



— GRUPO ZERO LYNX —



@jantonioCalles

OSINT

Inteligencia de fuentes abiertas

\$>Whoami

Juan Antonio Calles (@jantonioCalles)

- CEO de [Grupo Zerolynx](#)
- CSO de [Osane Consulting](#)
- Doctor, doble postgrado e ingeniero en informática por la URJC
- Co-fundador de Flu Project y X1RedMasSegura



¿Qué es la Ciberinteligencia?

- La ciberinteligencia es un término que ha sido acuñado para hacer referencia a las labores de inteligencia que requieren o tienen como destino el uso de sistemas de información. Su objetivo principal es el de recolectar y analizar datos, para generar información de valor que ayude a contestar una serie de cuestiones planteadas.
- Generalmente, la ciberinteligencia es utilizada en el mundo empresarial para identificar datos o **archivos exfiltrados**, localizar a **detractores de las marcas**, o alertar de la posible perpetración de un **ataque cibernético**.
- Al final, el valor en la inteligencia es poder extraer una gran cantidad de datos, correlarlos y analizarlos en tiempo y forma, para poder obtener información de valor que nos permita contestar esas preguntas que antes comentábamos.

El secreto está “en las fuentes”



Fuentes de inteligencia

- HUMINT: fuentes humanas
- SIGINT / ELINT: señales eléctricas
- GEOINT: información geoespacial
- COMINT: interceptación de comunicaciones
- OSINT: fuentes abiertas



Ciclo de inteligencia



Lo primero será “protegernos”



Hay que forjarse identidades digitales anónimas

- www.10minutemail.com | <https://www.minuteinbox.com/> | [mail2tor2zyjdctd.onion/squirrelmail/](mailto:mail2tor2zyjdctd.onion@squirrelmail.com) | protonmail.com
- <https://www.torproject.org/>
- <https://thispersondoesnotexist.com/>
- VPN:
 - CyberGhost
 - ExpressVPN
 - NordVPN
 - Surfshark
 - PureVPN
 - PrivateVPN



Los buscadores y sus potentes expresiones de búsqueda



Google Hacking

- **site:** permite listar toda la información de un dominio concreto.
- **ext:** permite buscar archivos de un formato determinado, por ejemplo pdfs, rdp (de escritorio remoto), imágenes png, jpg, etc. para obtener información EXIF y un largo etcétera.
- **intitle:** permite buscar páginas con ciertas palabras en el campo title.
- **inurl:** permite buscar páginas con palabras concretas en la URL.
- Interesante buscar frases tipo “**index of**” para encontrar listados de archivos de ftps, “**mysql server has gone away**” para buscar sitios web vulnerables a inyecciones SQL en Mysql, etc.

Google Hacking

- “*@empresa.com”: Emails/cuentas de dominio de empleados
- `ext:rdp screen`: Nos permitirá localizar archivos RDP (Remote Desktop Protocol), para conectarnos a Terminal Services y que podremos utilizar en la fase de fingerprint para obtener más información
- `ext:log ip`: Nos permitirá localizar archivos de logs.
- `ext:ini inurl:"/Desktop.ini"`: Nos permitirá listar carpetas Windows expuestas
- `inurl:"dominio:8080"` Con el que localizaremos aplicaciones tras puertos concretos

Google Hacking

- **ext:ovpn "C:\\" client:** Expone archivos de configuración de Open VPN alojados en la unidad C: de un sistema.
- **ext:sql:** Nos permitirá localizar archivos con instrucciones SQL
- **ext:sql user password:** Recuperando credenciales
- **ext:db "select *":** Profundizando en queries más concretas de selección
- **ext:sql "create table":** Recuperando la creación de tablas

Google Hacking

- `inurl:"readme.html" ext:html intitle:wordpress`: Buscando wordpress en Internet
- `inurl:wp-admin -site:wordpress.* "Parent Directory"`: Buscando el código fuente
- `inurl:bash_history mysql "-u"`: Historiales de bash
- `inurl:bash_history scp "/home"`: Carpetas Home indexadas en comandos scp
- `inurl:bash_history scp "/root"`: Carpetas del usuario Root

Google Hacking

- `inurl:bash_history scp "/var/www"`: Carpetas de Apache
- `inurl:bash_history "*.sql"`: archivos sql listados en historiales
- `ext:ica wfclient applicationserver`: archivos de conexión a sistemas citrix
- `ext:txt inurl:robots`: ¿qué ocultan las organizaciones en el fichero robots.txt?
- `ext:pdf intitle:"documents and settings"`: Rutas Windows expuestas

Google Hacking

- "apache/1.3.27 server" "port 80": buscando versiones de un servidor

Not Found

The requested URL

Apache/1.3.27 Serv

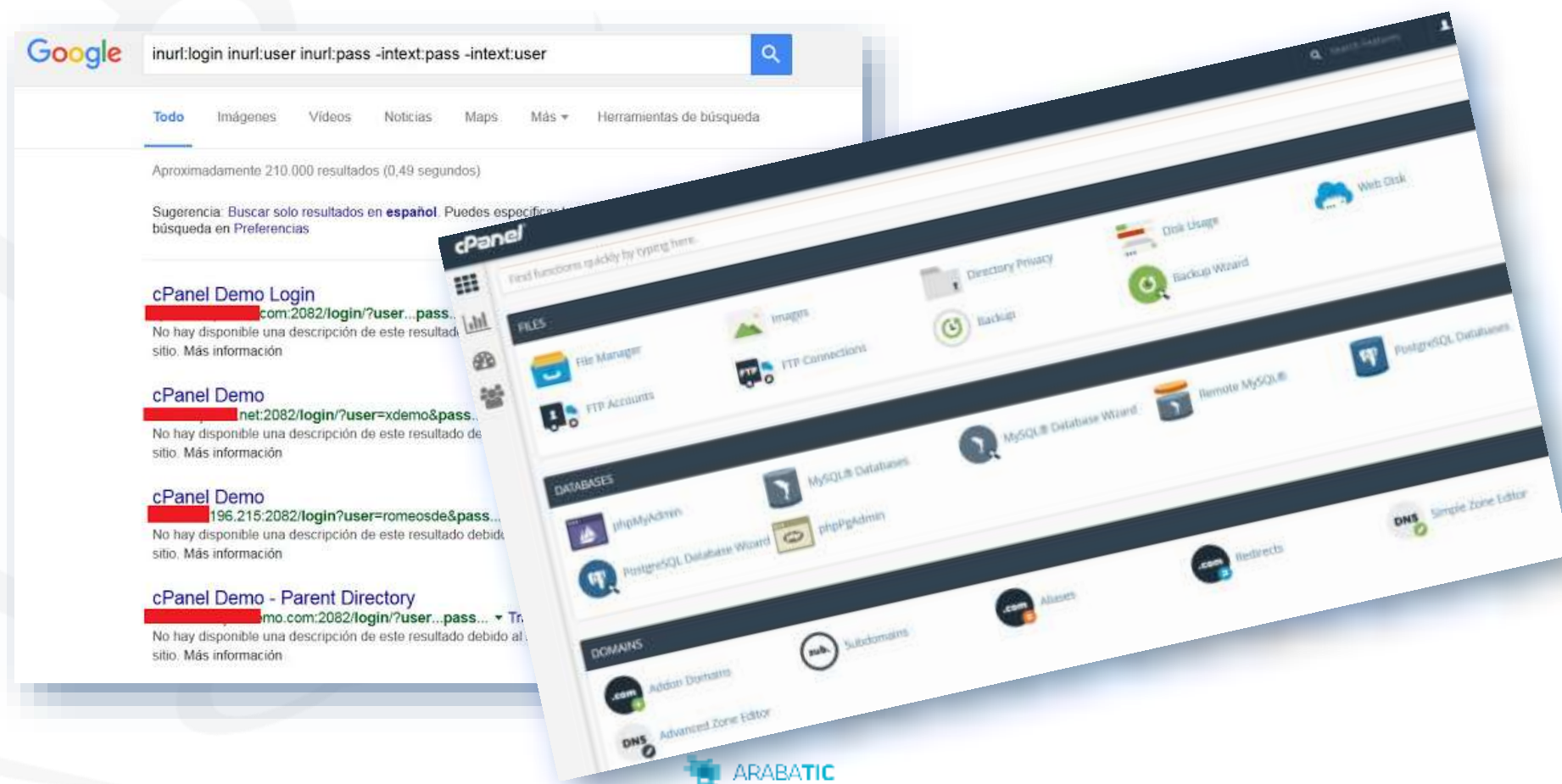
Server Error

404 - File or directory not found.

