HoneyCON
By HoneySec

Monta la NSA en tu casa

Inteligencia aplicada al mundo Ciber

Contenido

Who Am I

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

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

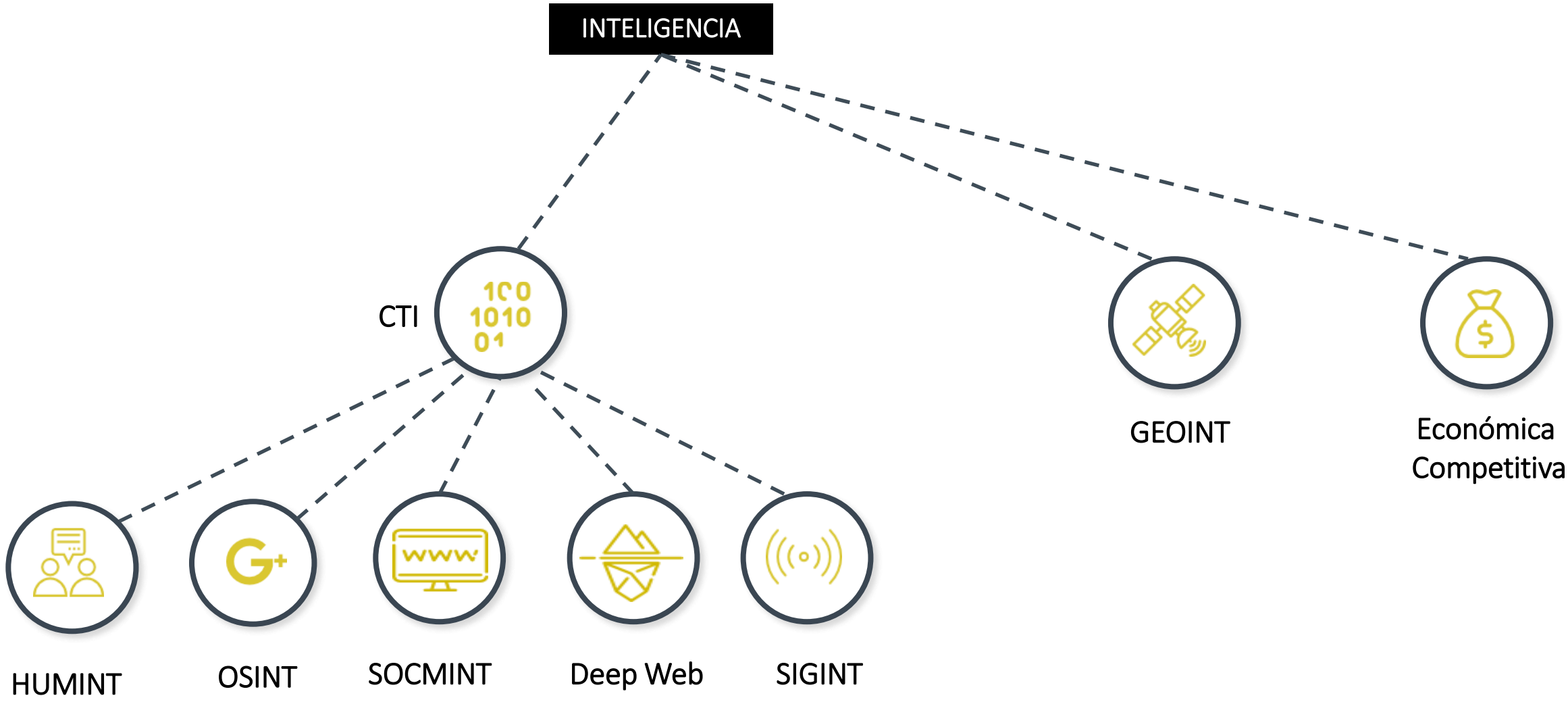
ivanportillomorales ivanPorMor

gonx0 gonx010

Introducción a la Inteligencia

- Inteligencia y sus fuentes
- Ciclo de Inteligencia
- Relación entre datos, información e inteligencia
- Amenaza VS Riesgo

Inteligencia y sus fuentes



Ciclo de Inteligencia

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

Generación y entrega de informe de inteligencia

Generación de conocimiento

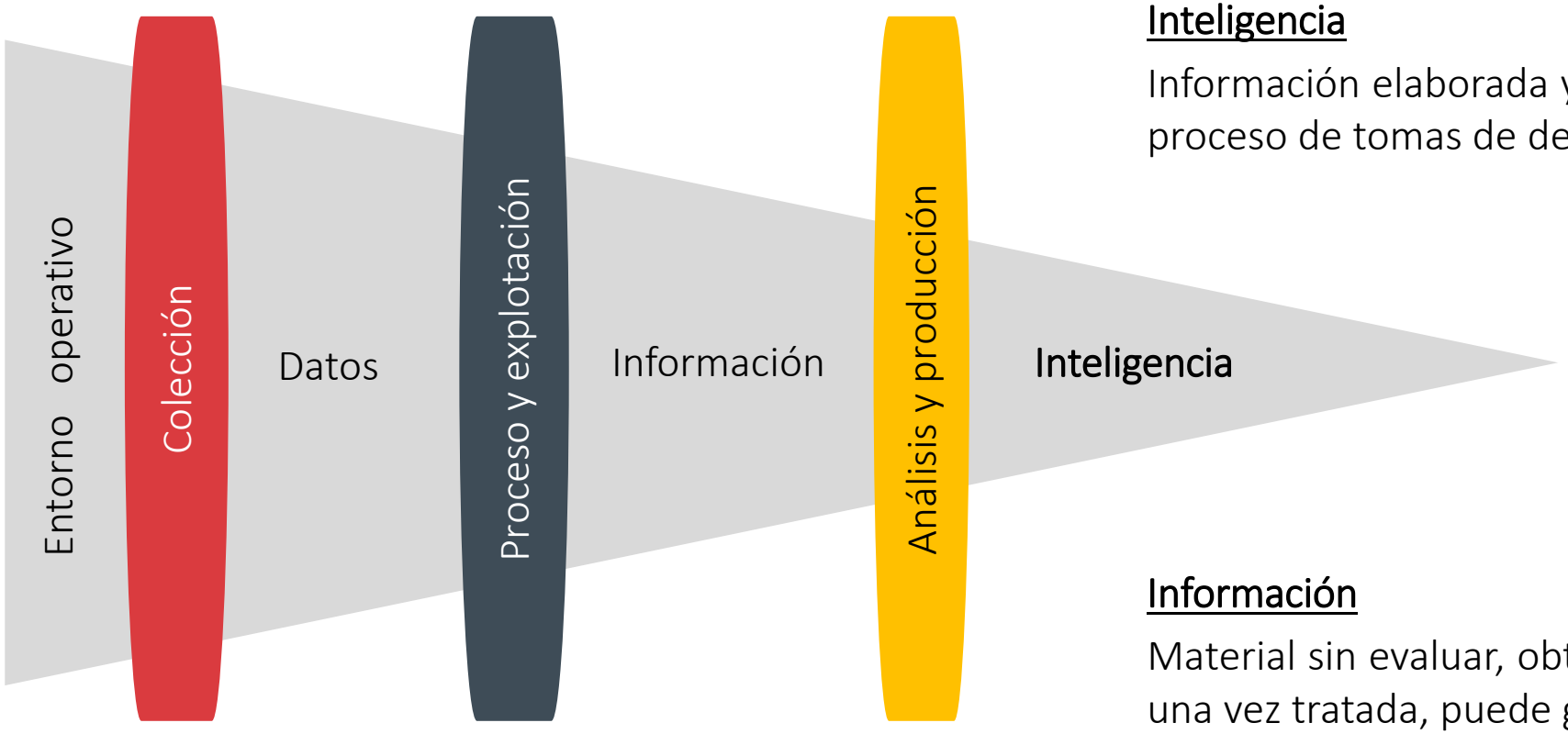
HUMINT
OSINT
CYBINT
SIGINT
Deep Web

CNI

Con origen en el ciclo de inteligencia militar

Relación entre datos, información e inteligencia

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.

Amenazas vs Riesgos

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.

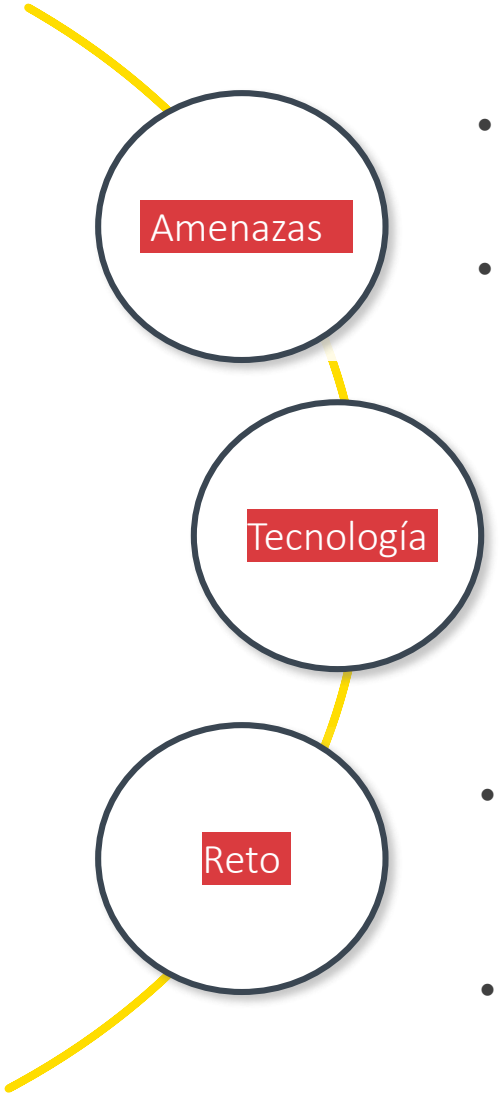
3. Todos los factores configuran la ecuación del riesgo.

TLP:GREEN

Conceptos y fundamentos de Ciberinteligencia

Noviembre 2018 / HoneyCon 4ª edición

Estado del arte ¿Para qué necesitamos esto?



- Las **motivaciones de los atacantes se están ampliando**.
- Las **amenazas continúan acelerándose**, **superando las defensas** de seguridad tradicionales y los enfoques operativos.
  - Las **defensas tradicionales** son cada vez **menos efectivas**.
  - La **tecnología está evolucionando**, muy rápido, y las empresas que no la sigan se quedarán atrás.
- 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.

Conceptos básicos

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.

Conceptos básicos

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

Ciclo de colección, análisis y producción de la información

Recoger

- **Monitorizar feeds,** Investigar amenazas / desarrollos.

EXTERNO
- Información de **inteligencia de amenaza**
- Casos de uso de operaciones de seguridad

INTERNO
- Datos de incidentes y eventos empresariales
- **Controlar brechas y vulnerabilidades**
- Datos de **activos críticos**

Analizar

- Correlación de tendencias.
- Evaluar la relevancia de los requisitos.
- Determine la priorización para la producción.
- **Identificar información de valor.**
  - Intención clave de la amenaza.
  - **Amenazas clave** TTPs.
  - Caminos de ataque vulnerables.
- Evaluar y **priorizar el riesgo**.

Producir

- Productos diseñados para cumplir con los requisitos.
- Información analizada fusionada en productos.
  - **Modelado de amenazas**
    - Escenarios de alto riesgo.
    - Brechas de control priorizadas.
  - **Árbol de ataque.**
  - Perfil de amenaza
  - Resumen ejecutivo.
  - Objetivos de operaciones de seguridad.

Integrar

- **Definir / refinar requisitos.**
- Entregar **procesos / productos para cumplir con los requisitos**.
  - **Integración** técnica de la inteligencia de amenazas derivadas (por ejemplo, **STIX / TAXII**).
  - Información / informes de la audiencia.
  - Utilice el **desarrollo de casos por analistas de seguridad**.
  - Implementación del caso.
  - Seguimiento de casos.
- Comentarios de proceso / producto.

TLP:GREEN

Interlocutores

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.

TLP:GREEN

Volumen de la información

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

Pongámonos nombres

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.

ESTRATÉGICO	TÁCTICO
OPERACIONAL	TÉCNICO

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.

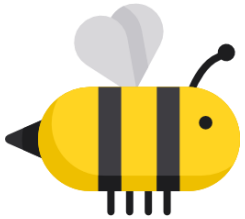
Necesito identificar los activos de la compañía y descubrir por dónde han podido atacarnos cuanto antes. Esta teniendo mucha repercusión.

Diego

Bee You Researcher
Investigadores de inteligencia del panal

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

TLP:GREEN

¿Qué ha pasado?

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

Julio

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

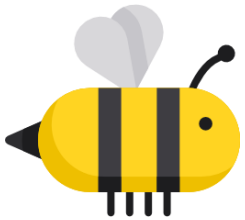
Me preocupa el correo por los datos sensibles de la empresa que hayan podido obtener los atacantes, pero sobre todo la seguridad de nuestras estaciones. Por favor, mantenme informado.

¿Qué ha pasado?

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

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.

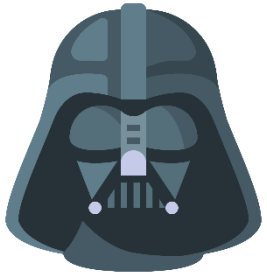
Nos ponemos a ello, no son muchos datos la verdad, pero usaremos nuestra inteligencia colectiva. ¿Alguna pista más?

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.

