
Monta la **NSA** en tu casa

Inteligencia aplicada al mundo Ciber





Contenido

Who Am I

Introducción a la Inteligencia

Ciberinteligencia



Noviembre 2018



HoneyCon 4ª edición



Iván Portillo

Cyber Intelligence Senior Analyst

- 8 años de experiencia
- Finalista en Cyberventures de Incibe con Hackdoor
- Cofundador de Comunidad de Inteligencia Ginseg
- Colaborador en Derechodelared

 ivanportillomorales

 ivanPorMor



Gonzalo González

Cyber Intelligence / Ethical Hacking Research

- 5 años de experiencia
- Cofundador del Blog 'Follow the White Rabbit', ganador del Premio Bitácoras en 2016 a "Mejor Blog de Seguridad Informática"
- Colaborador de Comunidad de Inteligencia Ginseg

 gonx0

 gonx010



Introducción a la Inteligencia

Inteligencia y sus fuentes

Ciclo de Inteligencia

Relación entre datos, información e inteligencia

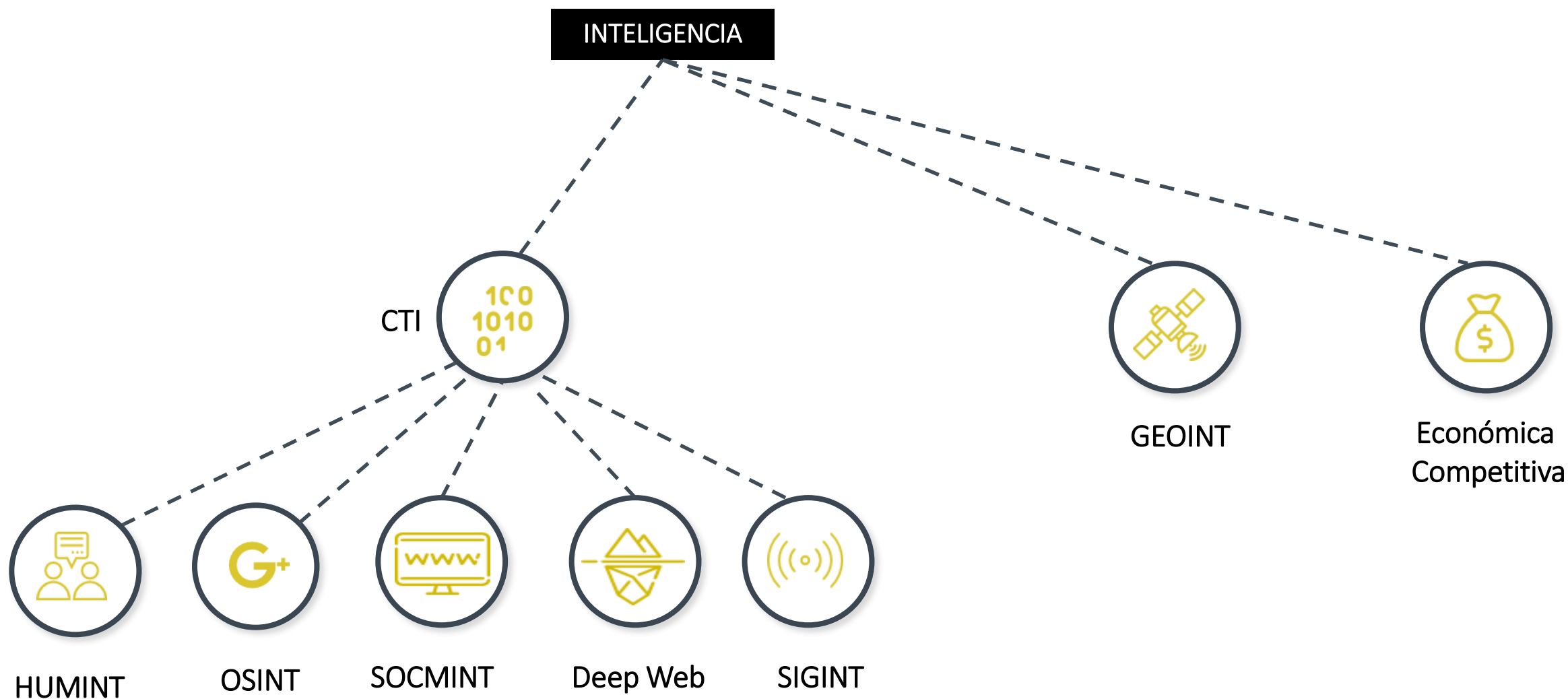
Amenaza VS Riesgo



Noviembre 2018



HoneyCon 4ª edición



Proceso de **generación y comunicación de conocimiento** ajustado a las necesidades y los requerimientos de un usuario a partir de la obtención y la transformación de información apropiada.

Secuencia de actividades mediante las que se obtiene **información que se convierte en conocimiento** (inteligencia) que se pone a disposición de un usuario.



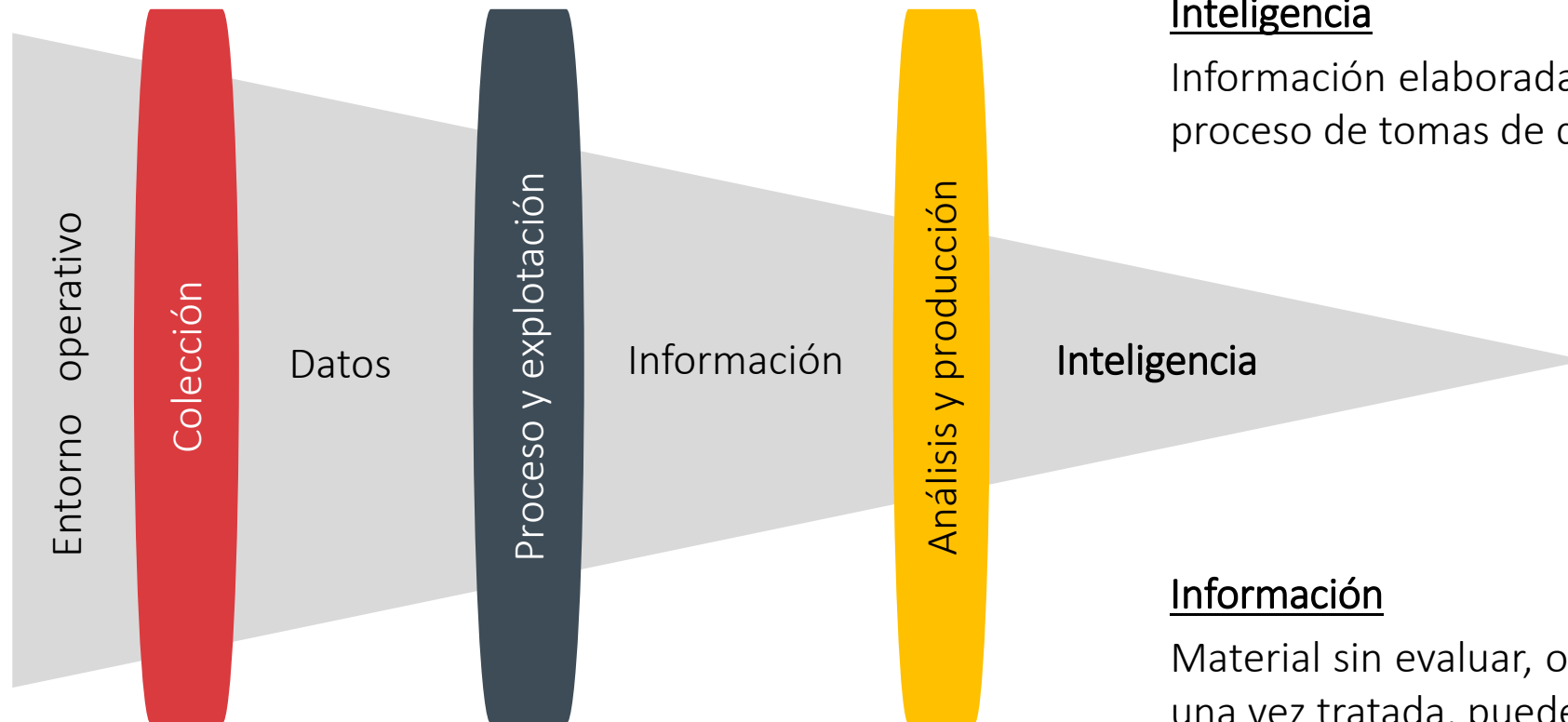
CIA



CNI

Con origen en el ciclo de inteligencia militar

Definiciones



Inteligencia

Información elaborada y tratada con el fin de ayudar al proceso de tomas de decisiones.

Información

Material sin evaluar, obtenida de cualquier fuente, que una vez tratada, puede generar inteligencia.



1

Los riesgos y las amenazas son conceptos relacionados pero diferentes.

2

El Riesgo es directamente proporcional a las amenazas, a las vulnerabilidades y los impactos.

3

Todos los factores configuran la ecuación del riesgo.



Conceptos y fundamentos de Ciberinteligencia

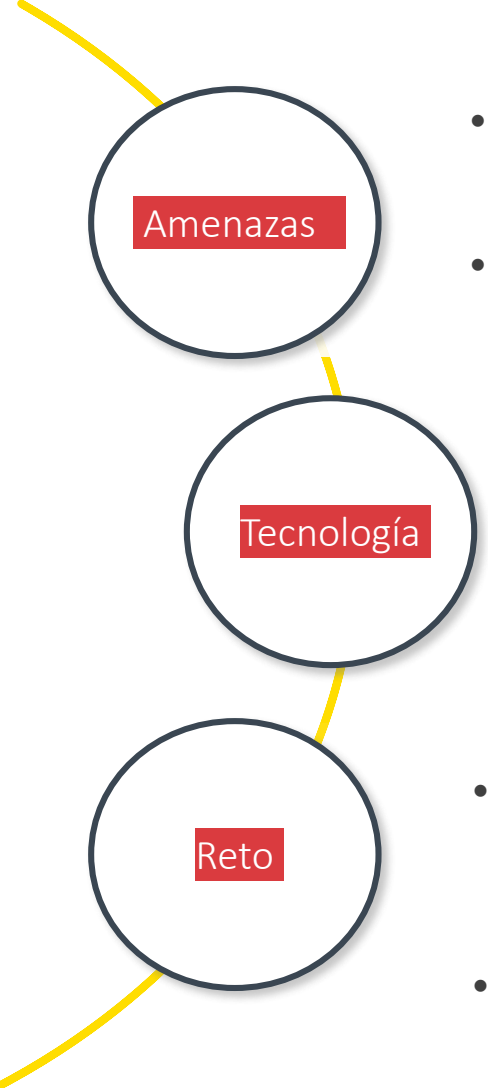


Noviembre 2018

/

HoneyCon 4ª edición





Amenazas

- Las motivaciones de los atacantes se están ampliando.
- Las **amenazas** continúan acelerándose, superando las defensas de seguridad tradicionales y los enfoques operativos.

Tecnología

- Las **defensas tradicionales** son cada vez **menos efectivas**.
- La **tecnología** está **evolucionando**, muy rápido, y las empresas que no la sigan se quedarán atrás.

Reto

- La mayoría de las **empresas** tienen **fundamentos de seguridad deficientes** y son reactivas frente a medidas proactivas.
- Las organizaciones están **mejorando** significativamente su **inversión** en ciberseguridad.



RIPE

Es el registro regional de internet encargado de supervisar y registrar los recursos de internet (Direcciones IP y AS) en las zonas de Europa, Oriente Medio y Asia Central.



TLD

Dominio de nivel superior: com, net, cn, info, es, jp, gov, edu, mil, uk, de, ...



Registro A

Tipo de registro DNS. Vinculan un nombre de host (dominio) a una dirección IP. Ej.: ftp.dominio.com. **A** 156.25.89.36



Registro NS

Tipo de registro DNS. Son los servidores DNS Autorizados para un dominio/subdominio y quien informará de cualquier petición solicitada al dominio. Ej.: dominio.com. **NS** ns1.dominio.com.



Registro MX

Tipo de registro DNS. Indica el servidor de correo responsable de distribuir y gestionar los correos relacionados con el dominio. Ej.: dominio.com. **MX** 10 mx01.dominio.com.



Registro CNAME

Tipo de registro DNS. Especifica las redirecciones desde los subdominios de un dominio hacia otros dominios/subdominios. Ej.: ftp.dominio.com. **CNAME** dominio.com.



Reverse DNS o
rDNS

Utiliza registro DNS PTR. Resuelve dirección IP hacia un nombre de host (dominio). Similar a Registro A pero a la inversa. Ej.: 44.33.22.11.in-addr.arpa **PTR** dominio.com.



IoC

Indicador de Compromiso. Ej.: Hash, Dirección IP, Dominio, etc.



TTP

Tácticas, Técnicas y Procedimientos.



TLP

Traffic Light Protocol. Esquema creado por US-CERT para compartir información en función de lo confidencial o sensible que sea esta. Existen 4 estados desde mas limitado a menos. **RED**, **AMBER**, **GREEN** y **WHITE**.



ASN

Distribución de **Números de Sistema Autónomo (AS)**. Un **AS** es un grupo de rangos de direcciones IPs gestionados por uno o mas operadores de red. El número específico de cada AS se denomina **ASN**.



El problema a resolver

Ciclo de colección de inteligencia y mensaje adaptado al interlocutor

Equipos y vías de comunicación

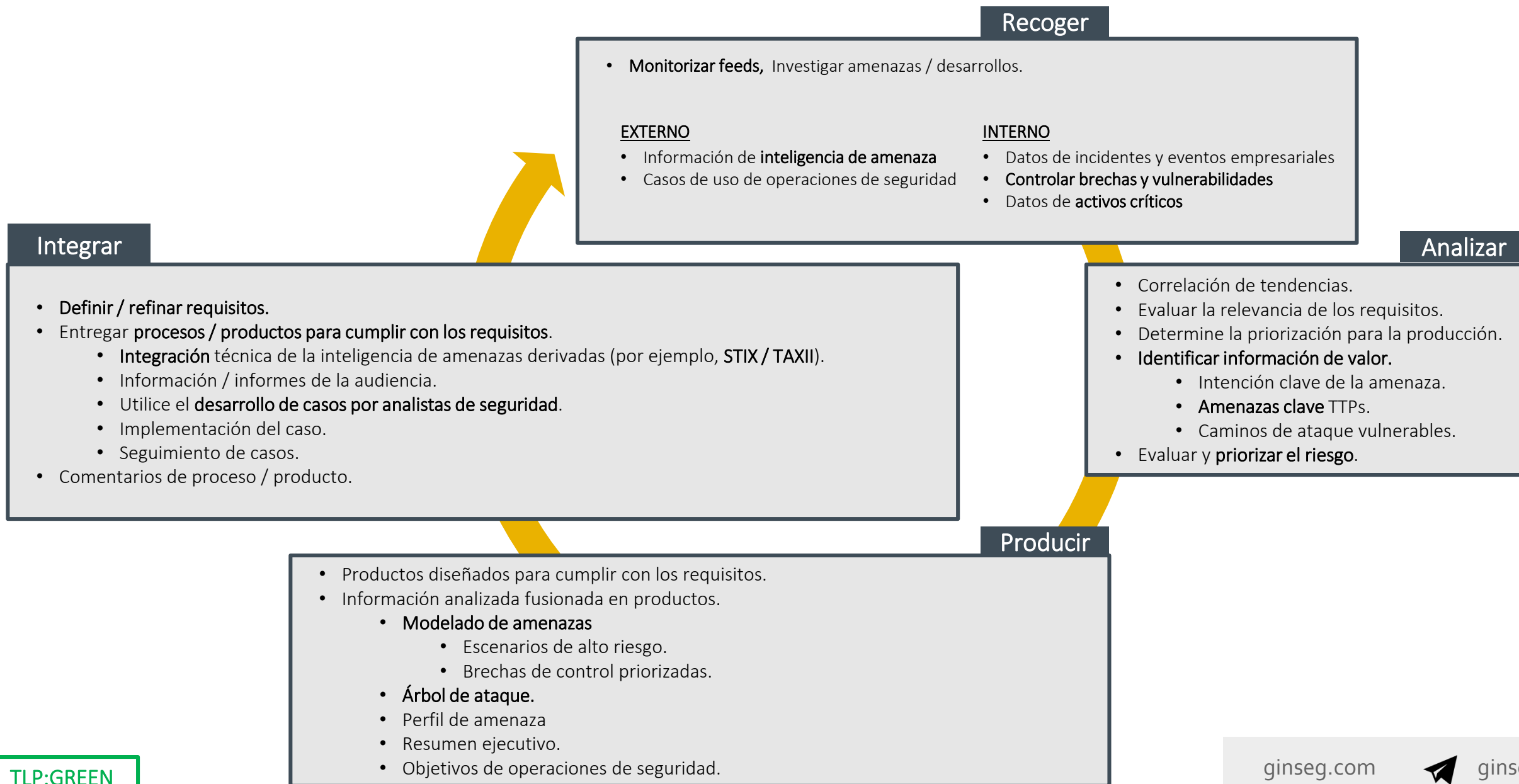
Nuestro escenario



Noviembre 2018



HoneyCon 4ª edición



Información relevante que se convierte en inteligencia a través de un **ciclo dinámico de colección, análisis, integración y producción**.

Esta **inteligencia** puede ser **consumida** por los **equipos de seguridad** así como por **altos cargos**.

Estratégico

Es **información de alto nivel**. Es poco probable que sea técnico y puede abarcar aspectos como el **impacto financiero** de la actividad cibernética, las **tendencias de ataque** y las áreas que pueden afectar las **decisiones comerciales** de alto nivel.

- Junta directiva / CEO.
- Otros altos responsables en la toma de decisiones

Operacional

Es información sobre ataques específicos que llegan a la organización.

- Personal de seguridad y defensa.

Táctica

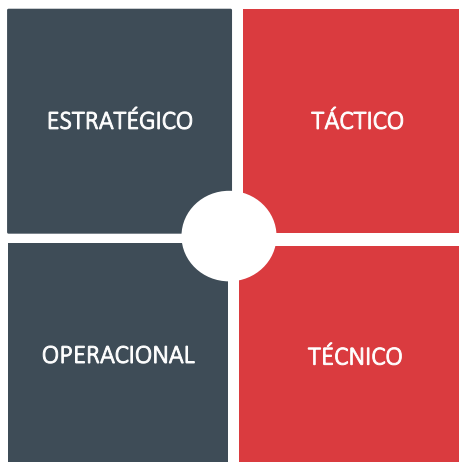
Tácticas, técnicas y procedimientos (TTP, por sus siglas en inglés) es información sobre cómo los actores pretender o están realizando sus ataques.

- Arquitectos y Sysadmins.

Técnico

Se trata de datos o información sobre indicadores de sucesos específicos. La inteligencia de amenaza técnica generalmente alimenta las funciones de investigación o supervisión de una empresa.

- Analistas SOC, IR e IT Staff.



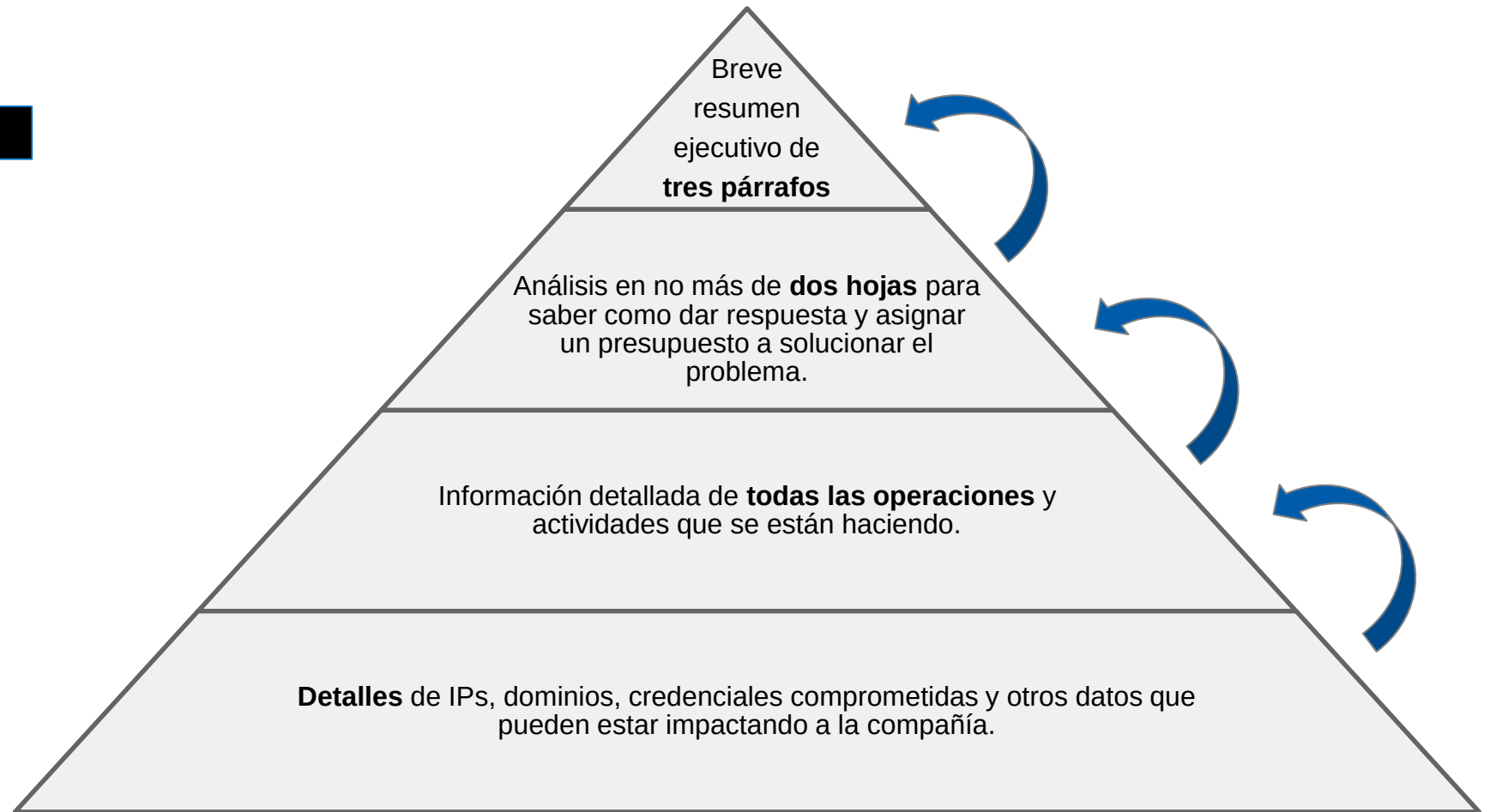
Es importante **ajustar el mensaje al interlocutor adecuado**, proporcionando la información clave con el nivel exacto de detalles para cada una de las partes receptoras de la inteligencia.

Estratégico

Táctica

Operacional

Técnico





Julio

Julio Petrolum Sánchez
CEO Director del negocio Petrodolar S.A.