The resource you are looking for might have been removed, had its name changed, or is temporarily unavailable.

Google Hacking

- `inurl:login inurl:?user intitle:main inurl:pass intitle:cpanel`



Google Hacking

- inurl:phpmyadmin "information_schema" filetype:php

Google search results for the query: `inurl:phpmyadmin "information_schema" filetype:php`

Aproximadamente 14.300 resultados (0,39 segundos)

Sugerencia: Buscar solo resultados en **español**. Puedes especificar tu búsqueda en Preferencias

Search results include:

- [file.com / db503580807.db.1and1.com ...](#)
- [com/phpMyAdmin/index.php?...info...](#)
- [information_schema.VIEWS running on localhost ...](#)
- [bank.com / localhost / information_schema ...](#)
- [information_schema running on localhost - phpMyAdmin 2.5...](#)

The phpMyAdmin interface shows the following table structure for the `information_schema` database:

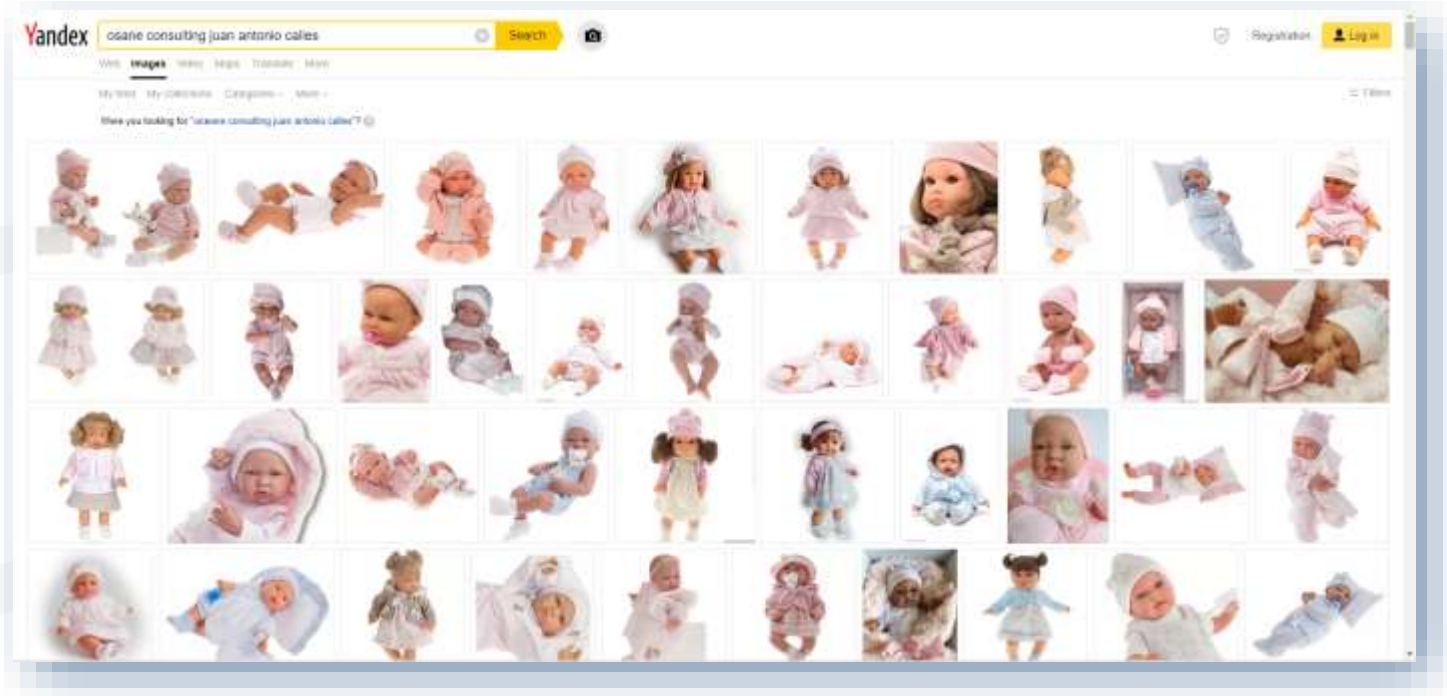
TABLE_CATALOG	TABLE_SCHEMA	TABLE_NAME	PARTITION
NULL	information_schema	CHARACTER_SETS	NULL
NULL	information_schema	COLLATIONS	NULL
NULL	information_schema	COLLATION_CHARACTER_SET_APPLICABILITY	NULL
NULL	information_schema	COLUMNS	NULL
NULL	information_schema	COLUMN_PRIVILEGES	NULL
NULL	information_schema	ENGINES	NULL
NULL	information_schema	EVENTS	NULL
NULL	information_schema	FILES	NULL
NULL	information_schema	GLOBAL_STATUS	NULL
NULL	information_schema	GLOBAL_VARIABLES	NULL
NULL	information_schema	KEY_COLUMN_USAGE	NULL

Bing Hacking

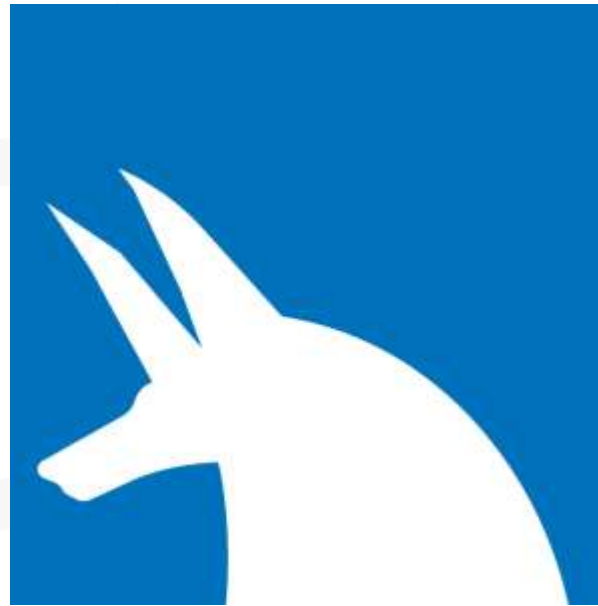
- **Domain:** ayuda a identificar subdominios
- **IP:** permite buscar sitios alojados tras una dirección IP

Otros buscadores

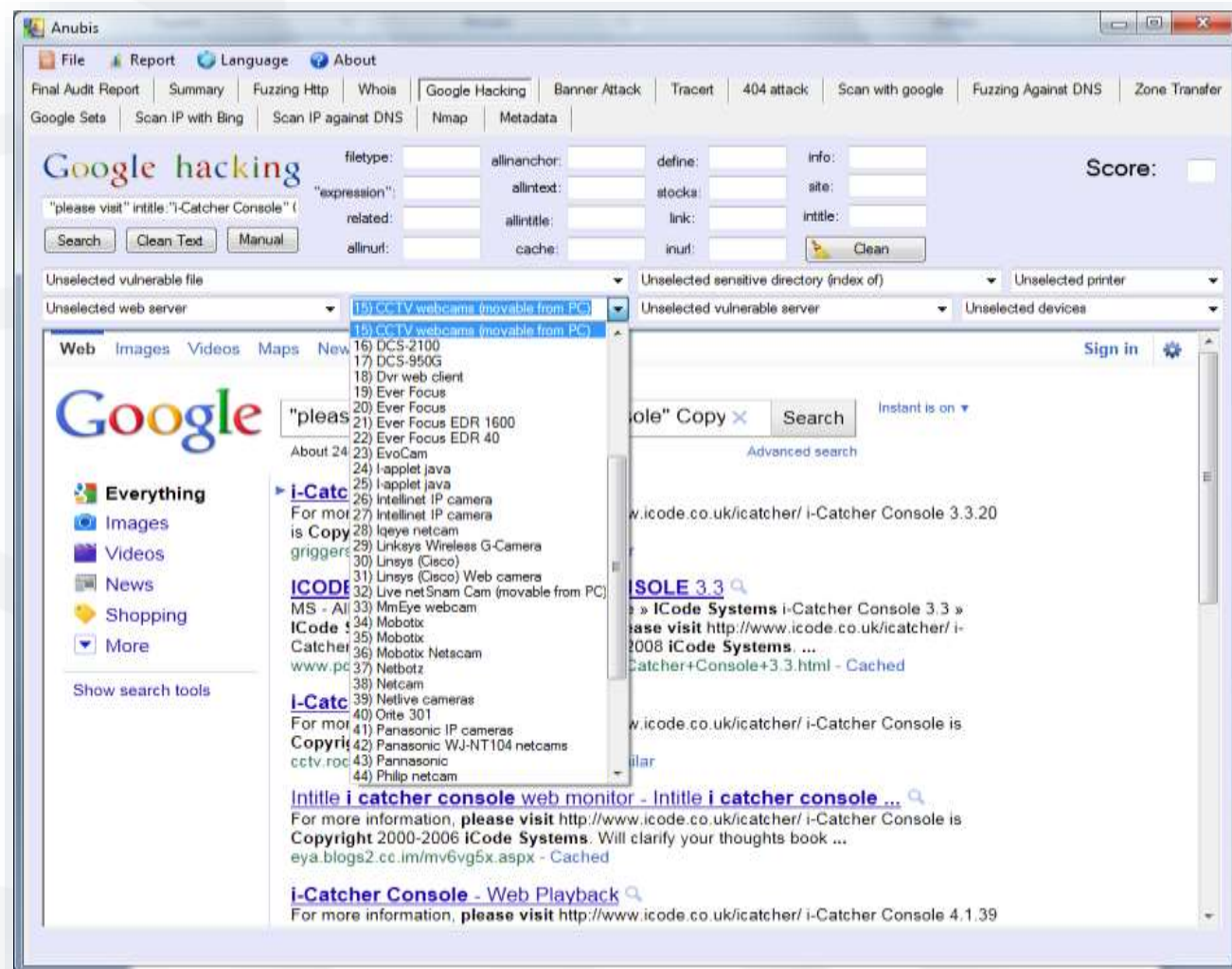
- <https://yandex.com/>
- <https://www.exalead.com/search/>
- <https://duckduckgo.com/>
- <https://www.baidu.com/>
- <https://scholar.google.es/>



