ÚLTIMOS INFORMES PUBLICADOS
Listado de altas	Semanal	31.10.2016 al 06.11.2016
Listado de altas	Mensual	Noviembre 2016
Estadísticas del ".es"	Mensual	Octubre 2016
Dominios activos por Agente Registrador	Mensual	Octubre 2016
Caracterización del ".es"	Trimestral	Septiembre 2016

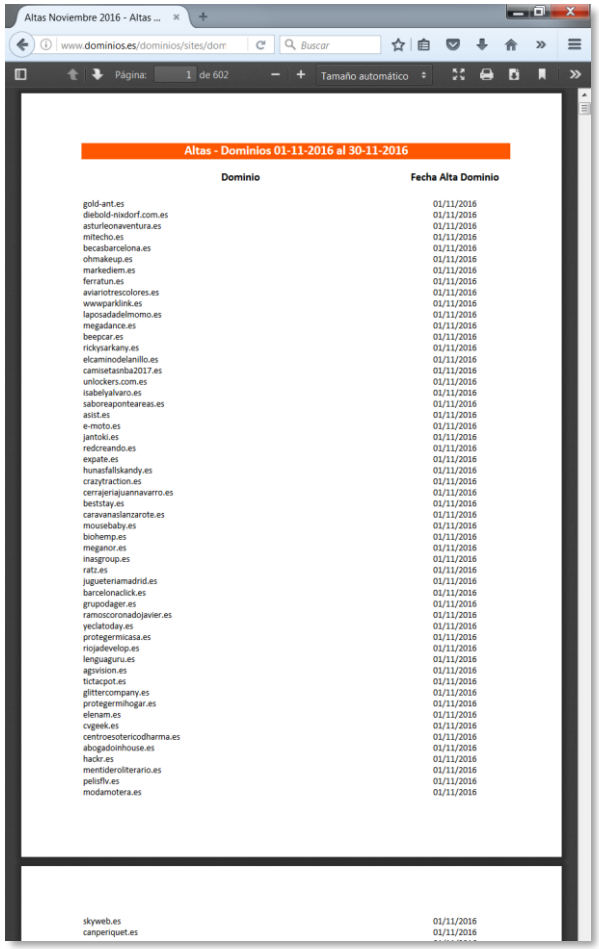
Ver años previos: 2007 2008 2009 2010 2011 2012 2013

Dominios.es / investigando el código fuente

view-source:http://www.dominios.es/dominios/es/todo-lo-que-necesitas-saber/estadisticas

```
<li><a href="/dominios/sites/dominios/files/Agentes_Registradores_Enero_2012.pdf">Agentes registradores</a></li>
<li><a href="/dominios/sites/dominios/files/Altas_por_mes.pdf">Altas por mes</a></li>
</ul><p> </p>
<p><a name="2011" id="2011"><strong>Estadísticas 2011</strong></a></p>
<p>Diciembre</p>
<ul><li><a href="/dominios/es/content/estadísticas-dominios-diciembre-2011">Dominios</a></li>
<li><a href="/dominios/es/content/estadísticas-agentes-registradores-diciembre-2011">Agentes registradores</a></li>
<li><a href="/dominios/sites/dominios/files/1325588227454.pdf">Altas por mes (ver pdf)</a></li>
</ul><p>Noviembre</p>
<ul><li><a href="/dominios/es/content/estadísticas-dominios-noviembre-2011">Dominios</a></li>
<li><a href="/dominios/es/content/estadísticas-agentes-registradores-noviembre-2011">Agentes registradores</a></li>
<li><a href="/dominios/sites/dominios/files/1323682279342.pdf">Altas por mes (ver pdf)</a></li>
</ul><p>Octubre</p>
<ul><li><a href="/dominios/es/content/estadísticas-dominios-octubre-2011">Dominios</a></li>
<li><a href="/dominios/es/content/estadísticas-agentes-registradores-octubre-2011">Agentes registradores</a></li>
<li><a href="/dominios/sites/dominios/files/1320324250653.pdf">Altas por mes (ver pdf)</a></li>
</ul><p>Septiembre</p>
<ul><li><a href="/dominios/es/content/estadísticas-dominios-septiembre-2011">Dominios</a></li>
<li><a href="/dominios/es/content/estadísticas-agentes-registradores-septiembre-2011">Agentes registradores</a></li>
<li><a href="/dominios/sites/dominios/files/1317898109921.pdf">Altas por mes (ver pdf)</a></li>
</ul><p>Agosto</p>
<ul><li><a href="/dominios/es/content/estadísticas-dominios-agosto-2011">Dominios</a></li>
<li><a href="/dominios/es/content/estadísticas-agentes-registradores-agosto-2011">Agentes registradores</a></li>
<li><a href="/dominios/sites/dominios/files/media/2011-08/1315382650263.pdf">Altas por mes (ver pdf)</a></li>
</ul><p>Julio</p>
<ul><li><a href="/dominios/es/content/estadísticas-dominios-julio-2011">Dominios</a></li>
<li><a href="/dominios/es/content/estadísticas-agentes-registradores-julio-2011">Agentes registradores</a></li>
<li><a href="/dominios/sites/dominios/files/media/2011-08/1312281764123.pdf">Altas por mes (ver pdf)</a></li>
</ul><p>Junio</p>
<ul><li><a href="/dominios/es/todo-lo-que-necesitas-saber/estadisticas/dominios-junio-2011">Dominios</a></li>
<li><a href="/dominios/es/todo-lo-que-necesitas-saber/estadisticas/agentes-registradores-junio-2011">Agentes registradores</a></li>
<li><a href="/dominios/sites/dominios/files/media/2011-07/1309521129412.pdf">Altas por mes (ver pdf)</a></li>
</ul><p>Mayo</p>
<ul><li><a href="/dominios/es/todo-lo-que-necesitas-saber/estadisticas/dominios-mayo-2011">Dominios</a></li>
<li><a href="/dominios/es/todo-lo-que-necesitas-saber/estadisticas/agentes-registradores-mayo-2011">Agentes registradores</a></li>
<li><a href="/dominios/sites/dominios/files/media/2011-06/1307011227495.pdf">Altas por mes (ver pdf)</a></li>
</ul><p>Abril</p>
<ul><li><a href="/dominios/es/todo-lo-que-necesitas-saber/estadisticas/dominios-abril-2011">Dominios</a></li>
<li><a href="/dominios/es/todo-lo-que-necesitas-saber/estadisticas/agentes-registradores-abril-2011">Agentes registradores</a></li>
<li><a href="/dominios/sites/dominios/files/media/2011-05/1304508496042.pdf">Altas por mes (ver pdf)</a></li>
</ul><p>Marzo</p>
<ul><li><a href="/dominios/es/todo-lo-que-necesitas-saber/estadisticas/dominios-marzo-2011">Dominios</a></li>
<li><a href="/dominios/es/todo-lo-que-necesitas-saber/estadisticas/agentes-registradores-enero-2011">Agentes registradores</a></li>
<li><a href="/dominios/sites/dominios/files/media/2011-04/1301657930627.pdf">Altas por mes (ver pdf)</a></li>
</ul><p>Febrero</p>
<ul><li><a href="/dominios/es/todo-lo-que-necesitas-saber/estadisticas/dominios-febrero-2011">Dominios</a></li>
<li><a href="/dominios/es/todo-lo-que-necesitas-saber/estadisticas/agentes-registradores-febrero-2011">Agentes registradores</a></li>
<li><a href="/dominios/sites/dominios/files/media/2011-03/1298998179111.pdf">Altas por mes (ver pdf)</a></li>
</ul><p>Enero</p>
```