Se que han comprometido mi empresa, pero no se ni quién ni por qué querría hacerlo. Quiero una solución urgente sea cual sea.

He encargado a Diego la investigación del incidente. Como acaba de llegar a la compañía, se coordinará junto con el equipo de Bee You para averiguar lo sucedido.



María

María Ninja Dance
Equipo de seguridad de Petrodolar S.A

Me han notificado que nos han podido comprometer, pero no tengo más que un Tweet que hace alusión al ataque. Se está haciendo revuelo en más medios, parece una amenaza real y lo he escalado.



Diego

Diego Gerente Frikazo
CISO de Petrodolar S.A

Acabo de incorporarme a la empresa en el mejor momento, el anterior director de seguridad ha muerto de un infarto.

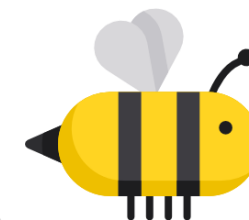
Necesito identificar los activos de la compañía y descubrir por dónde han podido atacarnos cuanto antes. Esta teniendo mucha repercusión.



Bee You Researcher
Investigadores de inteligencia del panel

Equipo designado que descubrirá lo que ha pasado y aportara un breve resumen al CISO el cual lo transmitirá al CEO.

Los datos de partida son escasos, ¿el nombre de la empresa? ¡Vaya! Nos espera un gran trabajo por delante, el mismo que el de los atacantes.



Bee You



Julio

Diego, me han llegado noticias de que nos han comprometido ¿Cómo de grave es el asunto?

Julio, parece haber evidencias después de una primera aproximación, de que nuestras **gasolineras están comprometidas** y no sabemos si ha sido por un posible **correo de phishing** qué parece haber recibido tu secretaria Anabel.



Diego

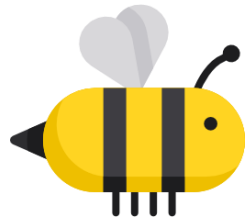
Me preocupa el correo por los datos sensibles de la empresa que hayan podido obtener los atacantes, pero sobre todo la seguridad de nuestras estaciones. Por favor, mantenme informado.



Diego

Hola Bee, me han llegado referencias de que sois los mejores en este tipo de investigaciones. Nos han comprometido y no sabemos ni por dónde ni si son de algún gobierno o universitarios, pero nuestro presidente esta muy preocupado. ¿Nos podéis ayudar?

Diego, tenemos la colmena perfecta para darte solución a este problema. **¿Qué datos tenemos de partida?**



Bee You

Acabo de incorporarme a la empresa y poco más se que el **nombre, Industrias Petrodolar S.A.** Buscad posibilidades como si fuerais los atacantes reales para encontrar información exfiltrada o puntos débiles.

Nos ponemos a ello, no son muchos datos la verdad, pero usaremos nuestra inteligencia colectiva. ¿Alguna pista más?

También ha llegado a mis oídos que una o varias de nuestras estaciones de servicio podrían estar comprometidas. Adicionalmente, hay claras sospechas de un correo de phishing abierto por Anabel, la secretaria del presidente.



Qué tenemos

- ▶ Nombre de una de las empresas del grupo.
- ▶ Indicios de estaciones de servicio comprometidas.
- ▶ Indicios de correo de phishing abierto por una empleada.



Qué buscamos

- ▶ Resto de empresas del grupo para conocer su exposición.
- ▶ Sus dominios asociados, direcciones IP, servidores de correo para reducir la superficie de búsqueda de credenciales, etc.
- ▶ Activos a nombre de la empresa, como estaciones de servicio, servidores, rangos de red, etc.
- ▶ Credenciales y datos confidenciales expuestos.
- ▶ Otros datos que puedan ser de interés para un atacante.

Qué necesitamos

- ▶ Establecer las herramientas que podemos usar, tanto distribuciones como otras open source.
- ▶ Crear herramientas adicionales si las herramientas disponibles no se adaptan a nuestras necesidades.
- ▶ Usar la metodología y ciclo de inteligencia para coleccionar y analizar los datos.
- ▶ Informar adecuadamente de los descubrimientos al interlocutor adecuado.
- ▶ Documentar nuestros hallazgos.





Recolección de Información

Cómo comenzar

Investigación objetivo

La importancia de las relaciones entre los datos - Orquestación de herramientas



Noviembre 2018



HoneyCon 4ª edición



Cómo comenzar...



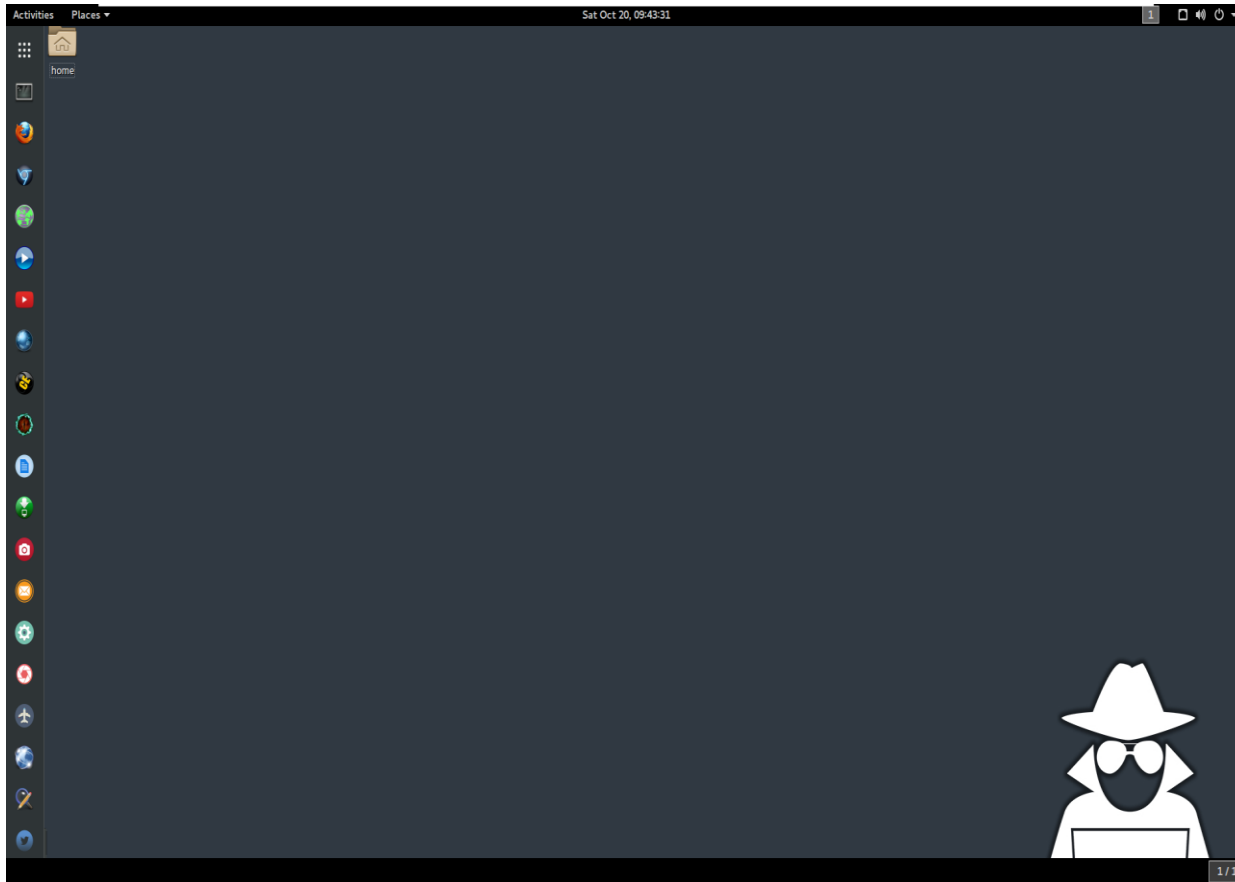
Noviembre 2018

/

HoneyCon 4ª edición



Buscador



Creador IntelTechniques

<https://inteltechniques.com/buscador/>

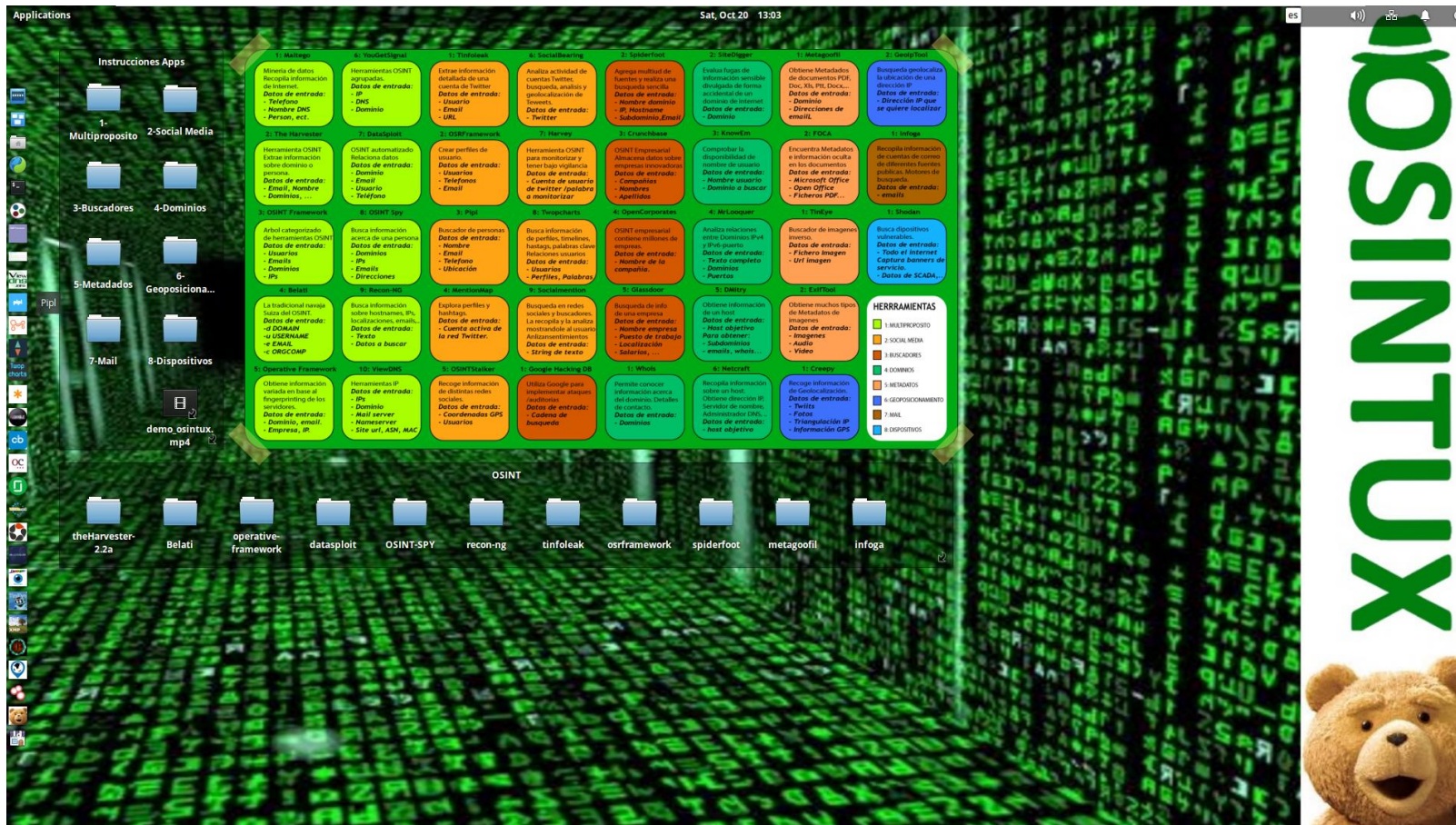
Centrado en Investigaciones sobre personas y organizaciones

- User: osint Password: osint

Herramientas a destacar:

- Extensiones con Firefox y Chrome
- Tor Browser
- Recon-NG
- Maltego
- Creepy
- Spiderfoot
- EyeWitness
- EmailHarvester
- The Harvester
- Aquatone
- Twitter Exporter
- TinfoLeak
- InstaLooter

Osintux



URL: <http://www.osintux.org/descargas>

User: osintux Password: osintux

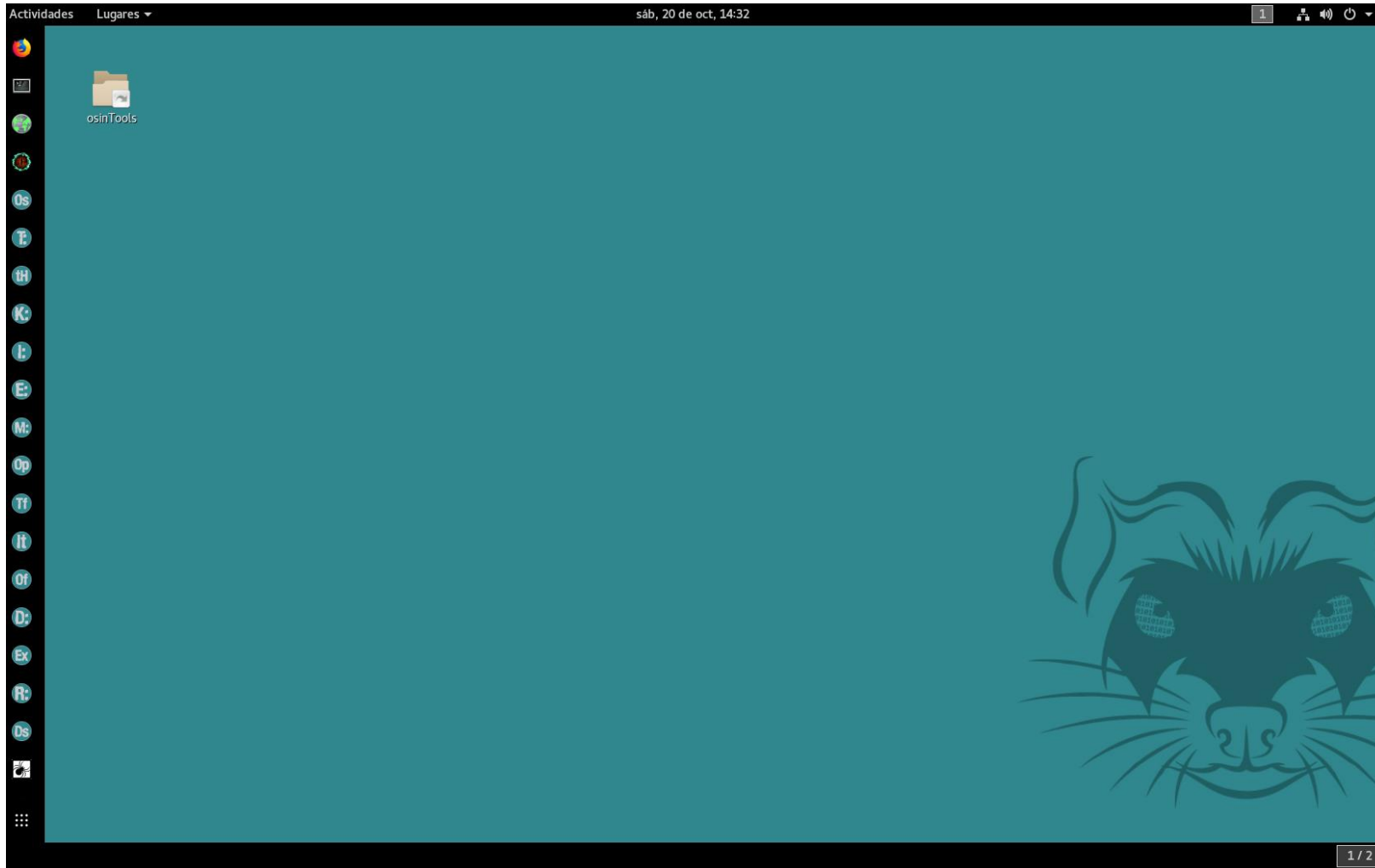
Documentación de cada herramienta

Enfocado para formación

Herramientas a destacar:

- DataSploit
- Crunchbase
- Infoga
- Glassdoor
- Recon-NG
- Maltego
- Creepy
- OSINT Spy
- OSINT Framework.
- OSRFramework
- The Harvester
- TinfoLeak

Huron



URL:

https://mega.nz/#F!SboFCQya!eChso_SMirLFbgzw3ZPMgA

- User: osint Password: osint

En continua actualización y mejora

Herramientas a destacar:

- Tor Browser y Firefox
- DataSploit
- Infoga
- Recon-NG
- EyesWitness
- Maltego
- Creepy
- Operative Framework
- OSINT Framework
- OSRFramework
- The Harvester
- TinfoLeak

https://scans.io/

Internet-Wide Scan Data Repository

The Internet-Wide Scan Data Repository is a public archive of research datasets that describe the hosts and sites on the Internet. The repository is hosted by Censys. While we publish much of the data, we are happy to host data from other researchers as well. A JSON interface to the repository is available. The data on the site is restricted to non-commercial use. Please contact support@censys.io with any questions.

Censys • Primary Datasets

The Censys Projects publishes daily snapshots of what we know about each IPv4 host, Alexa Top Million website, and known X.509 certificate. These datasets contain structured, non-ephemeral JSON records that identify a host's configuration. These records are constructed by combining all of our raw scans and provide a perspective similar to what is available in the Censys Search and SQL Interfaces. [More Information]

IPv4 Address Space Alexa Top Million Domains X.509 Certificates

Censys • Regularly Scheduled Scans

Below are the regularly scheduled scans that power Censys. For each scan, we publish the host discovery scans and parsed application handshakes. We typically scan each protocol at least once weekly.

Name	Port	Protocol	Subprotocol	Destination	Last Scan
0-icmp-echo_request-full_ipv4		icmp	echo request	full ipv4	2018-10-19 23:13:12
102-s7-szl-full_ipv4	102	s7	szl	full ipv4	2018-10-17 12:50:17
110-pop3-starttls-full_ipv4	110	pop3	starttls	full ipv4	2018-10-21 00:52:37
143-imap-starttls-full_ipv4	143	imap	starttls	full ipv4	2018-10-21 23:26:52
1900-upnp-discovery-full_ipv4	1900	upnp	discovery	full ipv4	2018-10-22 02:36:51
1911-fox-device_id-full_ipv4	1911	fox	device id	full ipv4	2018-10-22 12:18:14
20000-dnp3-status-full_ipv4	20000	dnp3	status	full ipv4	2018-10-20 12:48:06
21-ftp-banner-full_ipv4	21	ftp	banner	full ipv4	2018-10-22 23:06:21

Rapid7 • Forward DNS (FDNS)

DNS 'ANY', 'A', 'AAAA', 'TXT' and 'CNAME' responses for known forward DNS names

File Name	SHA1-Fingerprint	Size	Updated At
2018-09-30-1538276920-fdns_aaaa.json.gz	e6e979270926843151cceed21dcbf53b3e336b0b	732.0 MB	Sept. 30, 2018
2018-09-29-1538257451-fdns_cname.json.gz	d97865e991823fc2a4eb33920355caf2524625cd	1.3 GB	Sept. 30, 2018
2018-09-28-1538136264-fdns_ajson.gz	18755be44cc9a84f393f2954fc35e3817a4718ea	15.1 GB	Sept. 29, 2018
2018-09-28-1538093080-fdns_any.json.gz	ec36dbe9a9882f1e9a2f6246b617971f28a774c3	24.9 GB	Sept. 30, 2018
2018-09-23-1537723857-fdns_mx.json.gz	5c6221b2fba5390c3967f1899bd924e94b6a40aa	3.3 GB	Sept. 24, 2018
2018-09-23-1537671251-fdns_txt.json.gz	02f26c9d332e88a23217a55aed7e12c60cdf7425	2.9 GB	Sept. 23, 2018

Proyecto Censys: Repositorio de datos públicos creado por Censys, que recopila información sobre hosts IPv4, sitios web dentro de Alexa Top Million y certificados X.509 que se encuentren activos en Internet, mediante escaneos activos con ZMAP.

Proyecto Sonar: Repositorio de datos públicos creado por Rapid7, que realiza escaneos a diferentes servicios y protocolos en Internet para obtener información sobre exposición global a vulnerabilidades comunes.