Nos preparamos para la batalla

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

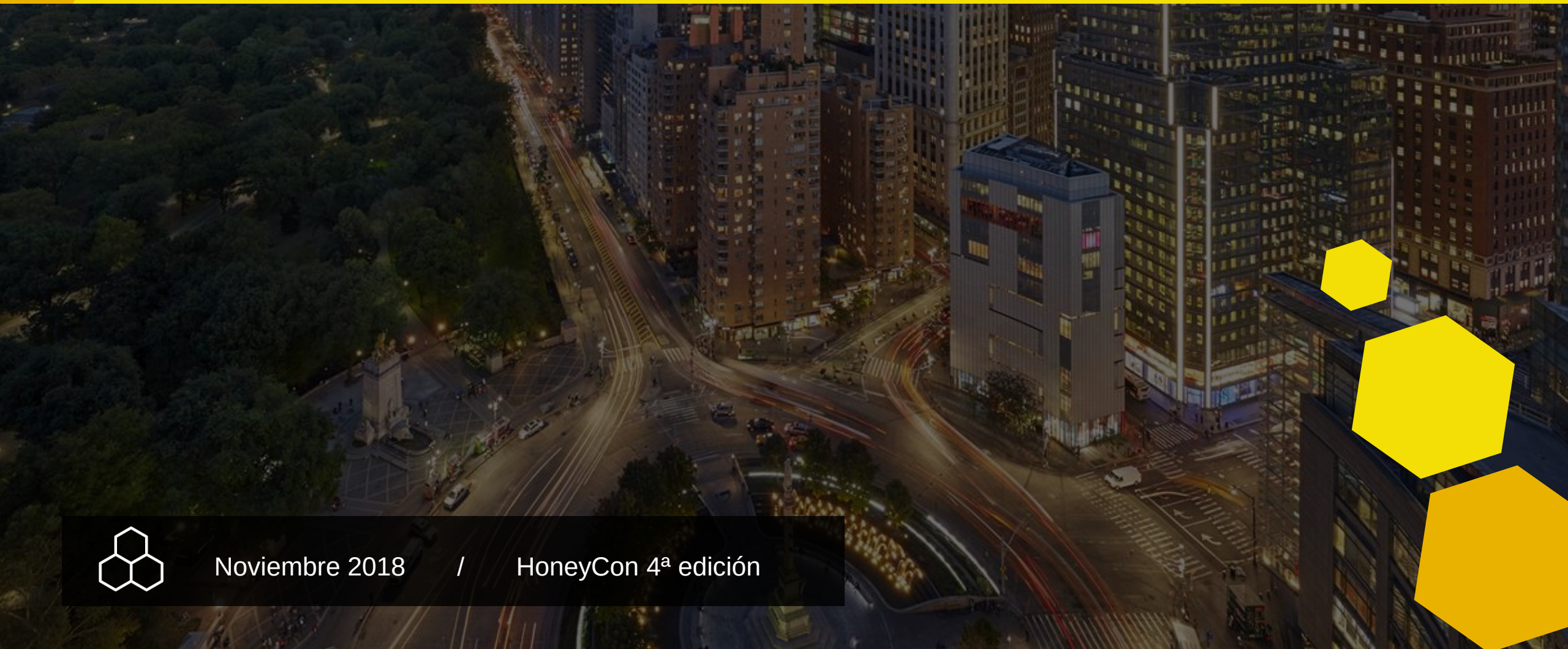
Cómo comenzar

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

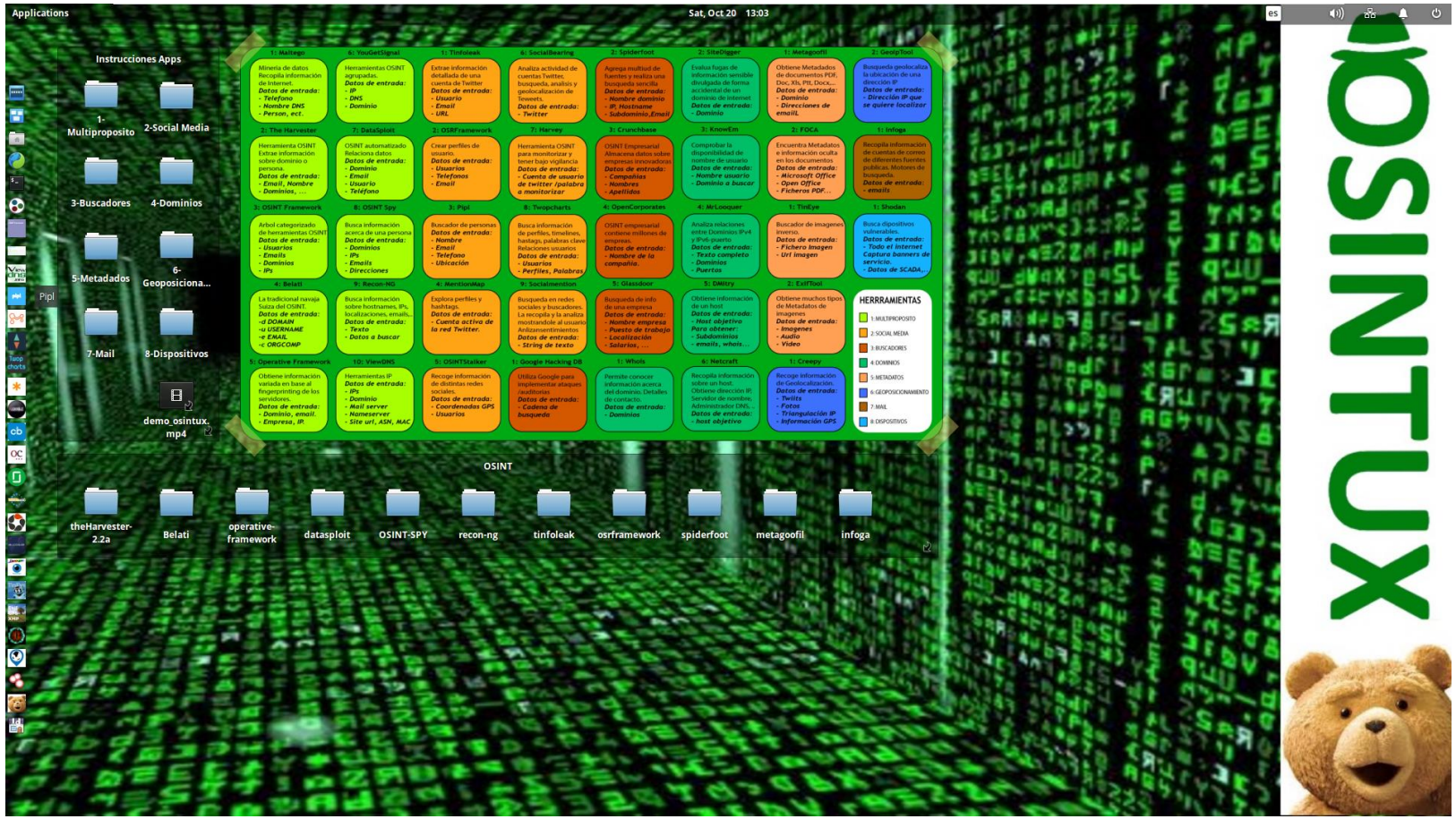
- User: osint Password: osint

Herramientas a destacar:

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

Conociendo Distribuciones OSINT - Osintux

Osintux



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

- User: osintux Password: osintux

Documentación de cada herramienta

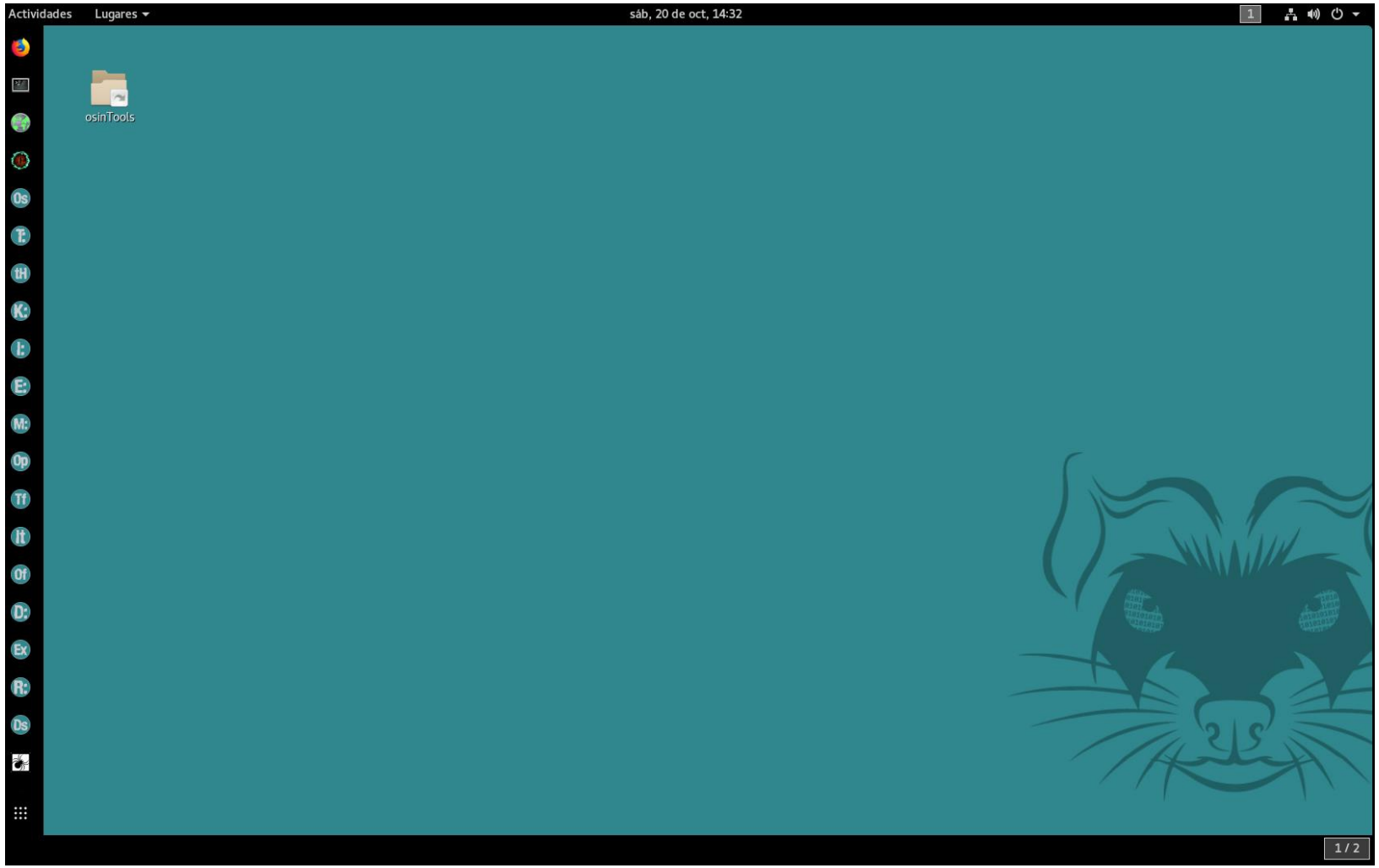
Enfocado para formación

Herramientas a destacar:

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

TLP:GREEN

Huron



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

- User: osint Password: osint

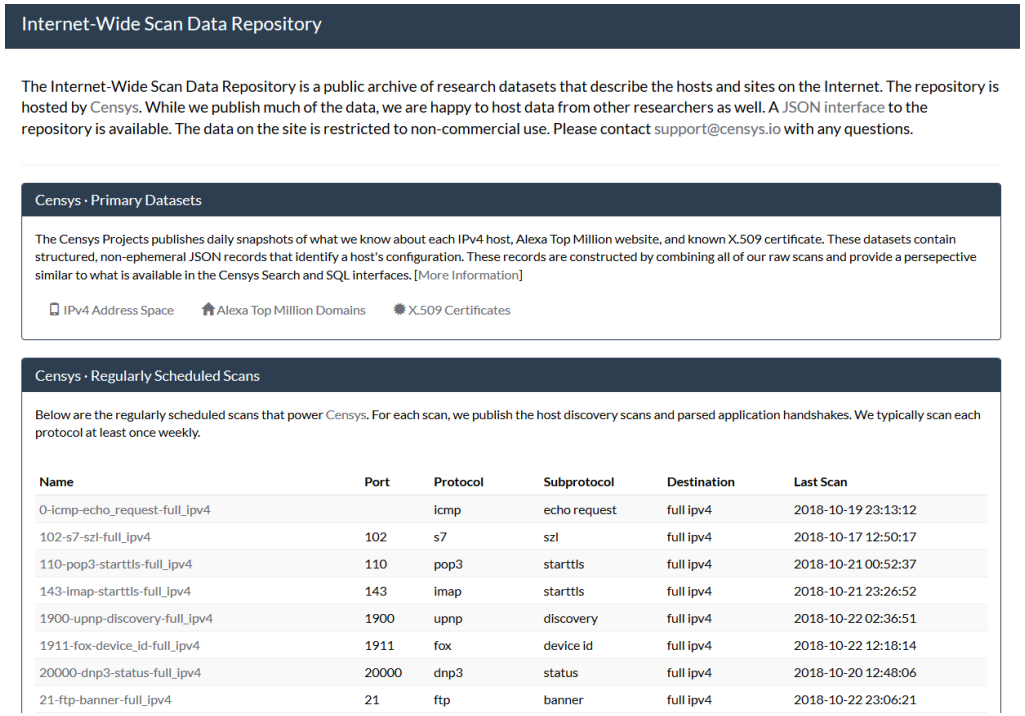
En continua actualización y mejora

Herramientas a destacar:

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

Cómo comenzar – Repositorios de Datos – SCANS.IO

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 persepective similar to what is available in the Censys Search and SQL interfaces. [More Information]

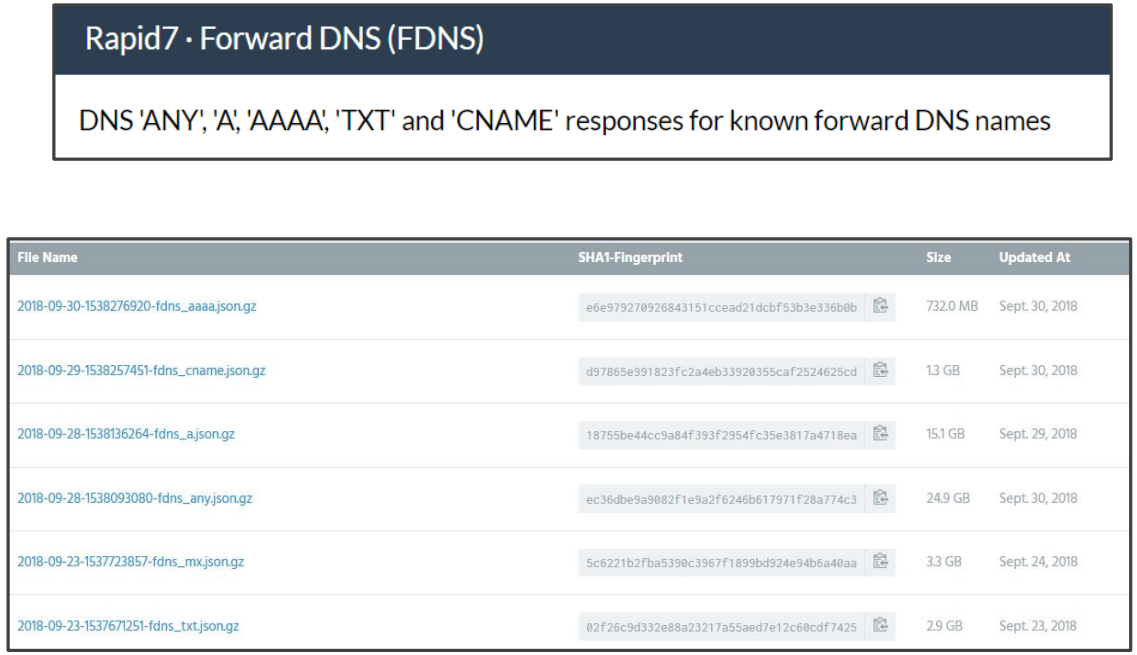
IPv4 Address Space Alexa Top Million Domains X.509 Certificates

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

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.