PDFs / todos los dominios registrados



Los bajamos con WGET para analizarlos

wget –r –A .pdf *http://www.dominios.es/dominios/es/todo-lo-que-necesitas-saber/estadisticas*

```
(ui                 ~/public_html/seguridad/dominiosES/dominios/cybercamp$ wget -A .pdf -r http://www.dominios.es/dominios/es/todo-lo-que-necesitas-saber/estadisticas

converted 'http://www.dominios.es/dominios/es/todo-lo-que-necesitas-saber/estadisticas' (ANSI_X3.4-1968) -> 'http://www.dominios.es/dominios/es/todo-lo-que-necesitas-s
aber/estadisticas' (UTF-8)
converted 'http://www.dominios.es/dominios/es/todo-lo-que-necesitas-saber/estadisticas' (ANSI_X3.4-1968) -> 'http://www.dominios.es/dominios/es/todo-lo-que-necesitas-s
aber/estadisticas' (UTF-8)
--2016-12-01 23:51:35--  http://www.dominios.es/dominios/es/todo-lo-que-necesitas-saber/estadisticas
Resolving www.dominios.es (www.dominios.es)... 194.69.254.120, 2001:67c:21cc:2000::64:120
Connecting to www.dominios.es (www.dominios.es)|194.69.254.120|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: unspecified [text/html]
Saving to: 'www.dominios.es/dominios/es/todo-lo-que-necesitas-saber/estadisticas'

www.dominios.es/dominios/es/todo-lo-que-n     [ <=>                                                                                ]  71.44K  --.-KB/s    in 0.1s

2016-12-01 23:51:37 (695 KB/s) - 'www.dominios.es/dominios/es/todo-lo-que-necesitas-saber/estadisticas' saved [73150]

converted 'http://www.dominios.es/dominios/sites/dominios/themes/redesms/favicon.ico' (ANSI_X3.4-1968) -> 'http://www.dominios.es/dominios/sites/dominios/themes/redesm
s/favicon.ico' (UTF-8)
converted 'http://www--dominios--es.insuit.net/i4tservice/jscm_loader.js' (ANSI_X3.4-1968) -> 'http://www--dominios--es.insuit.net/i4tservice/jscm_loader.js' (UTF-8)
converted 'http://www.dominios.es/dominios/es/todo-lo-que-necesitas-saber/estadisticas' (ANSI_X3.4-1968) -> 'http://www.dominios.es/dominios/es/todo-lo-que-necesitas-s
aber/estadisticas' (UTF-8)
converted 'http://www.dominios.es/dominios/es/node/15000' (ANSI_X3.4-1968) -> 'http://www.dominios.es/dominios/es/node/15000' (UTF-8)
converted 'http://www.dominios.es/dominios/sites/dominios/files/css/css_hHzQCK_94LxrjXf8lW6OXPZgTNVKlWXuvLkpcwvHva8.css' (ANSI_X3.4-1968) -> 'http://www.dominios.es/do
minios/sites/dominios/files/css/css_hHzQCK_94LxrjXf8lW6OXPZgTNVKlWXuvLkpcwvHva8.css' (UTF-8)
converted 'http://www.dominios.es/dominios/sites/dominios/files/css/css_YF9r8MqDGSM81yzr5XUmTB34WMnPSvm2Z_b666eV3Y0.css' (ANSI_X3.4-1968) -> 'http://www.dominios.es/do
```

ls -lisaR

```
./www.dominios.es/dominios/sites/dominios/files/files:
total 67524
5381780802    12 drwx---r-x 2                    8192 Dec  2 00:01 .
4296657645     8 drwx---r-x 4                    4096 Dec  1 23:59 ..
5369132768   632 -rw----r-- 1                  645965 Nov 13  2014 1-15  10  2007.pdf
5408502494   400 -rw----r-- 1                  406412 Mar 11  2013 Agentes Registradores Febrero 2013(1).pdf
5408513564   348 -rw----r-- 1                  355015 Dec 18  2012 Agentes Registradores Noviembre 2012.pdf
5408513568   352 -rw----r-- 1                  360047 Nov 16  2012 Agentes Registradores Octubre 2012.pdf
5408513559   348 -rw----r-- 1                  354482 Jan 15  2013 Agentes Registradores diciembre 2012.pdf
5408513552   348 -rw----r-- 1                  354053 Feb 11  2013 Agentes Registradores enero 2013.pdf
5383930970   896 -rw----r-- 1                  915420 May  5  2014 Altas Abril 2014 (espa??ol).pdf
5383610266  1220 -rw----r-- 1                 1245354 May  4  2015 Altas Abril 2015 (espa??ol).pdf
5408502476   704 -rw----r-- 1                  717582 Sep  4  2013 Altas Agosto 2013.pdf
5383930959  1452 -rw----r-- 1                 1483120 Sep  4  2014 Altas Agosto 2014(espa??ol)(1).pdf
5382381106   952 -rw----r-- 1                  972497 Sep  1  2015 Altas Agosto 2015 (espa??ol).pdf
5408513560  1492 -rw----r-- 1                 1524158 Jan 15  2013 Altas Diciembre 2012.pdf
5384162067   780 -rw----r-- 1                  795228 Jan  9  2014 Altas Diciembre 2013 (espa??ol)(1).pdf
5383930947   620 -rw----r-- 1                  634235 Jan  8  2015 Altas Diciembre 2014 (espa??ol).pdf
5408513556  1404 -rw----r-- 1                 1435928 Feb  4  2013 Altas Enero 2013 (espa??ol).pdf
5384162055   924 -rw----r-- 1                  942937 Feb  3  2014 Altas Enero 2014 (espa??ol).pdf
5383610286  1376 -rw----r-- 1                 1405625 Feb  4  2015 Altas Enero 2015 (espa??ol)(1).pdf
5408502496  1208 -rw----r-- 1                 1233310 Mar  4  2013 Altas Febrero 2013 (espa??ol).pdf
```

PDF Parser / Pasando de PDF a texto

https://github.com/smalot/pdfparser

PdfParser

Pdf Parser, a standalone PHP library, provides various tools to extract data from a PDF file.

build passing downloads 164.11 k Current Version HHVM Partial

Website : http://www.pdfparser.org

Test the API on our demo page.

This project is supported by Actualys.

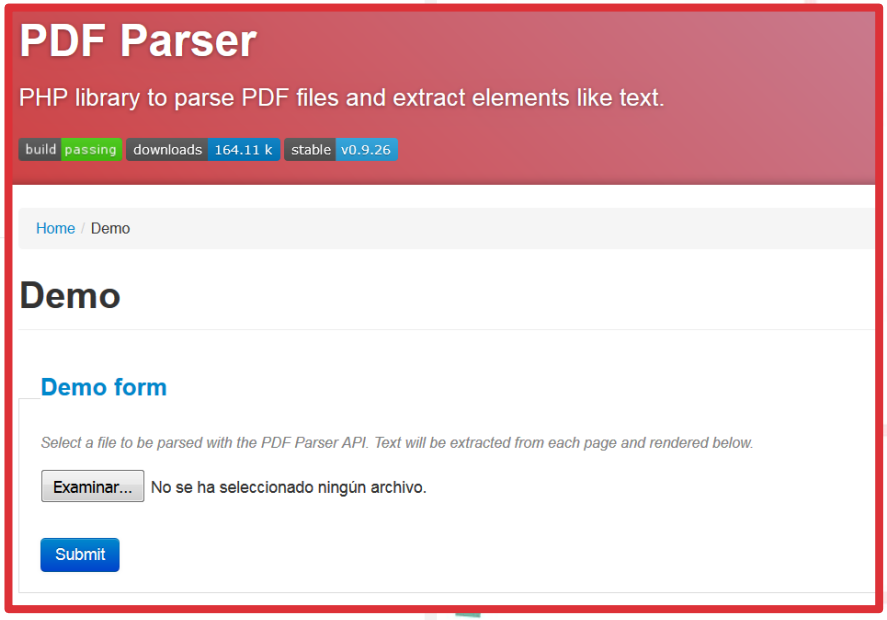
Features

Features included :