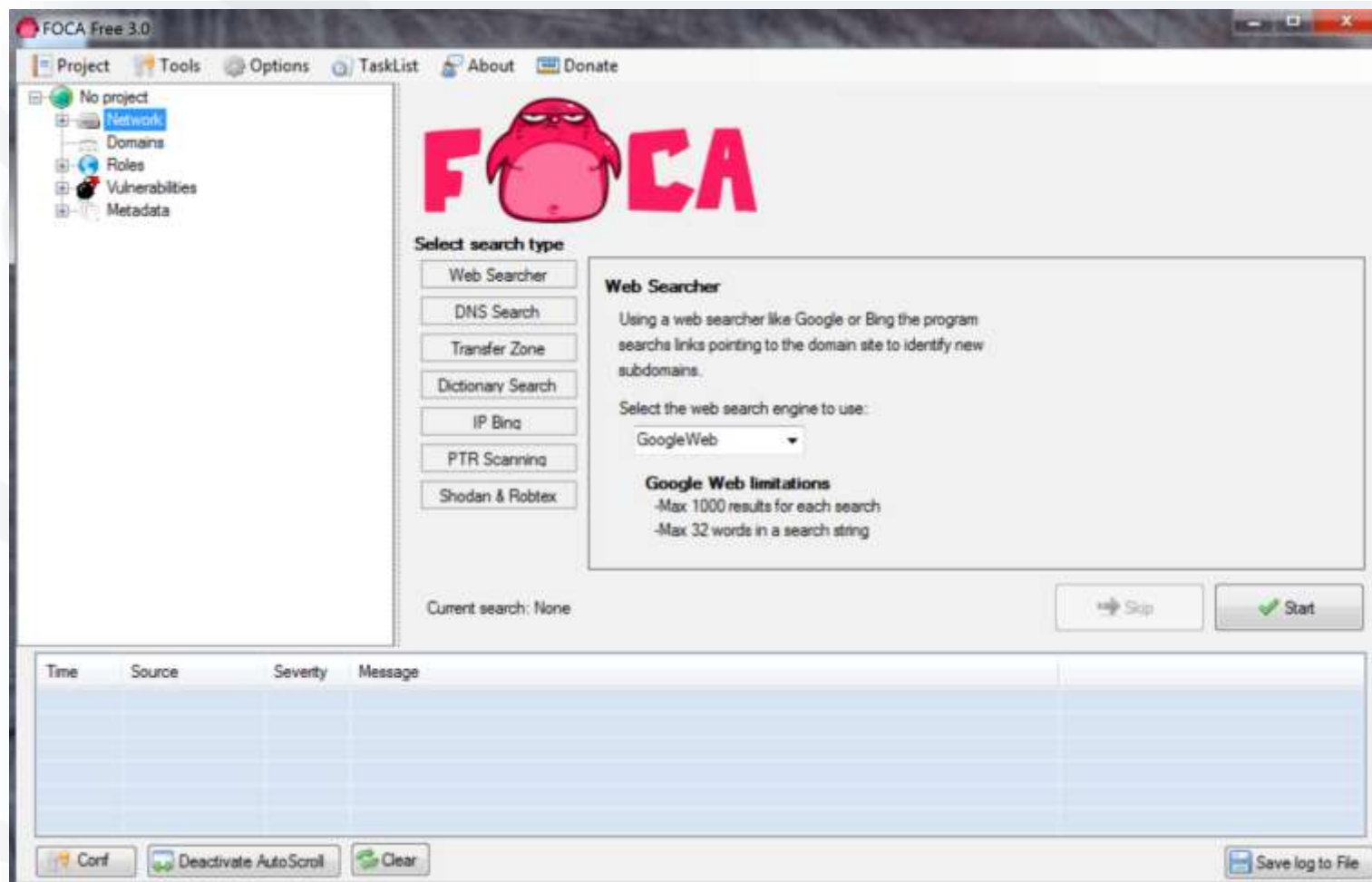
Herramientas para automatizar el hacking con buscadores



Anubis: *cámaras, impresoras, ...*



Foca: *extrayendo metadatos de documentos*

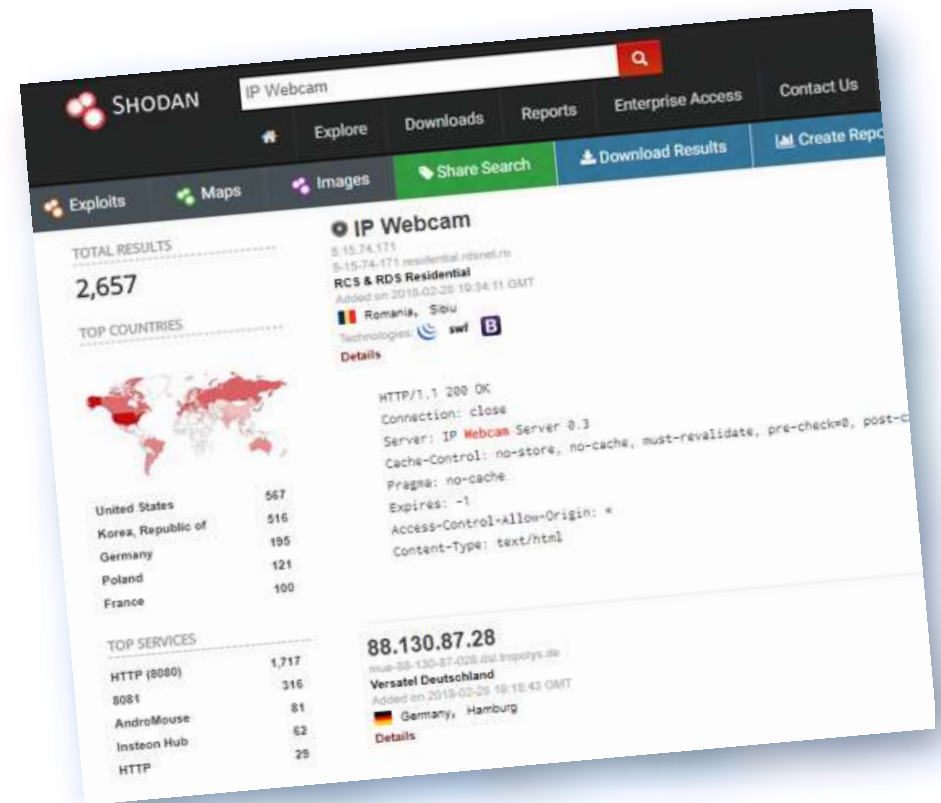


Buscadores de activos expuestos



Shodan

- Es un motor de búsqueda pero a diferencia de Google o Bing se encarga de indexar a nivel de servicio y puerto y no solo el servicio web.
- También tiene filtros avanzados.
- Web: <https://www.shodan.io>