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	e6e9792709268431 51ccead21dcbf53b3e336b0b	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_a.json.gz	18755be44cc9a84f393f2954fc35e3817a4718ea	15.1 GB	Sept. 29, 2018
2018-09-28-1538093080-fdns_any.json.gz	ec36dbe9a9082f1e9a2f6246b617971f28a774c3	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 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.

Cómo comenzar – Repositorios de Datos - RIPE

Descargando fichero

Index of /ripe/dbase

Name	Last modified	Size	Description
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

Name	Last modified	Size	Description
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/

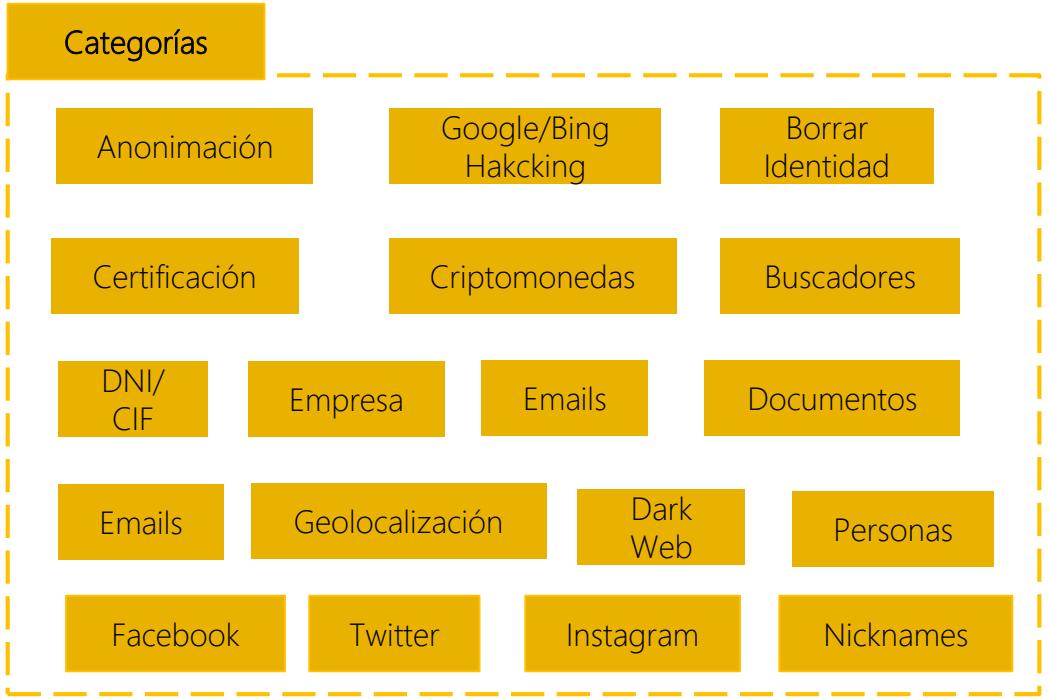
```
root@prometheus002:~/taller_ciberseg# cat ripe.db.inetnum
#
# The contents of this file are subject to
# RIPE Database Terms and Conditions
#
# http://www.ripe.net/db/support/db-terms-conditions.pdf
#

inetnum:        80.16.151.184 - 80.16.151.191
netname:        NETECONOMY-MG41731
descr:          TELECOM ITALIA LAB SPA
country:        IT
admin-c:        DUMY-RIPE
tech-c:         DUMY-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:        DUMY-RIPE
tech-c:         DUMY-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
```

Contenido de archivo parcial de ripe.db.inetnum

Cómo comenzar – Repositorio OSINT de Ciberpatrulla

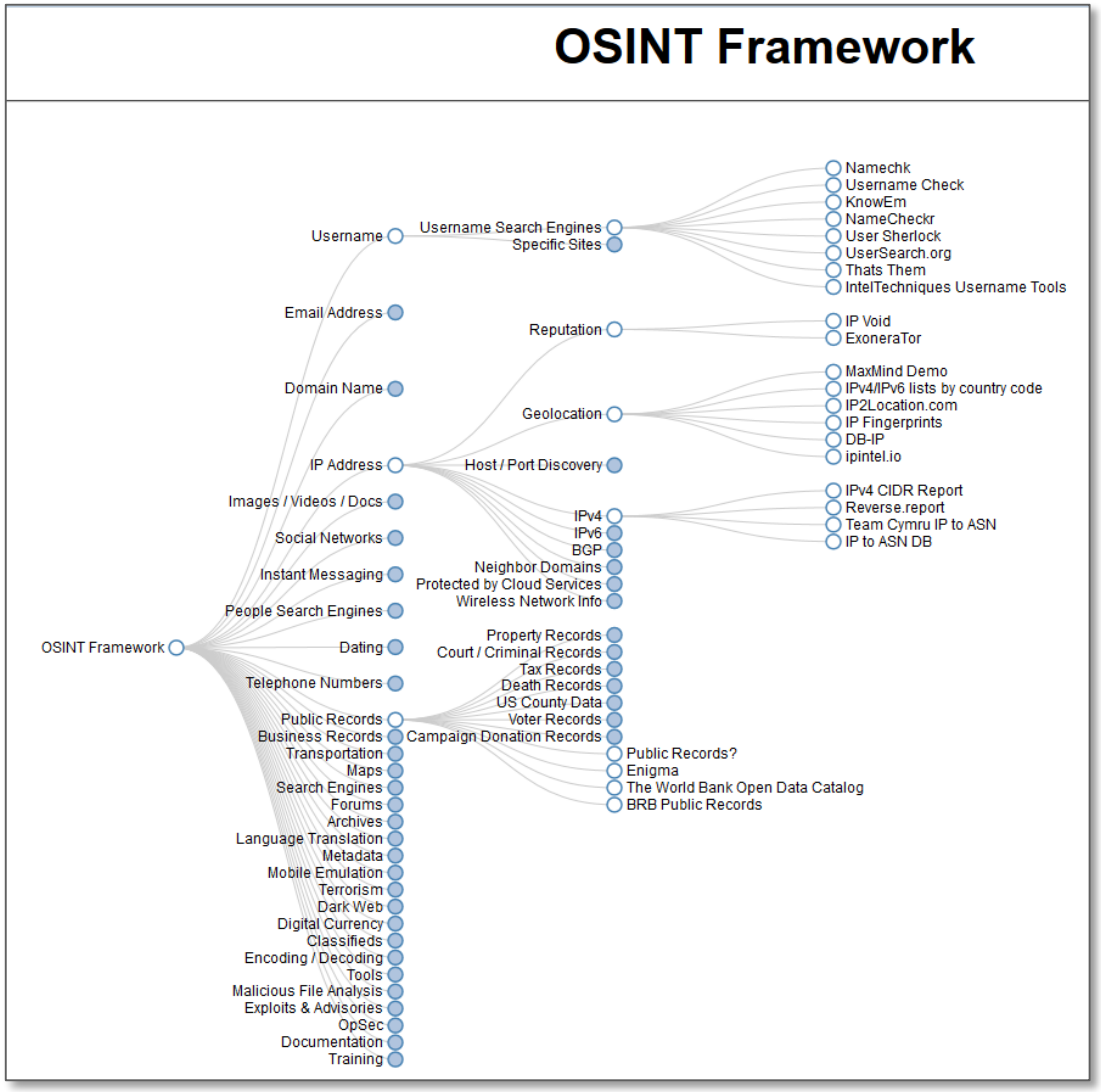
El sitio Web de Ciberpatrulla esta dedicado exclusivamente a Investigaciones OSINT, teniendo un apartado donde aloja un repositorio de herramientas categorizadas por grupos. En cada una de estas categorías, se engloban enlaces a herramientas relacionadas a su temática, facilitando su uso. En constante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

ciberpatrulla.com/links/



TLP:GREEN

Cómo comenzar – Repositorio de Datos - OSINT Framework



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.

TLP:GREEN

Cómo comenzar – Repositorio de Datos – IntelTechniques

https://inteltechniques.com/menu.html

El sitio Web de Intel Techniques esta enfocado a ofrecer formación OSINT, facilitando recursos como libros o podcasts. Dispone de un Portal OSINT dentro del menú Tools, donde aloja diferentes buscadores donde consultar por tipo de investigación.

Investigaciones

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

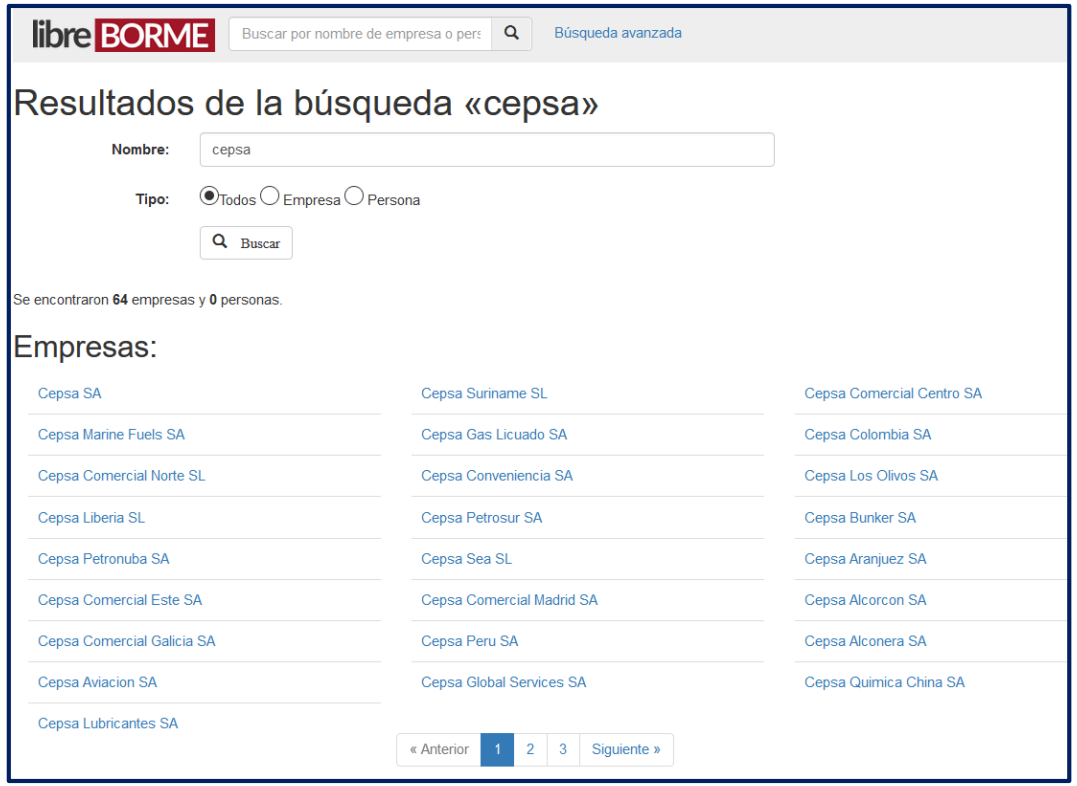
TLP:GREEN

Cómo comenzar – Localizar Empresas / Personas

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.

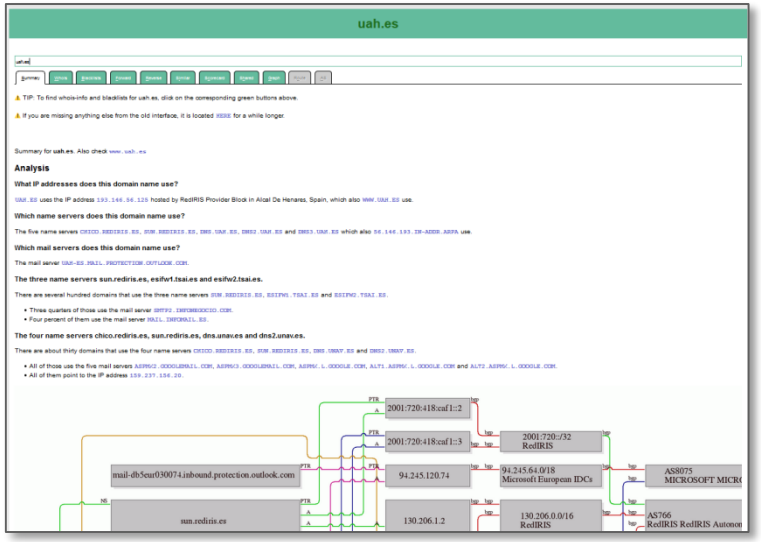
https://libreborme.net/

Input: Nombre Persona o empresa



TLP:GREEN

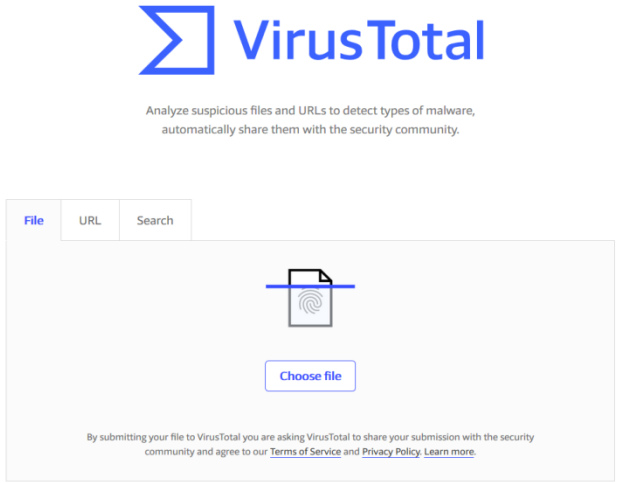
Cómo comenzar – Introduciendo Herramientas