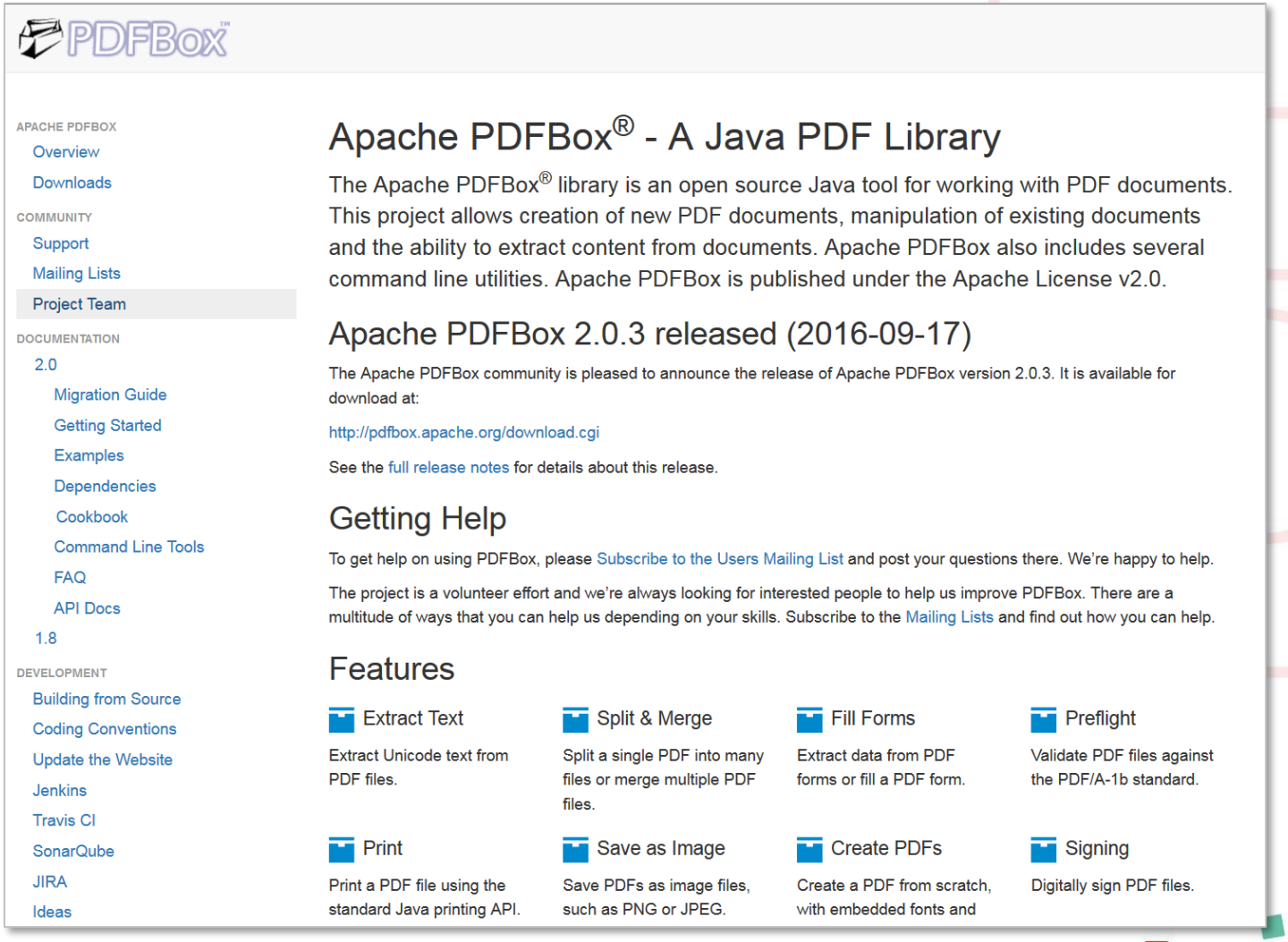
- Load/parse objects and headers
- Extract meta data (author, description, ...)
- Extract text from ordered pages
- Support of compressed pdf
- Support of MAC OS Roman charset encoding
- Handling of hexa and octal encoding in text sections
- PSR-0 compliant (autoloader)
- PSR-1 compliant (code styling)

Currently, secured documents are not supported.

This Library is still under active development. As a result, users must expect BC breaks when using the master version.



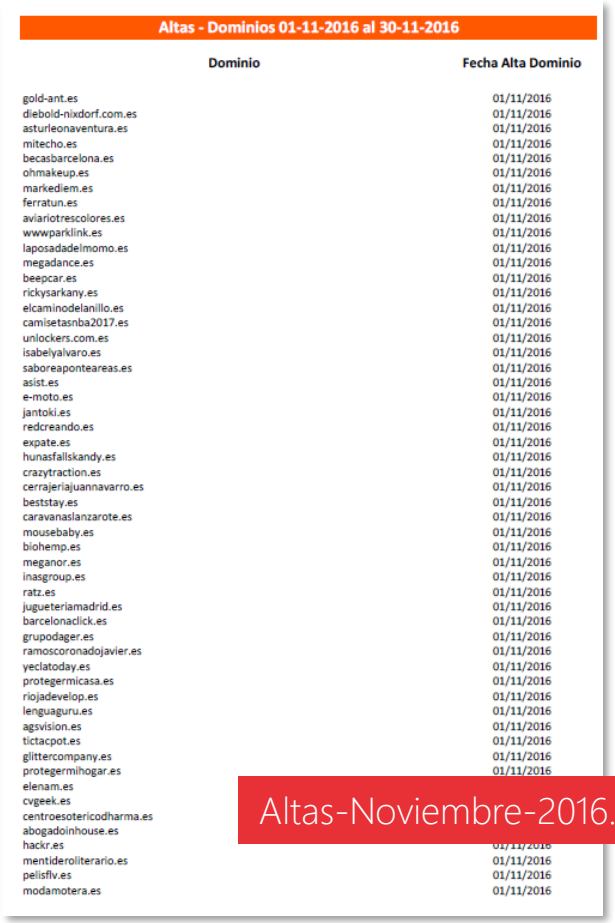
Apache PDFBox / PDF a Texto por CLI



Convirtiendo nuestro tesoro a texto

pdfbox-app-2.0.3.jar

java -jar pdfbox-app-2.0.3.jar ExtractText Altas-Noviembre-2016.pdf AltasNoviembre.txt



Altas - Dominios 01-11-2016 al 30-11-2016

Dominio	Fecha Alta Dominio
gold-ant.es	01/11/2016
diebold-nixdorf.com.es	01/11/2016
asturleonaventura.es	01/11/2016
mitecho.es	01/11/2016
becasbarcelona.es	01/11/2016
ohmakeup.es	01/11/2016
markediem.es	01/11/2016
ferratun.es	01/11/2016
aviariotrescolores.es	01/11/2016
wwwparklink.es	01/11/2016
laposadadelmomo.es	01/11/2016
megadance.es	01/11/2016
beepcar.es	01/11/2016
rickysarkany.es	01/11/2016
elcaminodelanillo.es	01/11/2016
camisetasnba2017.es	01/11/2016
unlockers.com.es	01/11/2016
isabelyalvaro.es	01/11/2016
saboreapontеareas.es	01/11/2016
asist.es	01/11/2016
e-moto.es	01/11/2016
jantoki.es	01/11/2016
redcreando.es	01/11/2016
expate.es	01/11/2016
hunasfallskandy.es	01/11/2016
crazytraction.es	01/11/2016
cerrajeriajuannavarro.es	01/11/2016
beststay.es	01/11/2016
caravanaslanzarote.es	01/11/2016
mousebaby.es	01/11/2016
biohemp.es	01/11/2016
meganor.es	01/11/2016
inasgroup.es	01/11/2016
ratz.es	01/11/2016
jugueteriamadrid.es	01/11/2016
barcelonaclick.es	01/11/2016
grupodager.es	01/11/2016
ramoscoronadojavier.es	01/11/2016
yeclatoday.es	01/11/2016
protegermicasa.es	01/11/2016
riojadevelop.es	01/11/2016
lenguaguru.es	01/11/2016
agsvision.es	01/11/2016
tictacpot.es	01/11/2016
glittercompany.es	01/11/2016
protegermihogar.es	01/11/2016
elenam.es	
cvgeek.es	
centroesotericodharma.es	
abogadoinhouse.es	
hackr.es	
mentideroliterario.es	01/11/2016
pelisflv.es	01/11/2016
modamotera.es	01/11/2016

Altas-Noviembre-2016.pdf

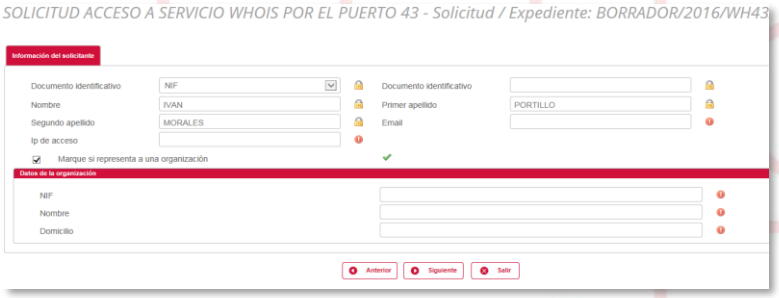
```
1  Dominio Fecha Alta Dominio
2  gold-ant.es 01/11/2016
3  diebold-nixdorf.com.es 01/11/2016
4  asturleonaventura.es 01/11/2016
5  mitecho.es 01/11/2016
6  becasbarcelona.es 01/11/2016
7  ohmakeup.es 01/11/2016
8  markediem.es 01/11/2016
9  ferratun.es 01/11/2016
10 aviariotrescolores.es 01/11/2016
11 wwwparklink.es 01/11/2016
12 laposadadelmomo.es 01/11/2016
13 megadance.es 01/11/2016
14 beepcar.es 01/11/2016
15 rickysarkany.es 01/11/2016
16 elcaminodelanillo.es 01/11/2016
17 camisetasnba2017.es 01/11/2016
18 unlockers.com.es 01/11/2016
19 isabelyalvaro.es 01/11/2016
20 saboreapontеareas.es 01/11/2016
21 asist.es 01/11/2016
22 e-moto.es 01/11/2016
23 jantoki.es 01/11/2016
24 redcreando.es 01/11/2016
25 expate.es 01/11/2016
26 hunasfallskandy.es 01/11/2016
27 crazytraction.es 01/11/2016
28 cerrajeriajuannavarro.es 01/11/2016
29 beststay.es 01/11/2016
30 caravanaslanzarote.es 01/11/2016
31 mousebaby.es 01/11/2016
32 biohemp.es 01/11/2016
33 meganor.es 01/11/2016
34 inasgroup.es 01/11/2016
35 ratz.es 01/11/2016
36 jugueteriamadrid.es 01/11/2016
37 barcelonaclick.es 01/11/2016
38 grupodager.es 01/11/2016
39 ramoscoronadojavier.es 01/11/2016
40 yeclatoday.es 01/11/2016
41 protegermicasa.es 01/11/2016
42 riojadevelop.es 01/11/2016
43 lenguaguru.es 01/11/2016
```

AltasNoviembre.txt

Whois43 / más fácil aun…

Se necesita

1) Url: https://sede.red.gob.es
2) Certificado Digital.