Descargando fichero

Index of /ripe/dbase

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
Parent Directory		-	
RIPE.CURRENTSERIAL	20-Jan-2017 00:00	8	
ripe.db.gz	20-Jan-2017 01:20	336M	
split/	20-Jan-2017 00:00	-	

<http://ftp.ripe.net/ripe/dbase/>

Index of /ripe/dbase/split

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
Parent Directory		-	
ripe.db.as-block.gz	20-Jan-2017 01:20	9.4K	
ripe.db.as-set.gz	20-Jan-2017 01:20	2.0M	
ripe.db.aut-num.gz	20-Jan-2017 01:20	7.5M	
ripe.db.domain.gz	20-Jan-2017 01:20	19M	
ripe.db.filter-set.gz	20-Jan-2017 01:20	395K	
ripe.db.inet-rtr.gz	20-Jan-2017 01:20	11K	
ripe.db.inet6num.gz	20-Jan-2017 01:20	23M	
ripe.db.inetnum.gz	20-Jan-2017 01:20	228M	
ripe.db.irt.gz	20-Jan-2017 01:20	27K	
ripe.db.key-cert.gz	20-Jan-2017 01:20	15M	
ripe.db.mntner.gz	20-Jan-2017 01:20	1.6M	
ripe.db.organisation.gz	20-Jan-2017 01:20	4.5M	
ripe.db.peering-set.gz	20-Jan-2017 01:20	72K	
ripe.db.person.gz	20-Jan-2017 01:20	409	
ripe.db.poem.gz	20-Jan-2017 01:20	29K	
ripe.db poetic-form.gz	20-Jan-2017 01:20	1.3K	
ripe.db.role.gz	20-Jan-2017 01:20	2.7M	
ripe.db.route-set.gz	20-Jan-2017 01:20	229K	
ripe.db.route.gz	20-Jan-2017 01:20	8.2M	
ripe.db.route6.gz	20-Jan-2017 01:20	713K	
ripe.db.rtr-set.gz	20-Jan-2017 01:20	2.4K	

<http://ftp.ripe.net/ripe/dbase/split/>

```
root@prometheus002:~/taller_ciberseg# cat ripe.db.inetnum
#
# The contents of this file are subject to
# RIPE Database Terms and Conditions
#
# http://www.ripe.net/db/support/db-terms-conditions.pdf
#
inetnum:      80.16.151.184 - 80.16.151.191
netname:      NETECONOMY-MG41731
descr:        TELECOM ITALIA LAB SPA
country:      IT
admin-c:      DUMMY-RIPE
tech-c:       DUMMY-RIPE
status:       ASSIGNED PA
notify:       neteconomy.rete@telecomitalia.it
mnt-by:       INTERB-MNT
created:      1970-01-01T00:00:00Z
last-modified: 2001-09-21T22:08:01Z
source:       RIPE
remarks:      *****
remarks:      * THIS OBJECT IS MODIFIED
remarks:      * Please note that all data that is generally regarded as personal
remarks:      * data has been removed from this object.
remarks:      * To view the original object, please query the RIPE Database at:
remarks:      * http://www.ripe.net/whois
remarks:      *****
% Tags relating to '80.16.151.184 - 80.16.151.191'
% RIPE-USER-RESOURCE

inetnum:      80.16.151.180 - 80.16.151.183
netname:      NETECONOMY-MG41731
descr:        TELECOM ITALIA LAB SPA
country:      IT
admin-c:      DUMMY-RIPE
tech-c:       DUMMY-RIPE
status:       ASSIGNED PA
notify:       neteconomy.rete@telecomitalia.it
mnt-by:       INTERB-MNT
created:      1970-01-01T00:00:00Z
last-modified: 2001-09-21T22:08:01Z
source:       RIPE
remarks:      *****
remarks:      * THIS OBJECT IS MODIFIED
remarks:      * Please note that all data that is generally regarded as personal
remarks:      * data has been removed from this object.
remarks:      * To view the original object, please query the RIPE Database at:
remarks:      * http://www.ripe.net/whois
remarks:      *****
```

Contenido de archivo parcial de ripe.db.inetnum

Enlaces a Herramientas OSINT

Mostrar todo

Anonimación

Bing Hacking

Borrar Identidad

Buscadores

Certificación

Clima/Horario

Criptomonedas

Dark Web

DNI/CIF

Documentos

Emails

Empresa/Profesional

Extensiones

Facebook

Geolocalizar

Google Hacking

Imágenes

Instagram

IPs

Mapas

Marcadores

Monitores

Nicknames

Otras RSS

Personas

Productividad

Repositorios

Software

Teléfonos

Twitter

Vehículos

Videos

Webcams

Webs

Anonimación

	Protonmail - Email seguro	14
	Simulator - Generador de perfiles y mensajes Fake	5
	Whonix - Sistema operativo navegación anónima	5
	Yopmail - Cuentas de Email temporales	4
	Gigatribe - Comparte archivos grandes encriptados	4
	Emkei - Suplantar el email de otra persona	4
	Emails y SMS anónimos	4
	Email Temporal gratis	3
	Tails - Sistema operativo navegación anónima	2
	Eff.org - Guías de privacidad y seguridad	2

Bing Hacking

	Sitios alojados en la misma IP	2
	Buscar por tipo de archivo en una web	1
	Ficheros con una extensión concreta	1

Borrar Identidad

	Eliminar Facebook	9
	Eliminar Instagram	4
	Eliminar cuenta de Google	2
	Desactivar Twitter	2
	Justdelete.me - Eliminar todas las cuentas de Internet	~

El sitio Web de Ciberpatrulla esta dedicado exclusivamente a Investigaciones OSINT, teniendo un apartado donde aloja un repositorio de herramientas categorizadas por grupos. En cada una de estas categorías, se engloban enlaces a herramientas relacionadas a su temática, facilitando su uso. En constante actualización.

ciberpatrulla.com/links/

Categorías

Anonimación

Google/Bing
Hacking

Borrar
Identidad

Certificación

Criptomonedas

Buscadores

DNI/
CIF

Empresa

Emails

Documentos

Emails

Geolocalización

Dark
Web

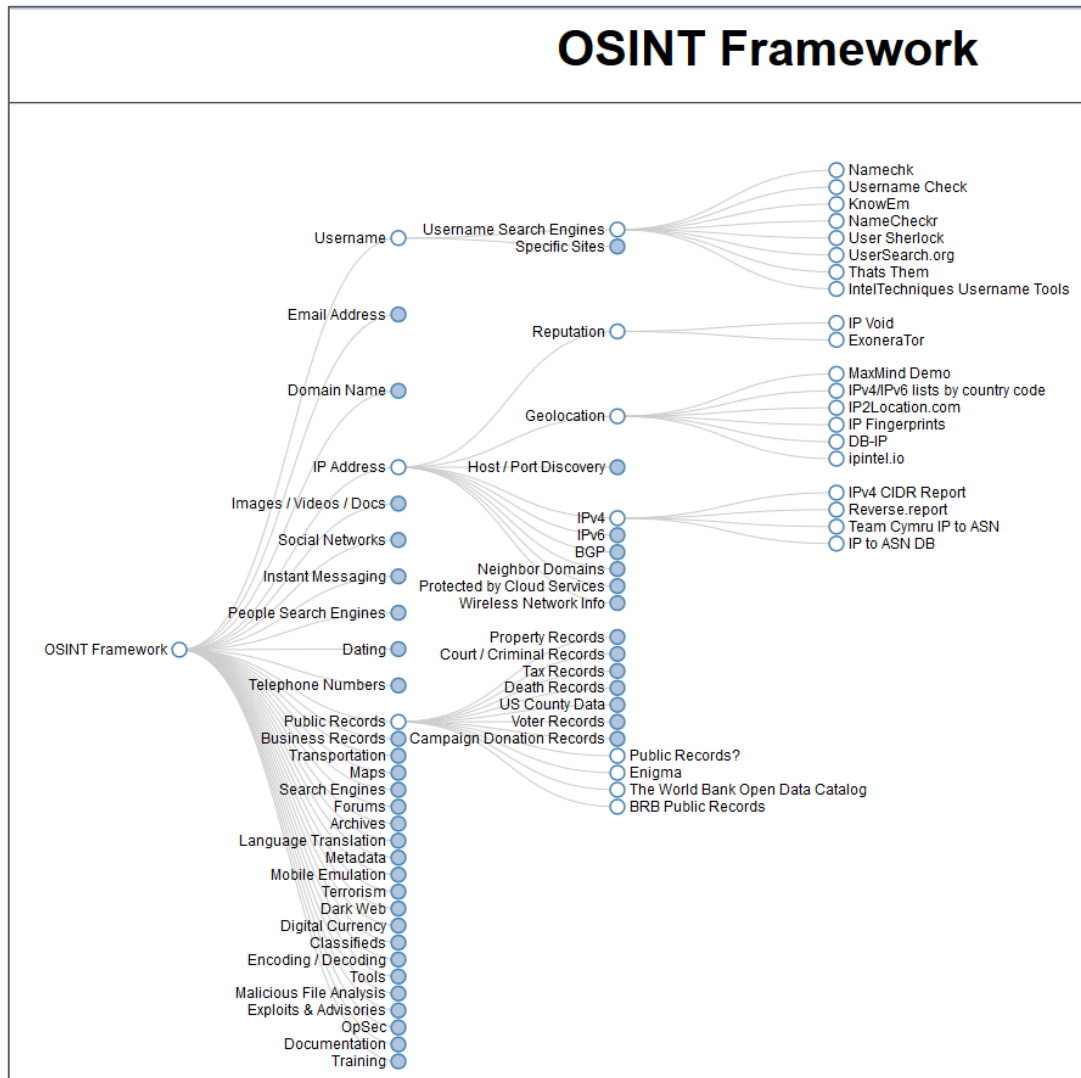
Personas

Facebook

Twitter

Instagram

Nicknames



<http://osintframework.com>

OSINT Framework es una web enfocada a investigaciones OSINT, alojando diferentes recursos en forma de enlaces a herramientas OSINT agrupadas por categorías y subcategorías en formato árbol.

<https://inteltechniques.com/menu.html>

```
graph TD; A[Investigaciones] --> B[Nombre Persona]; A --> C[Emails]; A --> D[Username]; B --> E[Perfiles Facebook]; B --> F[Perfiles Twitter]; B --> G[Perfiles Instagram]; C --> H[Teléfonos]; C --> I[Dominios]; C --> J[Dirección IP]; D --> K[Documentos]; D --> L[Videos]; D --> M[Imágenes]; E --> N[Empresa / Negocio]; F --> N; G --> N; H --> O[Geolocalización]; I --> O; J --> O; K --> O; L --> O; M --> O; N --> O
```

Diagrama de flujo de investigación de un caso de fraude por phishing:

- Investigaciones
 - Nombre Persona
 - Perfiles Facebook
 - Perfiles Twitter
 - Perfiles Instagram
 - Emails
 - Teléfonos
 - Dominios
 - Dirección IP
 - Username
 - Documentos
 - Videos
 - Imágenes
- Empresa / Negocio
- Geolocalización

LibreBorne es una plataforma web que permite consultar información sobre el Boletín Oficial del Registro Mercantil. En la actualidad, se mantiene actualizada la BBDD de la herramienta.

<https://libreborme.net/>

Input: Nombre Persona o empresa

libreBORME

Buscar por nombre de empresa o pers

Búsqueda avanzada

Resultados de la búsqueda «cepsa»

Nombre:

cepsa

Tipo:

☒ Todos ☐ Empresa ☐ Persona

Buscar

Se encontraron **64** empresas y **0** personas.

Empresas:

Cepsa SA	Cepsa Suriname SL	Cepsa Comercial Centro SA
Cepsa Marine Fuels SA	Cepsa Gas Licuado SA	Cepsa Colombia SA
Cepsa Comercial Norte SL	Cepsa Conveniencia SA	Cepsa Los Olivos SA
Cepsa Liberia SL	Cepsa Petrosur SA	Cepsa Bunker SA
Cepsa Petronuba SA	Cepsa Sea SL	Cepsa Aranjuez SA
Cepsa Comercial Este SA	Cepsa Comercial Madrid SA	Cepsa Alcorcon SA
Cepsa Comercial Galicia SA	Cepsa Peru SA	Cepsa Alconera SA
Cepsa Aviacion SA	Cepsa Global Services SA	Cepsa Quimica China SA
Cepsa Lubricantes SA		

« Anterior

1

2

3

Siguiente »



Sociedad «Cepsa SA»

Última actualización: 31 de Octubre de 2017.

Fuente de los datos: Agencia Estatal Boletín Oficial del Estado.

Empresas relacionadas: 0

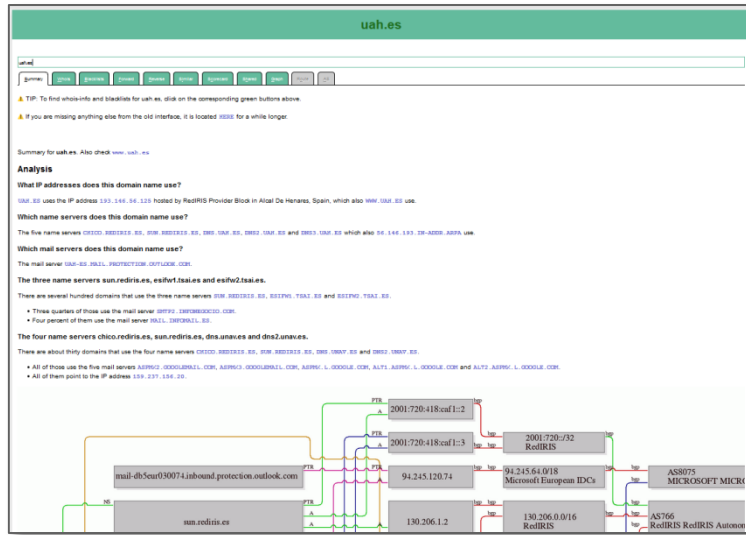
Personas relacionadas: 20

Situación mercantil: Activa

Cargos directivos:

CSV

Cargo	Persona física/jurídica	Desde	Hasta
Apoderado	Gordo De Julian Roberto	2013-03-13	Actualidad
Apoderado	Fernandez- Basanta Hernandez Ignacio	2013-03-13	Actualidad
Apoderado	Barbero Mejias Juan Francisco	2013-03-13	Actualidad
Apoderado	Lezana Palau Angel	2013-03-13	Actualidad
Apoderado	Cifuentes Huertas Jaime	2013-03-13	Actualidad
Apoderado	Lopez Arranz Maria Isabel	2013-03-13	Actualidad
Apoderado	Perales Martin Alberto	2013-03-13	Actualidad
Apoderado	Ramon Alba Sonia	2013-03-13	Actualidad
Apoderado	Gordo De Julian Roberto	2013-04-15	Actualidad
Apoderado	Fernandez- Basanta Hernandez Ignacio	2013-04-15	Actualidad
Apoderado	Barbero Mejias Juan Francisco	2013-04-15	Actualidad
Apoderado	Perales Martin Luis Alberto	2013-04-15	Actualidad
Apoderado	Lezana Palau Angel	2013-04-15	Actualidad
Apoderado	Cifuentes Huertas Jaime	2013-04-15	Actualidad



<https://www.robtx.com>

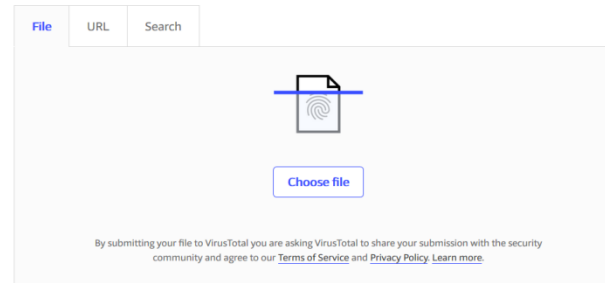
Herramienta pasiva que proporciona información relacionada con direcciones IP, dominios, subdominios, DNS, servidores de correo y blacklist.

Input: Dominio, IP, Rango IP o ASN

TLP:GREEN



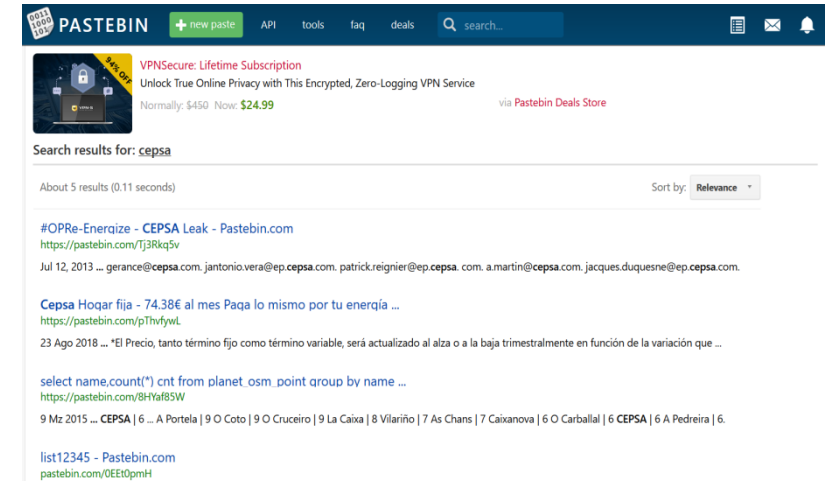
Analyze suspicious files and URLs to detect types of malware, automatically share them with the security community.



<https://www.virustotal.com>

VT es una herramienta que permite analizar ficheros, URLs, dominios, IP o Hashes para descubrir presencia Malware.

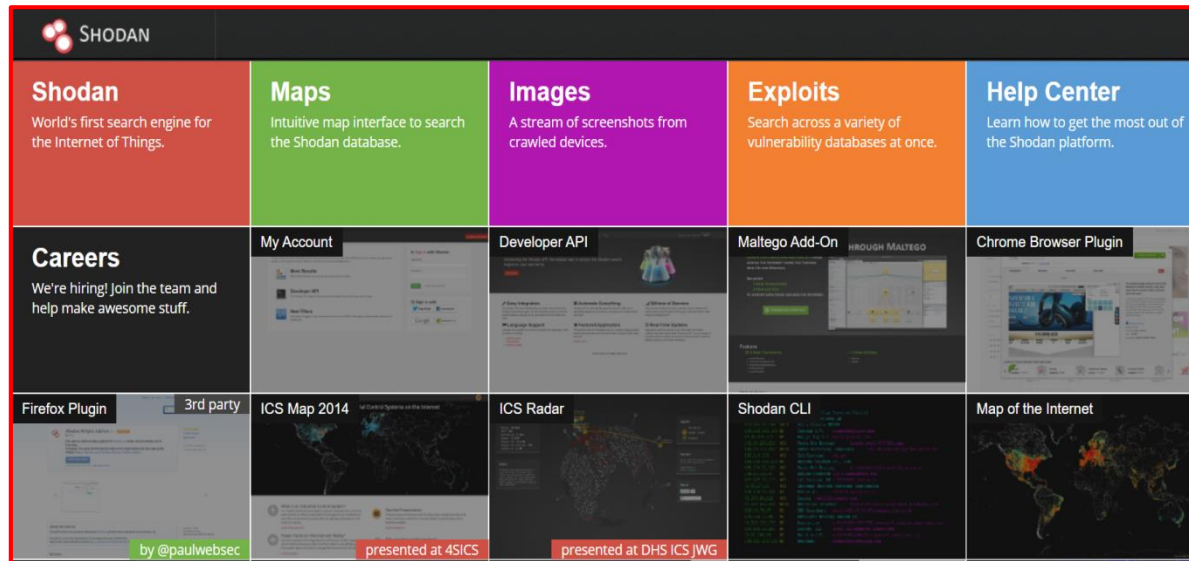
Input: URL, Dominio, IP, Hash, Fichero



<https://pastebin.com>

Pastebin es una herramienta que permite buscar fugas de Información publicadas.

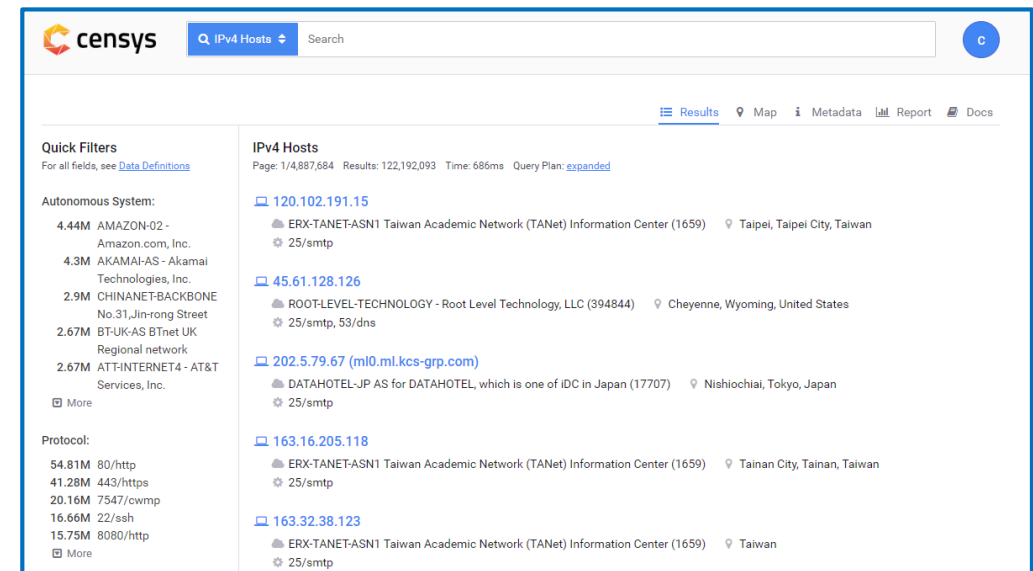
Input: Keyword



<https://www.shodan.io>

Shodan, herramienta ampliamente conocida, realiza un ZMAP hacia todos los dispositivos, dominios, direcciones IP conectados a Internet, ofreciendo información relacionada mediante un buscador. En desarrollo y evolución constante, como puede ser el módulo de Exploits para realizar búsquedas sobre vulnerabilidades.

Input: Dominio, IP, Rango IP, ASN, Nombre Organización



<https://censys.io>

Censys es una herramienta similar a Shodan, siendo el buscador desarrollado para Scans.io y poder localizar al vuelo activos conectados a Internet relacionados a IPv4, Sitios Webs y certificados.

Input: Dominio, IP, Rango IP, Keyword

ZoomEyo 首页 探索 开发 专题 商务 贡献 私有版

apache

搜索结果 统计报告 全球视角 相关漏洞

找到约 105.168.945 条结果 用时 1.508 秒

apache X

36.89.14.83	HTTP/1.1 200 OK Date: Mon, 05 Nov 2018 14:42:15 GMT Server: Apache/2.4.17 (Win32) OpenSSL/1.0.2d PHP/5.6.19 X-Powered-By: PHP/5.6.19 Set-Cookie: ci_session=4add71bf8857dfdc1f9613144f333b98504a40f2; expires: Thu, 19 Nov 1981 08:52:00 GMT Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-Pragma: no-cache
25000/http	
Indonesia, Banjarmasin	
2018-11-05 22:42	

36.91.54.213	HTTP/1.1 200 OK Date: Mon, 05 Nov 2018 14:42:29 GMT Server: Apache/2.4.16 (Win32) OpenSSL/1.0.1p PHP/5.6.12 X-Powered-By: PHP/5.6.12 Content-Length: 3724 Connection: close Content-Type: text/html; charset=UTF-8
25000/http	
Indonesia	
2018-11-05 22:42	

搜索类型

设备	71.653.216
网站	31.096.215

年份

2018	45.731.093
2017	23.258.378
2016	19.109.503
2015	12.975.856
2014	1.674.601

国家

United States	32.928.592
---------------	------------

<https://www.zoomeye.org>

Input: Dominio, IP, Rango IP,
Nombre Dispositivo

Fofa Pro

规则专题 API&SDK 规则列表 Fofa客户端

登录与注册

"apache"

收藏规则 下载数据 使用API

相关搜索: Apache-Tomcat Apache-Web-Server Apache-ActiveMQ 更多(13)

类型分布

协议	49137531
网站	40944690

年份

2018	78789204
2017	11293017

国家排名

美国	26180849
中国	9982206
德国	6820721
日本	5778079
英国	4005742

端口排名

80	50289585
443	31672116
7547	2148626
8080	1590695

搜索 "apache" 获得 90082221 条匹配结果, 用时 6123 毫秒, 模式: normal. 默认只显示一年内的数据, 点击 all 链接查看所有.

128.136.52.84

128.136.52.84

192.185.206.148

192.185.206.148

idp.dma.safemls.net

128.136.52.84

2018-11-05

United States / Charlotte

Apache-Coyote/1.1

HTTP/1.1 200 OK
Connection: close
Content-Length: 227
Content-Type: text/html; charset=ISO-8859-1
Date: Mon, 05 Nov 2018 14:54:18 GMT
P3ps: CP="CAO PSA OUR"

192.185.206.148

2018-11-05

United States / Houston

Apache/2.4.16 (Unix) OpenSSL/1.0.1e-fips mod_bwlimited/1.4

HTTP/1.1 200 OK
Connection: close
Content-Length: 111
Accept-Ranges: bytes
Content-Type: text/html
Date: Mon, 05 Nov 2018 14:54:18 GMT

<https://fofa.so/>

Input: Dominio, IP



File/URL Report Search YARA Search String Search

This is a free malware analysis service for the community that detects and analyzes unknown threats using a unique Hybrid Analysis technology.

Drag & Drop For Instant Analysis

or

Analyze

Powered by Falcon Sandbox v8.20 [🔗](#). Maximum upload size is 100 MB.
📘 Learn more about the [standalone version](#) or purchase a [private webservice](#).