https://www.robtex.com

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

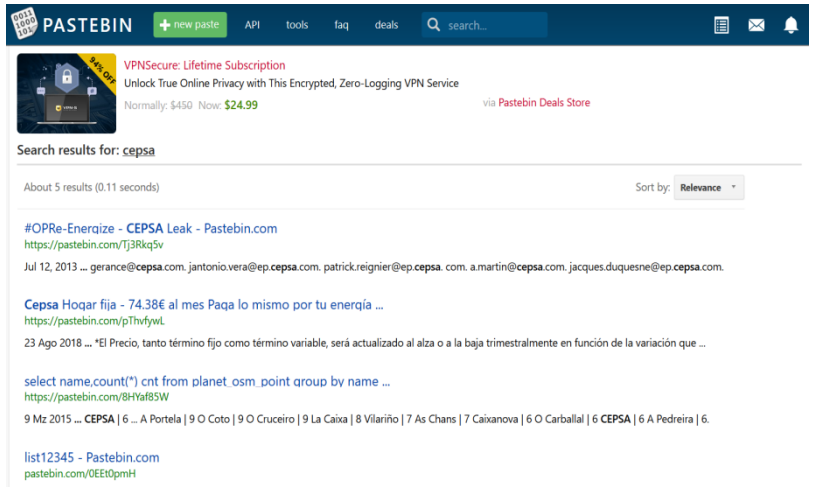
Input: Dominio, IP, Rango IP o ASN



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

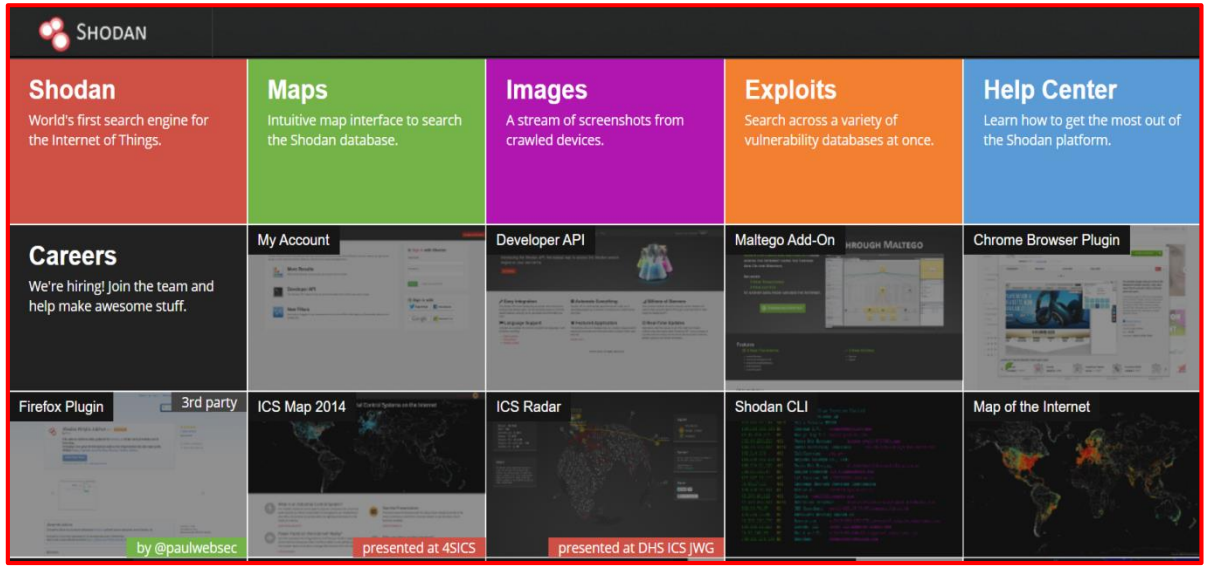


https://pastebin.com

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

Input: Keyword

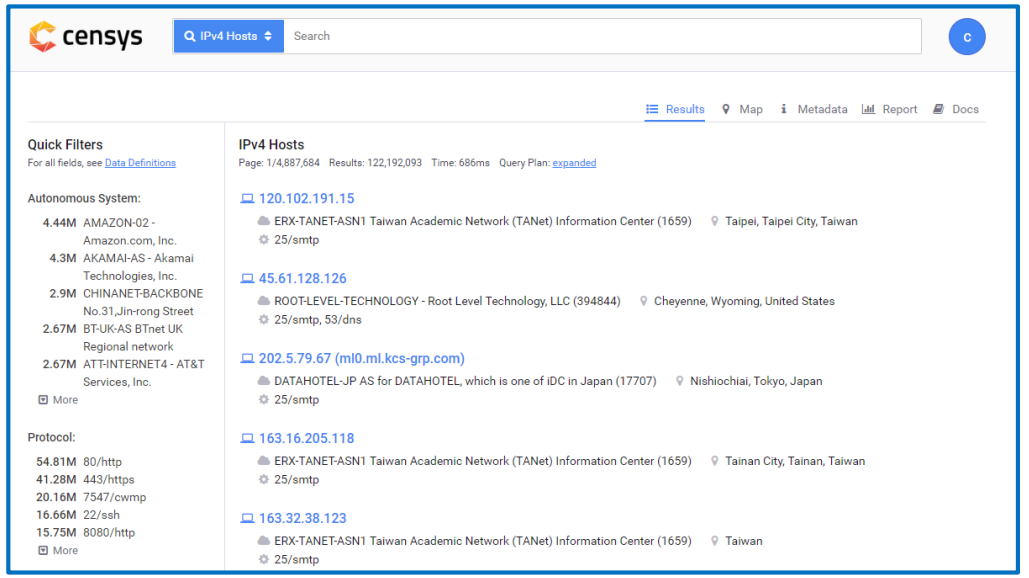
Cómo comenzar – Localizar Activos Expuestos en Internet



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

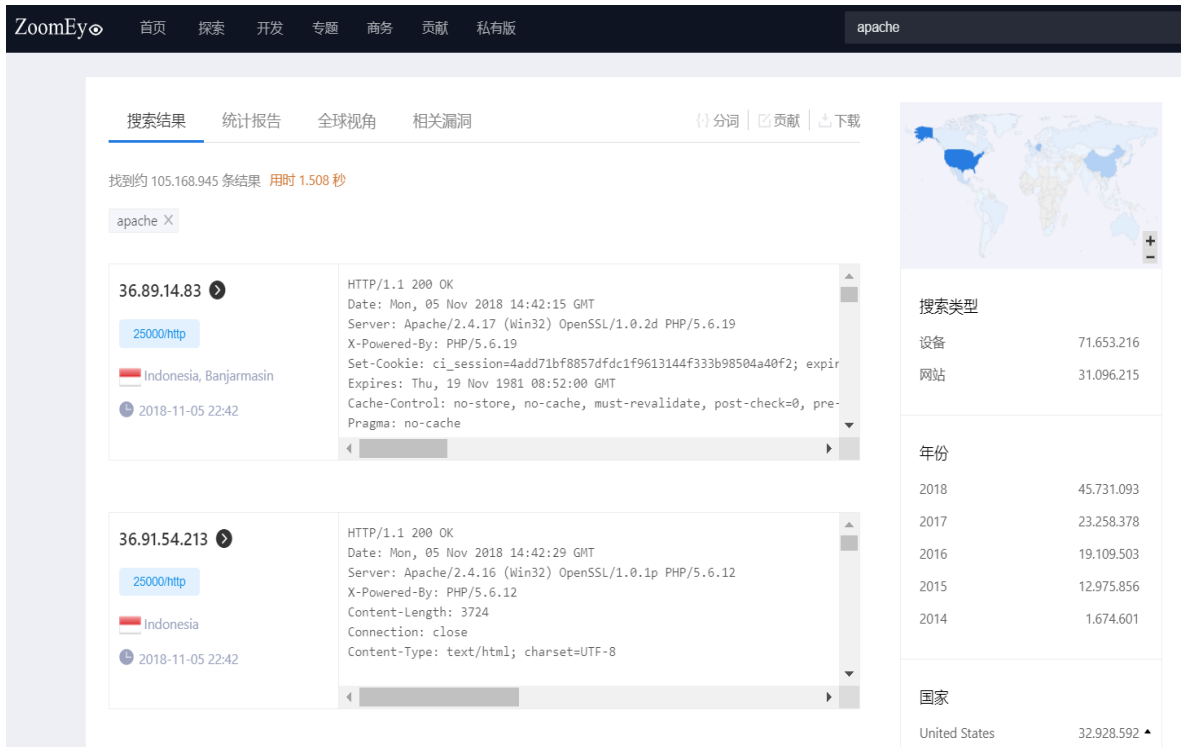


https://censys.io

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.

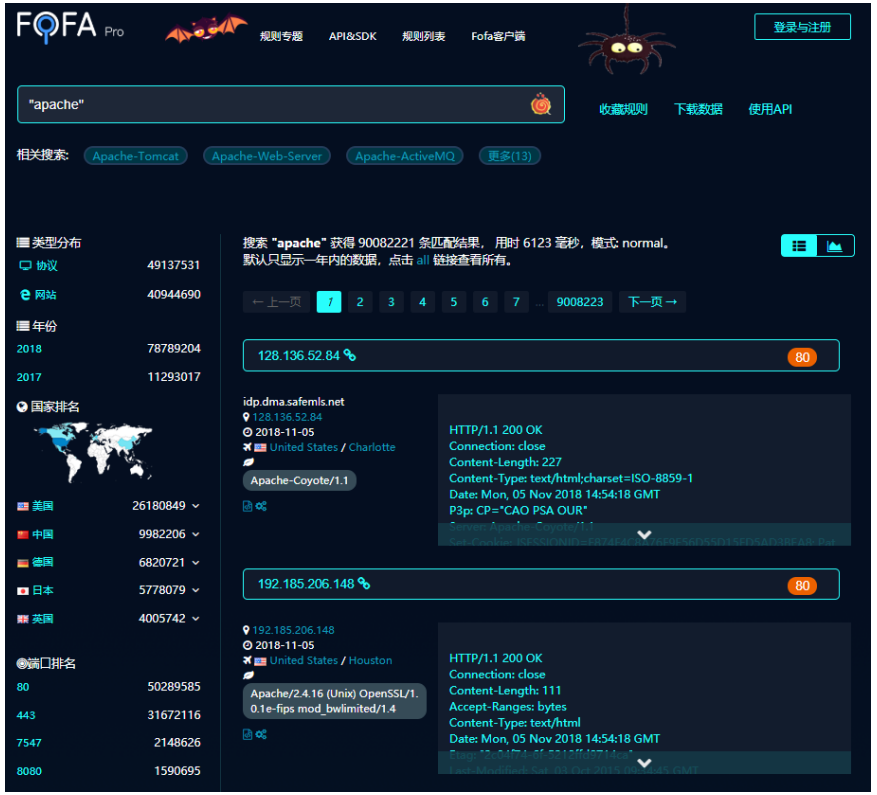
Input: Dominio, IP, Rango IP, Keyword

Cómo comenzar – Localizar Activos Expuestos en Internet



https://www.zoomeye.org

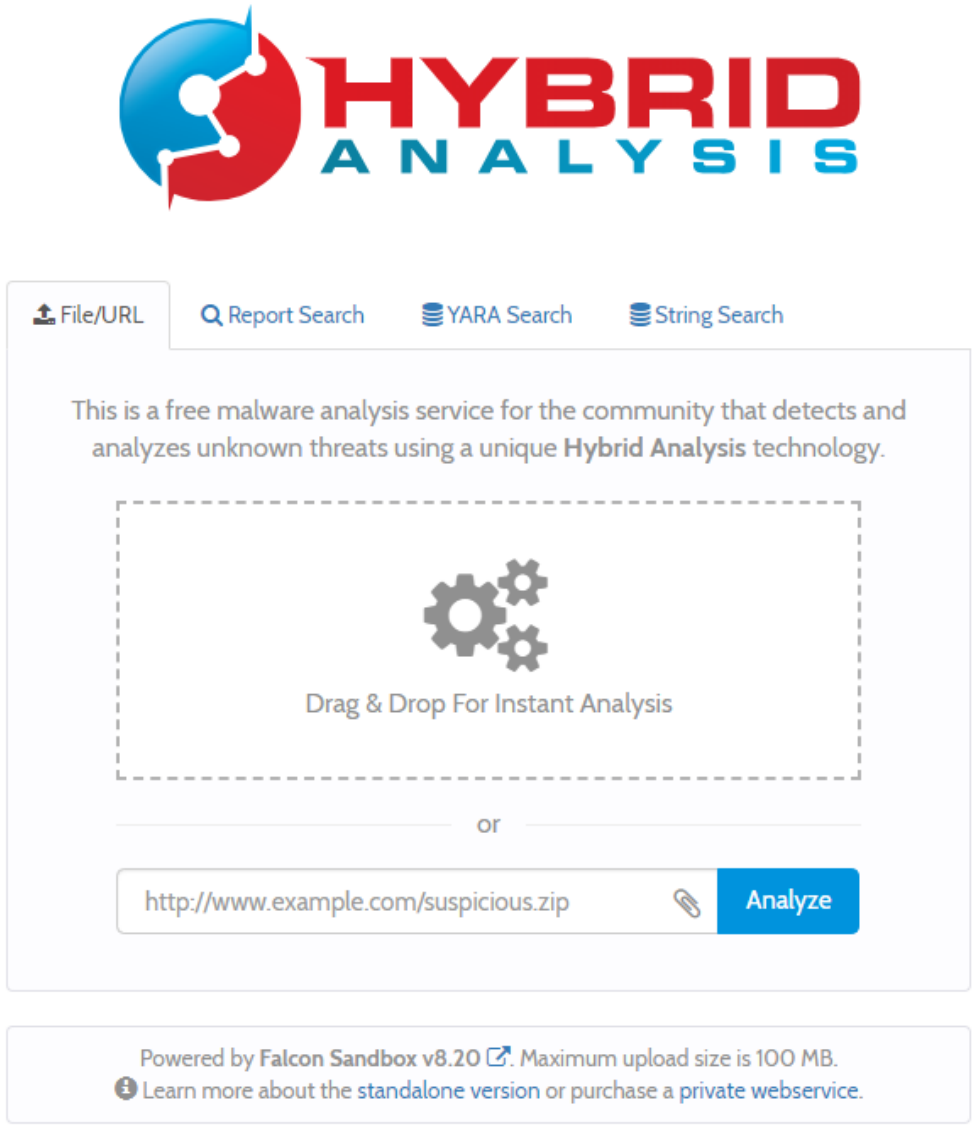
Input: Dominio, IP, Rango IP, Nombre Dispositivo