Whois43

```
Queries can be performed on second and third level domains.
---------------------------------------------------------------------------------------------------

Domain:
-------
   Domain Name:                 incibe.es

Registrant:
-----------
   Registrant Name:             INSTITUTO NACIONAL DE TECONOLOGIAS DE LA COMUNICACION, S.A.


>>> LAST UPDATE: 02/12/2016 07:00:04
---------------------------------------------------------------------------------------------------
More information on each domain may be consulted at www.dominios.es.
```

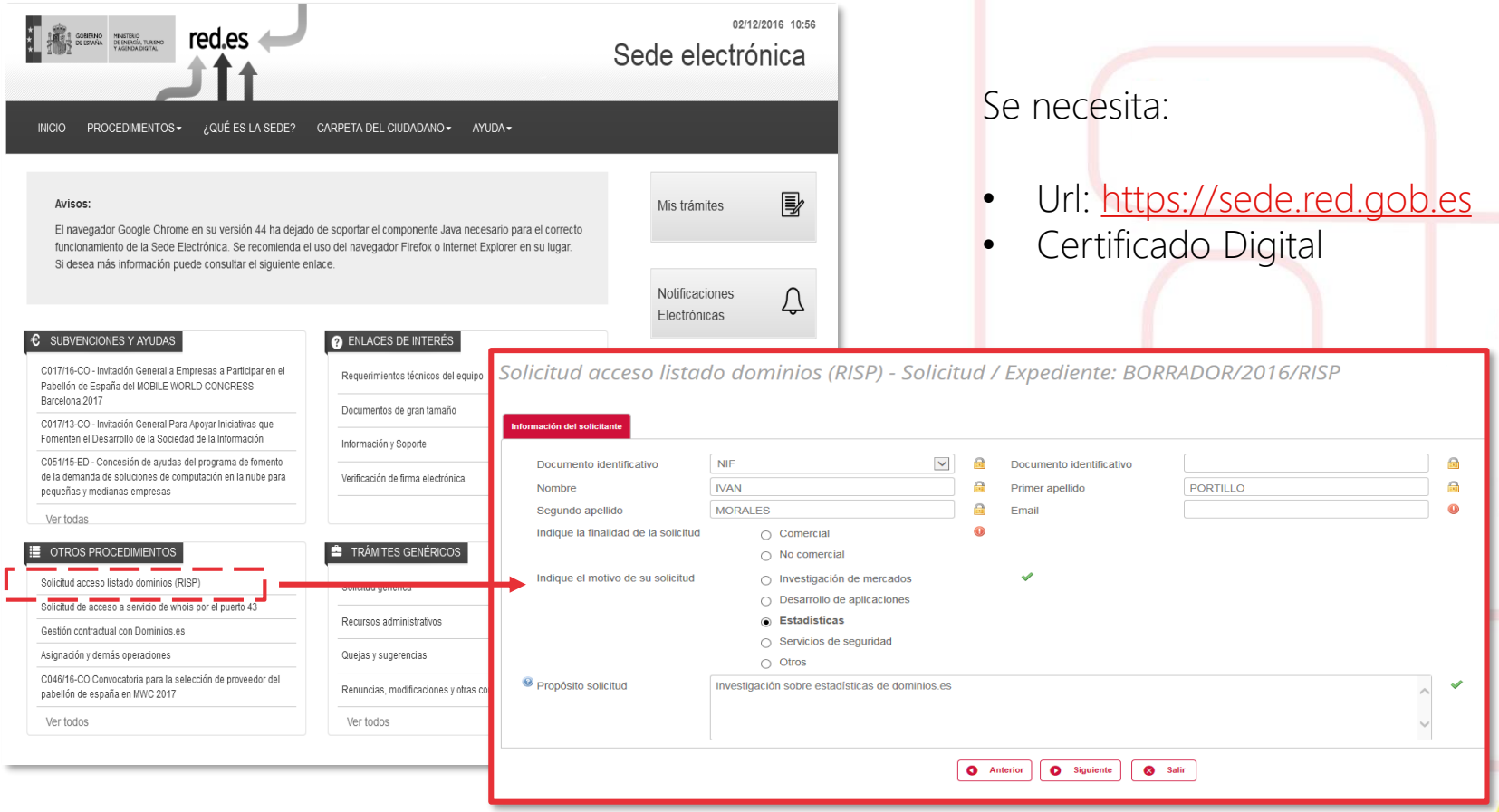
whois -h whois.nic.es -p 43 incibe.es

whois -h whois.nic.es -p 43 cybercamp.es

```
The data which can be consulted via this service include: availability and name of the holder of a
domain.

A maximum of 10 queries per minute can be made by each registered IP address. Should this limit be
exceeded, the service will be blocked for two hours, after which a new query may be performed.

Queries can be performed on second and third level domains.
---------------------------------------------------------------------------------------------------

Domain:
-------
   Domain Name:                 cybercamp.es

Registrant:
-----------
   Registrant Name:             Instituto Nacional de Tecnologias de la Comunicacion S.A.


>>> LAST UPDATE: 02/12/2016 07:00:04
---------------------------------------------------------------------------------------------------
More information on each domain may be consulted at www.dominios.es.
```

Datos resultantes Nombre Dominio, Registrante, Ultima Actualización

RISP / Toda la lista sobre la que trabajar



Se necesita:

- Url: https://sede.red.gob.es
- Certificado Digital

RISP / acceso a dominios .es

RISP_OTROS.csv

```
"NOMBRE_DOMINIO"|"NOMBRE_TITULAR"|"IDENTIFICACION"
"idealia.es"|"Idealia Comunicacion Y Marketing S.L.L."|"B-82554056"
"indcresa.es"|"Indcres S.A."|"A-08116808"
"fundacionpatrimoniocyl.es"|"Fundacion del Patrimonio Historico de Castilla y Leon"|"G-47392618"
"ecf.es"|"ECF Escriptori Comptable i Fiscal S.L."|"B-59927962"
"alimotor.es"|"Alimotor S.A."|"A-03303609"
"cofiber.es"|"Cofiber Financiera Establecimiento Financiero de Credito S.A."|"A-79352274"
"agroland.es"|"Alvaro Rodriguez Eiras S.L."|"B-27015304"
"vilalba.es"|"Ayuntamiento de Vilalba"|"P-2706500-B"
"powerline.es"|"Power Line Marketing Telefonico S.L."|"B-81072407"
"down21.es"|"Fundacion Down 21"|"G-82737024"
"dimac.es"|"Comercial Dimac S.L."|"B-58130626"
"arkhitekton.es"|"Arkhitekton S.A."|"A-39225859"
"cofeserbit.es"|"Cofeserbit S.L."|"B-60387859"
"microcad.es"|"Micro Cad Informatica S.L."|"B-29627510"
"neomania.es"|"Ibermaison S.L"|"B81049892"
"mfe.es"|"Mondial Forni Espan~a S.A."|"A-08396152"
"microtech.es"|"Microtech Sistemas S.L."|"B-61022943"
"carnesfrescassa.es"|"Carnes Frescas S.A."|"A-12027686"
"productosseco.es"|"Productos Seco S.L."|"B-24340382"
"fut.es"|"ORGANISME AUTONOM PER A LA SOCIETAT DE LA INFORMACIO"|"P4300025F"
"urv.es"|"Universitat Rovira i Virgili"|"Q-9350003-A"
"calvoymunarsa.es"|"Calvo y Munar S.A."|"A-28027068"
"ras.es"|"Grabados Electroquimicos Ras S.L."|"B-28004968"
"rafer.es"|"Comercial Rafer S.L."|"B-50045988"
"pmp.es"|"PMP Management Factory, S.L."|"B95590865"
"comtech.es"|"Computer Technology Catalunya S.L."|"B-60960200"
"tecna.es"|"Tecnologia de Aislamientos y Climatizacion S.L."|"B-81725970"
"albura.es"|"Asociacion Cultural Recreativo Deportiva Albura"|"G-79133245"
"belgicast.es"|"Belgicast Internacional S.L."|"B-48750806"
"arancia.es"|"Arancia S.L."|"B-20602264"
"toyser.es"|"Toyser S.A."|"A-58107053"
"querubin.es"|"Calzados Fal S.A."|"A-26004978"
"telecal.es"|"Telecal Instalaciones de Telefonia S.L."|"B-04264974"
"reteal.es"|"Red de Telefonia Almeriense S.L."|"B-04292082"
"rorschach.es"|"Sociedad Andaluza de Rorschach y Metodos Proyectivos"|"G-41830670"
"juarez.es"|"Graficas Juarez S.L."|"B-03422334"
"menta.es"|"Auna Telecomunicaciones S.A."|"A-60774429"
"indatronic.es"|"Indatronic S.L."|"B-04271193"
"movinet.es"|"Movinet Valencia S.L."|"B-96852421"
"irta.es"|"Institut de Recerca i Tecnologia Agroalimentaries"|"Q-5855049-B"
"consejo-estado.es"|"Consejo de Estado"|"S-2811013-H"
"bingosreunidos.es"|"Bingos Reunidos S.A."|"A-03193323"
"fripanel.es"|"Paneles Frigorificos S.A."|"A-08563009"
"lafincasomosaguas.es"|"Urbanizadora Somosaguas S.A.U."|"A-28069441"
"imathia.es"|"Imathia S.L."|"B-79158325"
"castillosasociacion.es"|"Asociacion Espan~ola de Amigos de los Castillos"|"G-28230746"
"scpsa.es"|"Servicios de la Comarca de Pamplona S.A."|"A-31118441"
"alpine.es"|"Alpine Electronics de Espan~a S.A."|"A-01102995"
"ums.es"|"United Metal Supply Spain S.A."|"A-82302886"
"kronospan.es"|"Kronospan Spain S.L."|"B-83020081"
"pgmedia.es"|"Promocion y Gestion Multimedia S.L."|"B-48832109"
"clubporsche.es"|"Club Porsche Espan~a"|"G-28786515"
"iccsa.es"|"Inmobiliaria Comercial Cerdena S.A."|"A-08100570"
"maper.es"|"Recubrimientos Maper S.L."|"B-96541099"
"fpa.es"|"Fundacion Principe de Asturias"|"G-33039348"
"uam.es"|"Universidad Autonoma de Madrid"|"Q-2818013-A"
```