<https://www.hybrid-analysis.com>

Hybrid Analysis es una herramienta similar a VirusTotal, enfocada a la detección de Malware. Permite subir ficheros o analizar URLs para su análisis y detectar IoC relacionados con alguna amenaza en concreto. Posee un buscador para localizar dominios, direcciones IP o hashes alojados en sus BBDD sobre IoC. También es posible configurar reglas YARA para identificar cualquier coincidencia que se produzca.

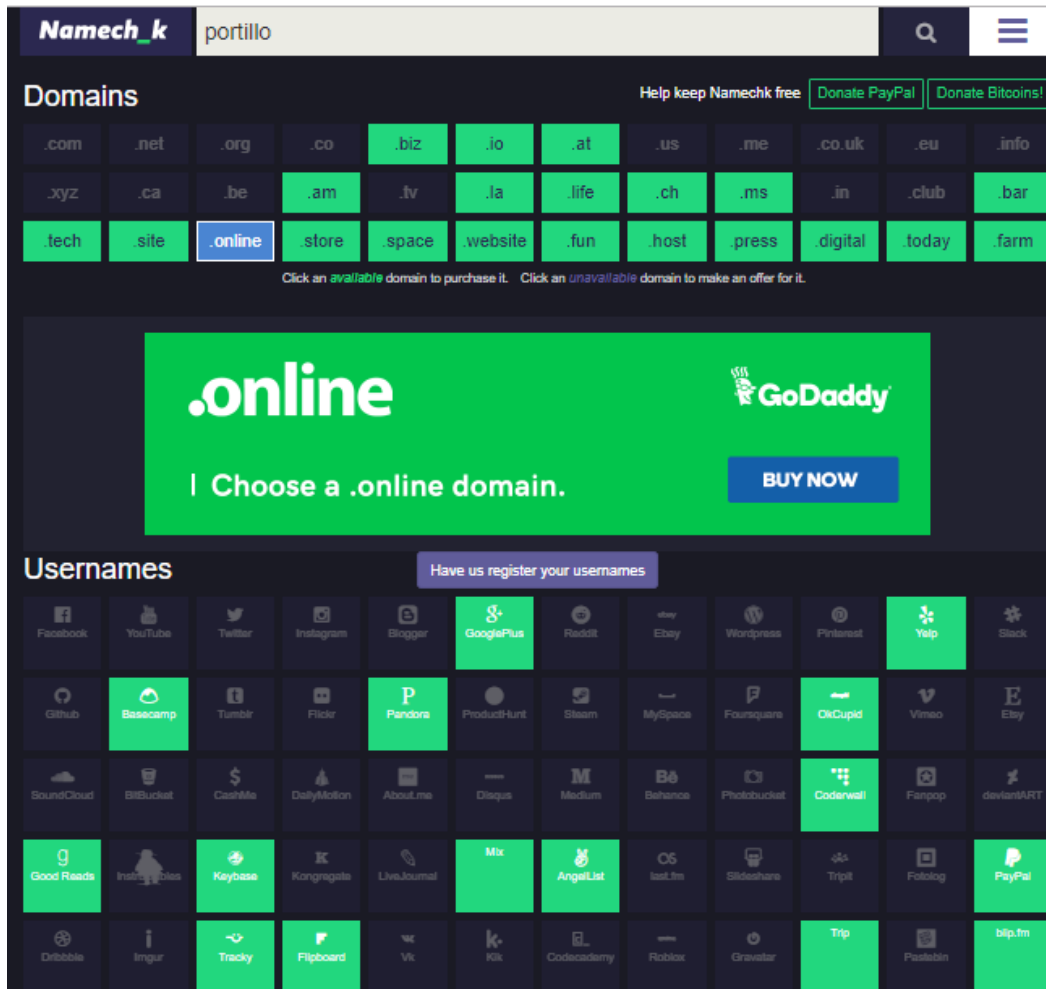
Input: Dominio, IP, Rango IP, ASN,
Nombre Organización

<http://ipv4info.com>

IPv4Info es una herramienta online que permite realizar investigaciones mediante un buscador obteniendo información relacionada a Dominios, Sitios Webs, DNS, Rangos IP, Direcciones IP, Sistemas Autónomos a partir de un input dado.

Input: Dominio, IP, ASN, Nombre Organización

Search results for "incibe"									
Ordered by block size.									
N	I	Block start	End of block	Size	D	AS	Block name	Organization	Country
1		195.53.165.0	195.53.165.255	256		AS3352	INCIBE	S.M.E. Instituto Nacional de Ciberseguridad de España, M.P., S.A Internet Public Addresses ___	ES, Leon
2		193.146.253.0	193.146.253.255	256		AS766	INCIBE	Instituto Nacional de Ciberseguridad	ES, Villablino
3		195.235.9.96	195.235.9.103	8		AS3352	INCIBE	S.M.E. Instituto Nacional de Ciberseguridad de España, M.P., S.A. Internet Public Addresses ___	ES, Madrid



<https://namechk.com>

Herramienta que permite realizar búsquedas a partir de un nombre de un usuario dado, comprobando coincidencias en las diferentes plataformas de Redes Sociales. También indica que dominios están libres relacionados al nombre de usuario introducido para poder ser registrados si se desea.

Input: Nombre Usuario

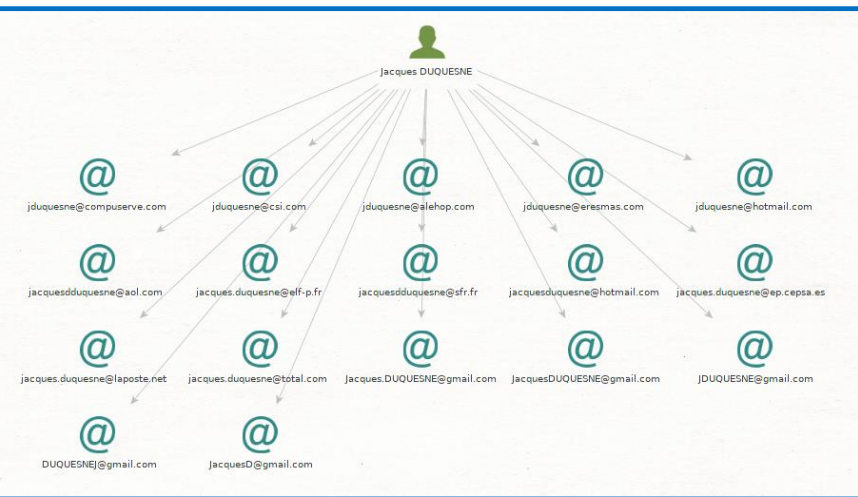
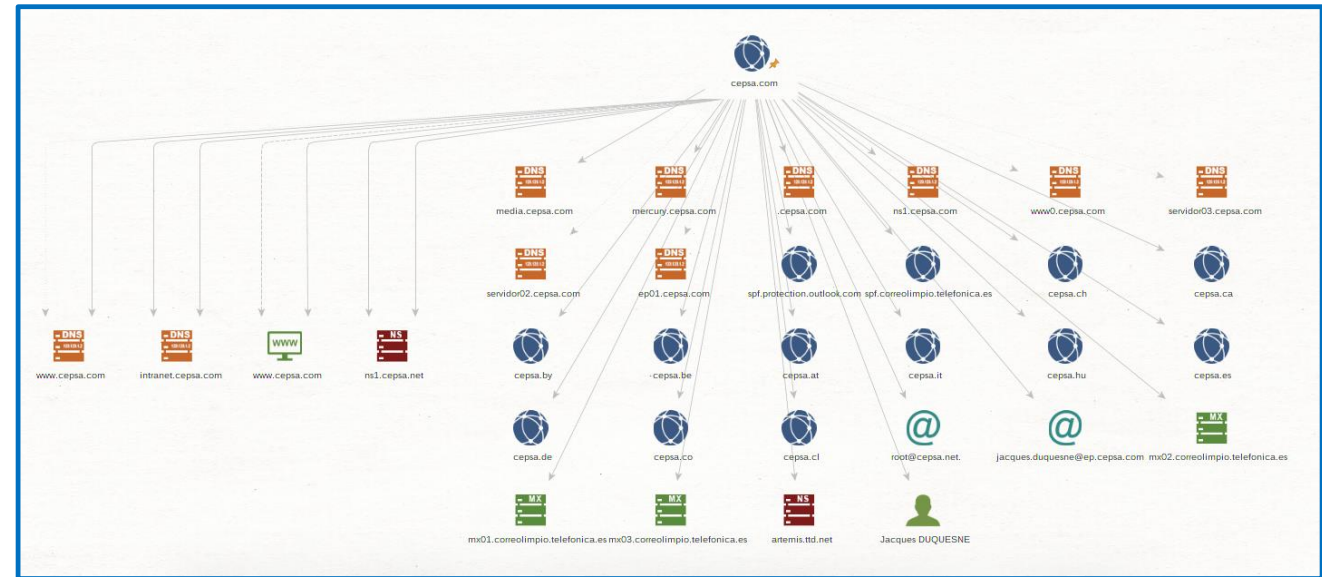
The screenshot shows the Pipl website interface. At the top, there is a search bar with the text 'mariano rajoy' and a placeholder 'Ubicación (opcional)'. Below the search bar, on the left, is a sidebar titled 'Resultados Para' (Results for) with a list of search criteria: Mariano Rajoy, Madrid, Spain, Marina Hurtado Mira, Lara Martín Gilarranz, Nuria Ortiz Olalla, and Real Estate Registrar. The main content area displays a profile for 'Mariano Rajoy'. The profile includes a purple square icon with a white 'M', the name 'Mariano Rajoy', and the text 'Hombre De Madrid, Spain'. Below this, there are sections for 'CARRERA:' (Career), 'EDUCACIÓN:' (Education), 'NOMBRE DE USUARIO:' (Username), 'ADICIONAL NOMBRE:' (Additional Name), 'UBICACIÓN:' (Location), and 'ASOCIADO CON:' (Associated with). The 'CARRERA:' section lists various roles including Prime Minister of Spain and Vice President of the Centrist Democrat International. The 'EDUCACIÓN:' section lists 'Real Estate Registrar (desde 1978)'. The 'NOMBRE DE USUARIO:' section lists 'marianorajoy'. The 'ADICIONAL NOMBRE:' section lists 'Mariano Rajoy Brey'. The 'UBICACIÓN:' section lists 'Madrid, Spain'. The 'ASOCIADO CON:' section lists 'Marina Hurtado Mira , Lara Martín Gilarranz , Nuria Ortiz Olalla , David Carrasco Salgueiro , Matilde Rodríguez'. At the bottom of the profile, there are four social media links: LinkedIn, Pinterest, Twitter, and Instagram, each with a small icon and the text 'Mariano Rajoy Brey, marianorajoy'.

<https://pipl.com>

Pipl es una herramienta online que permite obtener información sobre una persona, indicando si posee un perfil en cualquiera de las redes sociales mas importantes, además de ofrecer información básica de la persona.

Input: Nombre Persona, Email, Teléfono

Maltego es una herramienta que recopila información, mostrando las evidencias mediante grafos, siendo de gran ayuda en el análisis posterior de la información obtenida por los equipos de inteligencia y forense. Contiene una serie de módulos de aplicaciones externas (transforms) que complementan su potencial, además de una sencilla integración con APIs de distintas fuentes de información.



Comando: maltego

<https://www.paterva.com>

+	PATERVA CTAS CE	CaseFile Entities
	Paterva Standard Paterva Transforms FREE INSTALLED	Paterva Additional entities from CaseFile FREE INSTALLED
Cisco Threat Grid Cisco Threat Grid Query Threat Grid's database of threat intelligence. COMMERCIAL	Kaspersky Lab Kaspersky Lab Query Kaspersky Threat Intelligence Data Feeds. Note 1... INSTALLED	Shodan Andrew Paterva Query Shodan data from within Maltego! FREE INSTALLED
ZETalytics Massive Passive ZETalytics Fetches include billions of records for historical domains... FREE INSTALLED	Hybrid-Analysis Hybrid Analysis This set of transforms are based on the hybrid analysis... FREE INSTALLED	VirusTotal Public API Malformity Labs Query the VirusTotal Public API FREE INSTALLED
ThreatMiner ThreatMiner Query and pivot on data from ThreatMiner.org. FREE INSTALLED	PassiveTotal PassiveTotal Query PassiveTotal source and account data. FREE INSTALLED	Farsight DNSDB Farsight Security, Inc. Query the largest DNS intelligence database, 100+ Bill... FREE INSTALLED
Blockchain.info (Bitcoin) Blockchain.info For visualizing the Bitcoin blockchain. FREE INSTALLED	SocialLinks CE SocialLinks CE SocialLinks CE INSTALLED	The Movie Database The Movie Database Transforms that visualize the movie database (TMDB) FREE INSTALLED
Have I been Pwned? Have I been Pwned? Fetches insights into the people who matter most. FREE INSTALLED	People Mon People Mon Query People Mon FREE INSTALLED	CipherTrace CipherTrace Cryptocurrency forensics and anti money laundering (AML)... FREE INSTALLED
FullContact Christian Heinrich WHO insights into the people who matter most. FREE INSTALLED	Clearbit Christian Heinrich Enrich sign-ups, identify prospects and gain customer i... FREE INSTALLED	SocialLinks SocialLinks Social Networks, Search Engines, People and Companies COMMERCIAL
Recorded Future Inc. Recorded Future Inc. Query Recorded Future for threat intelligence information COMMERCIAL	ThreatConnect ThreatConnect ThreatConnect Platform Transform Set COMMERCIAL	Palo Alto Networks AutoFocus Palo Alto Networks Query Palo Alto Networks' AutoFocus API COMMERCIAL
ThreatGRID by Malformity Labs Malformity Labs No longer accepting new customers, please use the off... COMMERCIAL	Flashpoint Flashpoint Business Risk Intelligence (BRI) from the Deep and Dar... COMMERCIAL	Intel 471 Intel 471 Query Intel 471 for actor-centric intelligence information... COMMERCIAL



Investigación objetivo...



Noviembre 2018

/

HoneyCon 4ª edición



Se automatiza el proceso y se genera un CSV con los datos. El script consiste en la obtención de los rangos, nombre y descripciones por la que está registrado una organización buscada dentro de RIPE.

1.ripe.py



Comando:
python 1.ripe.py -f "listado_empresas" -o "fichero_salida"

	A	B	C	D
1	Range IP	Organization	Description	Country
2	193.148.246.0 - 193.148.246.255	CEPSA		ES
3	194.224.149.136 - 194.224.149.143	CEPSA	COMPANIA ESPANOLA DE PETROLEOS S.A.U.	ES
4	194.224.197.80 - 194.224.197.87	CEPSA	COMPañIA ESPAñOLA DE PETROLEOS, S.A.	ES
5	195.76.144.64 - 195.76.144.67	CEPSA	COMPANIA ESPANOLA DE PETROLEOS S A	ES
6	195.235.104.16 - 195.235.104.19	cepsa	Compania Espanola de Petroleos S.A.	ES
7	212.170.35.160 - 212.170.35.167	CEPSA	CEPSA	ES
8	213.4.82.160 - 213.4.82.191	CEPSA	CEPSA	ES
9	213.121.179.192 - 213.121.179.199	CEPSA	FTIP003330890 Cespa UK Ltd	GB

```
osintux@OSINTUX:~/OSINT/scripts-automatizados$ python 1.ripe.py -f empresas.txt -o salida
['cepsa']
08/11/2018 - 11:44:44

cepsa
[{'inetnum': '193.148.246.0 - 193.148.246.255'}, {'netname': 'CEPSA'}, {'country': 'ES'}]
[{'inetnum': '194.224.149.136 - 194.224.149.143'}, {'netname': 'CEPSA'}, {'descr': 'COMPANIA ESPANOLA DE PETROLEOS S.A.U.'}, {'descr': 'Internet Public Addresses'}, {'descr': '___'}, {'country': 'ES'}]
[{'inetnum': '194.224.197.80 - 194.224.197.87'}, {'netname': 'CEPSA'}, {'descr': 'COMPañIA ESPAñOLA DE PETROLEOS, S.A.'}, {'descr': 'Internet Public Addresses'}, {'descr': 'CHN2 60001'}, {'country': 'ES'}]
[{'inetnum': '195.76.144.64 - 195.76.144.67'}, {'netname': 'CEPSA'}, {'descr': 'COMPANIA ESPANOLA DE PETROLEOS S A'}, {'descr': 'Internet Public Addresses'}, {'country': 'ES'}]
[{'inetnum': '195.235.104.16 - 195.235.104.19'}, {'netname': 'cepsa'}, {'descr': 'Compania Espanola de Petroleos S.A.'}, {'descr': 'Internet Public Addresses'}, {'country': 'ES'}]
[{'inetnum': '212.170.35.160 - 212.170.35.167'}, {'netname': 'CEPSA'}, {'descr': 'CEPSA'}, {'descr': 'Internet Public Addresses'}, {'descr': 'cdg Alcala t142756'}, {'country': 'ES'}]
[{'inetnum': '213.4.82.160 - 213.4.82.191'}, {'netname': 'CEPSA'}, {'descr': 'CEPSA'}, {'descr': 'Internet Public Addresses'}, {'descr': 'TAH 133798'}, {'country': 'ES'}]
[{'inetnum': '213.121.179.192 - 213.121.179.199'}, {'netname': 'CEPSA'}, {'descr': 'FTIP003330890 Cespa UK Ltd'}, {'country': 'GB'}]
08/11/2018 - 11:44:44
osintux@OSINTUX:~/OSINT/scripts-automatizados$
```


Consiste en identificar nombres de empresas en LibreBorne a partir de una palabra de búsqueda para poder detectar datos relacionados como sociedades colaboradoras o cargos directivos de personas.

2.libreBorne.py

Comando:
python 2.libreBorne.py -f "listado_empresas" -o "fichero_salida"

Dependencias: pip install xlrd xlutils

Datos Empresa

Nombre Empresa, Tipo de Sociedad, Fuente, ¿Esta Activa?, Fecha Actualización

Cargos Directivos

Nombre Empresa, Nombre Persona, Cargo y Fecha Oficial de Incorporación

Sociedades Relacionadas

Nombre Empresa, Empresa, tipo y Fecha Inicial de relación

```
osintux@OSINTUX:~/OSINT/scripts-automatizados$ python 2.libreborne.py -f empresas.txt -o salida
['cepsa']
08/11/2018 - 12:02:17
-----
**Nombre Empresa: CEPSA
Número total de sociedades relacionadas: 0
Número total de directivos relacionadas: 23
**Nombre Empresa: CEPSA AVIACION
Número total de sociedades relacionadas: 12
Número total de directivos relacionadas: 63
**Nombre Empresa: CEPSA BUNKER
Número total de sociedades relacionadas: 0
Número total de directivos relacionadas: 0
**Nombre Empresa: CEPSA COLOMBIA
Número total de sociedades relacionadas: 7
Número total de directivos relacionadas: 165
**Nombre Empresa: CEPSA COMERCIAL CENTRO
Número total de sociedades relacionadas: 0
Número total de directivos relacionadas: 0
**Nombre Empresa: CEPSA COMERCIAL ESTE
Número total de sociedades relacionadas: 0
Número total de directivos relacionadas: 0
**Nombre Empresa: CEPSA COMERCIAL GALICIA
Número total de sociedades relacionadas: 0
Número total de directivos relacionadas: 0
```

1	Nombre Empresa	Tipo Empresa	URL Fuente	Activa	Fecha Creación	Fecha Actualización
2	CEPSA	SA	/borme/api/v1/empresa/cepsa/	VERDADERO		2017-10-31
3	CEPSA AVIACION	SA	/borme/api/v1/empresa/cepsa-aviacion/	VERDADERO		2017-11-21
4	CEPSA COLOMBIA	SA	/borme/api/v1/empresa/cepsa-colombia/	VERDADERO		2018-05-23
5	CEPSA COMERCIAL CENTRO	SA	/borme/api/v1/empresa/cepsa-comercial-centro/	FALSO		2015-11-20
6	CEPSA COMERCIAL ESTE	SA	/borme/api/v1/empresa/cepsa-comercial-este/	FALSO		2015-12-18
7	CEPSA COMERCIAL GALICIA	SA	/borme/api/v1/empresa/cepsa-comercial-galicia/	FALSO		2010-08-24
8	CEPSA COMERCIAL MADRID	SA	/borme/api/v1/empresa/cepsa-comercial-madrid/	VERDADERO		2010-08-24
9	CEPSA COMERCIAL NORTE	SL	/borme/api/v1/empresa/cepsa-comercial-norte/	FALSO		2014-12-29
10	CEPSA CONVENIENCIA	SA	/borme/api/v1/empresa/cepsa-conveniencia/	FALSO		2014-11-27
11	CEPSA GAS LICUADO	SA	/borme/api/v1/empresa/cepsa-gas-licuado/	FALSO		2013-12-12
12	CEPSA GLOBAL SERVICES	SA	/borme/api/v1/empresa/cepsa-global-services/	FALSO		2016-11-10
13	CEPSA LIBERIA	SL	/borme/api/v1/empresa/cepsa-liberia/	FALSO		2016-01-26
14	CEPSA LOS OLIVOS	SA	/borme/api/v1/empresa/cepsa-los-olivos/	FALSO		2018-01-05
15	CEPSA LUBRICANTES	SA	/borme/api/v1/empresa/cepsa-lubricantes/	FALSO		2014-07-04
16	CEPSA MARINE FUELS	SA	/borme/api/v1/empresa/cepsa-marine-fuels/	FALSO		2014-01-07
17	CEPSA PERU	SA	/borme/api/v1/empresa/cepsa-peru/	VERDADERO		2018-03-22
18	CEPSA PETRONUBA	SA	/borme/api/v1/empresa/cepsa-petronuba/	VERDADERO		2017-11-22
19	CEPSA PETROSUR	SA	/borme/api/v1/empresa/cepsa-petrosur/	FALSO		2009-03-03
20	CEPSA SEA	SL	/borme/api/v1/empresa/cepsa-sea/	VERDADERO		2018-03-20
21	CEPSA SURINAME	SL	/borme/api/v1/empresa/cepsa-suriname/	VERDADERO		2018-01-24

Gracias a este script obtendremos la información relacionada con los datos que Shodan posee sobre el objetivo a partir del nombre de la empresa. Además, y frente al buscador web, obtendremos acceso completo a todos los datos recopilados. Se automatiza el proceso y se genera un CSV con los datos.