https://fofa.so/

Input: Dominio, IP

TLP:GREEN

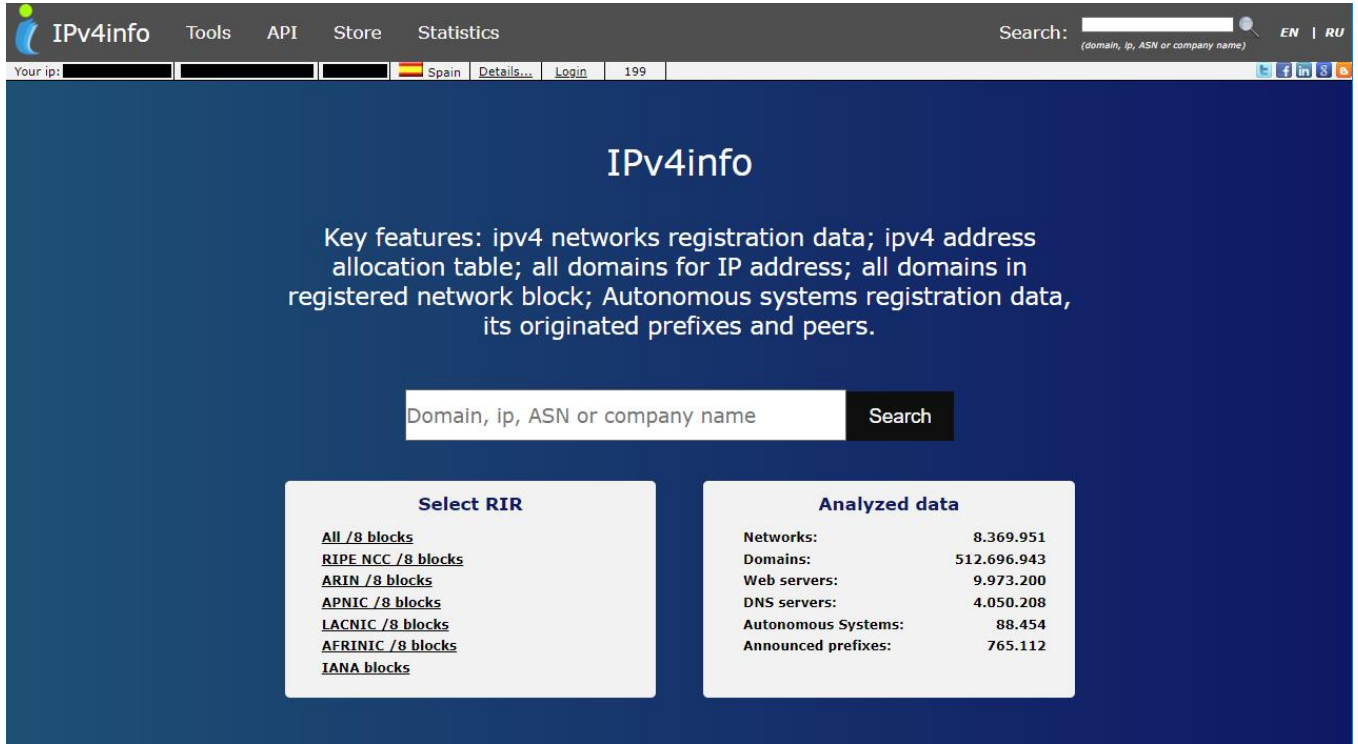


https://www.hybrid-analysis.com

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

Cómo comenzar – Localizar Activos de Red



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.

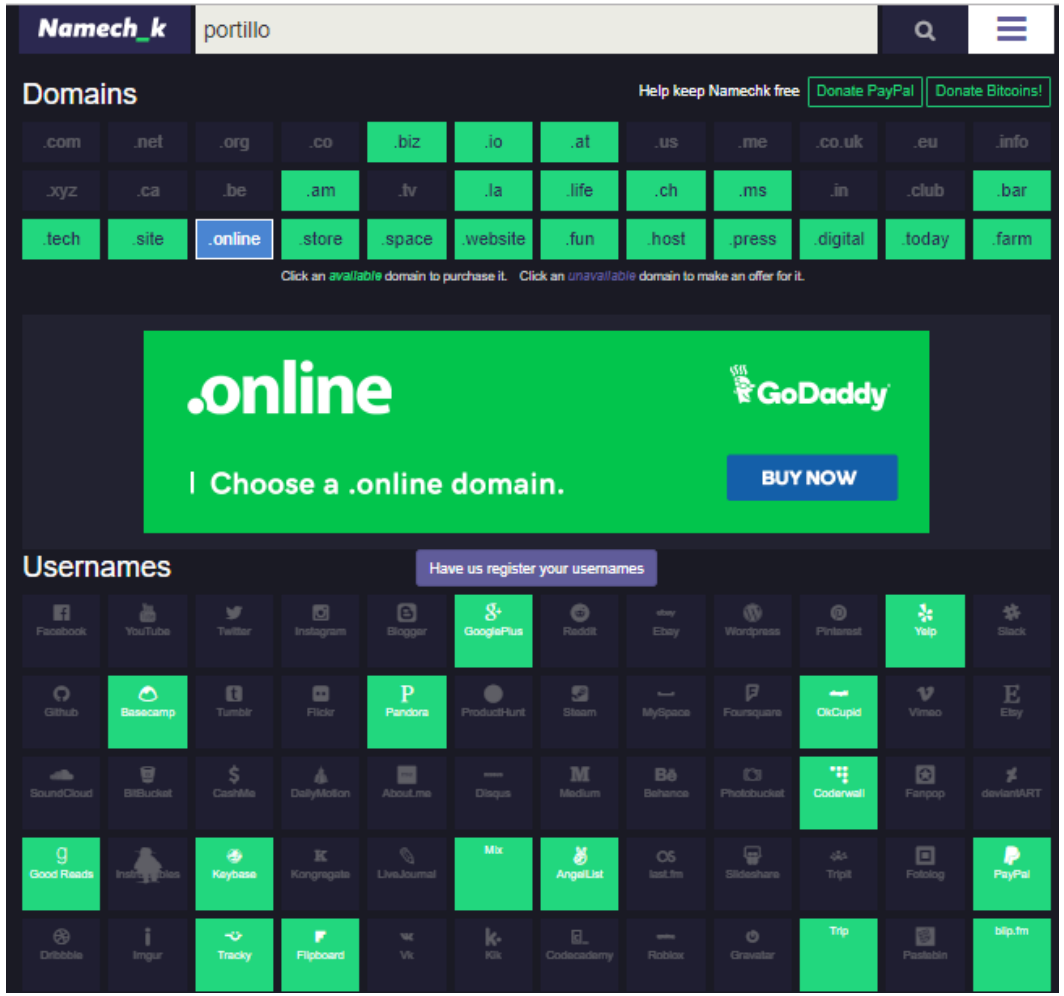
Input: Dominio, IP, ASN, Nombre Organización

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

Cómo comenzar – Localizar Nombres de Usuarios

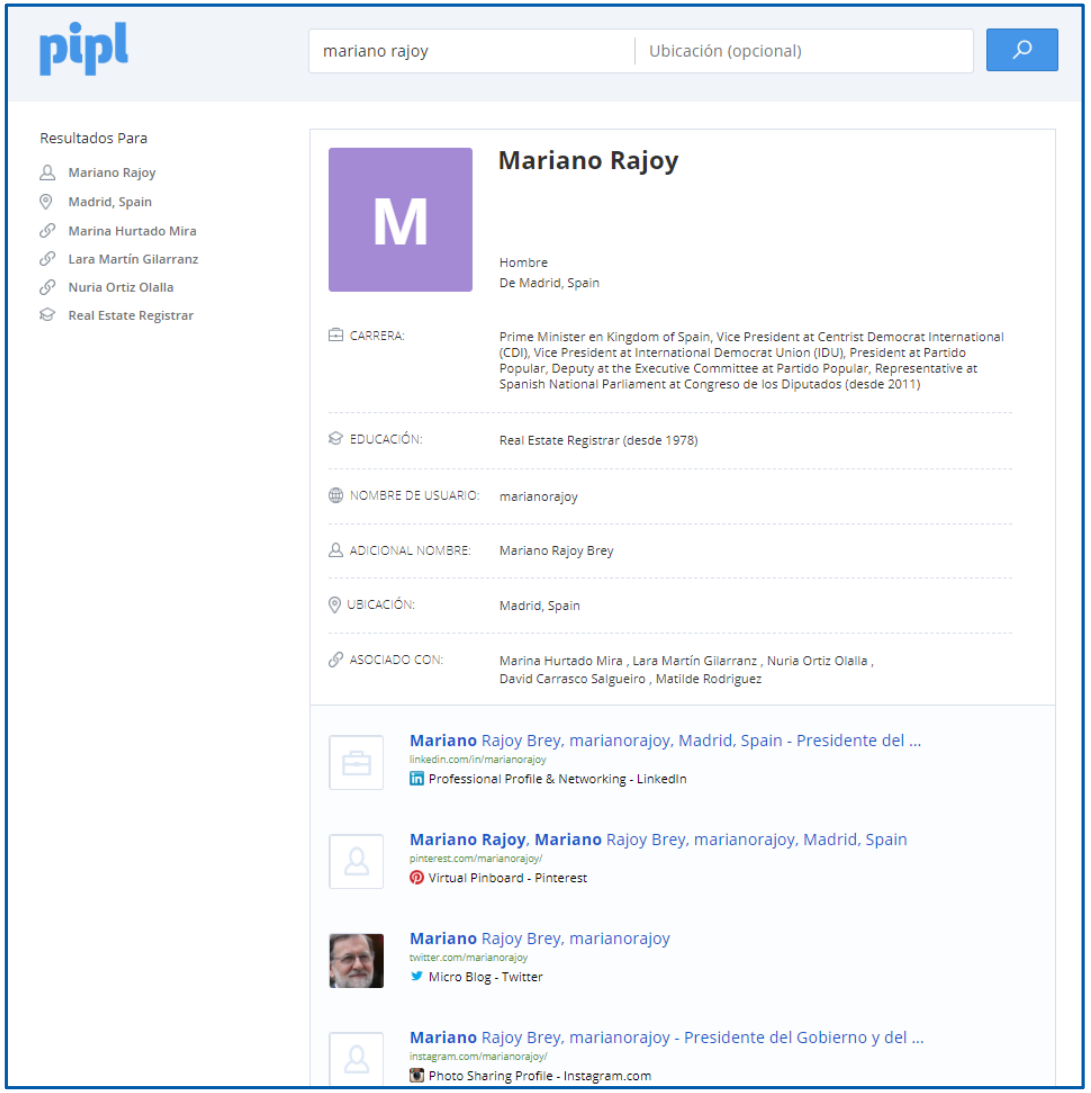


https://namechk.com

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

Cómo comenzar – Localizar Perfiles de Usuarios



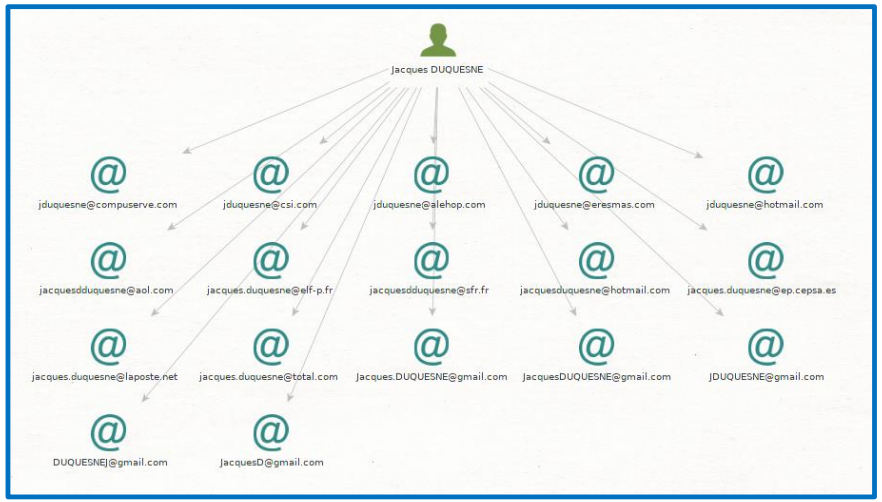
https://pipl.com

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.