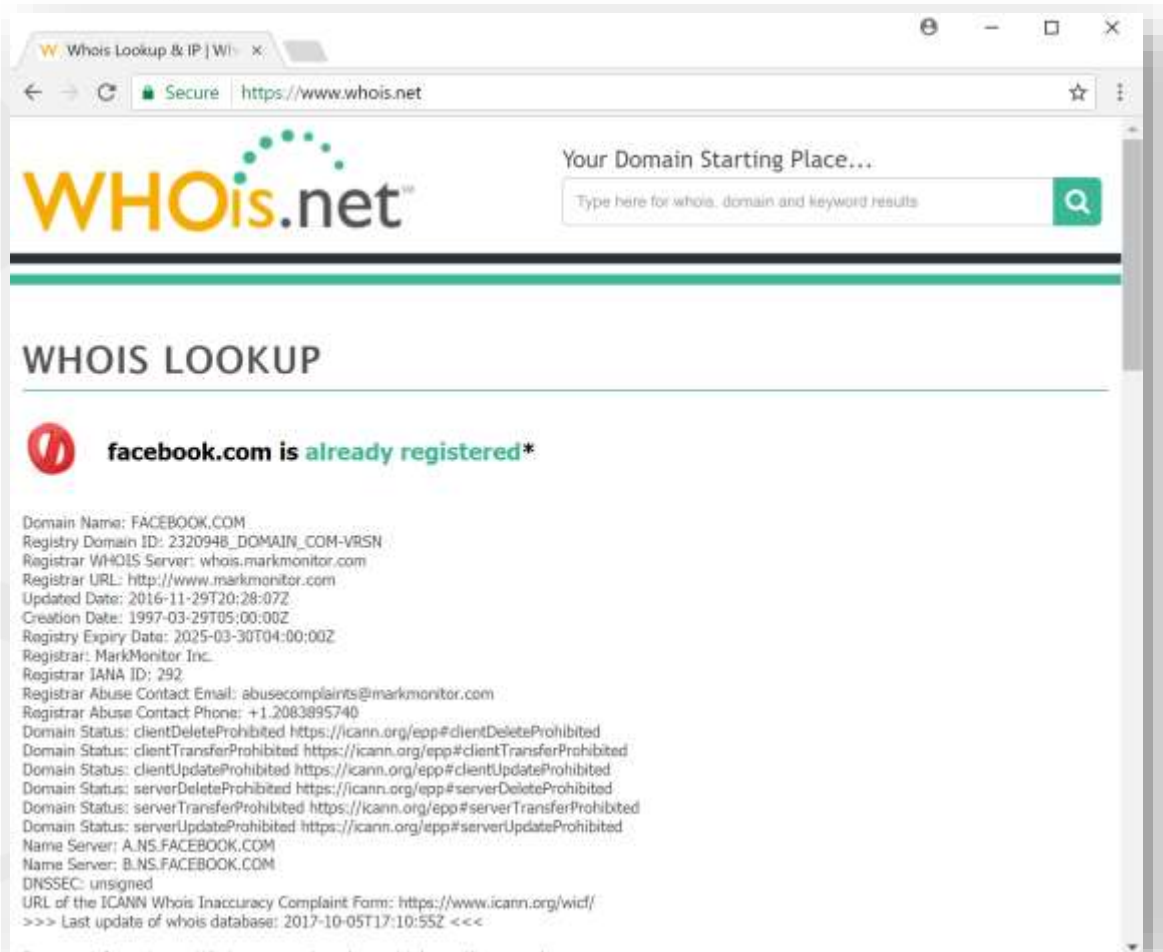
Shodan

- **country:** Permite filtrar por sistemas publicados en país en concreto.
- **city:** Filtrar por ciudad en la que se encuentra un sistema.
- **geo:** Puedes afinar más aún la búsqueda por las coordenadas de latitud y longitud.
- **port:** Permite hacer búsqueda por el puerto específico.
- **net:** Realiza una búsqueda por una IP específica o por rangos de IP.
- **os:** Búsqueda basada en el sistema operativo.
- **hostname:** Realiza una búsqueda que coincida con el nombre del host.
- **before/after:** Limita la búsqueda a un periodo concreto.

Extracción de datos sobre dominios/IPs de organizaciones



Whois, ¿quién ha registrado un dominio?

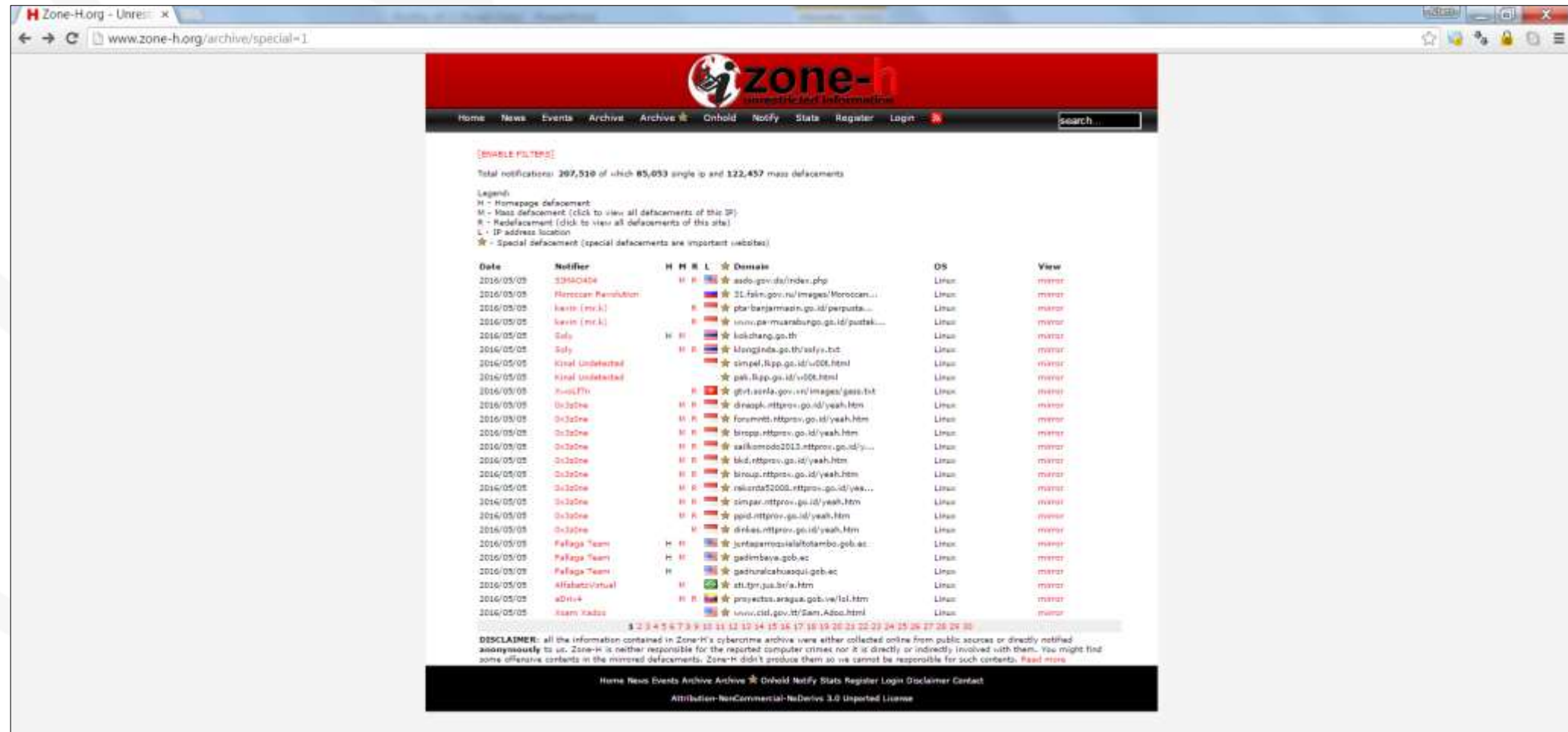


Archive.org

- Historia de un sitio web
- Web: <https://web.archive.org/>

WayBackMachine

Zone-h



The screenshot shows the Zone-H.org website interface. The browser address bar displays "www.zone-h.org/archive/special=1". The website has a red header with the "zone-h" logo and navigation links: Home, News, Events, Archive, Archive (selected), Onhold, Notify, Stats, Register, Login, and a search bar. Below the header, there is a "Legend" section explaining the symbols used in the table: H for Homepage defacement, M for Mass defacement, R for Redefacement, L for IP address location, and a star for Special defacements. The main content is a table with columns: Date, Notifier, H, M, R, L, Domain, OS, and View. The table lists various defacement incidents, including those on Moroccan Revolution, kwin (mr.k), kwin (mr.k), Solo, Kinal Undetected, Kinal Undetected, Kwin (mr.k), dnapk, foremnt, biropg, saikomodo2013, bld, binou, rikorda2000, simpar, poid, dnas, Palaga Team, gadimbaya, gadunicalhuasqui, AlfabatoVirtual, aDri4, and Sam Xadso. The table is paginated, showing 30 items per page. A disclaimer at the bottom states that Zone-H is not responsible for the reported computer crimes and that the information is collected from public sources or directly notified. The footer includes navigation links and a license notice: Attribution-NonCommercial-NoDerivs 3.0 Unported License.