Pasos a seguir

- Acceso CSV durante 5 días.
- Control de Base de Datos de 1.842.568 de dominios .es.

Investigando un dominio

DNS server handling your query: localhost
DNS server's address: 127.0.0.1#53

Non-authoritative answer:
Name: cybercamp.es
Address: 195.53.165.58

cybercamp.es text = "v=spf1 mx a:correo.incibe.es a:correo.inteco.es a:correo2.inteco.es -all"

cybercamp.es mail exchanger = 20 mail2.cybercamp.es.
cybercamp.es mail exchanger = 10 mail.cybercamp.es.

cybercamp.es origin = ns1.cdmon.net mail addr = hostmaster.cybercamp.es serial = 1477731448 refresh = 10000 retry = 3600 expire = 604800 minimum = 21600

cybercamp.es nameserver = ns3.cdmon.net.
cybercamp.es nameserver = ns1.cdmon.net.
cybercamp.es nameserver = ns2.cdmon.net.

Soluciones OpenSource / DNSTwist

DNSTwist es una librería open-source creada por el analista de seguridad *Marcin Ulikowski* (Polonia) para análisis de amenazas de typosquatting y suplantación de dominios.

https://github.com/elceef/dnstwist

Las principales características de la librería son:

- Amplia gama de **algoritmos eficientes** de generación de nombres de dominio.
- **Resolución de nombres** de dominio a IPv4 e IPv6 y consultas de registros **NS y MX**.
- **Evaluación de sitios** web **similares** mediante hashes difusos (**Fuzzy hashing**) para encontrar sitios phishing.
- **Comprobación de hosts MX** (servidor de correo), su utilización para interceptación de mensajes de correo electrónico mal dirigidos (**espionaje corporativo**).
- Generación de variaciones de dominios adicionales utilizando archivos de tipo diccionario.
- Información sobre **Geolocalización IP**.
- Operaciones de búsqueda WHOIS para fechas de creación y modificación.
- Formatos de salida **CSV**, **JSON y Terminal**.

Soluciones OpenSource / DNSTwist

Comando: python dnstwist.py -b -w -g -m google.es

Soluciones OpenSource / DNSTwist Demo

Soluciones OpenSource / URLCrazy

URLCrazy es una librería Open-source desarrollada por el analista de seguridad *Andrew Horton* (Melbourne, Australia), para generar y comprobar errores tipográficos y variaciones para dominios web en la detección y realización de Typosquatting, URL Hijacking, y Phishing.

https://www.morningstarsecurity.com/research/urlcrazy

Las principales utilidades de esta librería son:

- Detección de diferentes técnicas de Typosquatting / Desarrollado en Ruby.
- Protección de marcas corporativas mediante el registro de los errores tipográficos más populares.
- Detección de conductas de ataques de phishing durante pruebas de penetración.
- Obtención de dirección IP, Consulta de registros MX e información sobre Geolocalización IP.
- Múltiples tipologías de teclado: QWERTY, AZERTY, QWERTZ, Dvorak.

Soluciones OpenSource / URLCrazy

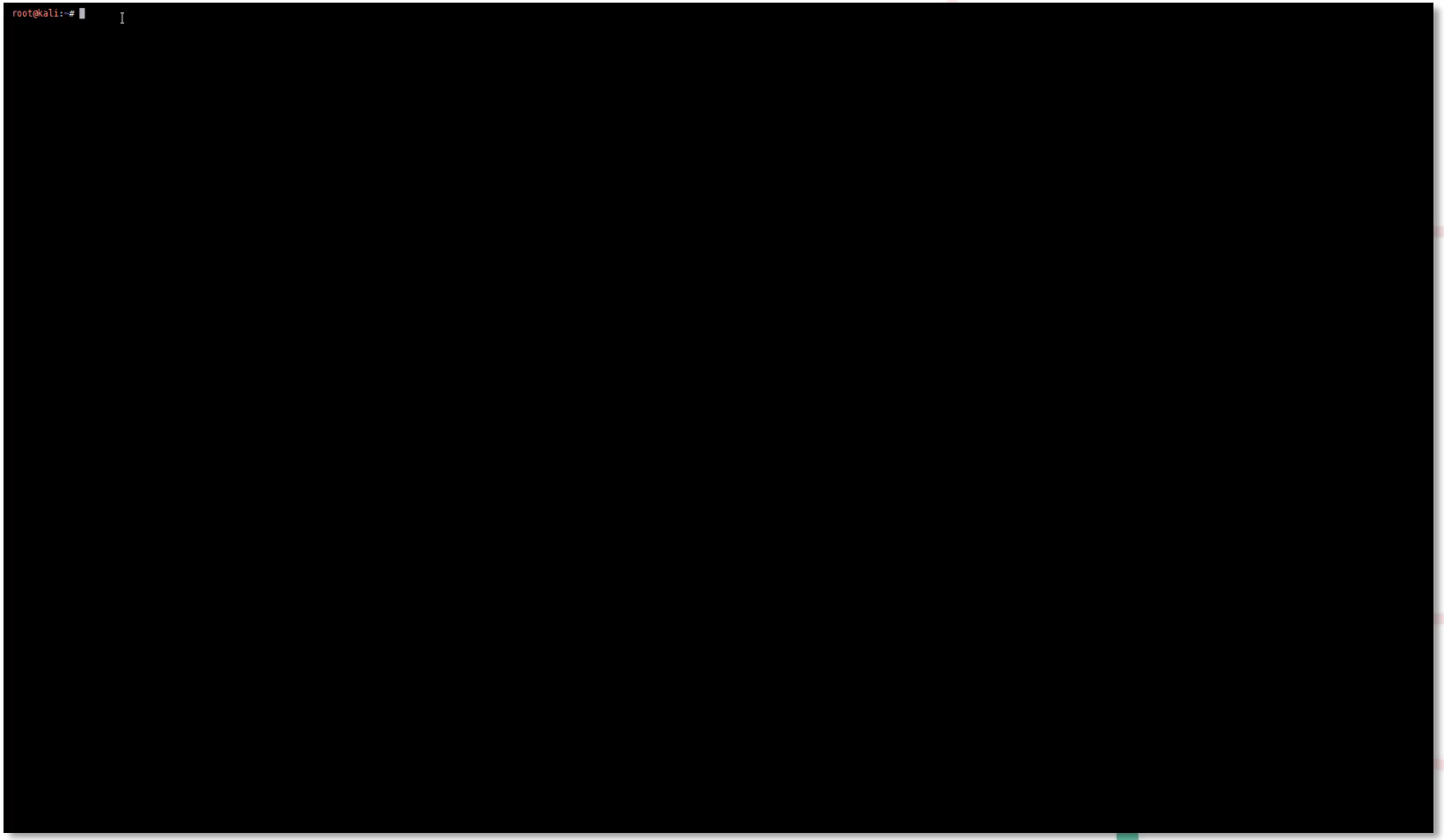
URLCrazy Domain Report
Domain : google.es
Keyboard : qwerty
At : 2016-12-02 13:08:33 +0100