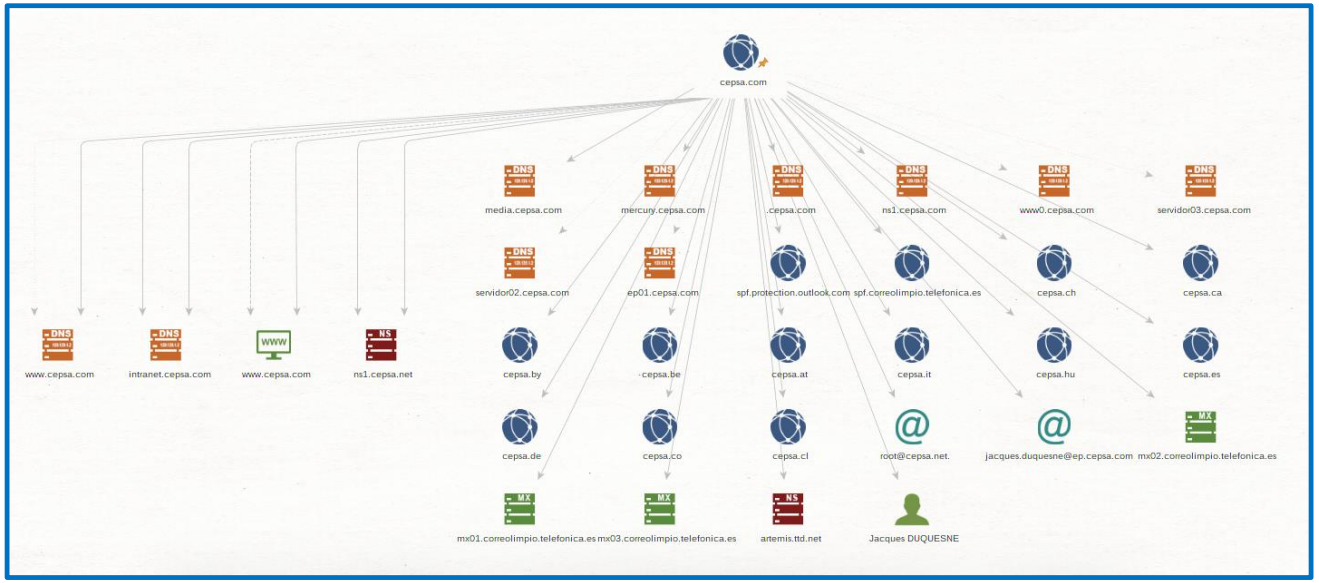
Input: Nombre Persona, Email, Teléfono

Cómo comenzar – Localizar Información mediante Grafos

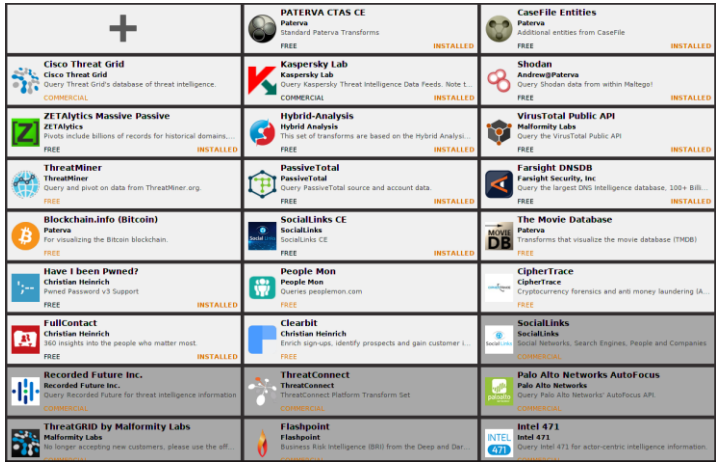
Maltego es una herramienta que recopila información, mostrando las evidencias mediante grafos, siendo de gran ayuda en el análisis posterior de la información obtenida por los equipos de inteligencia y forense. Contiene una serie de módulos de aplicaciones externas (transforms) que complementan su potencial,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



https://www.paterva.com

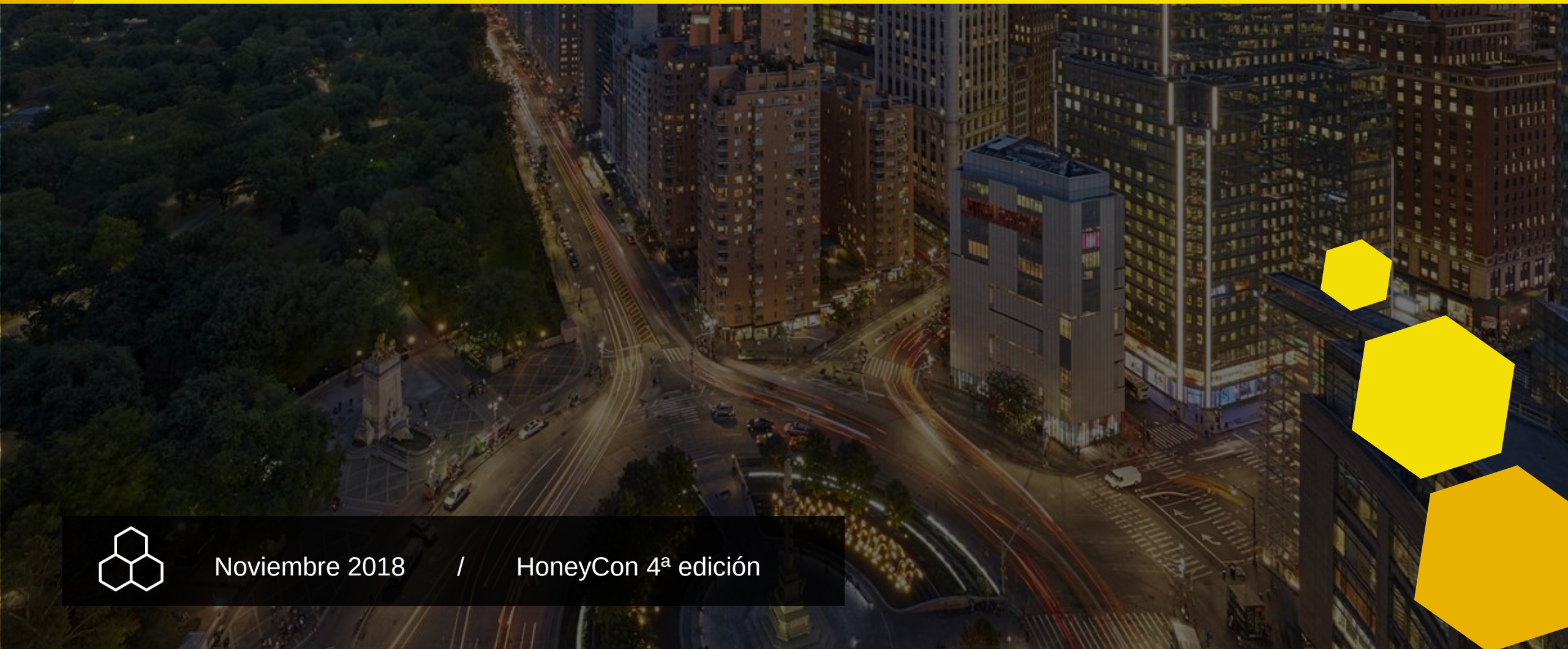


Comando: maltego



TLP:GREEN

Investigación objetivo…



Noviembre 2018 / HoneyCon 4ª edición

Investigación Objetivo – Buscar Información sobre la Organización

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	COMPAÃ‘IA ESPAÃ‘OLA 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': 'COMPA\xc3\x91IA ESPA\xc3\x91OLA 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 Adresses'}, {'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$
```

Investigación Objetivo – Buscar Información sobre la Organización

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.

```
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
```

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

	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		2017-11-22
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

Investigación Objetivo – Localizar Activos expuestos en Internet a partir de la Organización

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

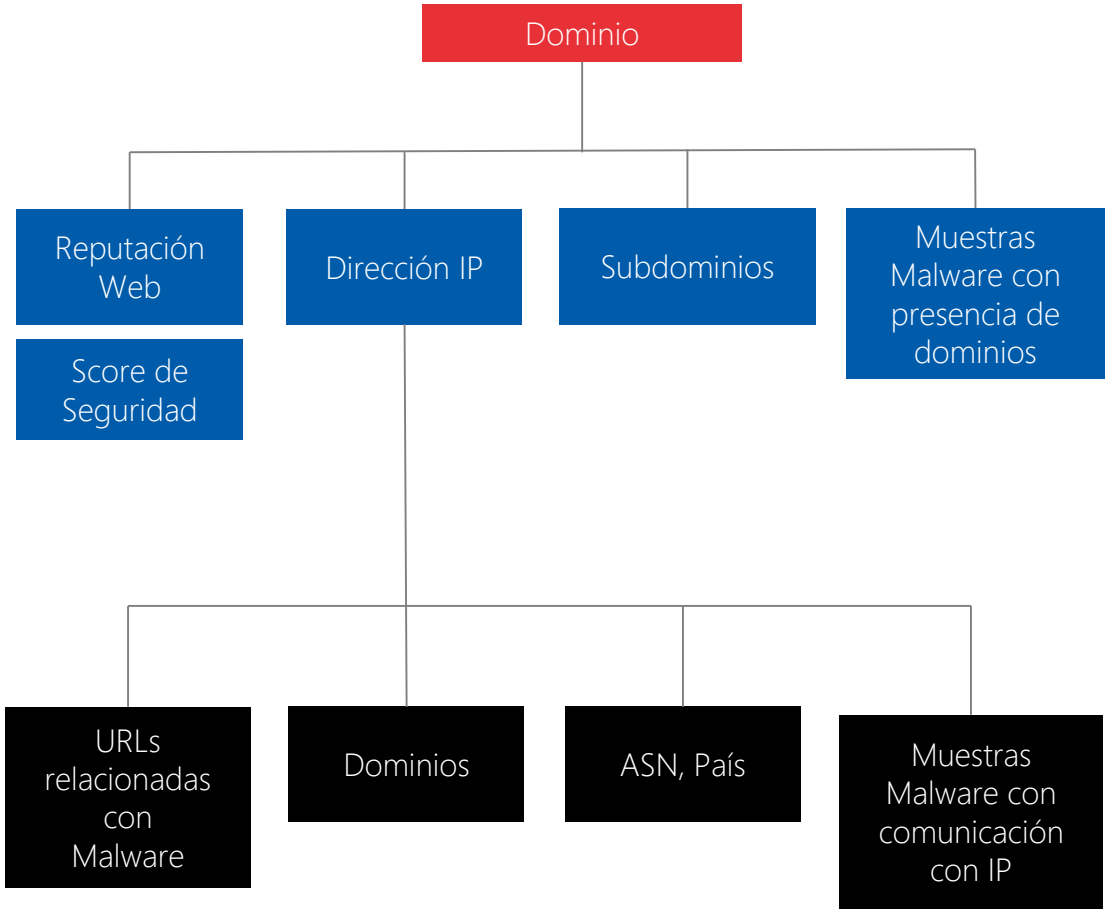
Comando:
python 7.shodan.py –f "listado_empresas" –o "fichero_salida"

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		

Investigación Objetivo – Buscar Información sobre Dominio Principal


```
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.

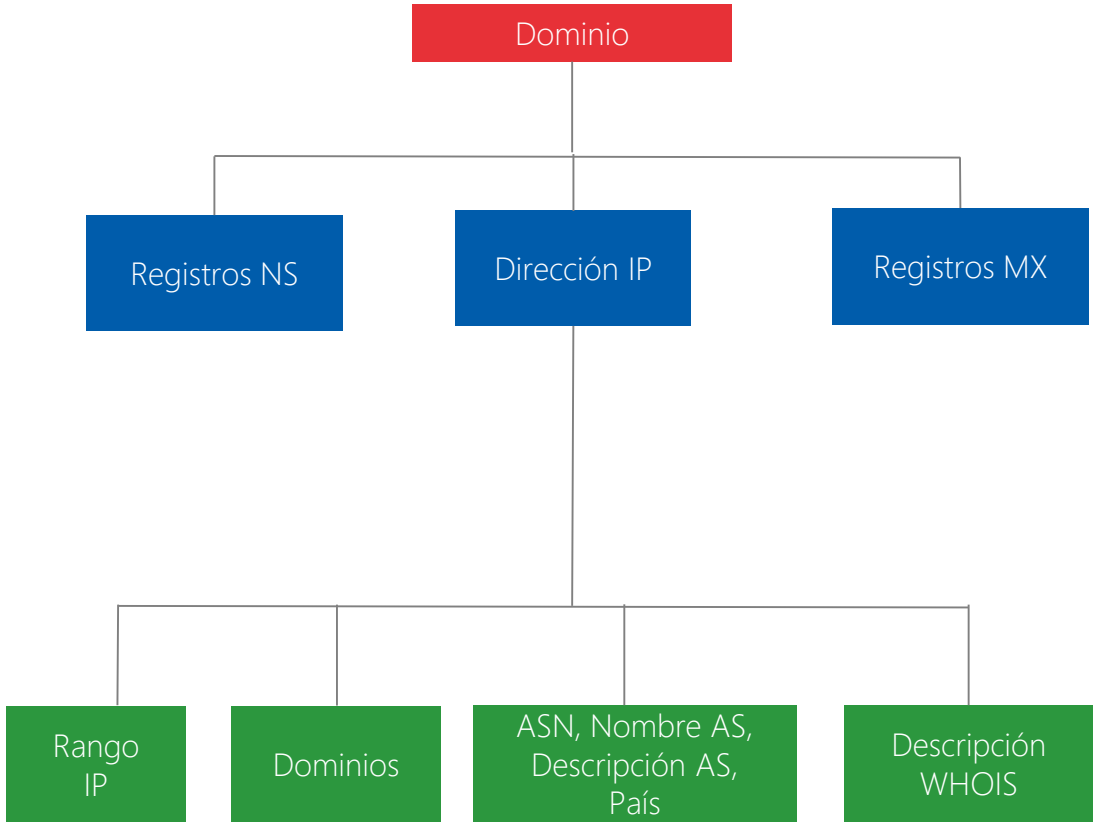
3.virustotal.py

Comando:
python 3.virustotal.py –f “listado_dominios” –o “fichero_salida”