Date	Notifier	H	M	R	L	Domain	OS	View
2016/05/05	33560454	H				asdo.gov.da/index.php	Linux	mirror
2016/05/05	Moroccan Revolution					3L-fslm.gov.nu/images/Moroccan...	Linux	mirror
2016/05/05	kwin (mr.k)					parbanjarmasin.go.id/perpustakaan...	Linux	mirror
2016/05/05	kwin (mr.k)					univ.parmuanaburgo.go.id/pustak...	Linux	mirror
2016/05/05	Solo	H				lokichang.go.th	Linux	mirror
2016/05/05	Solo	H				longinda.go.th/saiys.txt	Linux	mirror
2016/05/05	Kinal Undetected					simpel.kpp.go.id/v001.html	Linux	mirror
2016/05/05	Kinal Undetected					pel.kpp.go.id/v001.html	Linux	mirror
2016/05/05	Kwin (mr.k)					gtrt.asia.gov.vn/images/gaoi.txt	Linux	mirror
2016/05/05	0x3a0ne	H				dnapk.nttpro.go.id/yeah.htm	Linux	mirror
2016/05/05	0x3a0ne	H				foremnt.nttpro.go.id/yeah.htm	Linux	mirror
2016/05/05	0x3a0ne	H				biropg.nttpro.go.id/yeah.htm	Linux	mirror
2016/05/05	0x3a0ne	H				saikomodo2013.nttpro.go.id/y...	Linux	mirror
2016/05/05	0x3a0ne	H				bld.nttpro.go.id/yeah.htm	Linux	mirror
2016/05/05	0x3a0ne	H				binou.nttpro.go.id/yeah.htm	Linux	mirror
2016/05/05	0x3a0ne	H				rikorda2000.nttpro.go.id/yea...	Linux	mirror
2016/05/05	0x3a0ne	H				simpar.nttpro.go.id/yeah.htm	Linux	mirror
2016/05/05	0x3a0ne	H				poid.nttpro.go.id/yeah.htm	Linux	mirror
2016/05/05	0x3a0ne	H				dnas.nttpro.go.id/yeah.htm	Linux	mirror
2016/05/05	Palaga Team	H				jeritagamozialatotambo.gov.ac...	Linux	mirror
2016/05/05	Palaga Team	H				gadimbaya.gob.ac	Linux	mirror
2016/05/05	Palaga Team	H				gadunicalhuasqui.gob.ac	Linux	mirror
2016/05/05	AlfabatoVirtual	H				atttpr.jus.br/a.htm	Linux	mirror
2016/05/05	aDri4	H				proyectos.aragaa.gov.ve/ol.htm	Linux	mirror
2016/05/05	Sam Xadso	H				www.ctd.gov.br/Sam_Adoc.html	Linux	mirror

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30

DISCLAIMER: all the information contained in Zone-H's cybercrime archive were either collected online from public sources or directly notified anonymously to us. Zone-H is neither responsible for the reported computer crimes nor it is directly or indirectly involved with them. You might find some offensive contents in the mirrored defacements. Zone-H didn't produce them so we cannot be responsible for such contents. [Read more](#)

Home News Events Archive Archive Onhold Notify Stats Register Login Contact

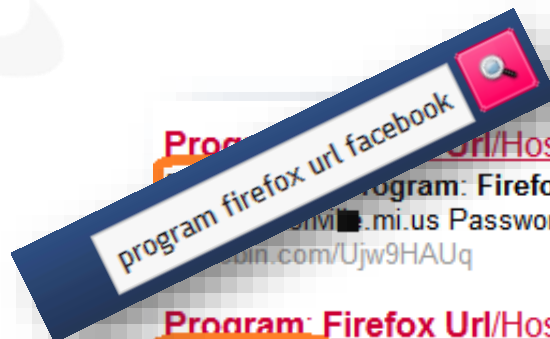
Attribution-NonCommercial-NoDerivs 3.0 Unported License

Sitios web de “pegado” de contenidos



Pastes

- <http://pastebin.com>



Program: Firefox Url/Host: <http://apps.facebook.com/...>
25 Jul 2010 ...
Program: Firefox Url/Host: <https://login.facebook.com/>
antare@hotmail.com Password: [REDACTED] Computer: [REDACTED]
pastebin.com/jX5dUXau

Program: Firefox Url/Host: <https://login.facebook.com/>
25 Jul 2010 ...
Program: Firefox Url/Host: <https://login.facebook.com/>
antare@hotmail.com Password: [REDACTED] Computer: [REDACTED]
pastebin.com/jX5dUXau

Program: Firefox Url/Host: <http://www.facebook.com/>

29 Aug 2010 ...
Program: Firefox Url/Host: <http://www.facebook.com/> Login:
nitro[REDACTED]@gmail.com Password: [REDACTED] Computer: [REDACTED] N-PC ...
pastebin.com/WcJLGHw

Program: Firefox Url/Host: <http://infernaltacker.com/>

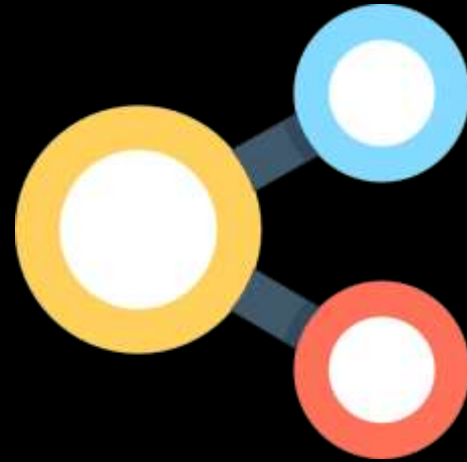
30 Jan 2011 ...
Program: Firefox Url/Host: <http://www.facebook.com/> Login:
[REDACTED]gontaru@yahoo.com Password: [REDACTED] Computer: [REDACTED] n-PC ...
pastebin.com/QvXK0k9j

Program: Firefox Url/Host: <http://www.pla...>

19 Jan 2011 ...
Program: Firefox Url/Host: <http://www.facebook.com/> Login:
[REDACTED]@hotmail.com Password: [REDACTED] Computer: [REDACTED] C. Date: Dump 15:31:29 ...
pastebin.com/RqXtctkf