Please wait. 96 hostnames to process

Typo Type	Typo	DNS-A	CC-A	DNS-MX	Extn
Character Omission	gogle.es	82.98.152.141	ES,SPAIN	gogle.es	es
Character Omission	googe.es	5.135.225.188	FR,FRANCE		es
Character Omission	googl.es		?		es
Character Omission	goole.es	185.53.179.9		mail.h-email.net	es
Character Repeat	ggoogle.es	104.31.65.90			es
Character Repeat	googgle.es	185.53.178.6		mail.h-email.net	es
Character Repeat	googlee.es	185.53.178.9		ma	
Character Repeat	googlle.es	72.52.4.120	▓,	loca	
Character Repeat	gooogle.es		?		
Character Swap	gogole.es	37.152.88.54	CA,CANADA		
Character Swap	googel.es	217.160.0.145	IT,ITALY	mx	
Character Swap	google.se	216.58.201.131	US,UNITED STATES	al	
Character Swap	goolge.es	127.0.0.1	ZZ,RESERVED		es
Character Swap	ogogle.es		?		es
Character Replacement	foogle.es	185.53.178.7		mail.h-email.net	es
Character Replacement	giogle.es	72.52.4.120	US,UNITED STATES	localhost	es
Character Replacement	goigle.es	199.59.243.120	CN,CHINA		es
Character Replacement	goofle.es	213.186.33.5	FR,FRANCE	redirect.ovh.net	es
Character Replacement	googke.es	185.53.178.9		mail.h-email.net	es
Character Replacement	google.rs	216.58.210.163	US,UNITED STATES	google.com.s9b1.psmtp.com	rs
Character Replacement	google.ws	216.58.214.163	US,UNITED STATES	google.com.s9a1.psmtp.com	ws
Character Replacement	googlr.es	5.135.225.188	FR,FRANCE		es
Character Replacement	googlw.es	5.135.225.188	FR,FRANCE		es
Character Replacement	goohle.es	166.78.238.48		mx.goohle.es	es
Character Replacement	gopgle.es	72.52.4.120	US,UNITED STATES	localhost	es
Character Replacement	gpogle.es	213.186.33.5	FR,FRANCE	redirect.ovh.net	es
Character Replacement	hoogle.es	72.52.4.120	US,UNITED STATES	localhost	es
Double Character Replacement	giigle.es		?		es
Double Character Replacement	gppgle.es	217.76.156.252	ES,SPAIN		es
Character Insertion	gfoogle.es	217.76.156.252	ES,SPAIN		es
Character Insertion	ghoogle.es	184.168.221.13	US,UNITED STATES	mailstore1.secureserver.net	es
Character Insertion	goiogle.es	213.186.33.5	FR,FRANCE	redirect.ovh.net	es
Character Insertion	googfle.es	213.186.33.5	FR,FRANCE	redirect.ovh.net	es
Character Insertion	googhle.es	72.52.4.120	US,UNITED STATES	localhost	es
Character Insertion	googler.es	82.194.64.60	ES,SPAIN	mx01.canaldominios.com	es
Character Insertion	googlew.es	188.165.119.163	FR,FRANCE	yahoo.es	es
Character Insertion	googlke.es	72.52.4.120	H5,	localhost	es
Character Insertion	gooigle.es		?		es
Character Insertion	goopgle.es	50.63.202.1	US,UNITED STATES	mailstore1.secureserver.net	es
Character Insertion	gopogle.es	184.168.221.6	US,UNITED STATES	mailstore1.secureserver.net	es
Missing Dot	googlees.com	116.212.117.220	HK,HONG KONG		com
Missing Dot	wwwgoogle.es	5.135.225.188	US,UNITED STATES		es
Singular or Pluralise	googles.es	185.53.178.7		mail.h-email.net	es
Vowel Swap	gaagle.es		?		es
Vowel Swap	geegle.es		?		es
Vowel Swap	googla.as		?		as
Vowel Swap	googli.is		?		is
Vowel Swap	googlu.us	75.126.100.25	US,UNITED STATES		us
Vowel Swap	guugle.es	217.76.156.252	ES,SPAIN		es
Bit Flipping	coogle.es	37.152.88.54	ES,SPAIN		es
Bit Flipping	eoogle.es		?		es
Bit Flipping	ggogle.es	0.0.0.0	ZZ,RESERVED		es
Bit Flipping	gkogle.es		?		es