7.shodan.py



Comando:

```
python 7.shodan.py -f "listado_empresas" -o "fichero_salida"
```

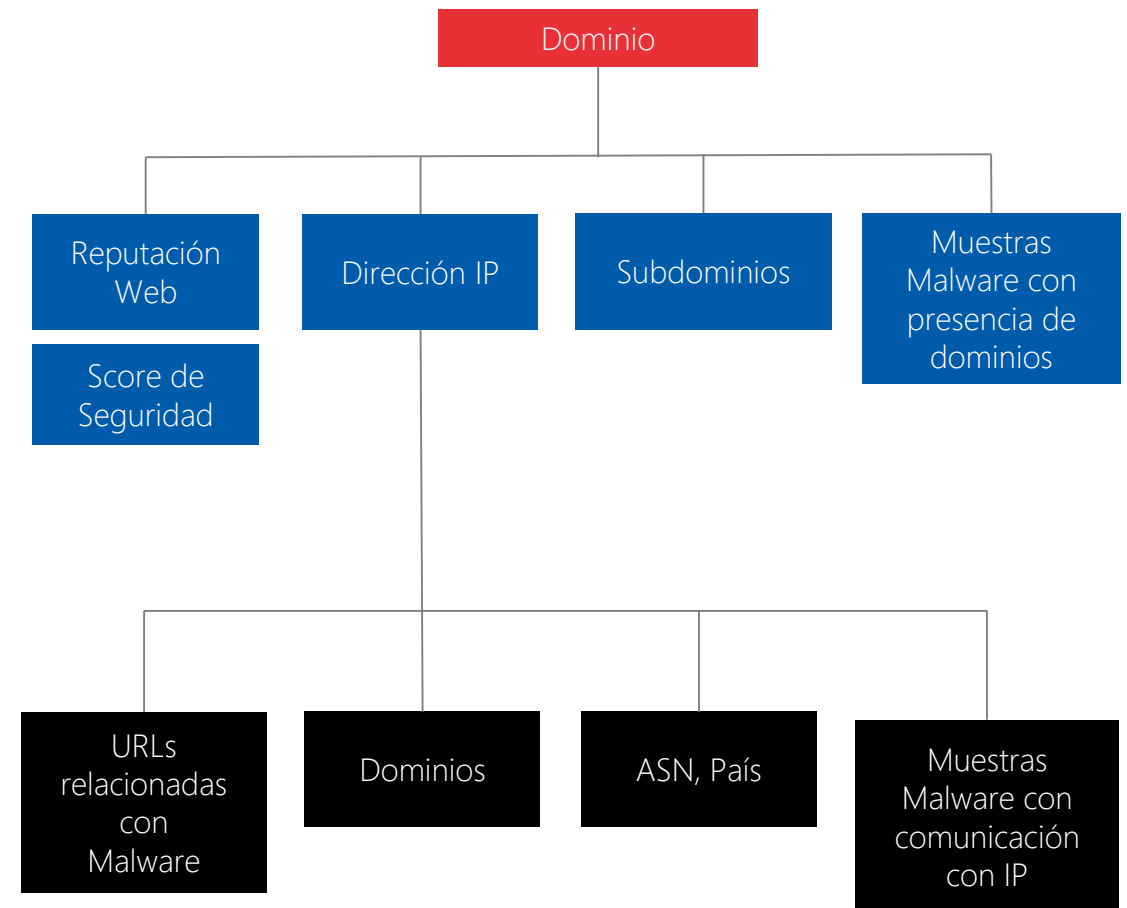
Dependencias: pip install shodan

IP Address	Organization	Port 1	Port 2	Port 3	Port 4	ISP	Location	Protocol	Title	Product	CPE 1	CPE 2	OS	ASN	Domain 1
190.171.231.127	Repsol Ypf Bolivia SA	443	902			Cotas Ltda.	Bolivia	https		VMware VirtualCenter Web service			None	AS25620	cotas.com.bo
185.145.228.18	Repsol S.A.	80				Repsol S.A.	Spain	http					None		
185.145.228.29	Repsol S.A.	443				Repsol S.A.	Spain	https					None		
185.145.228.23	Repsol S.A.	443	9443	80		Repsol S.A.	Spain	https					None		
185.145.228.31	Repsol S.A.	443	80			Repsol S.A.	Spain	https					None		
185.145.230.27	Repsol S.A.	80				Repsol S.A.	Spain	http					None		
185.145.228.22	Repsol S.A.	443				Repsol S.A.	Spain	https					None		
185.145.228.21	Repsol S.A.	9443	443	80		Repsol S.A.	Spain	https					None		
185.145.228.19	Repsol S.A.	80				Repsol S.A.	Spain	http					None		
185.145.228.27	Repsol S.A.	80				Repsol S.A.	Spain	http					None		
185.145.230.18	Repsol S.A.	80				Repsol S.A.	Spain	http					None		
185.145.228.20	Repsol S.A.	80				Repsol S.A.	Spain	http					None		
185.145.230.19	Repsol S.A.	80				Repsol S.A.	Spain	http					None		



```
osintux@OSINTUX:~/OSINT/scripts-automatizados$ python 3.virustotal.py -f domain.txt -o result_vt
Drop empty line
['cepsa.com']
08/11/2018 - 12:07:20
-----
Dominio analizado: cepsa.com
*** Numero de total de subdominios detectados: 23
*** Numero de total dominios que comparten dirección IP: 173
*** Numero de total de muestras detectadas relacionadas con el dominio: 0
*** Numero de total de muestras detectadas comunicandose con la IP: 1
*** Numero de total URLs con presencia de Malware detectadas: 1
08/11/2018 - 12:07:21
osintux@OSINTUX:~/OSINT/scripts-automatizados$
```

A través de **VirusTotal** se analiza un dominio detectando información relativa a este (subdominios, muestras de malware con la presencia del dominio). Mediante la dirección IP, se obtienen dominios que comparten la misma IP, además de URLs y muestras malware que evidencian comunicación hacia dicha.



3.virustotal.py

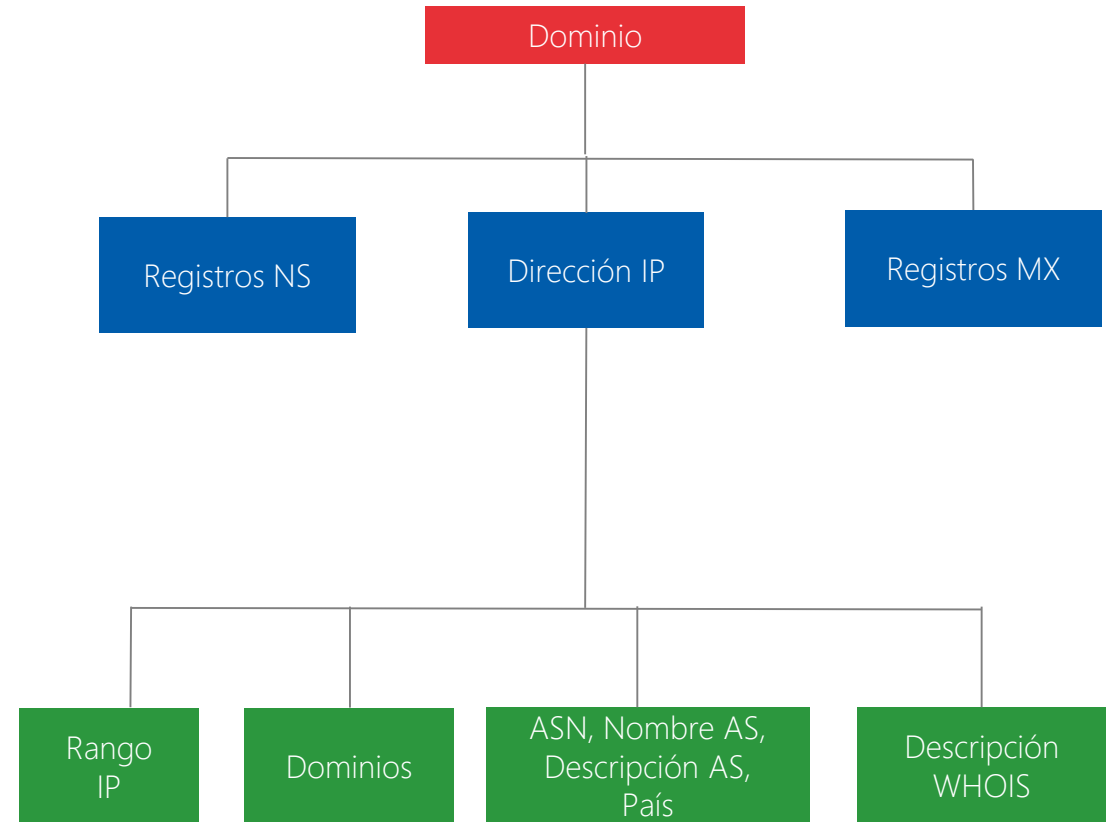


Comando:

python 3.virustotal.py -f "listado_dominios" -o "fichero_salida"


```
osintux@OSINTUX:~/OSINT/scripts-automatizados$ python 4.robtex.py -f domain.txt -o result
Drop empty line
['cepsa.com']
08/11/2018 - 12:15:14
-----
*** Dominio Analizado: cepsa.com
*** Direccion IP: 213.4.82.173
*** Numero de dominios que comparten dirección IP: 20
08/11/2018 - 12:15:16
osintux@OSINTUX:~/OSINT/scripts-automatizados$
```

A través de **Robtex** se analiza un dominio detectando información relativa a este, como la Dirección IP, Registros MX y NS. Mediante la dirección IP, se obtienen dominios que comparten la misma IP, además de un whois.



4.robtex.py



Comando:
python 4.robtex.py -f "listado_dominios" -o "fichero_salida"



<https://spiderfoot.net/download/>

SpiderFoot es una herramienta OSINT enfocada a la recopilación de información, permitiendo seleccionar el tipo de investigación mediante fuentes concretas, tipos de datos o caso de uso. Integra multitud de fuentes, tanto privadas como públicas, de manera modular.

Comando:

```
sudo python spiderfoot/sf.py 0.0.0.0:5001
```

Dependencias:

```
pip install lxml netaddr M2Crypto cherrypy mako
```

Acceso :

Dirección_IP:5001

Target:



Usage

The *Seed Target* can be one of the following. SpiderFoot will automatically detect the target type based on the format of your input.

Domain Name: e.g. *example.com*

IP Address: e.g. *1.2.3.4*

Hostname/Sub-domain: e.g. *abc.example.com*

Subnet: e.g. *1.2.3.0/24*

E-mail address: e.g. *target.bob@example.com*



Consiste en la obtención de información relacionada con la geolocalización de un dominio concreto. Se automatiza el proceso para varios dominios y se genera un CSV con los datos resultantes.

5.geoip.py

>

Comando:
python 5.geoip.py -f "listado_dominios" -o "fichero_salida"

Dependencias: pip install python-geoip-geolite2

```
osintux@OSINTUX:~/OSINT/scripts-automatizados$ python 5.geoip.py -f dominios.txt -o salida
['cepsa.com']
08/11/2018 - 12:17:37
-----
cepsa.com
<IPInfo ip='213.4.82.173' country='ES' continent='EU' subdivisions=frozenset([]) timezone='None' location=(40.4, -3.6833)>
-----
08/11/2018 - 12:17:37
osintux@OSINTUX:~/OSINT/scripts-automatizados$
```

	A	B	C	D	E	F
1	Domain	IP	Country	Continent	Timezone	Location
2	cepsa.com	213.4.82.173	ES	EU	None	(40.4, -3.6833)

Datasploit es una potentísima herramienta escrita en los resultados y mostrando los resultados de manera consolidada. Busca credenciales, api-keys, tokens, subdominios, historiales del dominio, ...

Además, genera informes en HTML y JSON, lo que puede servir como entrada para otras herramientas.

```
----> Finding DNS Records.
A Records
213.4.82.173
MX Records
10 mx03.correolimpio.telefonica.es.
10 mx01.correolimpio.telefonica.es.
10 mx02.correolimpio.telefonica.es.
SOA Records
ns1.cepsa.net. root.cepsa.net. 2018021378 360 7200 2592000 172800
Name Server Records
ns1.cepsa.net.
artemis.ttd.net.
TXT Records
"v=spf1 mx include:spf.correolimpio.telefonica.es include:spf.protection.outlook.com ~all"
"MS=ms29288367"
"cgKUEw/4FjwIXq/h/N0sHFRBAm8Fb1vfm5P9u1cLRUjhledWQxEdiw7SWSNnDAsd7lo0hrQEPj+uaJyetYzFBg=="
CNAME Records
No Records Found
AAAA Records
No Records Found

----> Finding Whois Information.
{u'updated_date': '12/31/2017', u'status': [u'ok https://icann.org/epp#ok', u'ok http://www.icann.org/epp#ok'], u'dnssec': u'unsigned', u'domain_name': [u'CEPSA.COM', u'cepsa.com'], u'whois_server': u'whois.acens.net', u'address': None, u'name_servers': [u'ARTEMIS.TTD.NET', u'NS1.CEPSA.NET', u'artemis.ttd.net', u'ns1.cepsa.net'], u'org': u'Compania Espanola de Petroleos', u'creation_date': '01/02/1998', u'emails': u'abuse@acens.net', u'city': None, u'name': None, u'expiration_date': '01/01/2019', u'zipcode': None, u'state': u'Madrid', u'registrar': u'acens Technologies, S.L', u'country': u'ES'}

----> Waplyzing web page of base domain:
Hitting HTTP and HTTPS:
[+] Third party libraries in Use for HTTP:
Java
Google Tag Manager
YouTube
[+] Third party libraries in Use for HTTPS:
Java
Google Tag Manager
YouTube
```

<https://github.com/DataSploit/datasploit>

Comando
Principal

`python datasploit.py -i cepsa.com`

Investigación
Email

`python emails/email_basic_checks.py
correo@correo.com`

Investigación
Username

`python username/username_gitscrape.py
username`

Input: Dominio, Email, Username, Teléfono, IP

<https://bitbucket.org/LaNMaSteR53/recon-ng.git>

```
[recon-ng][honey18][netcraft] > use recon/domains-hosts/google_site_web
[recon-ng][honey18][google_site_web] > run

-----
CEPSA.COM
-----
[*] Searching Google for: site:cepsa.com
[*] [host] asphalts.cepsa.com (<blank>)
[*] [host] pt.cepsa.com (<blank>)
[*] [host] ww.cepsa.com (<blank>)
[*] [host] aviation.cepsa.com (<blank>)
[*] Searching Google for: site:cepsa.com -site:asphalts.cepsa.com -site:pt.cepsa.com -site:ww.cepsa.com -site:aviation.cepsa.com
[*] [host] fundacion.cepsa.com (<blank>)
[*] [host] ww.es.cepsa.com (<blank>)
[*] Searching Google for: site:cepsa.com -site:asphalts.cepsa.com -site:pt.cepsa.com -site:ww.cepsa.com -site:aviation.cepsa.com -site:fundacion.cepsa.com -site:ww.es.cepsa.com
[*] [host] prv.cepsa.com (<blank>)
[*] Searching Google for: site:cepsa.com -site:asphalts.cepsa.com -site:pt.cepsa.com -site:ww.cepsa.com -site:aviation.cepsa.com -site:fundacion.cepsa.com -site:ww.es.cepsa.com -site:prv.cepsa.com
[*] No New Subdomains Found on the Current Page. Jumping to Result 201.
[*] Searching Google for: site:cepsa.com -site:asphalts.cepsa.com -site:pt.cepsa.com -site:ww.cepsa.com -site:aviation.cepsa.com -site:fundacion.cepsa.com -site:ww.es.cepsa.com -site:prv.cepsa.com

-----
SUMMARY
-----
[*] 7 total (6 new) hosts found.
[recon-ng][honey18][google_site_web] > 
```

```
[recon-ng][honey18][punkspider] > use recon/domains-vulnerabilities/xssed
[recon-ng][honey18][xssed] > run

-----
CEPSA.COM
-----

[*] Category: XSS
[*] Example: http://www.cepsa.com/portal/site/cepsa/buscador?q=%22%3E%3Cscript%3Ealert%28%27xss%27%29;%3C/script%3C-br>3
[*] Host: www.cepsa.com
[*] Publish Date: 2011-12-11 00:00:00
[*] Reference: http://xssed.com/mirror/72598/
[*] Status: unfixed
[*] -----

-----
SUMMARY
-----

[*] 1 total (1 new) vulnerabilities found.
[recon-ng][honey18][xssed] > 
```

DNSTwist es una librería open-source creada para el análisis de amenazas de Typosquatting y suplantación de dominios.

<https://github.com/elceef/dnstwist>

Comando:

```
python dnstwist.py -b -w -g -m google.es
```

Dependencias: pip install GeolIP

dnspython requests ssdeep

Input: Dominio

```
dnstwist (1.04b)
Disabling multithreaded job distribution in order to query WHOIS servers
Processing 190 domain variants .....20%.....41%.....62%.....
..... 85 hits (42%)

Original* google.es 216.58.201.131/United States 2a00:1450:4003:804::2003 NS:ns1.google.com MX:alt1.aspmx.l.google.com HTTP:"gws" SMTP:"mx.google.com ESMTP l131si2660871lfb.6 - gsmtp"
Addition google.es 176.28.103.205/Spain NS:ns1.srv-hostalia.com MX:mx.google.es HTTP:"Apache" SMTP:"relayin06.dominioabsoluto.net ESMTP"
Addition google.es -
Addition googled.es 185.53.177.20/Germany NS:ns1.eurodns.com MX:mail.googled.es HTTP:"nginx" SMTP:"corellia.eurodns.com EuroDNS Mail Server"
Addition google.es 185.53.178.9/Germany NS:ns1.parkingcrew.net MX:mail.h-email.net HTTP:"nginx"
Addition google.es -
Addition googleg.es 217.76.128.34/Spain NS:dns23.servidoresdns.net HTTP:"Microsoft-IIS/7.5"
Addition googleh.es -
Addition googlei.es 212.227.247.183/Germany NS:ns63.land1.es MX:mx00.land1.es HTTP:"Apache" SMTP:"554-kundenserver.de (mxue003) Nemesi E"
Addition googlej.es -
Addition googlek.es -
Addition googlem.es -
Addition googlen.es -
Addition googleo.es -
Addition googlep.es -
Addition googleg.es -
Addition googler.es 82.194.64.60/Spain NS:dns1.canaldominios.com MX:mx01.canaldominios.com HTTP:"Apache" SMTP:"mx01.canaldominios.com ESMTP"
Addition googles.es 185.53.178.7/Germany NS:ns1.parkingcrew.net MX:mail.h-email.net HTTP:"nginx"
Addition googlet.es -
Addition googlew.es -
Addition googlev.es 188.165.119.163/Spain NS:ns1.cdmon.net MX:yahoo.es HTTP:"Apache"
Addition googlex.es -
Addition googley.es 37.152.88.54/Spain NS:ns2.dondominio.com HTTP:"Apache"
Addition googlez.es 185.53.178.7/Germany NS:ns1.parkingcrew.net MX:mail.h-email.net HTTP:"nginx"
Bitsquatting foogle.es -
Bitsquatting eoogle.es -
Bitsquatting coogle.es 37.152.88.54/Spain NS:ns1.dondominio.com HTTP:"Apache"
Bitsquatting ooogle.es 50.63.202.19/United States NS:ns61.domaincontrol.com MX:mailstore1.secureserver.net HTTP:"HTTP 302" SMTP:"554 p3plbsmtp02-12.prod.phx3.secureserv"
Bitsquatting woogle.es 37.152.88.54/Spain NS:ns2.dondominio.com HTTP:"Apache"
Bitsquatting gnogle.es -
Bitsquatting gmogle.es -
Bitsquatting gkogle.es 0.0.0.0 NS:ns1.google.es
Bitsquatting ggogle.es -
Bitsquatting gongle.es -
Bitsquatting gomgle.es -
Bitsquatting gokgle.es -
Bitsquatting google.es 213.186.33.5/France NS:dns10.ovh.net MX:redirect.ovh.net HTTP:"nginx"
Bitsquatting goofle.es -
Bitsquatting goole.es 37.152.88.54/Spain NS:ns1.dondominio.com HTTP:"Apache"
Bitsquatting goole.es 50.63.202.14/United States NS:ns61.domaincontrol.com MX:mailstore1.secureserver.net HTTP:"HTTP 302" SMTP:"554 p3plbsmtp01-09.prod.phx3.secureserv"
Bitsquatting google.es -
Bitsquatting googme.es -
Bitsquatting googne.es -
Bitsquatting googhe.es -
Bitsquatting googde.es -
Bitsquatting googld.es -
```

El script consiste en la generación de un listado de un dominio, combinándolo con diferentes TLDs para obtener de manera automatizada todos los registros A, NS y MX de cada uno de ellos.

6.tlds.py



Comando:

```
python 6.tlds.py -f "listado_dominios" -o "fichero_salida" -i "fichero_tlds"
```

```
osintux@OSINTUX:~/OSINT/scripts-automatizados$ python 6.tlds.py -f dominios.txt -o salida -i tld.txt
cepsa.com
['cepsa.it', 'cepsa.biz', 'cepsa.eu', 'cepsa.net', 'cepsa.org', 'cepsa.com', 'cepsa.info', 'cepsa.gov.it', 'cepsa.ch', 'cepsa.ru', 'cepsa.us', 'cepsa.post', 'cepsa.es', 'cepsa.fr', 'cepsa.int', 'cepsa.pro', 'cepsa.tel', 'cepsa.co', 'cepsa.uk', 'cepsa.su', 'cepsa.ar', 'cepsa.at', 'cepsa.ae', 'cepsa.be', 'cepsa.br', 'cepsa.ca', 'cepsa.cl', 'cepsa.cy', 'cepsa.cz', 'cepsa.de', 'cepsa.dk', 'cepsa.ee', 'cepsa.gr', 'cepsa.fi', 'cepsa.hk', 'cepsa.hr', 'cepsa.lu', 'cepsa.mc', 'cepsa.me', 'cepsa.nl', 'cepsa.no', 'cepsa.pt', 'cepsa.pl', 'cepsa.py', 'cepsa.se', 'cepsa.si', 'cepsa.ua']
08/11/2018 - 12:54:12
-----
cepsa.it
['185.53.179.6'] cepsa.it ['ns1.parkingcrew.net.', 'ns2.parkingcrew.net.'] [<DNS name mail.h-email.net.>]
-----
cepsa.biz
cepsa.biz [] []
-----
cepsa.eu
cepsa.eu ['ns1.cepsa.net.', 'artemis.ttd.net.'] []
-----
cepsa.net
['213.4.82.173'] cepsa.net ['ns1.cepsa.net.', 'artemis.ttd.net.'] [<DNS name mx02.correolimpio.telefonica.es.>, <DNS name mx01.correolimpio.telefonica.es.>, <DNS name mx03.correolimpio.telefonica.es.>]
-----
cepsa.org
['213.4.82.173'] cepsa.org ['artemis.ttd.net.', 'ns1.cepsa.net.'] []
-----
cepsa.com
['213.4.82.173'] cepsa.com ['artemis.ttd.net.', 'ns1.cepsa.net.'] [<DNS name mx02.correolimpio.telefonica.es.>, <DNS name mx03.correolimpio.telefonica.es.>, <DNS name mx01.correolimpio.telefonica.es.>]
-----
cepsa.info
cepsa.info [] []
-----
cepsa.gov.it
cepsa.gov.it [] []
-----
```


<https://github.com/laramies/theHarvester>

```
python theHarvester.py -d cepsa.com -l 300 -b all -f result.html
```

Input: Dominio

Listado de Subdominios e IPs

Listado de nombres de usuarios de Redes Sociales

```
*****
*
* TheHarvester
*
* TheHarvester Ver. 2.7
* Coded by Christian Martorella
* Edge-Security Research
* cmartorella@edge-security.com
*****

Usage: theharvester options

-d: Domain to search or company name
-b: data source: baidu, bing, bingapi, dogpile, google, googleCSE,
    googleplus, google-profiles, linkedin, pgp, twitter, vhost,
    yahoo, all

-s: Start in result number X (default: 0)
-v: Verify host name via dns resolution and search for virtual hosts
-f: Save the results into an HTML and XML file (both)
-n: Perform a DNS reverse query on all ranges discovered
-c: Perform a DNS brute force for the domain name
-t: Perform a DNS TLD expansion discovery
-e: Use this DNS server
-l: Limit the number of results to work with(bing goes from 50 to 50 results,
    google 100 to 100, and pgp doesn't use this option)
-h: use SHODAN database to query discovered hosts

Examples:
theHarvester.py -d microsoft.com -l 500 -b google -h myresults.html
theHarvester.py -d microsoft.com -b pgp
theHarvester.py -d microsoft -l 200 -b linkedin
theHarvester.py -d apple.com -b googleCSE -l 500 -s 300
```

Mediante la automatización de **Hunter.io** se obtiene información relacionada con perfiles de empleados/usuarios como pueden ser Email, Nombre, Apellidos, Posición, Departamento, Antigüedad, Numero Teléfono y perfiles usados en Twitter/Linkedin, a partir de un dominio dado.