TLP:GREEN

Investigación Objetivo – Buscar Información sobre Dominio Principal

```
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”

Investigación Objetivo – Buscar Información sobre Dominio Principal

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. *bob@example.com*

TLP:GREEN

Investigación Objetivo – Buscar Geoposicionamiento sobre Dominio Principal

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)

Investigación Objetivo – Buscar Información sobre Dominio Principal

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.

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

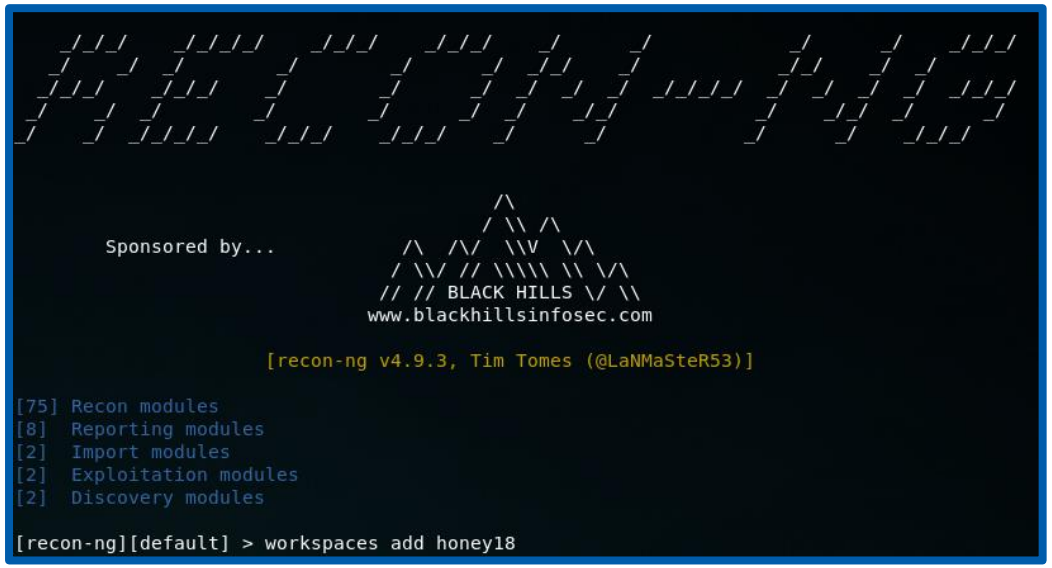
Input: Dominio, Email, Username, Teléfono, IP

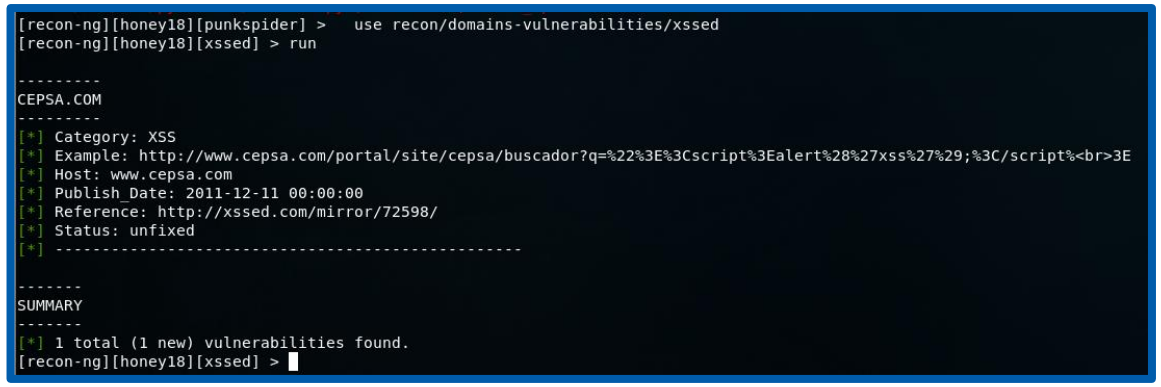
Investigación Objetivo – Buscar Información sobre dominios asociados detectados

Recon-ng es un framework que permite obtener información sobre diferentes tipos de objetivos. Posee una interfaz por línea de comandos muy similar a Metasploit. Se integra con APIs de multitud de plataformas, interacciona con bases de datos, y utiliza gran variedad de módulos para poder realizar un reconocimiento de cualquier tipo de investigación y generar resultados para diferentes tipos de informes.

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

Comando: python recon-ng





Investigación Objetivo – Buscar amenazas sobre TypoSquatting

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 GeoIP dnspython requests ssdeep

Input: Dominio


{1.04b}
Disabling multithreaded job distribution in order to query WHOIS servers
Processing 198 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 googlea.es 176.28.103.205/Spain NS:ns1.srv-hostalia.com MX:mx.googlea.es HTTP:"Apache" SMTP:"relayin06.dominioabsoluto.net ESMTP"
Addition googleb.es -
Addition googlec.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 googlee.es 185.53.178.9/Germany NS:ns1.parkingcrew.net MX:mail.h-email.net HTTP:"nginx"
Addition googlef.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.landl.es MX:mx00.landl.es HTTP:"Apache" SMTP:"554-kundenserver.de (mxeue003) Nemesis E"
Addition googlej.es -
Addition googlek.es -
Addition googlel.es -
Addition googlem.es -
Addition googlen.es -
Addition googleo.es -
Addition googlep.es -
Addition googleq.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 googleu.es -
Addition googlev.es -
Addition googlew.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 -
Bitsquatting foogle.es 185.53.178.7/Germany NS:ns1.parkingcrew.net MX:mail.h-email.net HTTP:"nginx"
Bitsquatting eoogle.es -
Bitsquatting coogle.es 37.152.88.54/Spain NS:ns1.dondominio.com HTTP:"Apache"
Bitsquatting oogle.es 50.63.202.19/United States NS:ns61.domaincontrol.com MX:mailstore1.secureserver.net HTTP:"HTTP 302" SMTP:"554 p3plibsmtp02-12.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 -
Bitsquatting ggogle.es 0.0.0.0 NS:ns1.ggogle.es
Bitsquatting gongle.es -
Bitsquatting gomgle.es -
Bitsquatting gokgle.es -
Bitsquatting goggle.es -
Bitsquatting goofle.es 213.186.33.5/France NS:dns10.ovh.net MX:redirect.ovh.net HTTP:"nginx"
Bitsquatting gooele.es -
Bitsquatting goocle.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 p3plibsmtp01-09.prod.phx3.secureserv"
Bitsquatting goowle.es -
Bitsquatting googme.es -
Bitsquatting googne.es -
Bitsquatting googhe.es -
Bitsquatting googde.es -
Bitsquatting googld.es -

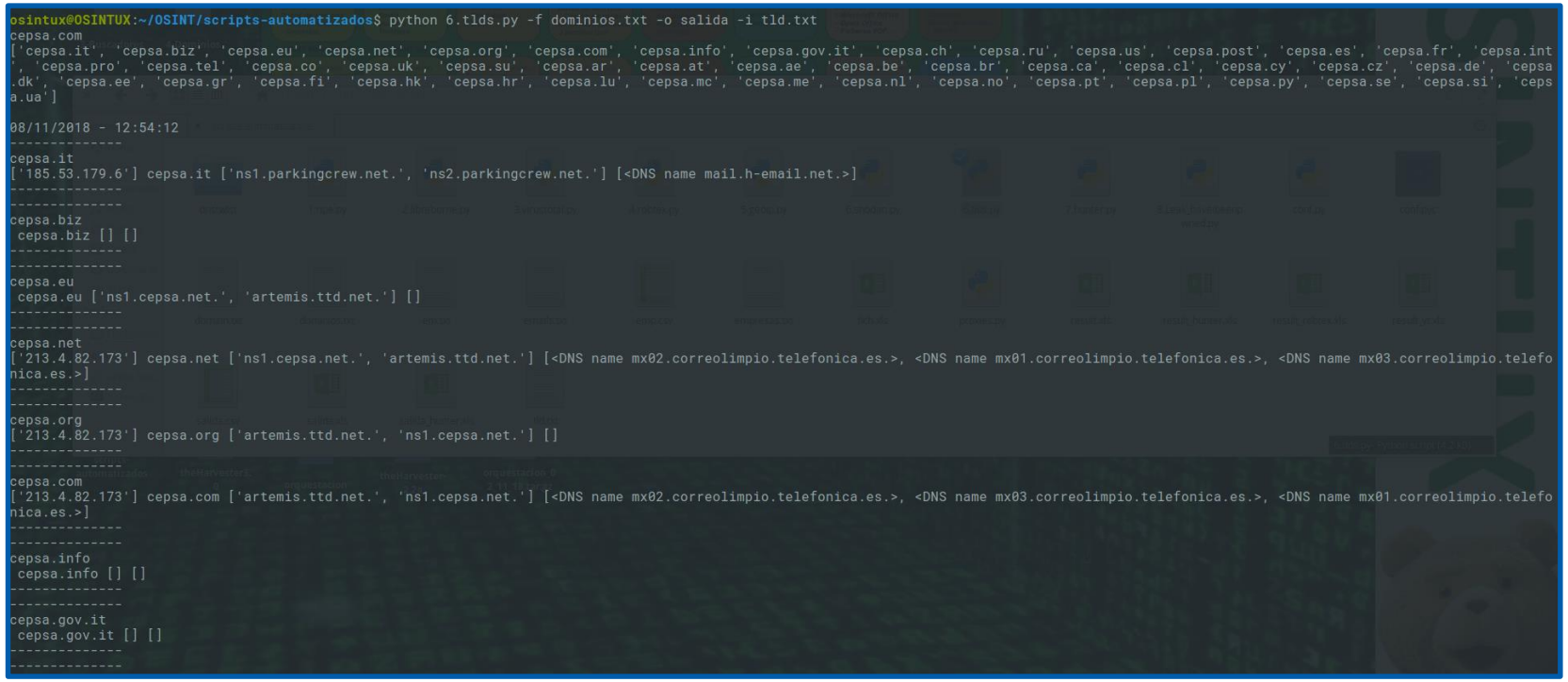
TLP:GREEN

Investigación Objetivo – Localizar Dominios con otros TLDs

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"



Investigación Objetivo – Localizar Emails

TheHarvester es una herramienta que permite recopilar información sobre un objetivo de manera pasiva, usando los motores de búsquedas de Bing, Google, Yahoo, Baidu, además de Shodan, ThreatCrowd, y de manera mas activa, realizando Fuerza Bruta DNS. Se pueden obtener emails, subdominios, IPs, nombre de perfiles de usuario en redes sociales.

https://github.com/laramies/theHarvester

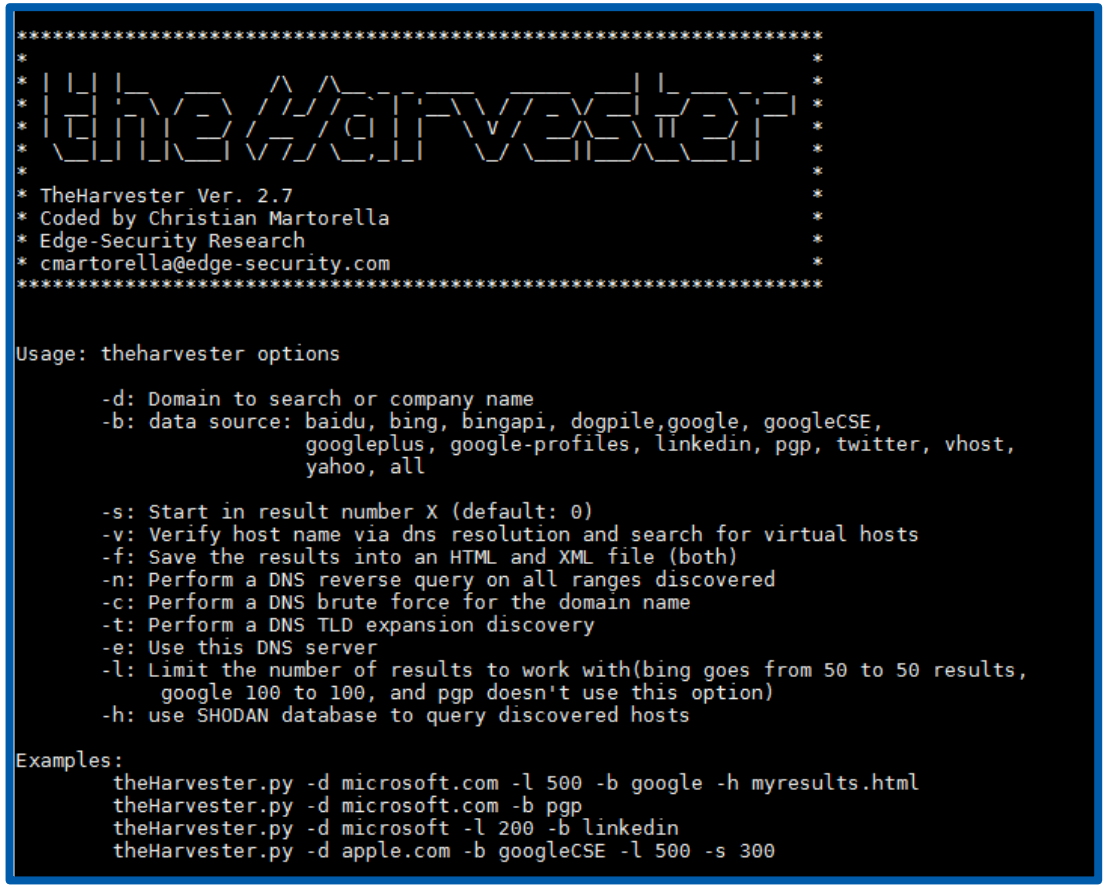
Comando:
python theHarvester.py -d cepsa.com -l 300 -b all -f result.html

Input: Dominio

Listado de Emails

Listado de Subdominios e IPs

Listado de nombres de usuarios de Redes Sociales



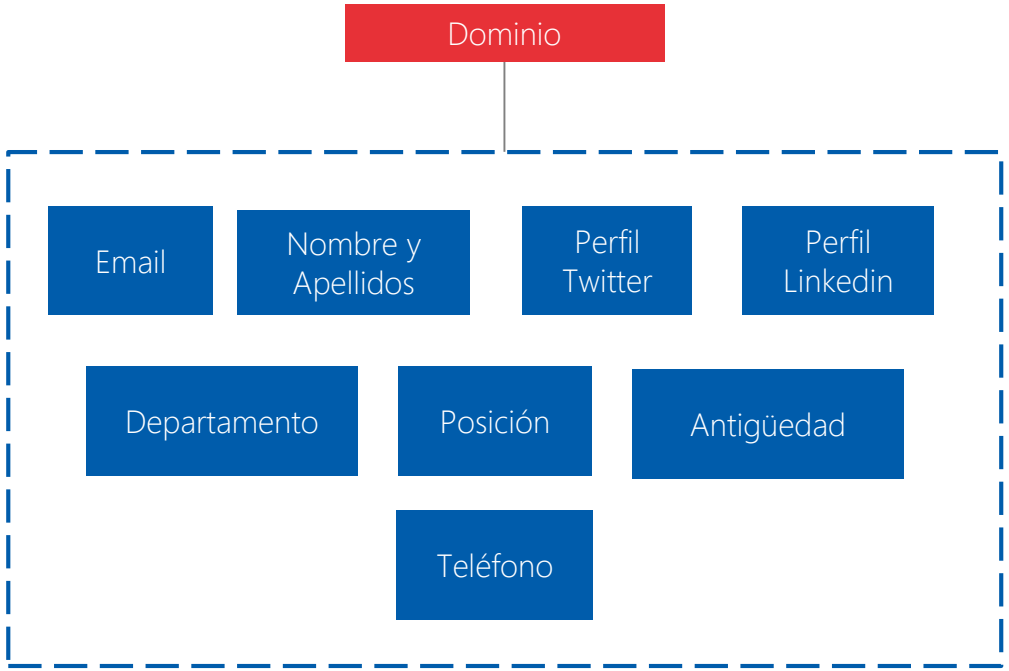
Investigación Objetivo – Localizar Emails / Perfiles usuarios / Personas

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$
```