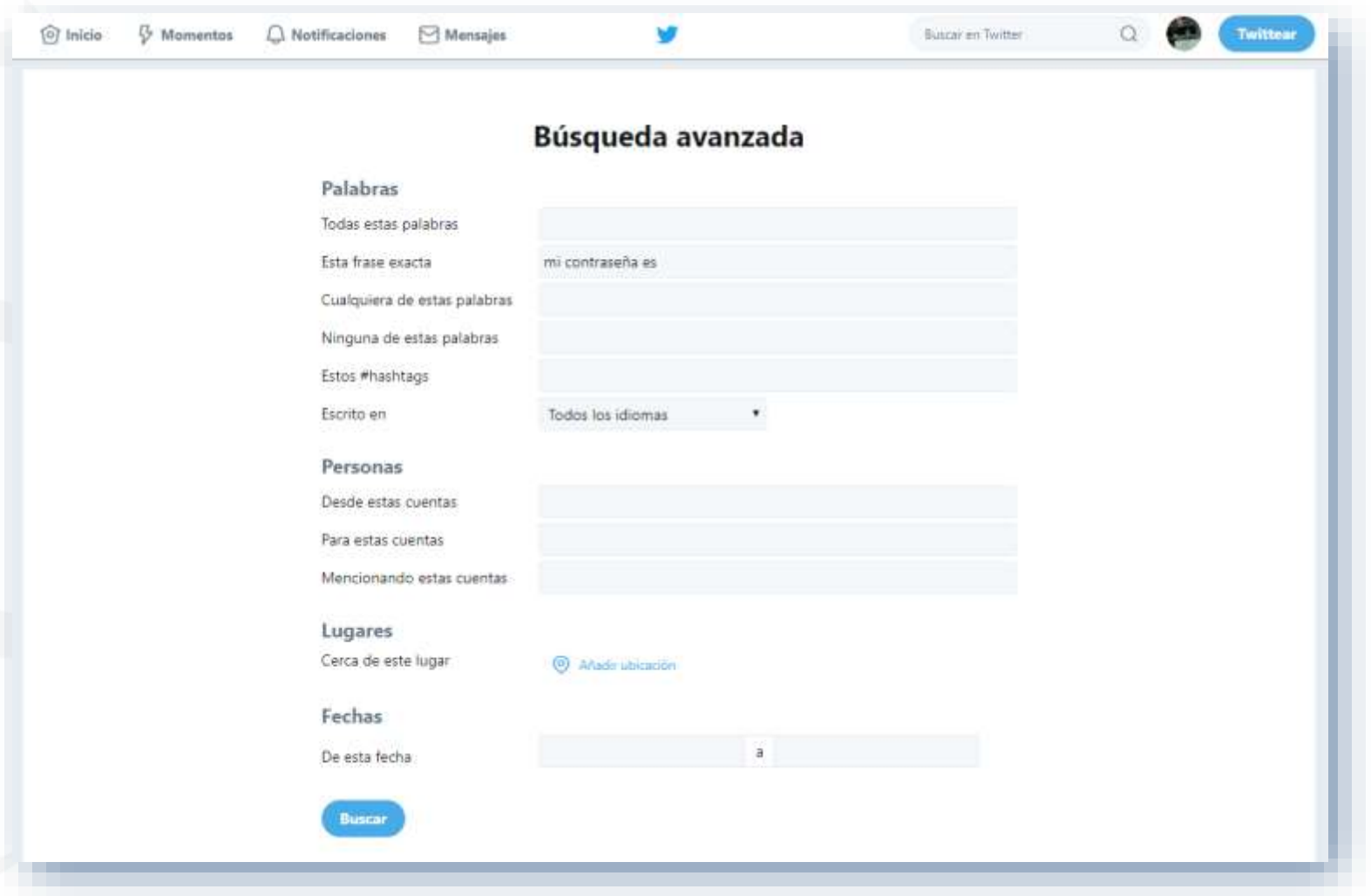


Búsquedas principales en redes sociales



Twitter

- Twitter:
 - <https://twitter.com/search-advanced>



The screenshot shows the Twitter 'Búsqueda avanzada' (Advanced Search) page. The interface is in Spanish and includes a navigation bar at the top with links to 'Inicio', 'Momentos', 'Notificaciones', and 'Mensajes'. A search bar at the top right contains the text 'Buscar en Twitter' and a magnifying glass icon. The main content area is titled 'Búsqueda avanzada' and is divided into several sections for filtering search results:

- Palabras** (Words):
 - Todas estas palabras (All these words)
 - Esta frase exacta (This exact phrase)
 - Cualquiera de estas palabras (Any of these words)
 - Ninguna de estas palabras (None of these words)
 - Estos #hashtags (These #hashtags)
 - Escrito en (Written in): A dropdown menu showing 'Todos los idiomas' (All languages).
- Personas** (People):
 - Desde estas cuentas (From these accounts)
 - Para estas cuentas (For these accounts)
 - Mencionando estas cuentas (Mentioning these accounts)
- Lugares** (Locations):
 - Cerca de este lugar (Near this location): A button labeled 'Añadir ubicación' (Add location).
- Fechas** (Dates):
 - De esta fecha (From this date): Two date input fields separated by 'a' (to).

A blue 'Buscar' (Search) button is located at the bottom of the form.

Twitter

- Es recomendable construir una lista de personas “clave” para nuestra labor de Inteligencia.
- Fuentes como Maldito Bulo, serán de mucha utilidad para evitar las Fake News y confiar en fuentes fiables:

- <https://twitter.com/malditobulo>



Instagram

- Instagram:
 - <https://web.stagram.com/search>
 - <https://storiesig.com/?username=ronaldo>

IntelTechniques

- Dispone de un conjunto de herramientas orientadas a OSINT.
- Se encuentran categorizadas según la fuente.
- Web: <https://inteltechniques.com>

INTELTECHNIQUES
By Michael Bazzell




OSINT TRAINING
PRIVACY CONSULTING
DIGITAL SECURITY

Búsquedas de Phishings



Phishtank

 **PhishTank**®

Out of the Net, into the Tank.

[Home](#) [Add A Phish](#) [Verify A Phish](#) [Phish Search](#) [Stats](#) [FAQ](#) [Developers](#) [Mailing Lists](#) [My Account](#)

cleanmx MODERATOR

Real Name: Gerhard W. Recher

Website: <http://www.clean-mx.de>

Member Since: Nov 7th 2005

cleanmx has submitted **2,682,887** and verified **85,478** phishes.

Last 5 Submissions → [view all](#)

ID	Phish URL	Submitted
5793275	http://datascope.cl/bacc/c1d1b565580d5775eb14a413f31dfc?login=&... added on Sep 24th 2016 5:46 PM	by cleanmx
5793274	https://mijn-evaluabe.nl/mijn.ica/Mijn%20ICS%20Validatie.php... added on Sep 24th 2016 5:46 PM	by cleanmx
5793273	https://mijn-evaluabe.nl/mijn.ics/Mijn%20ICS%20Gegevens.php... added on Sep 24th 2016 5:45 PM	by cleanmx
5793272	https://mijn-evaluabe.nl/mijn.ics/ added on Sep 24th 2016 5:45 PM	by cleanmx
5793271	http://realisemagic.net/comcast/ added on Sep 24th 2016 5:43 PM	by cleanmx

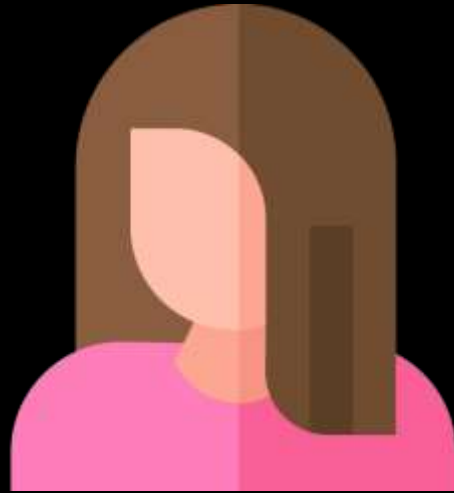
Last 5 Verifications → [view all](#)

ID	Phish URL	Submitted
5325414	https://sites.google.com/site/info2213997g/ added on Oct 23rd 2017 5:24 PM	by sofeix
5325887	http://sonzidane.com/de/index.php/ added on Nov 14th 2017 2:12 PM	by 0x0f0d0d0d
5325891	http://sparkasse-filiale.service-filiale-sicherheit.info/de/login-on... added on Nov 14th 2017 2:12 PM	by 0x0f0d0d0d
5334720	https://www.fidoc.de added on Nov 15th 2017 10:32 AM	by comodo
5689545	http://https://www.opendns.com/ added on Jun 8th 2018 6:58 PM	by Carson12

[Friends of PhishTank](#) [Terms of Use](#) [Privacy](#) [Contact](#)