8.hunter.py



Comando:
python 8.hunter.py -f "listado_dominios"
-o "fichero_salida"

```
osintux@OSINTUX:~/OSINT/scripts-automatizados$ python 8.hunter.py -f dominios.txt -o salida_hunter
['cepsa.com']
08/11/2018 - 13:34:09

-----

Dominio analizado: cepsa.com

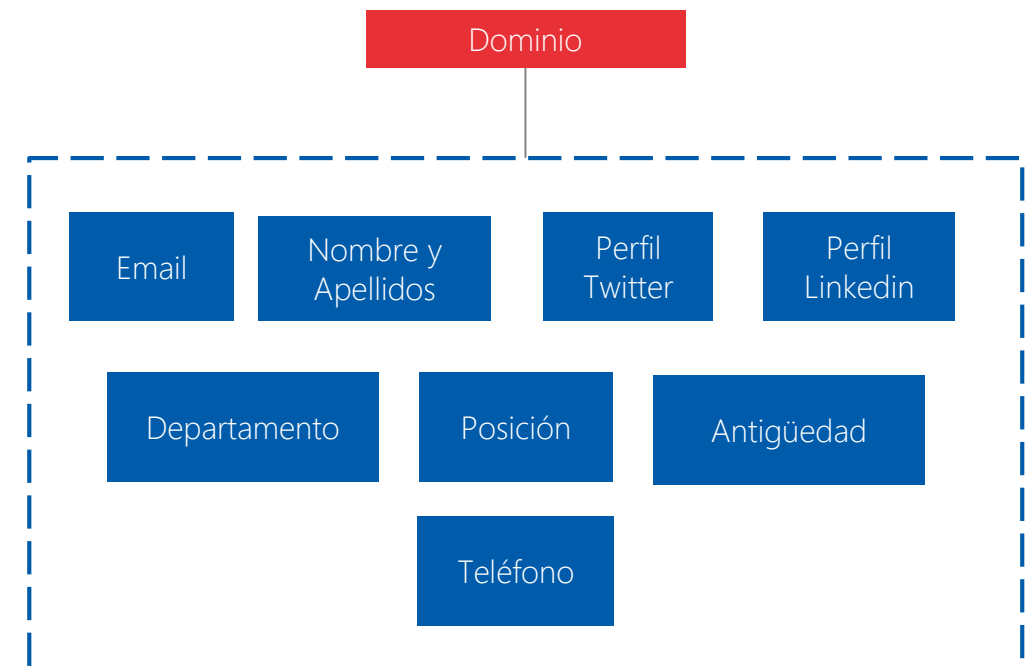
*** Numero de personas detectadas: 100

*** Numero de perfiles de Linkedin detectadas: 0

*** Numero de perfiles de Twitter detectadas: 0

-----

08/11/2018 - 13:34:10
osintux@OSINTUX:~/OSINT/scripts-automatizados$
```



9.Leak_haveibeenpwned.py

<https://haveibeenpwned.com/>

HavelbeenPwned es una herramienta web que permite comprobar si un email se encuentra en alguna de las bases de datos que han sido comprometidas (leaks). Mediante este script y realizando peticiones a su API, podemos consultar de manera masiva un listado de correos y comprobar si se encuentra en alguna de las base de datos leakeadas.

```
osintux@OSINTUX:~/OSINT/scripts-automatizados$ python 9.Leak_haveibeenpwned.py -f emails.txt -o salida_leak
Listado correos: ['jacques.meunier@cepsa.com', 'miguel.barbosa@cepsa.com', 'ignacio.rodriguez-solano@cepsa.com', 'ignacio.nieto@cepsa.com', 'abelardo.mayo@cepsa.com', 'ana.igualada@cepsa.com', 'emiliano.lopez@cepsa.com', 'daniel.demiguel@cepsa.com', 'catherine.gauthier@cepsa.com', 'angelo.carretero@cepsa.com', 'comunicacion@cepsa.com', 'porquetuvuelves@cepsa.com', 'csdpdm@cepsa.com', 'buzonbajas@cepsa.com', 'bunker@cepsa.com', 'i.ballester@cepsa.com', 'alvaro.camacho@cepsa.com', 'carolina.delaguardia@cepsa.com', 'josemaria.jimenez@cepsa.com', 'enrique.alas@cepsa.com', 'juan.arrazola@cepsa.com', 'matias.mayor@cepsa.com', 'rodrigo.garcia@cepsa.com', 'marcel.aschenbrenner@cepsa.com', 'tineke.poot@cepsa.com', 'angelo.carnevali@cepsa.com', 'felipe.seco@cepsa.com', 'joan.planes@cepsa.com', 'dpo@cepsa.com', 'cepcarco@cepsa.com', 'comunicacion.huelva@cepsa.com', 'e-center@cepsa.com', 'amarco@cepsa.com', 'quimica@cepsa.com', 'cge-comercial@cepsa.com', 'relaciones.institucionales@cepsa.com', 'castelobranco@cepsa.com', 'orbita@cepsa.com', 'fiorellavaldez@cepsa.com', 'brand@cepsa.com', 'recursos.humanos@cepsa.com', 'atencionstarressa@cepsa.com', 'saclubricantes@cepsa.com', 'asphalts@cepsa.com', 'n.datos@cepsa.com', 'responsabilidad.corporativa@cepsa.com', 'mjesus.simon@cepsa.com', 'seguridad.productos@cepsa.com', 'apoiocliente@cepsa.com', 'atc@cepsa.com', 'st.lubes@cepsa.com', 'cge-liquidaciones@cepsa.com', 'aviation.division@cepsa.com', 'satencion.cliente@cepsa.com', 'contratacionpublicamp@cepsa.com', 'jean.quesy@cepsa.com', 'vr.jimenez@cepsa.com', 'prosexport@cepsa.com', 'comunicacao@cepsa.com', 'sat@cepsa.com', 'cge-cogeneracion@cepsa.com', 'cgc@cepsa.com', 'cepsagas@cepsa.com', 'comunicacion.sanroque@cepsa.com', 'atencionweb@cepsa.com', 'colectivospt@cepsa.com', 'ecansa.lps@cepsa.com', 'sales@cepsa.com', 'tarjetas@cepsa.com', 'tarjetas@cepsa.com', 'atencion.cliente@cepsa.com', 'autogas@cepsa.com', 'cge-mercados@cepsa.com', 'cge-trading@cepsa.com', 'transclub@cepsa.com', 'siac.lubricantes@cepsa.com', 'jm.rodriguez@cepsa.com', 'joseluis.almeida@cepsa.com', 'apoiocliente@cepsa.com', 'contactcqb@cepsa.com', 'bunkers.panama@cepsa.com', 'csdfax@cepsa.com', 'cge-despacho@cepsa.com', 'parafinas@cepsa.com', 'asfaltos@cepsa.com', 'igarcia@cepsa.com', 'juanmiguel.garcia@cepsa.com', 'apoiocliente.gas@cepsa.com', 'jorge.navarro@cepsa.com', 'derechos.arco@cepsa.com', 'katie.bernard@cepsa.com', 'juana.frontela@cepsa.com', 'marta.martinez@cepsa.com', 'richard.perron@cepsa.com', 'javier.nieto@cepsa.com', 'javier.criado@cepsa.com', 'pierre.lahaie@cepsa.com', 'ccoo@cepsa.com', 'celia.martin@cepsa.com', 'luc.vanhoecke@cepsa.com']

08/11/2018 - 13:36:50
jacques.meunier@cepsa.com [u'Apollo']
-----
miguel.barbosa@cepsa.com [u'Apollo', u'LinkedIn', u'OnlinerSpambot', u'TrikSpamBotnet']
-----
ignacio.rodriguez-solano@cepsa.com [u'Apollo', u'OnlinerSpambot']
-----
No data for this mail
ignacio.nieto@cepsa.com []
-----
No data for this mail
abelardo.mayo@cepsa.com []
-----
ana.igualada@cepsa.com [u'LinkedIn']
-----
No data for this mail
emiliano.lopez@cepsa.com []
```

Comando: python 9.Leak_haveibeenpwned.py -f "listado_correos" -o "fichero_salida"

1	Email	Leak
2	jacques.duquesne@ep.cepsa.com	[]
3	lubrificantes.pedidos@cepsa.com	[]
4	relaciones.institucionales@cepsa.com	[u'Apollo']
5	cristina.artech@cepsa.com	[]
6	antonio.perea@cepsa.com	[u'Apollo']
7	jesus.mota@cepsa.com	[u'LinkedIn']
8	cesar.lavayen@cepsa.com.ec	[u'Apollo']
9	fernando.davila@cepsa.com.ec	[]
10	julia.montero@cepsa.com	[]
11	vetting@cepsa.com	[]
12	Shirley.deng@cepsa.com	[]
13	luisantonio.alonso@cepsa.com	[]
14	jacques.meunier@cepsa.com	[u'Apollo']
15	miguel.barbosa@cepsa.com	[u'Apollo', u'LinkedIn', u'OnlinerSpambot', u'TrikSpamBotnet']
16	ignacio.rodriguez-solano@cepsa.com	[u'Apollo', u'OnlinerSpambot']
17	ignacio.nieto@cepsa.com	[]
18	abelardo.mayo@cepsa.com	[]
19	ana.igualada@cepsa.com	[u'LinkedIn']
20	emiliano.lopez@cepsa.com	[]
21	daniel.demiguel@cepsa.com	[u'LinkedIn', u'OnlinerSpambot']
22	catherine.gauthier@cepsa.com	[]
23	angelo.carretero@cepsa.com	[]
24	comunicacion@cepsa.com	[]
25	porquetuvuelves@cepsa.com	[u'OnlinerSpambot']
26	csdpdm@cepsa.com	[]
27	buzonbajas@cepsa.com	[]
28	bunker@cepsa.com	[u'OnlinerSpambot']
29	i.ballester@cepsa.com	[u'LinkedIn']
30	alvaro.camacho@cepsa.com	[]
31	carolina.delaguardia@cepsa.com	[]
32	josemaria.jimenez@cepsa.com	[]
33	enrique.alas@cepsa.com	[]
34	juan.arrazola@cepsa.com	[]
35	matias.mayor@cepsa.com	[]
36	rodrigo.garcia@cepsa.com	[]
37	marcel.aschenbrenner@cepsa.com	[]
38	tineke.poot@cepsa.com	[u'LinkedIn', u'TrikSpamBotnet']
39	angelo.carnevali@cepsa.com	[u'OnlinerSpambot']

<https://github.com/m4ll0k/Infoga>

Infoga es una herramienta desarrollada en Python que permite recopilar información de cuentas de correo electrónico (IP, host, país, ASN, ...) de diferentes fuentes públicas, y verifica si los correos se encuentran en listados de correos que aparecen en leaks. Una de las ventajas de utilizar esta herramienta es que indica la ubicación de física de dónde se alojan dichos correos, pudiendo así identificar así posibles ataques de phishing.

Comando:

```
python3 infoga.py --domain "dominio" --source google --verbose 3
```

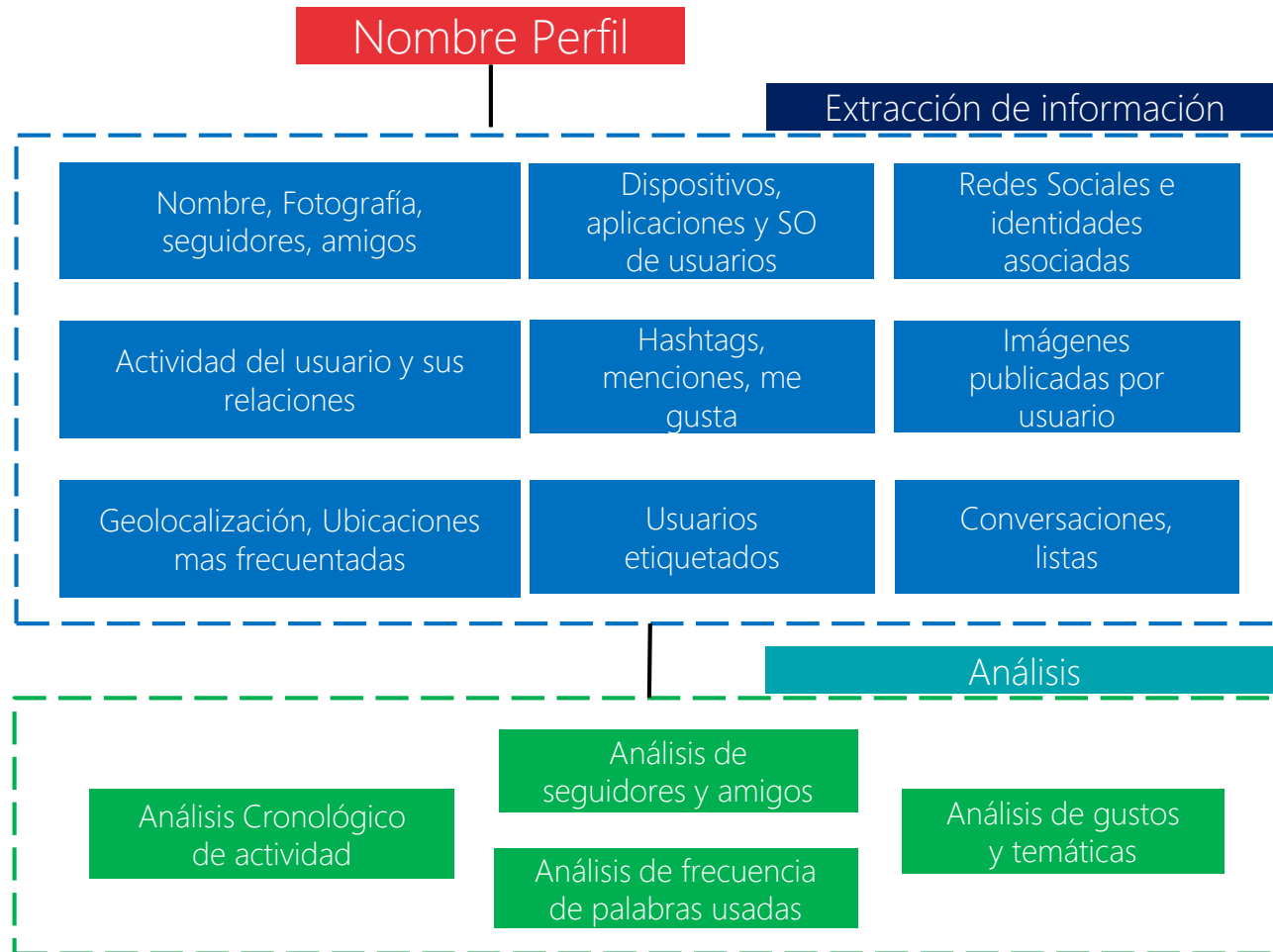
Comando: `python3 infoga.py --info "correo" --breach --verbose 3`

En caso de tener errores en su ejecución, cambiar línea 98 del archivo `infoga.py` por:

```
data(i,json.loads(self.shodan(i).decode('utf-8')),email,self.verbose)
```

```
root@OSINTUX:/home/osintux/OSINT/infoga# python3 infoga.py --domain cepsa.com --source google -v 3
-----
Infoga - Email Information Gathering
Momo Outaadi (m4ll0k)
https://github.com/m4ll0k
-----
[*] Searching "cepsa.com" in Google...
[i] Found 20 emails in Google
[+] Email: dpo@cepsa.com (81.47.205.118)
| Hostname: aristoteles.correolimpio.telefonica.es
| Country: ES (Spain)
| City: Amézqueta (59)
| ASN: AS6813
| ISP: Telefonica de Espana
| Map: Map: https://www.google.com/maps/@43.0680000000001,-2.083400000000117,10z (43.0680000000001,-2.083400000000117)
| Organization: Telefonica Soluciones
| Ports: [25, 993, 143]
[+] Email: dpo@cepsa.com (217.124.240.200)
| Hostname: copernico.correolimpio.telefonica.es
| Country: ES (Spain)
| City: Barcelona (56)
| ASN: AS3352
| ISP: Telefonica de Espana
| Map: Map: https://www.google.com/maps/@41.3888,2.158999999999992,10z (41.3888,2.158999999999992)
| Organization: Telefonica de Espana
| Ports: [443, 25]
[+] Email: dpo@cepsa.com (81.47.205.114)
| Hostname: plank.correolimpio.telefonica.es
| Country: ES (Spain)
| City: Amézqueta (59)
| ASN: AS6813
| ISP: Telefonica de Espana
| Map: Map: https://www.google.com/maps/@43.0680000000001,-2.083400000000117,10z (43.0680000000001,-2.083400000000117)
| Organization: Telefonica Soluciones
| Ports: [25, 143, 993]
[+] Email: porquetuvuelves@cepsa.com (217.124.240.201)
| Hostname: arquimedes.correolimpio.telefonica.es
| Country: ES (Spain)
| City: Barcelona (56)
| ASN: AS3352
| ISP: Telefonica de Espana
| Map: Map: https://www.google.com/maps/@41.3888,2.158999999999992,10z (41.3888,2.158999999999992)
| Organization: Telefonica de Espana
| Ports: [80, 25]
| Vulns: ['CVE-2012-4558', 'CVE-2013-1896', 'CVE-2012-3499', 'CVE-2014-0231', 'CVE-2017-7679', 'CVE-2013-2249', 'CVE-2016-4975', 'CVE-2013-5704', 'CVE-2017-7668', 'CVE-2013-6438', 'CVE-2012-2687', 'CVE-2017-3167', 'CVE-2017-3169', 'CVE-2014-0098', 'CVE-2013-1862', 'CVE-2016-8612']
```


Tinfoleak es una herramienta SOCMINT enfocada a Twitter, que permite extraer información y realizar un análisis sobre un perfil de dicha red social.



<https://github.com/vaguileradiaz/tinfoleak>

Antes de comenzar, se necesita:

APP de Twitter: <https://apps.twitter.com/>

API Key y Token asociados a APP:

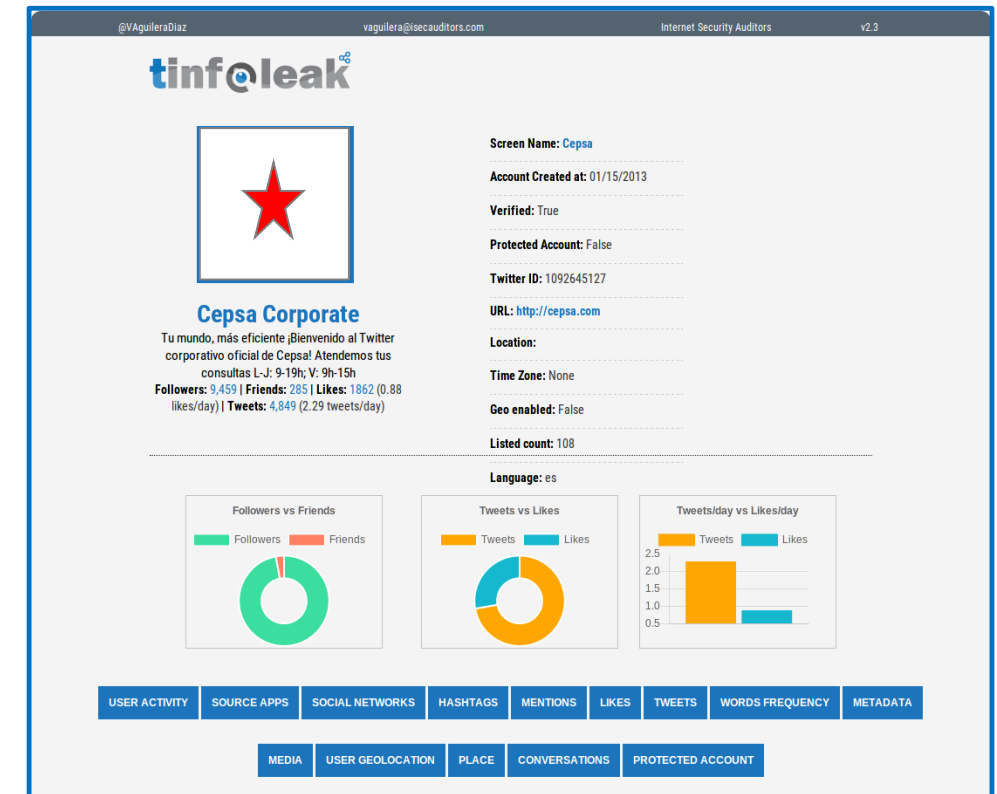
CONSUMER_KEY ACCESS_TOKEN
CONSUMER_SECRET ACCESS_TOKEN_SECRET

Añadir API keys a archivo de configuración de la herramienta: [tinfoleak/tinfoleak.conf](#)

Comando:
sudo python tinfoleak/tinfoleak.py

Informe:
tinfoleak/Output_Reports/tinfoleak.html

The screenshot shows the tinfoleak v2.4 application window. It has a 'Target of Analysis' section with radio buttons for 'User' (selected), 'Place', and 'Timeline'. The 'User' section has a text input for '@ cepsa', a 'File' button, and fields for 'Users' (50), 'Last file', and 'Relations'. Below this is the 'Operations' section with checkboxes for 'Account information', 'Likes', 'Lists', 'Collections', 'Followers', 'Friends', 'Locations', 'Protected account', 'Conversations', 'Hashtags', 'Mentions', 'Multimedia', 'Words frequency', 'User activity', 'Social networks', 'Source applications', 'Metadata', 'Download multimedia', and 'Show tweets'. There are also input fields for 'Number of tweets' (50) and 'Output file' (tinfoleak.html). The 'Filters' section includes date range selectors (Start date: 2018-10-21, End date: 2018-11-05), time range selectors (Start time: 00:00:00, End time: 23:59:59), and fields for 'Include words', 'Don't include words', and 'Source application'. There are also radio buttons for 'Retweet' and 'Multimedia'. The 'Messages' section at the bottom shows a log of system messages. The 'Latest Targets Analyzed' section shows a table with columns 'Date time', 'ToA', 'Information', and 'Additional'. The table has two rows: one for '@Cepsa' (Cepsa Corporate) and one for '@IvanPorMor' (Ivan Portillo). The application was created by Vicente Aguilera Diaz.