Comando urlcrazy google.es

Soluciones OpenSource / URLCrazy Demo



Plataforma web para detección

Índice

Descripción

Capacidades

Arquitectura

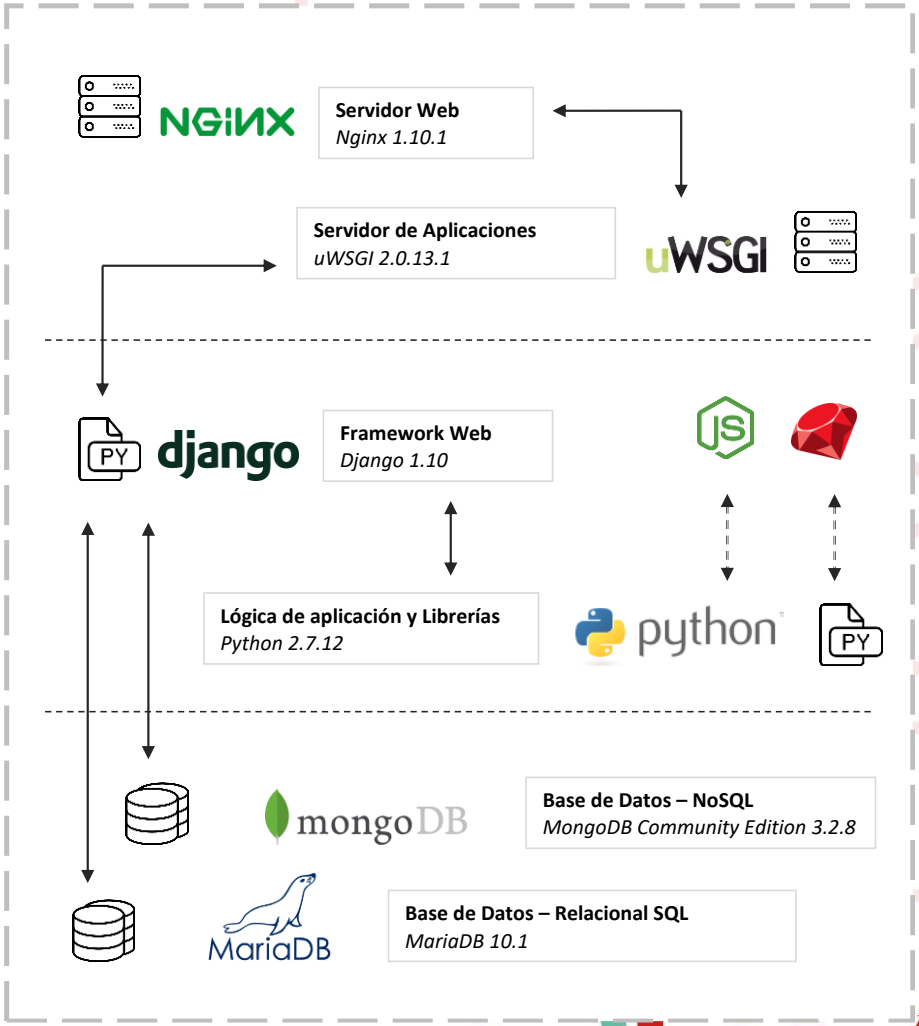
Video / Demo

Web abierta en vivo

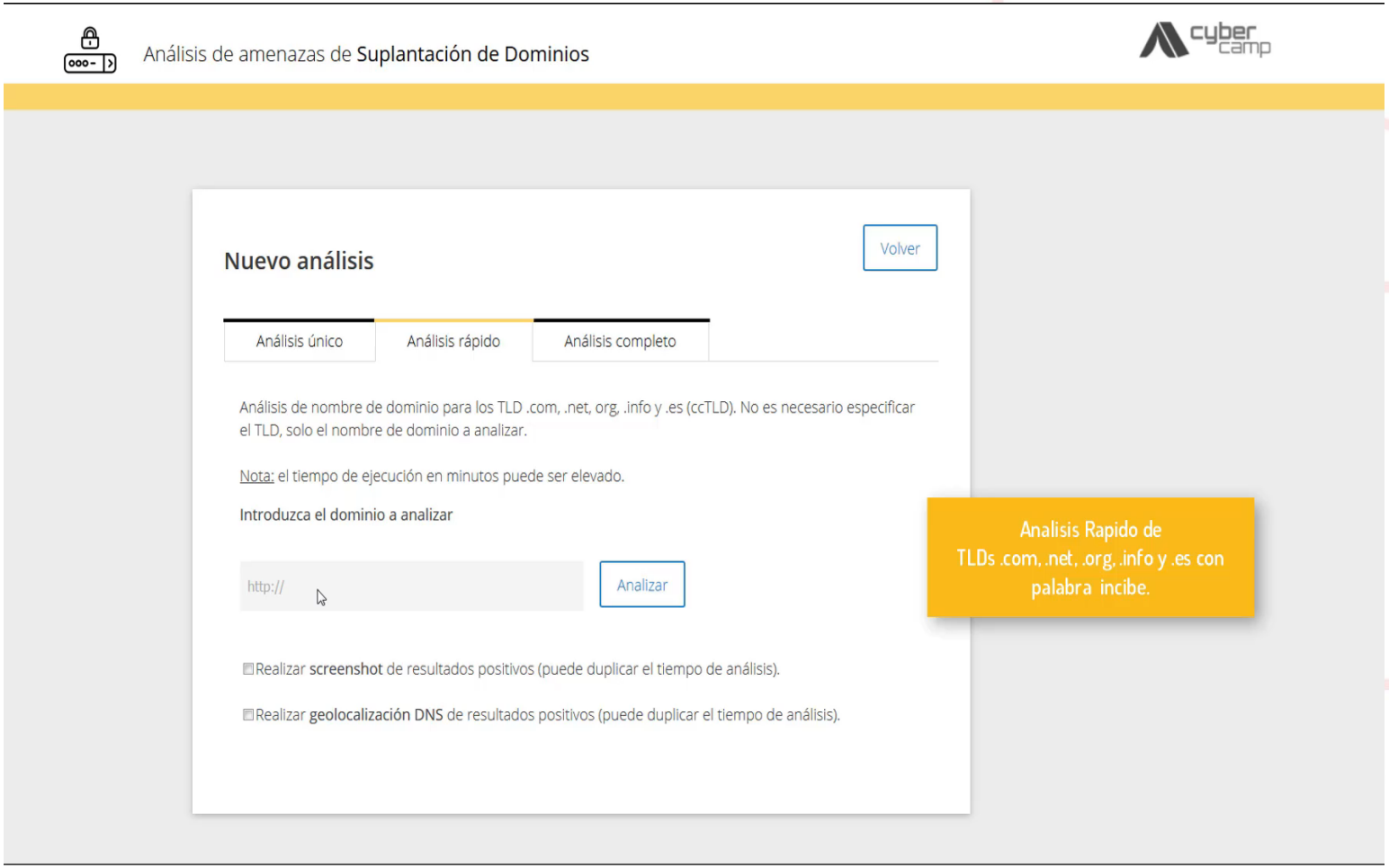
Arquitectura del sistema

Sistema Operativo
Ubuntu Server 16.04.1 LTS

- Ubuntu Server 16.04.1 LTS
- Nginx 1.10.1
- uWSGI 2.0.13.1
- Django 1.10
- Python 2.7.12
- MongoDB Community Edition 3.2.8
  - Colecciones: análisis, resultados, whois …
- Ruby 2.0
- NodeJS 4.2.6
- MariaDB 10.0.26
  - Tabla dominios (.es) + índices



Video / Demo plataforma web



RISP / un ejemplo de búsqueda por dominio…

```
^C(uiserver):u70710359:~/public_html/squatting.es$ cat RISP_OTROS.csv | grep lacaixa.es
"lacaixa.es"|"F          ANCARIA CAIXA D'ESTALVIS I PENSIONS DE BARCELONA, \"LA CAIXA\""|"G58899998"
"fundaciolacaixa.es"|"FUNDACION BANCARIA CAIXA D'ESTALVIS I PENSIONS DE BARCELONA, \"LA CAIXA\""|"G58899998"
"elacaixa.es"|"FUNDACION BANCARIA CAIXA D'ESTALVIS I PENSIONS DE BARCELONA, \"LA CAIXA\""|"G58899998"
"agendacentresobrasociallacaixa.es"|"FUNDACION BANCARIA CAIXA D'ESTALVIS I PENSIONS DE BARCELONA, \"LA CAIXA\""|"G58899998"
"agendacentrosobrasociallacaixa.es"|"FUNDACION BANCARIA CAIXA D'ESTALVIS I PENSIONS DE BARCELONA, \"LA CAIXA\""|"G58899998"
"bancolacaixa.es"|"CAIXA D'ESTALVIS I PENSIONS DE BARCELONA"|"G58899998"
"becarioslacaixa.es"|"FUNDACION BANCARIA CAIXA D'ESTALVIS I PENSIONS DE BARCELONA, \"LA CAIXA\""|"G58899998"
"becarislacaixa.es"|"FUNDACION BANCARIA CAIXA D'ESTALVIS I PENSIONS DE BARCELONA, \"LA CAIXA\""|"G58899998"
"bloglacaixa.es"|"Caixa d´Estalvis i Pensions de Barcelona"|"G58899998"
"contactlesslacaixa.es"|"FUNDACION BANCARIA CAIXA D'ESTALVIS I PENSIONS DE BARCELONA, \"LA CAIXA\""|"G58899998"
"convocatoriaslacaixa.es"|"FUNDACION BANCARIA CAIXA D'ESTALVIS I PENSIONS DE BARCELONA, \"LA CAIXA\""|"G58899998"
"convocatorieslacaixa.es"|"FUNDACION BANCARIA CAIXA D'ESTALVIS I PENSIONS DE BARCELONA, \"LA CAIXA\""|"G58899998"
"e-lacaixa.es"|"FUNDACION BANCARIA CAIXA D'ESTALVIS I PENSIONS DE BARCELONA, \"LA CAIXA\""|"G58899998"
"fblacaixa.es"|"Fundación Bancaria Caixa D´Estalvis i Pensions de Barcelona, \"La Caixa\""|"G58899998"
"fotopreslacaixa.es"|"FUNDACION BANCARIA CAIXA D'ESTALVIS I PENSIONS DE BARCELONA, \"LA CAIXA\""|"G58899998"
"fundaciobancarialacaixa.es"|"Fundación Bancaria Caixa D´Estalvis i Pensions de Barcelona, \"La Caixa\""|"G58899998"
"fundacionbancarialacaixa.es"|"Fundación Bancaria Caixa D´Estalvis i Pensions de Barcelona, \"La Caixa\""|"G58899998"
"fundacionlacaixa.es"|"FUNDACION BANCARIA CAIXA D'ESTALVIS I PENSIONS DE BARCELONA, \"LA CAIXA\""|"G58899998"
"grandespersonaslacaixa.es"|"Fundación Bancaria Caixa d´Estalvis i Pensions de Barcelona \"la Caixa\""|"G58899998"
"granspersoneslacaixa.es"|"Fundación Bancaria Caixa d´Estalvis i Pensions de Barcelona \"la Caixa\""|"G58899998"
"grupasseguradorlacaixa.es"|"Caixa d´Estalvis i Pensions de Barcelona"|"G58899998"
```

▪ ▪ ▪

```
"targetaslacaixa.es"|"CAIXA D´ESTALVIS I PENSIONS DE BARCELONA"|"G58899998"
"tarjetaslacaixa.es"|"CAIXA D´ESTALVIS I PENSIONS DE BARCELONA"|"G58899998"
"voluntarioslacaixa.es"|"FUNDACION BANCARIA CAIXA D'ESTALVIS I PENSIONS DE BARCELONA, \"LA CAIXA\""|"G58899998"
"activitatseducativesfundaciolacaixa.es"|""|""
"bancaprivadalacaixa.es"|""|""
"cajalacaixa.es"|""|""
"engañadosporlacaixa.es"|""|""
"llacaixa.es"|""|""
"particulareslacaixa.es"|""|""
"portal-lacaixa.es"|""|""
"portallacaixa.es"|""|""
"viviendapensionlacaixa.es"|""|""
"wwlacaixa.es"|""|""
"www-lacaixa.es"|""|""
"wwwlacaixa.es"|""|""
"wwwwlacaixa.es"|""|""
```