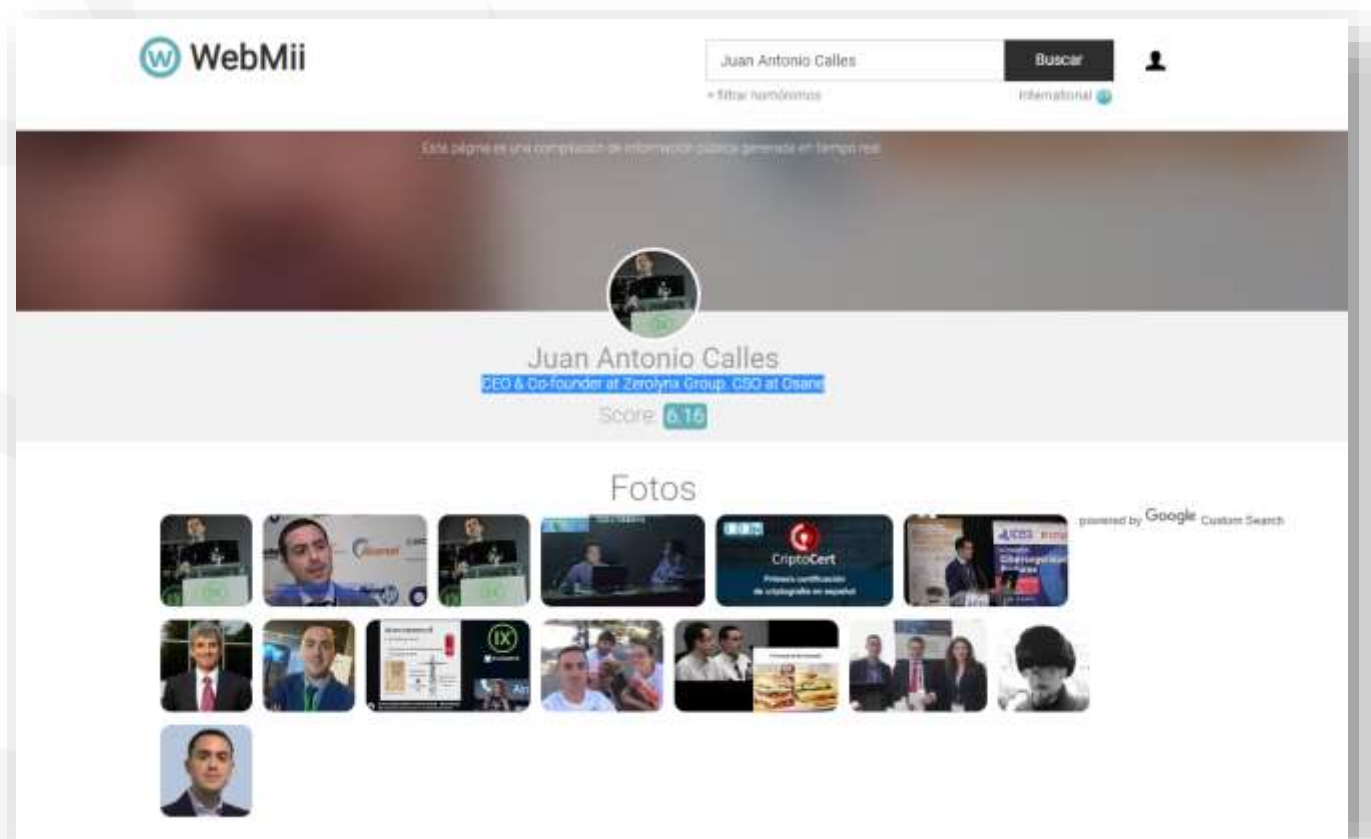
PhishTank is operated by [OpenDNS](#). Learn more about [PhishTank](#) or [OpenDNS](#).

Datos sobre personas y perfiles



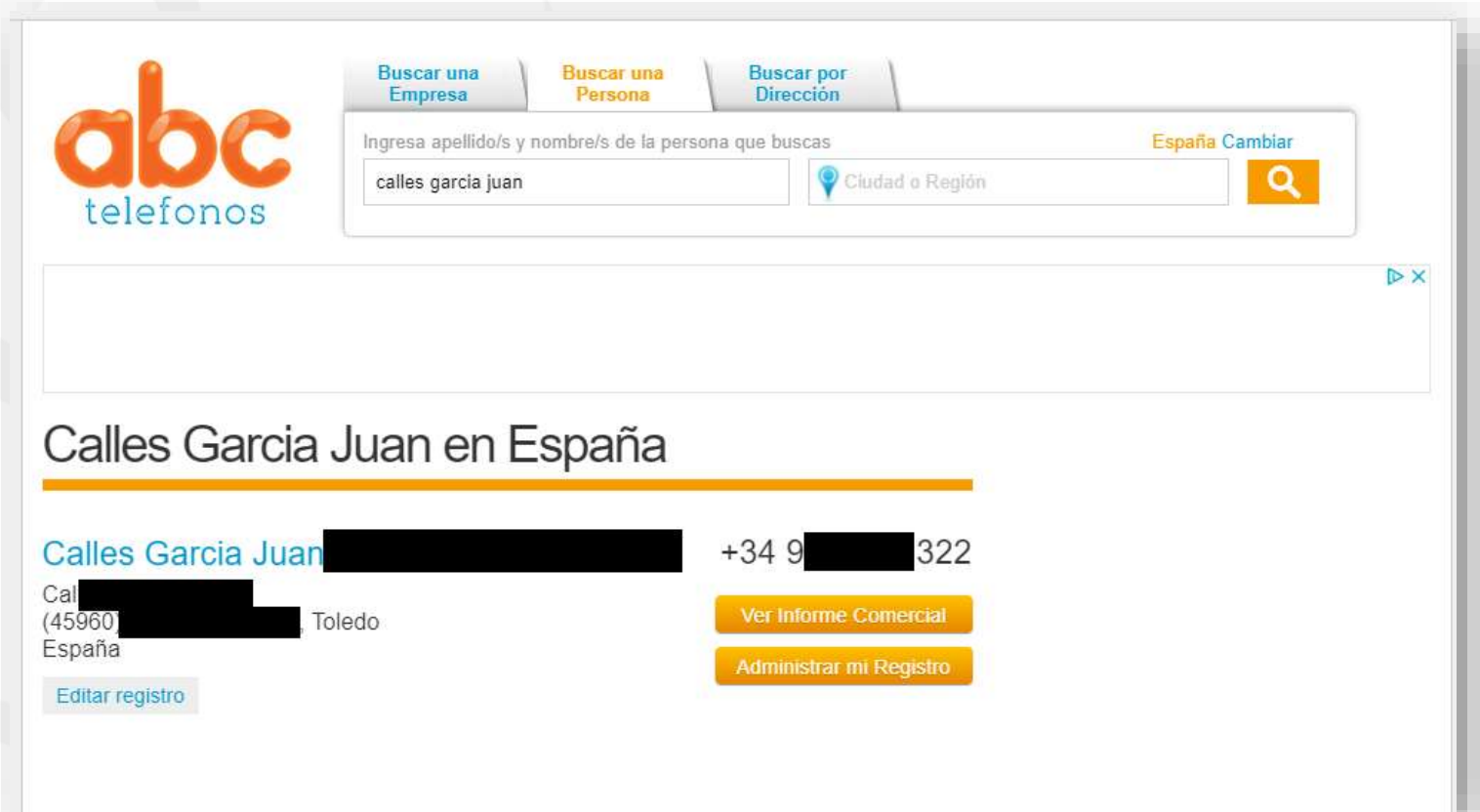
¿Qué hay en Internet sobre una persona?