OSRFramework es una herramienta que permite obtener información referente a perfiles de usuarios. Esta desarrollada de manera modular, ofreciendo diferentes herramientas dentro del mismo framework

```
OSRFramework
Version: OSRFramework 0.18.7
Created by: Felix Brezo and Yaiza Rubio, (i3visio)

Usufy | Copyright (C) F. Brezo and Y. Rubio (i3visio) 2014-2018

This program comes with ABSOLUTELY NO WARRANTY. This is free software, and you
are welcome to redistribute it under certain conditions. For additional info,
visit https://www.gnu.org/licenses/agpl-3.0.txt

2018-11-05 19:40:53.548597 Starting search in 279 platform(s)... Relax!

Press <Ctrl + C> to stop...

2018-11-05 19:41:36.262187 A summary of the results obtained is shown below:

Sheet Name: Profiles recovered (2018-11-5_19h41m).
+-----+-----+-----+
| i3visio_uri | i3visio_alias | i3visio_platform |
+-----+-----+-----+
| https://www.freelancer.com/u/cepsa.html | cepsa | Freelancer |
+-----+-----+-----+
| http://www.myfitnesspal.com/user/cepsa/profile/cepsa | cepsa | MyFitnessPal |
+-----+-----+-----+
| https://github.com/cepsa | cepsa | Github |
+-----+-----+-----+
| http://www.forocoches.com/foro/member.php?username=cepsa | cepsa | Forocoches |
+-----+-----+-----+
| http://www.buzznet.com/author/cepsa | cepsa | Buzznet |
+-----+-----+-----+
| https://angel.co/cepsa | cepsa | Angel |
+-----+-----+-----+
| http://www.chess.com/members/view/cepsa | cepsa | Chess |
+-----+-----+-----+
```

<https://github.com/i3visio/osrframework>

Módulo Usufy

Permite verificar la existencia de un Username en un total de 306 plataformas.

Comando: python usufy.py -n cepsa -p all

Módulo Mailfy

Permite verificar la existencia de un email en los diferentes proveedores de correo.

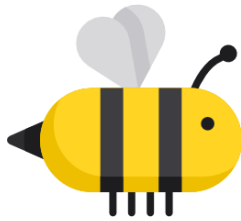
Comando: python mailfy.py -m correo

Módulo Searchfy

Permite verificar la existencia de perfiles en redes sociales a través del nombre completo de una persona.

Comando: python searchfy.py -q "Ivan Portillo"

Input: Email, Username, Teléfono, Nombre Persona



Bee You

Tenemos identificadas las herramientas y las fuentes

Conocemos los datos de partida, vamos a ver que podemos obtener (cuantifica y córrela la información)

- *Empresas del grupo, Personas, Credenciales, Dominios e IP, Leaks*

Vamos a optimizar los procesos, la recolección manual puede ser costosa y no aporta una visión global

- Dependiendo de tu nivel:
 - Usa las herramientas open source online
 - Complementa con las herramientas por consola
 - Ejecuta los scripts y orquesta todas las herramientas para optimizar el proceso
 - Añade nuevas fuentes con nuevos scripts
- Para todos
 - Cuantifica la información obtenida
 - Cualifícala: ¿es interesante y aporta valor?

Generemos un informe resumen para el CISO con los hallazgos obtenidos

- Resumen breve para el comité ejecutivo (facilitemos el trabajo al CISO preparando el informe para el CEO)
- Propongamos ideas para solucionar el incidente:
 - Cambiar de dirección de correo en las cuentas expuestas y comprometidas en brechas de seguridad
 - Revisar que los activos no tengan vulnerabilidades conocidas publicadas en foros, listas negras, paginas de bug bounties, etc (de forma pasiva)
 - Realizar campañas de concienciación para la gerencia, de que se debe y que no hacer



La importancia de las relaciones entre los datos

¿Por qué son importantes las relaciones?

Conociendo RabbitMQ

Conociendo NED4J

Orquestación de herramientas relacionando datos



Noviembre 2018



HoneyCon 4ª edición

Fuentes

+

Agregación de datos

- *Online pastes*
- *Honeynets*
- *BBDDs threat intelligence*
- *Trapmails*
- *Online trackers*
- *Referers*
- *BBDDs antivirus*
- *CERTs*
- *xBIs*
- *Spam blacklists*
- *Safe browsing*
- *Cybersquatting*
- *APK Markets*
- *TOR crawler*
- *Hidden IRC*
- *STIX / TAXII*
- *IoC*
- *Malware*
- *Botnets / C&C*
- *Social Media*

Formatos para compartir información

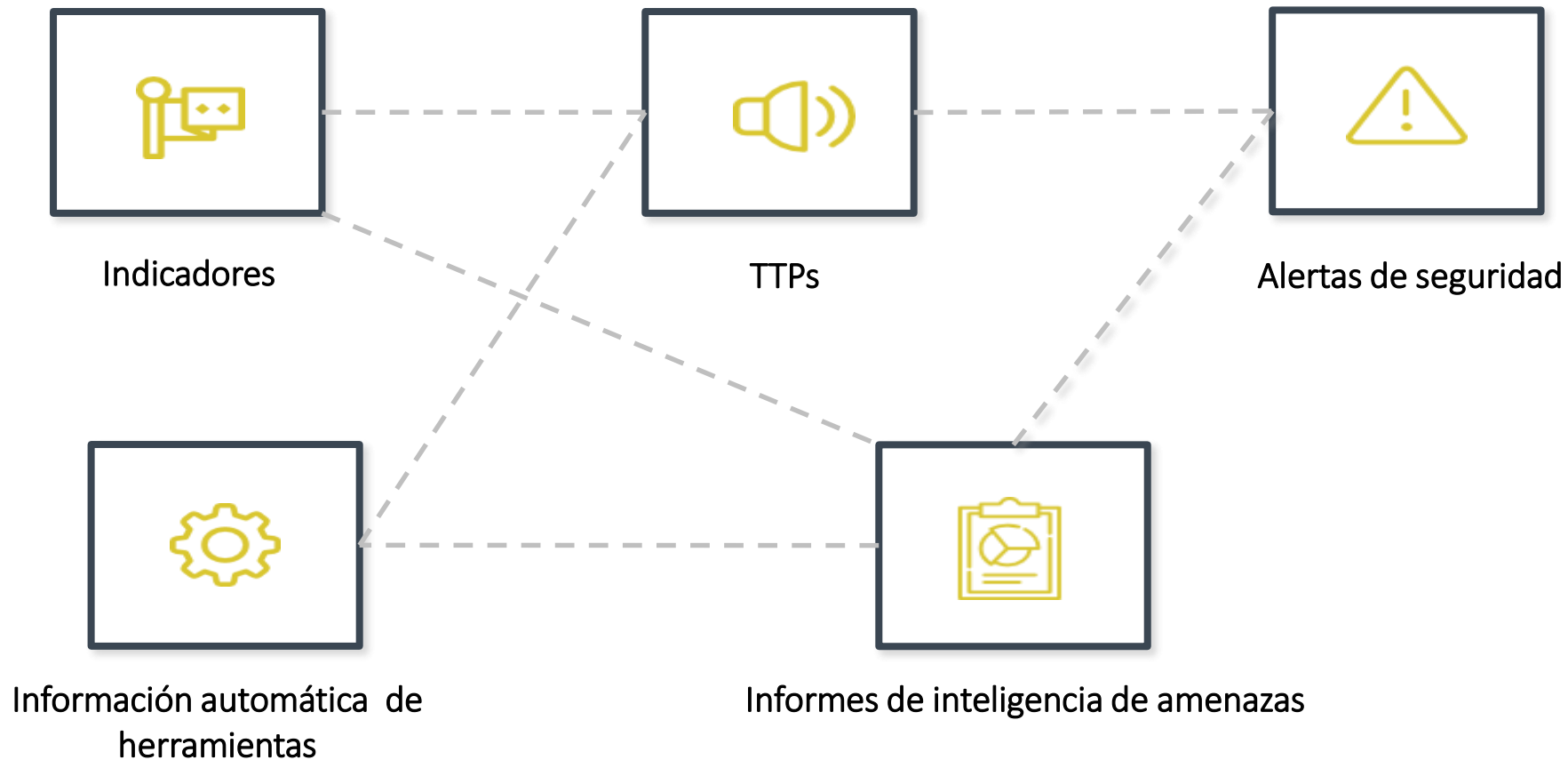
- Collective Intelligence Framework (CIF)
- Cyber Observable eXpression (CybOX)
- Incident Object Description and Exchange Format (IODEF)
- Open Indicators of Compromise (OpenIOC)
- Open Threat Exchange (OTX)
- Structured Threat Information Expression (STIX)
- Trusted Automated eXchange of Indicator Information (TAXII)
- Vocabulary for Event Recording and Incident Sharing (VERIS)



- ▶ Existen muchísimas fuentes abiertas y comerciales, con diferentes formados. Para nosotros es vital organizar, entender y obtener la información relevante y poder consumirla adecuadamente para ser tratada y analizada.
- ▶ Una vez analizada podremos ver relaciones que no eran evidentes y en un contexto global y agrupado si que nos pueden dar la pista que nos faltaba para obtener la inteligencia requerida.



Una vez afinadas las herramientas, coordinamos todo el ecosistema para generar inteligencia accionable, conociendo las intenciones de nuestros adversarios.





Investigación objetivo mediante relaciones



Noviembre 2018

/

HoneyCon 4ª edición





¿Qué es?

- Gestor de colas de mensajes para comunicar la información entre diferentes sistemas, aplicaciones, etc.
- Software Libre y compatible con diferentes protocolos de mensajería.

¿Qué Ofrece?

- Alta Disponibilidad
- Garantía de entrega
- Escalabilidad
- Distribución de mensajes a múltiples destinatarios
- Ordena y prioriza tareas
- Balanceo de carga de trabajo



User: guest
RabbitMQ 3.2.4, Erlang R16B03 [Log out](#)

[Overview](#) [Connections](#) [Channels](#) [Exchanges](#) **[Queues](#)** [Admin](#)

Queues

▼ All queues

Filter:

96 items (show at most)

Overview					Messages			Message rates		
Name	Exclusive	Parameters	Policy	Status	Ready	Unacked	Total	incoming	deliver / get	ack
cert				Idle	0	0	0			
cert.herschel				Idle	0	0	0			
cert_fanout_9589f00b487e4a72bb6936d5743d8f44		AD		Idle	0	0	0			
cinder-scheduler				Idle	0	0	0			
cinder-scheduler.herschel				Idle	0	0	0			
cinder-scheduler_fanout_24c4663799e446099f46d3bec1024cf8		AD		Idle	0	0	0	0.00/s	0.00/s	0.00/s
cinder-volume				Idle	0	0	0			
cinder-volume.herschel@zfssa				Idle	0	0	0			
cinder-volume_fanout_a3a1be3bfa114fd9bed5df12846bff96		AD		Idle	0	0	0			
compute				Idle	0	0	0			
compute.herschel				Idle	0	0	0			
compute_fanout_cd8b13216000448ab7b38ba7b8c0eb7c		AD		Idle	0	0	0			
conductor				Active	0	0	0	0.00/s	0.20/s	0.20/s
conductor.herschel				Idle	0	0	0			
conductor_fanout_00601bcd7d894735862da794c10291f7		AD		Idle	0	0	0			
conductor_fanout_043e47bee548478e9267818b8446301b		AD		Idle	0	0	0			

Instalación

- Se instala paquete Erlang, necesario para RabbitMQ

```
sudo apt-get install erlang-nox
```

- Se añaden los repositorios de RabbitMQ

```
echo 'deb http://www.rabbitmq.com/debian/ testing main' | sudo  
tee /etc/apt/sources.list.d/rabbitmq.list
```

```
wget -O- https://www.rabbitmq.com/rabbitmq-release-signing-  
key.asc | sudo apt-key add -
```

- Instalación de RabbitMQ

```
sudo apt-get update
```

```
sudo apt-get install rabbitmq-server
```

Configuración

- Cargar servicio por defecto en arranque de SO.

```
sudo update-rc.d rabbitmq-server defaults  
sudo service rabbitmq-server start  
sudo service rabbitmq-server stop
```

- Creación de Usuario Super Admin

```
sudo rabbitmqctl add_user admin password  
sudo rabbitmqctl set_user_tags admin administrator  
sudo rabbitmqctl set_permissions -p / admin ".*" ".*" ".*"
```

- Activar Plugins de gestión web de RabbitMq

```
sudo rabbitmq-plugins enable rabbitmq_management
```

- Escuchando por dirección IP y puerto

<http://192.168.18.132:15672>

Usuario: admin

Password: password



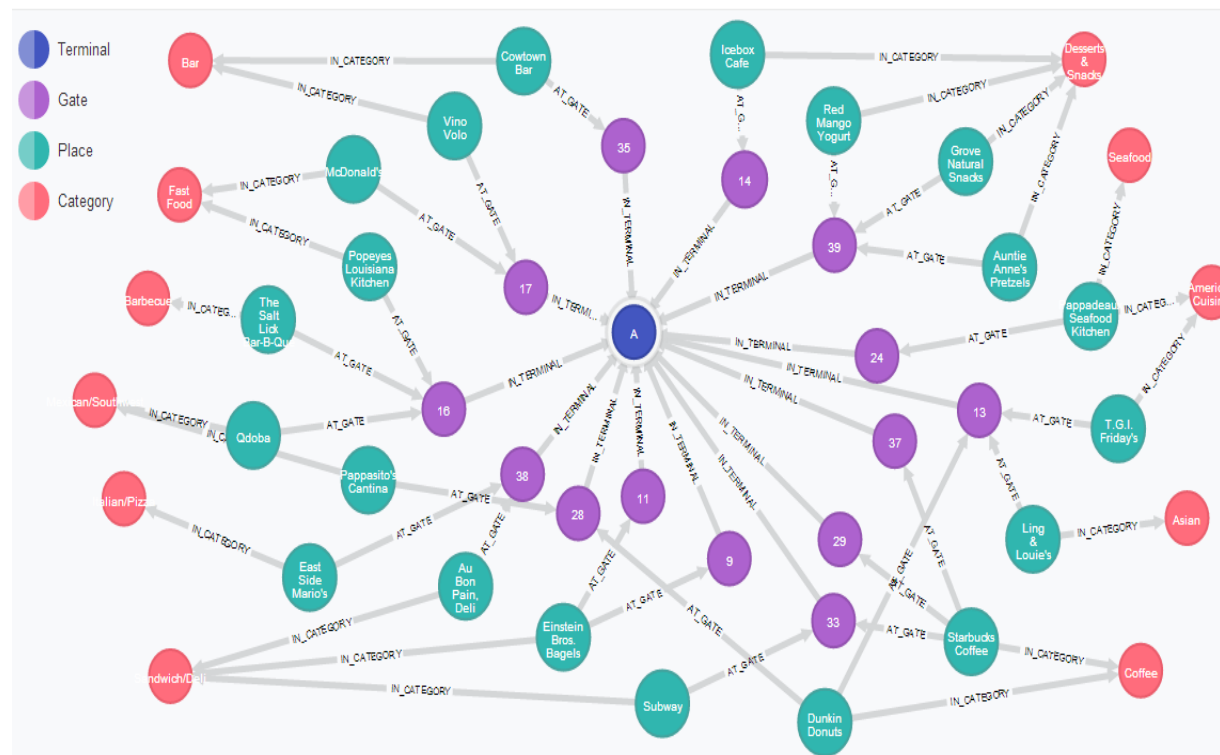
¿Qué es?

- Es una base de datos orientada a grafos, que permite obtener relaciones entre diferentes nodos
- Dispone de Versión Community y versión de Pago

¿Qué ofrece?

- Soporta transacciones ACID (Atomicidad, Consistencia, Aislamiento, Durabilidad)
- Agilidad para gestionar grandes cantidades de datos
- Flexibilidad y escalabilidad
- Alta disponibilidad y Balanceo de carga

```
CYPHER MATCH p = (:Category)<--(:Place)-[*]>(:Terminal {name:'A'}) RETURN p
```



Instalación

- Se instala java si no esta en SO:

```
sudo add-apt-repository ppa:webupd8team/java  
sudo apt-get update  
sudo apt-get install oracle-java8-installer
```

- Se añaden los repositorios de Neo4J

```
wget -O - https://debian.neo4j.org/neotechnology.gpg.key | sudo  
apt-key add -
```

```
echo 'deb https://debian.neo4j.org/repo stable/' | sudo tee -a  
/etc/apt/sources.list.d/neo4j.list
```

- Instalación de Neo4J

```
sudo apt-get update
```

```
sudo apt-get install neo4j
```

Configuración

- Cargar servicio por defecto en arranque de SO.

```
sudo update-rc.d neo4j defaults  
sudo service neo4j start  
sudo service neo4j stop
```

- Activar conexiones fuera de equipo local

Acceder a /etc/neo4j/neo4j.conf
dbms.connectors.default_listen_address=192.168.18.132

- Activar HTTP / HTTPS

dbms.connector.http.listen_address=:7474
dbms.connector.https.listen_address=:7473

Acceso: <http://192.168.18.132:7474/browser/>

Usuario: neo4j

Password por defecto: neo4j

Password taller: Password

Dependencias Python

Ubicación Archivo Requirements

- `/home/osintux/OSINT/orquestación/orquestación/requirements.txt`
- `pip install -r requirements.txt`

Librerías necesarias

- Conector Rabbitmq (Pika)
- Conector NEO4J (Py2neo, Pprint)
- Shodan
- Librerías para realizar peticiones a APIs
 - Requests
 - Urllib2

Modo Ejecución

Pasos a seguir

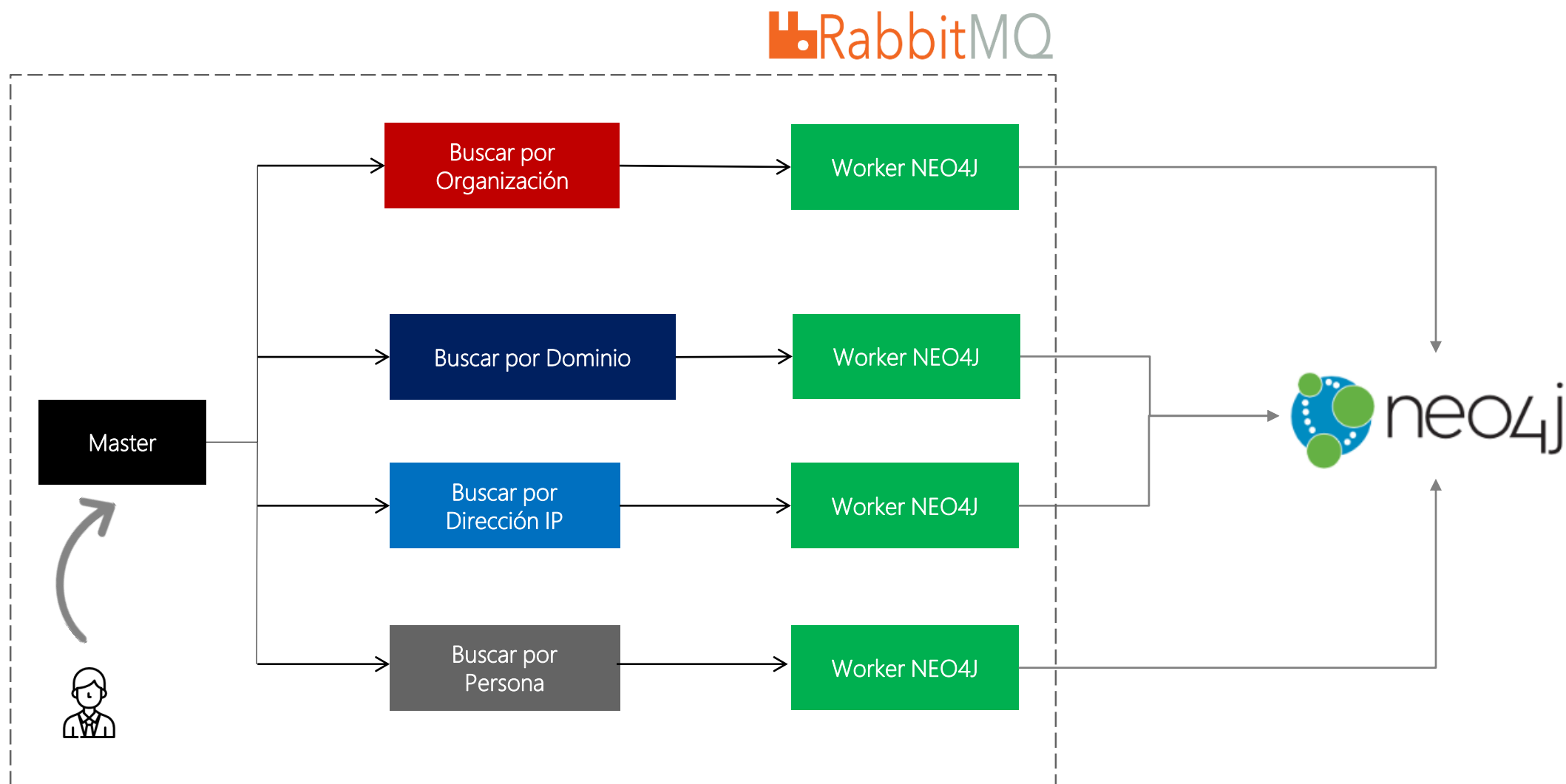
- Carpeta: `/home/osintux/OSINT/orquestación`
- Activar Virtualenv dentro de carpeta: `source bin/actívale (virtualenv)`
- Ejecutar Monitor de Workers: `sh monitor_orquestador.sh`
- Enviar información para investigar
 - Investigación de Organización:
 - `python send_organization.py -f "fichero de entrada con nombre organización"`
 - Investigar de Dominios:
 - `python send_domains.py "fichero de entrada con dominios"`