RISP / un ejemplo de búsqueda por CIF…

```
(uiserver):u70710359:~/public_html/squatting.es$ cat RISP_OTROS.csv | grep G58899998
"lacaixa.e          ION BANCARIA CAIXA D'ESTALVIS I PENSIONS DE BARCELONA, \"LA CAIXA\""|"G58899998"
"caixagirona.es"|"Fundación Bancaria Caixa d´Estalvis i Pensions de Barcelona \"la Caixa\""|"G58899998"
"segurcaixa.es"|"Caixa d´estalvis i Pensions de Barcelona"|"G58899998"
"lacaixaoberta.es"|"FUNDACION BANCARIA CAIXA D'ESTALVIS I PENSIONS DE BARCELONA, \"LA CAIXA\""|"G58899998"
"agencaixa.es"|"Caixa d´Estalvis i Pensions de Barcelona"|"G58899998"
"fundaciolacaixa.es"|"FUNDACION BANCARIA CAIXA D'ESTALVIS I PENSIONS DE BARCELONA, \"LA CAIXA\""|"G58899998"
"elacaixa.es"|"FUNDACION BANCARIA CAIXA D'ESTALVIS I PENSIONS DE BARCELONA, \"LA CAIXA\""|"G58899998"
"bancoeuropa.es"|"FUNDACION BANCARIA CAIXA D'ESTALVIS I PENSIONS DE BARCELONA, \"LA CAIXA\""|"G58899998"
"rentcaixa.es"|"Caixa d´Estalvis i Pensions de Barcelona"|"G58899998"
"cosmocaixa.es"|"FUNDACION BANCARIA CAIXA D'ESTALVIS I PENSIONS DE BARCELONA, \"LA CAIXA\""|"G58899998"
"1acaixa.es"|"CAIXA D'ESTALVIS I PENSIONS DE BARCELONA"|"G58899998"
"1lineaabierta.es"|"CAIXA D'ESTALVIS I PENSIONS DE BARCELONA"|"G58899998"
```

▪ ▪ ▪

```
"vidacaixaprevisiosocial.nom.es"|"Caixa d´Estalvis i Pensions de Barcelona"|"G58899998"
"vidacaixaprevisiosocial.org.es"|"Caixa d´Estalvis i Pensions de Barcelona"|"G58899998"
"vidacaixaps.com.es"|"Caixa d´Estalvis i Pensions de Barcelona"|"G58899998"
"vidacaixaps.es"|"Caixa d´Estalvis i Pensions de Barcelona"|"G58899998"
"vidacaixaps.nom.es"|"Caixa d´Estalvis i Pensions de Barcelona"|"G58899998"
"vidacaixaps.org.es"|"Caixa d´Estalvis i Pensions de Barcelona"|"G58899998"
"vidacaixasalud.es"|"Caixa d´Estalvis i Pensions de Barcelona"|"G58899998"
"vidacaixasalut.es"|"Caixa d´Estalvis i Pensions de Barcelona"|"G58899998"
"vidacaixavida.com.es"|"Caixa d´Estalvis i Pensions de Barcelona"|"G58899998"
"vidacaixavida.es"|"Caixa d´Estalvis i Pensions de Barcelona"|"G58899998"
"vidacaixavida.nom.es"|"Caixa d´Estalvis i Pensions de Barcelona"|"G58899998"
"vidacaixavida.org.es"|"Caixa d´Estalvis i Pensions de Barcelona"|"G58899998"
"voluntarioslacaixa.es"|"FUNDACION BANCARIA CAIXA D'ESTALVIS I PENSIONS DE BARCELONA, \"LA CAIXA\""|"G58899998"
(uiserver):u70710359:~/public_html/squatting.es$ cat RISP_OTROS.csv | grep G58899998 | wc -l
356
```

Distancia de Levenshtein

- La distancia de Levenshtein, distancia de edición o distancia entre palabras es el número mínimo de operaciones requeridas para transformar una cadena de caracteres en otra, se usa ampliamente en teoría de la información y ciencias de la computación.

- Se entiende por operación, bien una inserción, eliminación o la sustitución de un carácter. Esta distancia recibe ese nombre en honor al científico ruso Vladimir Levenshtein, quien se ocupó de esta distancia en 1965. útil para determinar cuán similares son dos cadenas de caracteres.

- Por ejemplo, la distancia de Levenshtein entre "casa" y "calle" es de 3 porque se necesitan al menos tres ediciones elementales para cambiar uno en el otro.

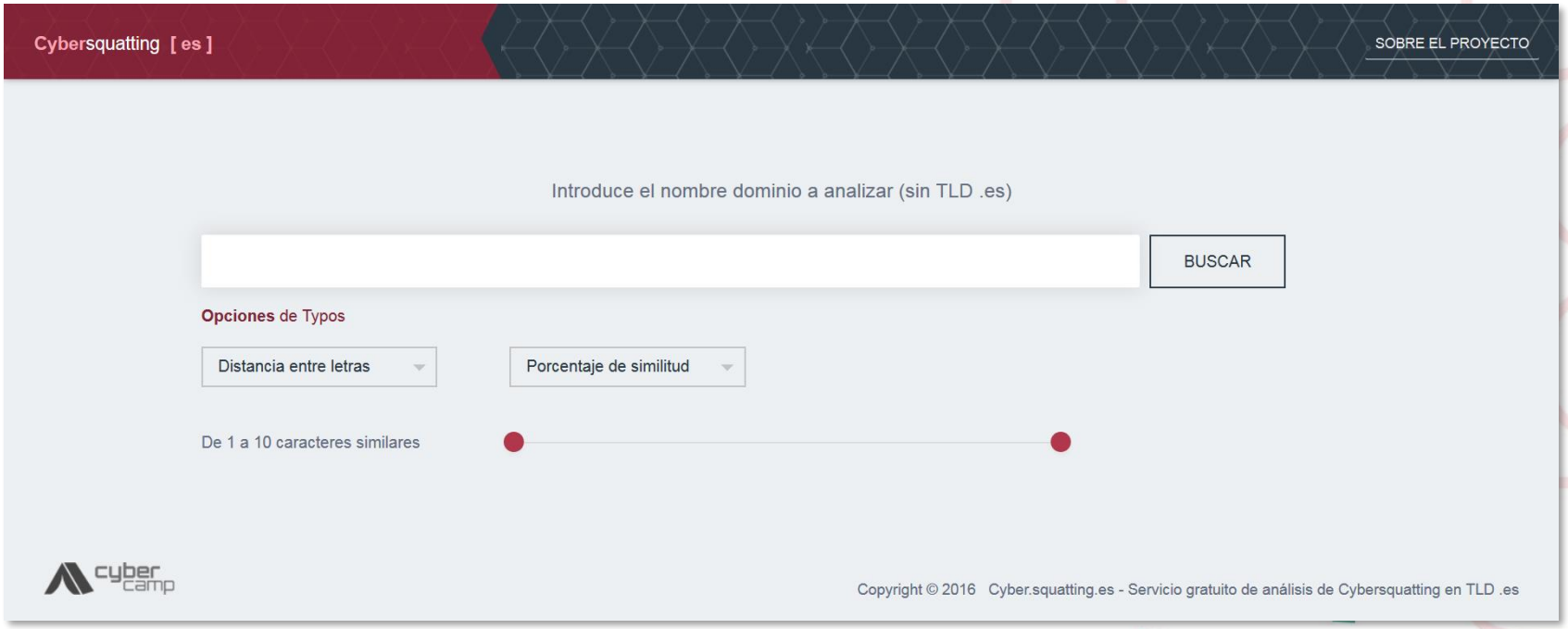
  - casa → cala (sustitución de 's' por 'l').
  - cala → calla (inserción de 'l' entre 'l' y 'a').
  - calla → calle (sustitución de 'a' por 'e').

Distancia de Levenshtein

	Levenshtein	Caracteres iguales	Longitud	Similitud %
lacaixa.es	0	7	7	100%
lacaixa.com.es	0	7	7	100%
lacaixa.nom.es	0	7	7	100%
lacaixa.org.es	0	7	7	100%
elacaixa.es	1	7	8	93.33%
1acaixa.es	1	6	7	85.71%
elacaixa.com.es	1	7	8	93.33%
lacavita.es	2	6	8	80%
...	..	..	..	..
lacaña.es	2	5	7	71.43%
laciaxa.es	2	6	7	85.71%
lacika.es	2	4	6	61.54%
laixa.es	2	5	5	83.33%
wwlacaixa.es	2	7	9	87.5%

Bonus / Squatting.es

Buscador de libre acceso para localizar amenazas en dominios.es



http://cyber.squatting.es

Siguientes pasos

- Optimizar el proceso.
- Alertas al email.
- Módulo de Bitsquatting.
- Módulo de investigación.
  - Localización IP Reverse / MX / NS
- Histórico de información de dominios.
- Módulo de screenshots de dominios.
- Exportación de resultados en PDF, CSV.
- Sistema API de consultas.
- Otras sugerencias y peticiones.

¿Preguntas? ¡Comentarios!

Canal de Telegram

https://telegram.me/CyberSquatting

Hashtag

#CyberSquattingDotES

Gracias por su atención

cyber camp
CYBERSECURITY EVENT
2016

GOBIERNO DE ESPAÑA
MINISTERIO DE ENERGÍA, TURISMO Y AGENDA DIGITAL

incibe_
2006-2016
TRABAJANDO POR LA CONFIANZA DIGITAL