- <http://webmii.com>



Buscando direcciones físicas

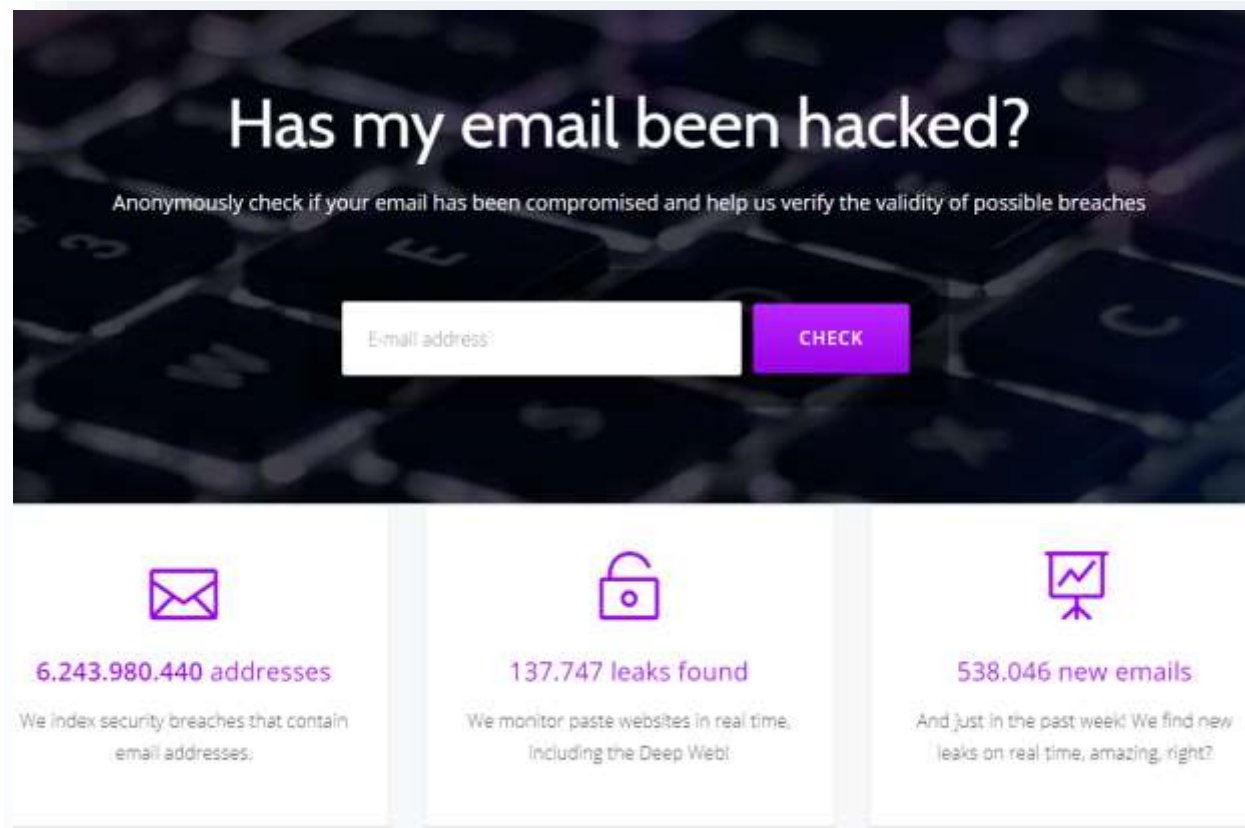
- <http://www.abctelefonos.com>



The screenshot shows the 'abc telefonos' website interface. At the top, there are three tabs: 'Buscar una Empresa' (selected), 'Buscar una Persona', and 'Buscar por Dirección'. Below the tabs is a search bar with the text 'Ingresa apellido/s y nombre/s de la persona que buscas'. The search input contains 'calles garcia juan'. To the right of the search input is a dropdown menu for 'Ciudad o Región' and a search button with a magnifying glass icon. The results section is titled 'Calles Garcia Juan en España'. Below the title, there is a list of results. The first result shows 'Calles Garcia Juan' followed by a redacted address and the phone number '+34 9 [redacted] 322'. Below the address, it says 'Cal [redacted] (45960) Toledo España'. To the right of the address, there are two buttons: 'Ver Informe Comercial' and 'Administrar mi Registro'. Below the address, there is a button labeled 'Editar registro'.

Contraseñas leakeadas




- <https://hacked-emails.com>
- <https://haveibeenpwned.com>



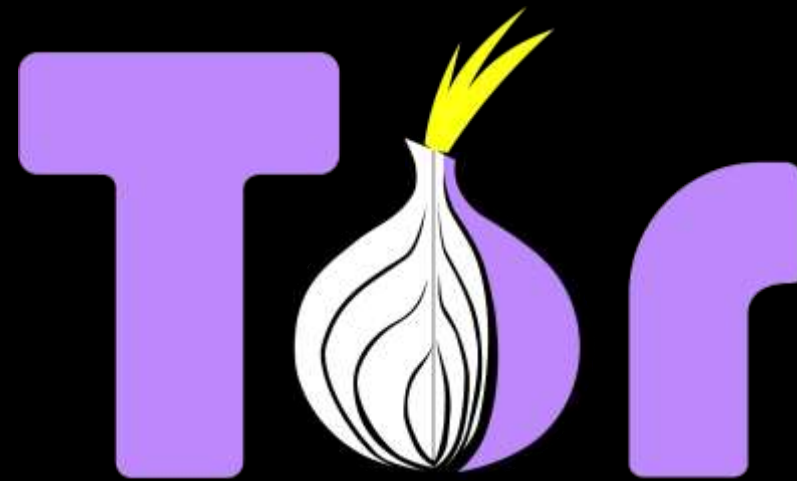
The screenshot shows the homepage of a website titled "Has my email been hacked?". The background is dark with a blurred image of a keyboard. The main heading is in large white font. Below it is a subtitle in smaller white font. A search form with a white input field and a purple "CHECK" button is centered. Below the form are three white boxes, each with a purple icon, a purple heading, and a description in grey text.

Has my email been hacked?
Anonymously check if your email has been compromised and help us verify the validity of possible breaches

E-mail address: **CHECK**

Icon	Heading	Description
	6.243.980.440 addresses	We index security breaches that contain email addresses.
	137.747 leaks found	We monitor paste websites in real time, including the Deep Web!
	538.046 new emails	And just in the past week! We find new leaks on real time, amazing, right?

La red TOR



Contraseñas leakeadas

- TOR es una red viva
- Varía diariamente
- Es imposible obtener una estadística realista
- 2,5 millones de usuarios
- Tráfico de estupefacientes
 - Armas
 - Tarjetas de crédito
 - Cuentas Paypal
 - Terrorismo
 - Sicarios
 - Hackers mercenarios
 - Redes Sociales
 - Foros
 - Blogs y webs

Category	Websites
None	2,482
Other	1,021
Drugs	423
Finance	327
Other illicit	198
Unknown	155
Extremism	140
Illegitimate pornography	122
Nexus	118
Hacking	96
Social	64
Arms	42
Violence	17
Total	5,205
Total active	2,723
Total illicit	1,547

Cuentas de paypal

Verified Personal USA Paypal Accounts

I have available a limited supply of Verified Personal or Business Paypal accounts with Zero Balance.

These accounts make excellent middleman accounts for money transfer.

These accounts are verified with either a credit card or bank account attached and have verified transaction history.


USA accounts only unless you ask via PM for other countries. We sometimes have UK and other EU nations.

Ships from: Torland
Ships to: Torland
Brought to you by: [psycherdude](#) · 1-2 ⭐

Price: 0.03836889 ₤

Available shipping:

Free Online Delivery, + 0.00000000 ₤(0.00000000 ₤)



NO PHOTO

Tarjetas

- US (Visa/Master) = \$6 por 1
- US (Amex, Dis) = \$7 por 1
- —————
- UK (Visa/Master) = \$14 por 1
- UK (Amex, Dis) = \$22 por 1
- —————
- CA (Visa/Master) = \$15 por 1
- CA (Amex) = \$20 por 1
- —————
- AU (Visa/Master) = \$18
- AU (Amex, Dis) = \$20 por 1
- AU Bin = \$20, AU Dob = \$25
- AU Todo = \$30 por 1

- Italy = \$20 por 1
- **Spain = \$20 por 1**
- Denmark = \$25 por 1
- Sweden = \$20 por 1
- France = \$20 por 1
- Germany = \$20 por 1
- Ireland = \$20 por 1
- Mexico = \$15 por 1
- Asia = \$15 por 1



Cuentas de sitios web



Seller	xanabji (n/a - 0)
Price	5.41 USD
FE	No
Shipping from	WorldWide
Shipping to	WorldWide
Currency	Bitcoin ▼
Quantity	1 ▼
5.41 USD - French Amazon accounts + cb attached +least 6mo ▼	

Cuentas de redes sociales

Market / Fraud Related / Accounts / 1 Hacked facebook account



★ 1 Hacked facebook account

Price: **\$4.99 USD** / 0.018608290 BTC [ESCROW](#) [Multisig](#) [PGP](#)

Quantity: unavailable/999

Ships from: Worldwide

Vendor: **ROOT** (0.0% from 0 users)

User: ROOT

Contact:

[Add Contact](#) [Send Message](#) [Subscribe Vendor](#) [Report Listing](#)

Shipping Option:



Worldwide - : \$0.00 USD / 0.000000000 BTC

Quantity:

[Buy Now](#)

Pasaportes

Hungarian professional certificate



Seller	hackminister (n/a - 0)
Price	545 USD
FE	No
Shipping from	Hungary
Shipping to	WorldWide
Currency	Bitcoin
Quantity	1
0 USD - free - 5 days	
Buy It Now	

Alquiler de servicios



Conclusiones

- La *ciberinteligencia* no depende “de una herramienta o de un conjunto de herramientas”.
- Al igual que en la *Inteligencia*, depende de tener buenas fuentes.
- Y por supuesto..., **de saber explotarlas.**





— GRUPO ZEROLYNX —



www.osaneconsulting.com



[@osaneconsulting](https://twitter.com/osaneconsulting)