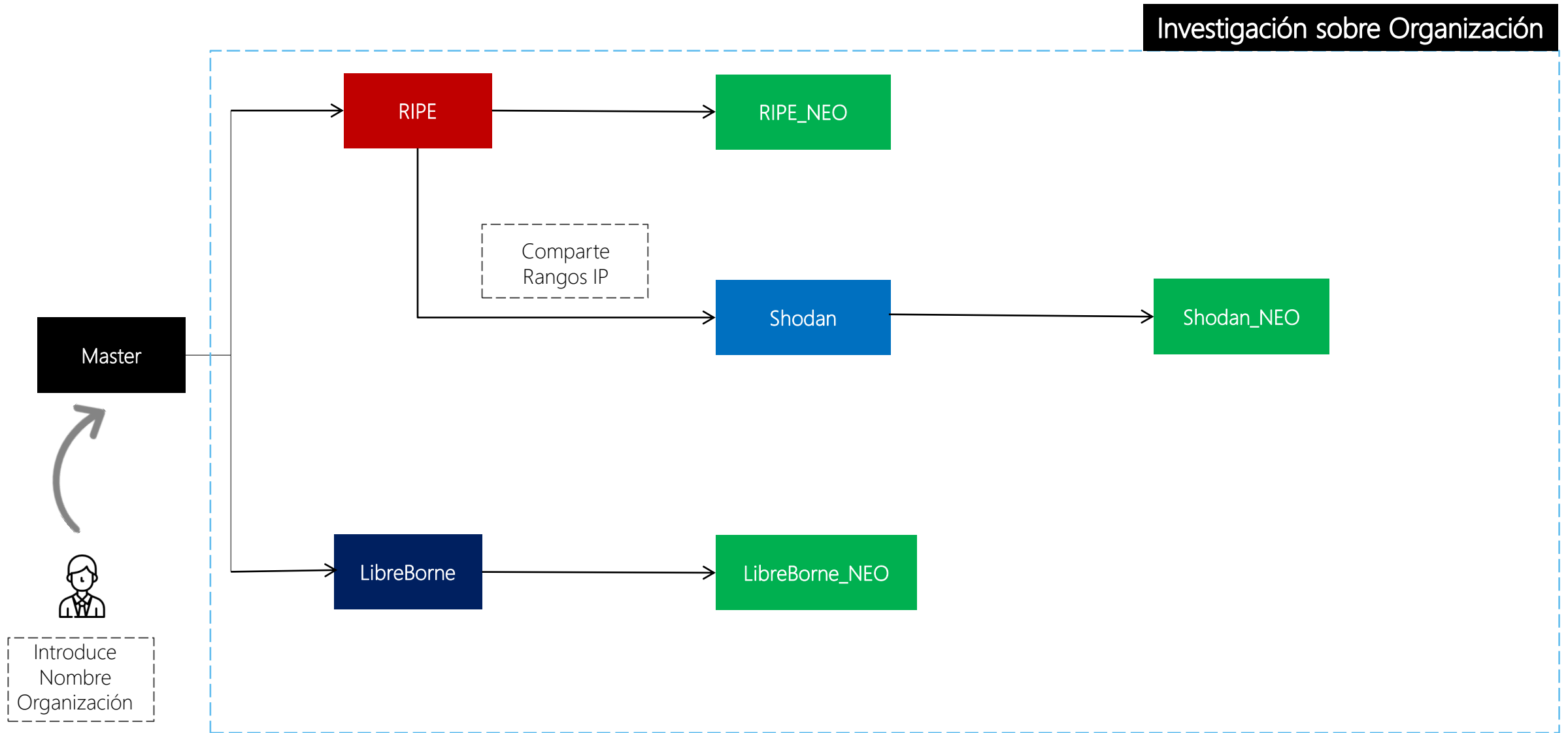
Eliminar colas existentes

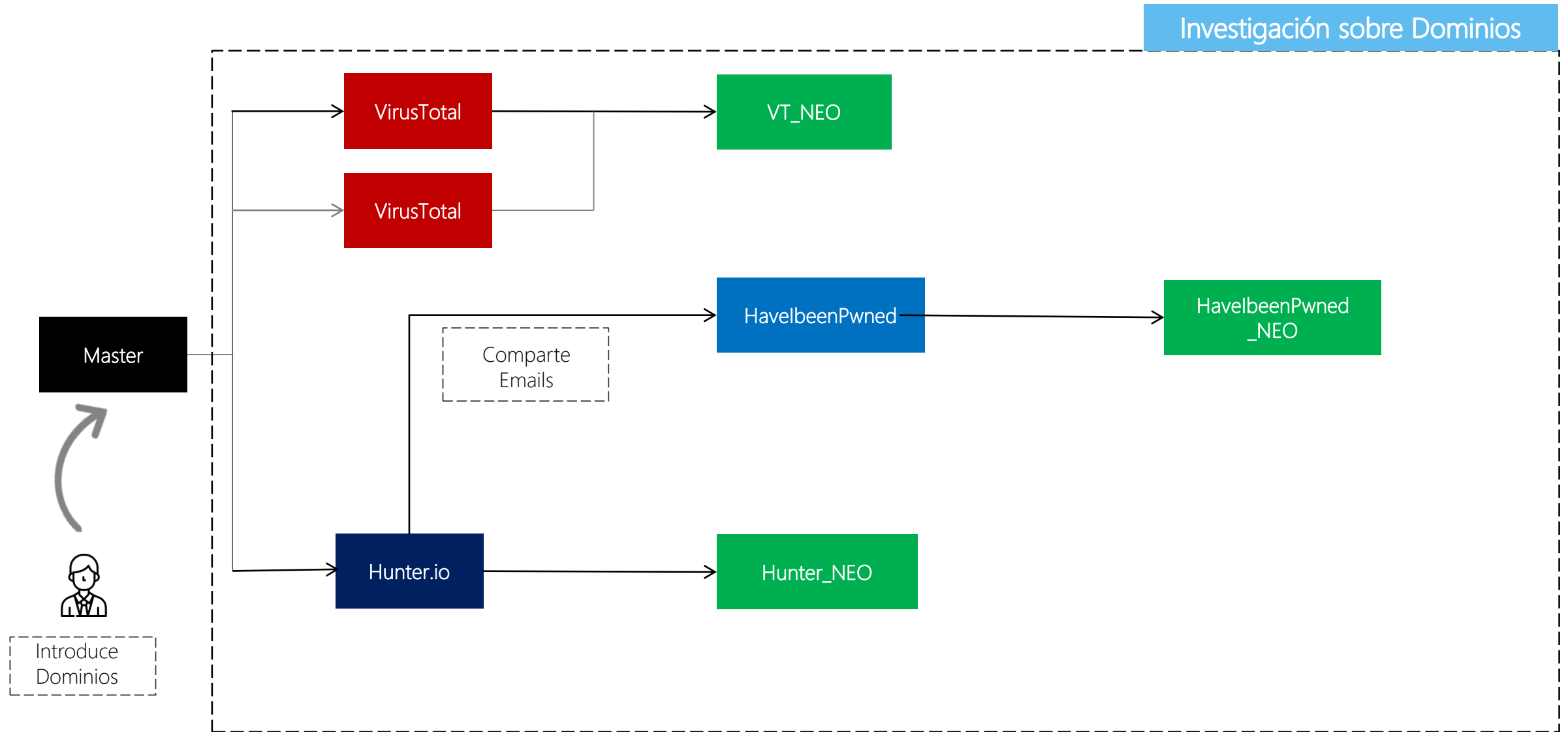
```
sudo rabbitmqctl list_queues | python eliminar_colas.py -r IP -u user -p password
```

Ubicación Configuración APIs

```
/home/osintux/OSINT/orquestación/lib/python2.7/confOrquestador.py
```



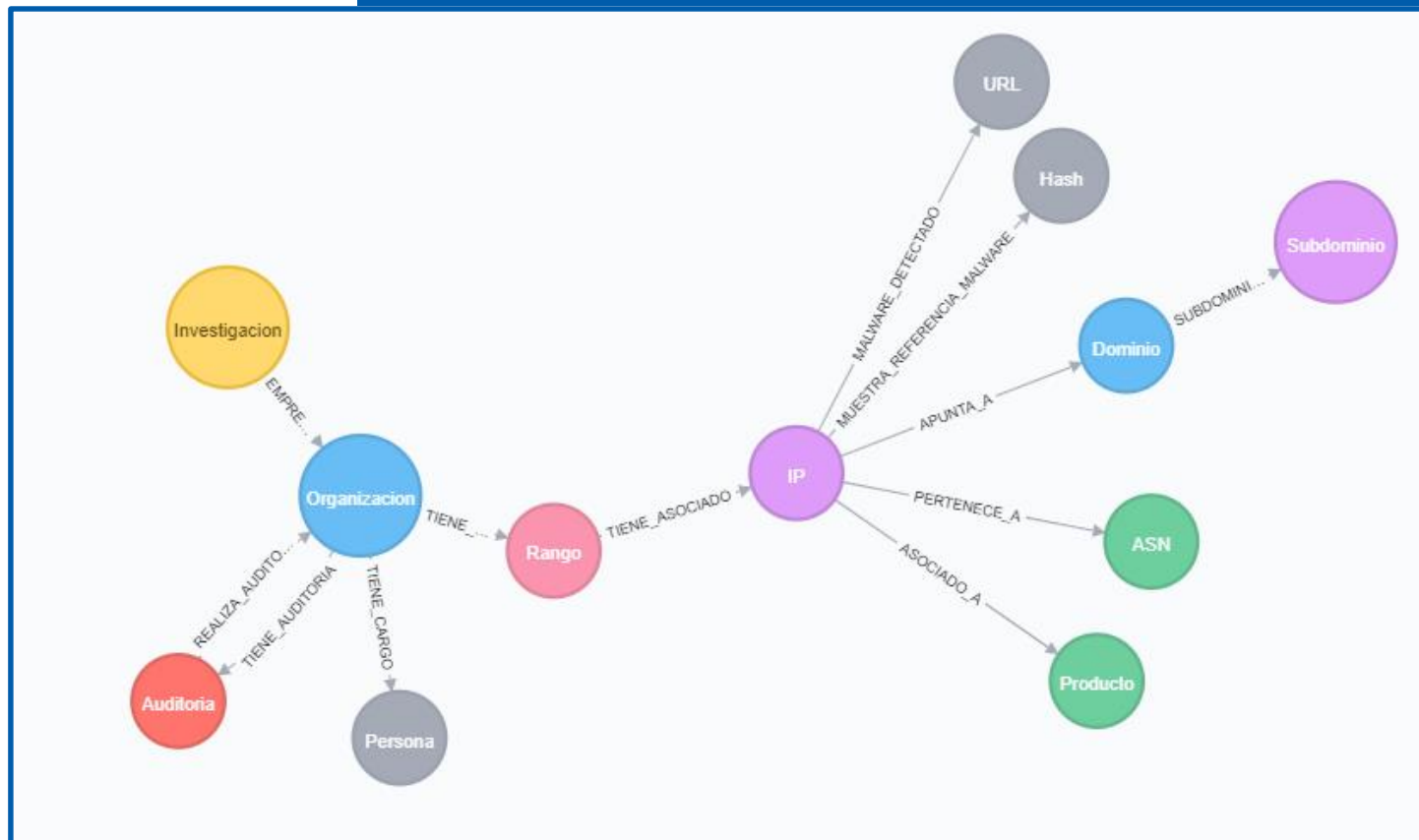




Mapa gráfico de bbdd de NEO4J

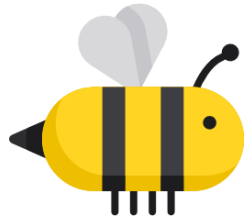
Comando NEO4J para grafo de
Nodos y Relaciones:

call apoc.meta.graph



*(12) ASN(1) Auditoria(1) Dominio(1) Hash(1) IP(1) Investigacion(1) Organizacion(1) Persona(1) Producto(1) Rango(1) Subdominio(1) URL(1)

*(12) REALIZA_AUDITORIA(1) TIENE_CARGO(1) SUBDOMINIO_DETECTADO(1) ASOCIADO_A(1) TIENE_ASOCIADO(1) TIENE_AUDITORIA(1) APUNTA_A(1) MALWARE_DETECTADO(1) EMPRESAS_DETECTADAS(1) PERTENECE_A(1)



Bee You

Partiendo sólo de los tres datos facilitados hemos resuelto la adivinanza:

1. En el caso de las gasolineras comprometidas: estudiantes con ganas de curiosar, pérdidas económicas de 100€ y no futura repercusión en comunidades criminales.
2. El caso del correo de phishing, no ha sido un grupo de estado intentando obtener propiedad intelectual. Han sido estos mismos estudiantes con el fin de poder pagar la gasolina para venir a un congreso de seguridad en el panal.

Gracias Bee, ¿puedes facilitarme el inventario de activos comprometidos para verificar posibles puntos débiles?



Diego

Claro Diego, tenemos la lista de datos requeridos. También podemos mostrarte de forma muy gráfica como hemos relacionado todos estos datos para sacar las conclusiones pertinentes.

Me encantaría. Ahora mandadme el resumen ejecutivo y nos ponemos seguidamente a explorar toda la información relevante que tengamos expuesta para protegerla adecuadamente.

Julio, tenemos identificado el origen del ataque. Ha sido un grupo de estudiantes ocasionales que han localizado un punto débil en la corporación y lo han usado para ocasionar perdidas económicas insignificantes. Para esto ya hemos:

1. Solucionado el origen de la brecha
2. Explorado el resto de activos para evitar que esta situación se pudiera replicar en el futuro.



Diego

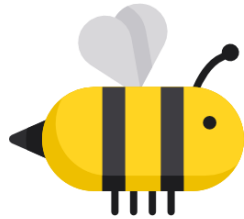
Me alegra oír eso Diego. Quisiera un plan de acción que implique de forma proactiva la monitorización de los activos internos y externos. Quiero que hagas crecer el departamento de seguridad por si este tipo de incidentes se repite. Gracias.



Julio

Gracias a usted Julio, ampliaremos el plan de ciberinteligencia para tener esta información en tiempo real y poder cotejarla ante posibles futuros ataques.

Usaremos a la colmena del panal ya que nos ha proporcionado información precisa en los plazos requeridos. Le mantendré informado.



Bee You

- Hemos aprendido qué es la inteligencia, qué es ciberinteligencia, y cómo se relaciona.
- Hemos descubierto posibles problemas reales de cualquier empresa y como atajarlos.
- Hemos visto que al afrontar el reto, existen muchas herramientas y fuentes, y es complejo el manejo de toda esa información. Para ello hemos:
 - Evaluado las herramientas open source tanto web, como por consola
 - Evaluado fuentes de datos, datos que tenemos de entrada y que podemos enriquecer para obtener siguientes datos en la salida
 - Aprendido a optimizar y orquestar las herramientas necesarias para facilitarnos el trabajo
 - Aprendido a añadir nuevas herramientas y expandir nuestro proyecto
- Finalmente hemos visto que con poca información de partida hemos obtenido bastantes datos relevantes para un atacante real sobre una organización. Entendiendo estos datos y la relevancia de los mismos podemos priorizar los posibles riesgos y brechas que han podido impactar la organización.
- Hemos visto como reportar esta información y subirla desde el nivel técnico al nivel ejecutivo, teniendo que reducir y explicar con palabras menos técnicas amenazas del mundo ciber para interlocutores que no están familiarizados con este entorno.



Agradecimientos



Noviembre 2018

/

HoneyCon 4ª edición



Wiktor Nykiel

Cyber Intelligence & Security Senior Manager

#Creative and #innovative in #cyberintelligence.
IT enthusiast, security researcher, #entrepreneur.



wiktornykiel



[wiktornykiel](https://twitter.com/wiktornykiel)



Gonzalo Espinosa

Cybersecurity Consultant

#Vulnerabilities #Incident&Response #Cyberintelligence



gonzaloespinosa





Recursos y referencias



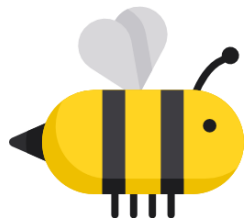
Noviembre 2018

/

HoneyCon 4ª edición



Usa los recursos para educación



Bee You

- Hay servidores en AWS, cuentas en github, etc
- Regístrate en nuevas fuentes y servicios como Shodan, si eres estudiante pide la ampliación de tu cuenta

Revisa las referencias publicadas, seguro que hay cosas interesantes de las que puedes tirar del hilo para seguir aprendiendo.

Únete a nuestros grupos y comunidades para actualizar tus conocimientos.

<https://ginseg.com>

Código de Invitación: Honey18

- <https://t.me/ginseg>
- <https://derechodelared.com>
- <https://t.me/codeislawddr>
- <https://www.fwhibbit.es/>
- <https://t.me/Fwhibbit>



<https://education.github.com/pack>

aws  educate

Education

 DigitalOcean

 UDACITY

Microsoft Imagine 

 axosoft GitKraken

 CrowdFlower

// FLATIRON
SCHOOL

 namecheap

 SendGrid

 DATADOG

 bitnami

 ATOM

dn simple

<https://imagine.microsoft.com>

 Technologies  Documentation  Resources  Sign in

Microsoft Imagine  Account Downloads  Code  Compete  About  Blog

By using this site you agree to the use of cookies for analytics, personalized content and ads. [Learn More.](#)

Software and services catalog

Microsoft Imagine has the tools you need to build a game, design an app or launch a project.

Sign in or create an account to download these software & development tools at no cost.

[Sign in /create profile >](#)

Featured

Services

Microsoft Azure for Students

Free cloud services

Develop in the cloud at no cost with Azure App Services, Notification Hubs, SQL database, and more.

[Get Azure](#)

Tools

Parallels Desktop for Mac Pro Edition

Free 3-month trial

Powerful virtualization solution for running Windows and Mac apps side-by-side, without rebooting.

[Download Parallels](#)

Tools

Visual Studio Community 2015

Free, fully-featured, extensible IDE

Create modern apps for Android, iOS, and Windows as well as web apps and cloud services.

[Download Visual Studio Community](#)



Leverage the Power of Shodan

Introducing the Shodan API, the easiest way to access the Shodan search engine on your own terms.

[Get Started](#)



Easy Integration

The Shodan API is the easiest way to provide users of your tool access to the Shodan data. The API provides access to all of the search features, allowing you to get exactly the information you want.



Beyond the Web

The website only shows a small fraction of the information that is gathered by Shodan. Use the API to gain full access to all the data collected and extract the information you care about.



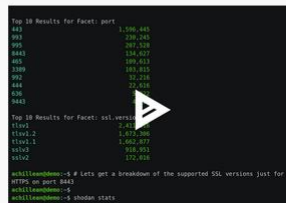
Automate Everything

Use the API to automatically generate reports, notify you if something popped up on Shodan or keep track of results over time.



Real-Time Notifications

The Streaming API gives you the ability to subscribe to events in real-time so you can immediately respond to new discoveries.



Command-Line Friendly

The Shodan command-line interface exposes most of the API in a user-friendly way so you can access the Shodan database without needing to write your own scripts.

[Install the CLI](#)

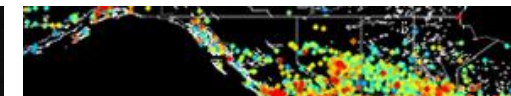
API-First Development

The Shodan website, including Shodan Images and Shodan Maps, are powered by the API. Anything that can be done using those websites you can also do directly via the API. To get started find an API binding in your favorite language:

[Browse available libraries](#)



Shodan © 2013-2018, All Rights Reserved



Crear cuenta de Shodan

Solicitar upgrade por mail a jmath@shodan.io



John Matherly

@achilleian

Founder of Shodan, Internet Cartographer

Austin, Texas

shodan.io

Se unió en octubre de 2007

1. <http://aisel.aisnet.org/cgi/viewcontent.cgi?article=1091&context=wi2017>
2. <http://apwg.eu>
3. <http://csirtgadgets.org/>
4. <http://detect-respond.blogspot.com.es/2013/03/the-pyramid-of-pain.html>
5. <http://hailataxi.com/>
6. <http://malwareanalysis.tools/?from=t.me/ginseg>
7. <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-150.pdf>
8. <http://resources.infosecinstitute.com/osint-open-source-intelligence/>
9. <http://www.misp-project.org/>
10. <http://www.osintframework.com/?from=t.me/ginseg>
11. <http://www.robertmlee.org/data-information-and-intelligence-your-threat-feed-is-not-threat-intelligence/>
12. <http://www.spiderfoot.net/>
13. <http://www.threathunting.net/>
14. <https://community.blueliv.com>
15. <https://community.riskiq.com/>
16. <https://ecrimex.net/>
17. <https://exchange.xforce.ibmcloud.com/>
18. <https://github.com/1aN0rmus/TekDefense-Automater>
19. <https://github.com/certtools/intelmq>
20. <https://github.com/ciscocsirt/gosint>
21. https://github.com/CyberMonitor/APT_CyberCriminal_Campagin_Collections
22. <https://github.com/hslatman/awesome-threat-intelligence>
23. <https://github.com/kbandla/APTnotes>
24. <https://github.com/MISP/misp-taxonomies>
25. <https://github.com/mlsecproject/tiq-test>
26. <https://github.com/rshipp/awesome>
27. <https://github.com/S03D4-164/Hiryu>
28. <https://github.com/syphon1c/Threatelligence>
29. https://github.com/Yelp/threat_intel
30. <https://intel.criticalstack.com/dashboard/>
31. <https://malwarehunterteam.com/>
35. <https://oasis-open.github.io/cti-documentation/stix/intro>
36. <https://otx.alienvault.com>
37. <https://riskdiscovery.com/honeydb/>
38. <https://virusshare.com/>
39. <https://www.alienvault.com/open-threat-exchange>
40. <https://www.enisa.europa.eu/events/cti-eu-event/cti-eu-event-presentations/active-defence-with-attack-trees-deception/>
41. <https://www.enisa.europa.eu/events/cti-eu-event/cti-eu-event-presentations/cert-eu-presentation/>
42. <https://www.enisa.europa.eu/events/cti-eu-event/cti-eu-presentations>
43. https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2016/at_download/fullReport
44. https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/enisa-thematic-landscapes/threat-landscape-of-the-internet-infrastructure/threat-mind-map/at_download/file
45. <https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/enisa-threat-landscape/etl2015/enisa-threat-taxonomy-a-tool-for-structuring-threat-information>
46. https://www.ncsc.gov.uk/content/files/protected_files/guidance_files/MWR_Threat_Intelligence_whitepaper-2015.pdf
47. <https://www.recordedfuture.com/>
48. <https://www.slideshare.net/cisoplatfrom7/security-strategy-and-tactic-with-cyber-threat-intelligence-cti-68988770>
49. <https://www.sans.org/course/cyber-threat-intelligence>
50. <https://www.sans.org/reading-room/whitepapers/analyst/who-039-s-cyberthreat-intelligence-how-35767>
51. <https://www.sans.org/summit-archives/file/summit-archive-1492113006.pdf>
52. <https://www.symantec.com/content/dam/symantec/docs/reports/gistr22-government-report.pdf>
53. <https://www.threatminer.org>
54. <https://www.us-cert.gov/tlp>
55. <https://www.virustotal.com>

Follow us...



Ginseg

Comunidad de Inteligencia: <https://ginseg.com>

Telegram: <https://t.me/ginseg>

Derecho de la red

Web: <https://derechodelared.com>

Telegram: <https://t.me/codeislawddr>

Fwhibbit

Web: <https://www.fwhibbit.es>

Telegram: <https://t.me/Fwhibbit>