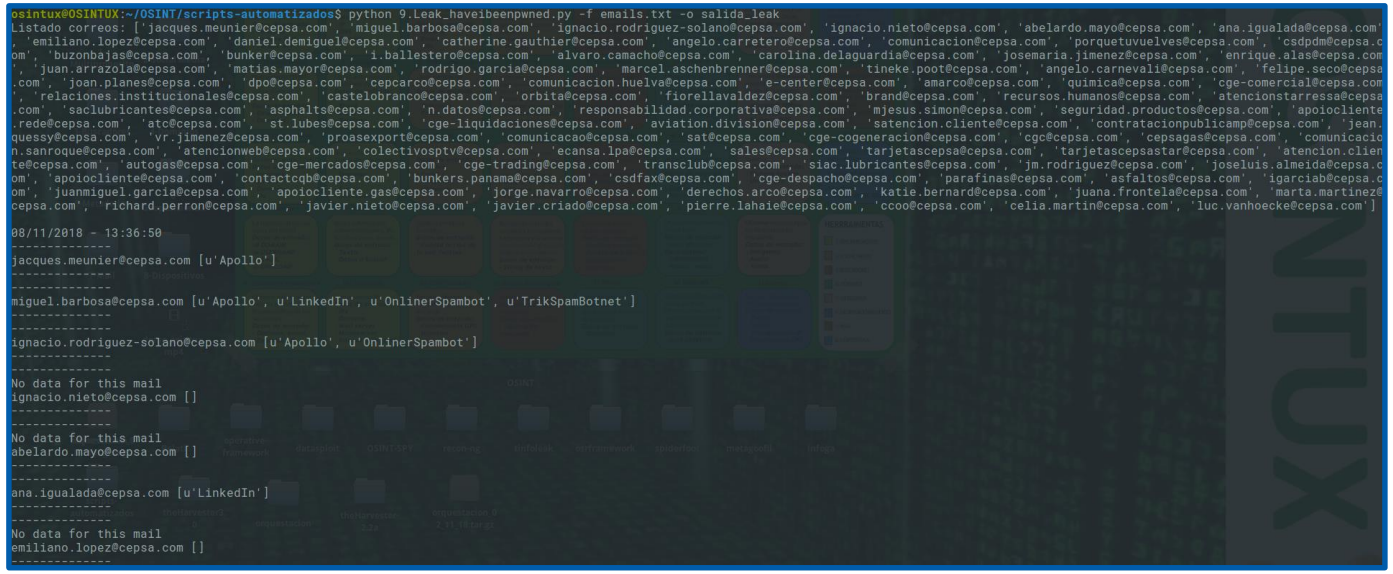
Investigación Objetivo – Localizar Leaks

https://haveibeenpwned.com/

HaveIbeenPwned 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.

9.Leak_haveibeenpwned.py

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



	Email	Leak
2	jacques.duquesne@ep.cepsa.com	[]
3	lubrificantes.pedidos@cepsa.com	[]
4	relaciones.institucionales@cepsa.com	[u'Apollo']
5	cristina.arteche@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.ballestero@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']

Investigación Objetivo – Localizar Leaks

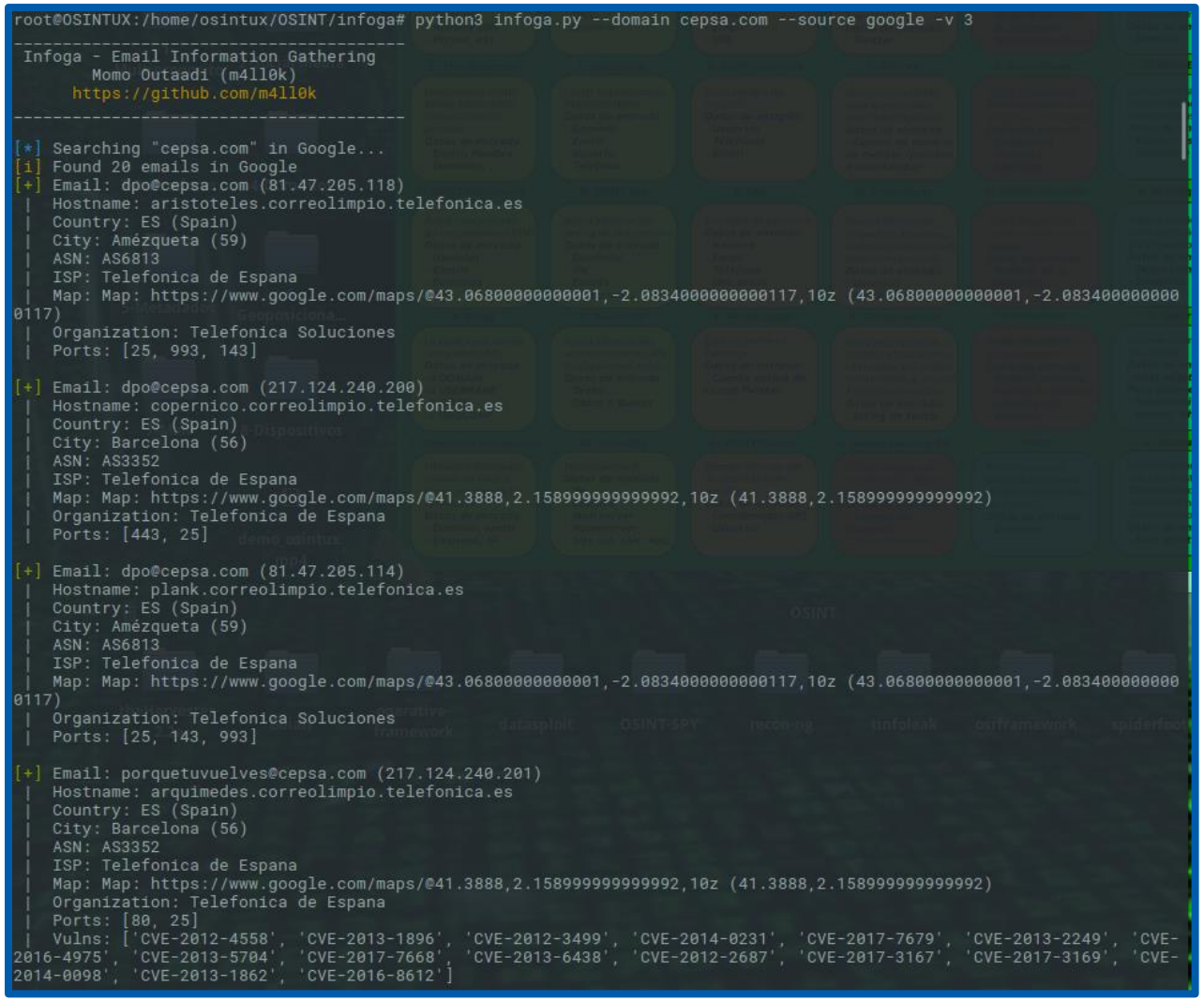
https://github.com/m4ll0k/Infoga

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

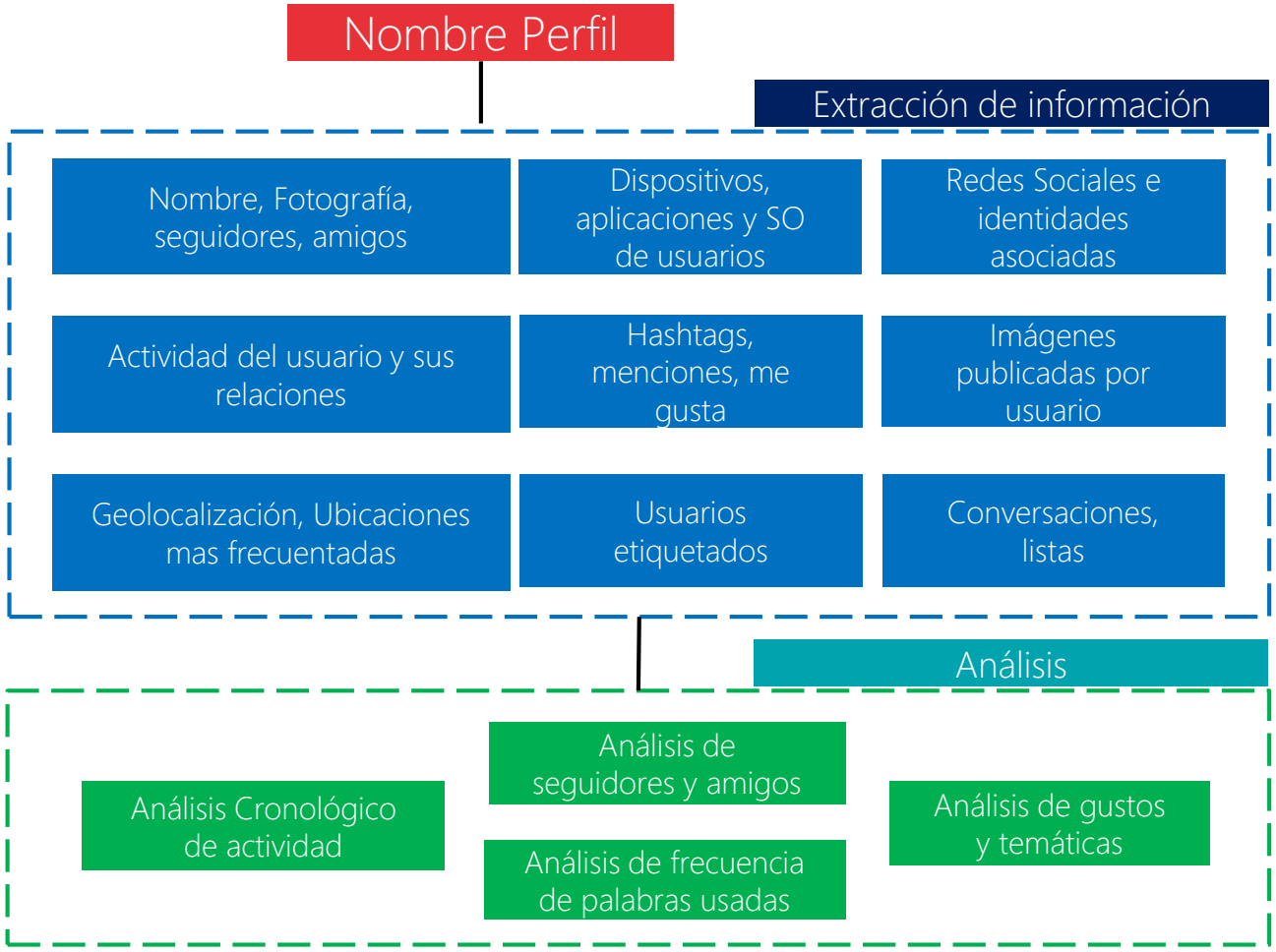
Comando: python3 infoga.py --info "correo" --breach --verbose 3

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)



Investigación Objetivo – Localizar y Analizar Perfil de Twitter

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/

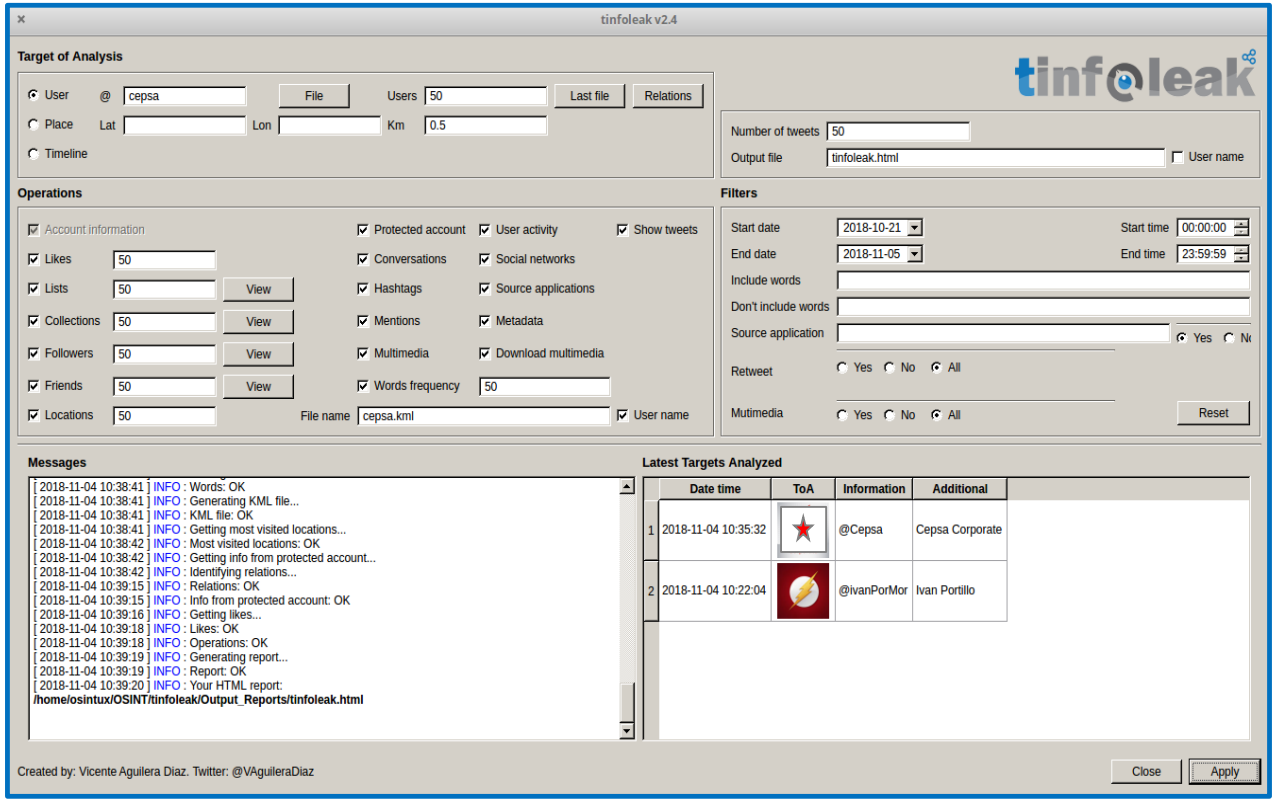
API Key y Token asociados a APP:

CONSUMER_KEY ACCESS_TOKEN
CONSUMER_SECRET ACCESS_TOKEN_SECRET

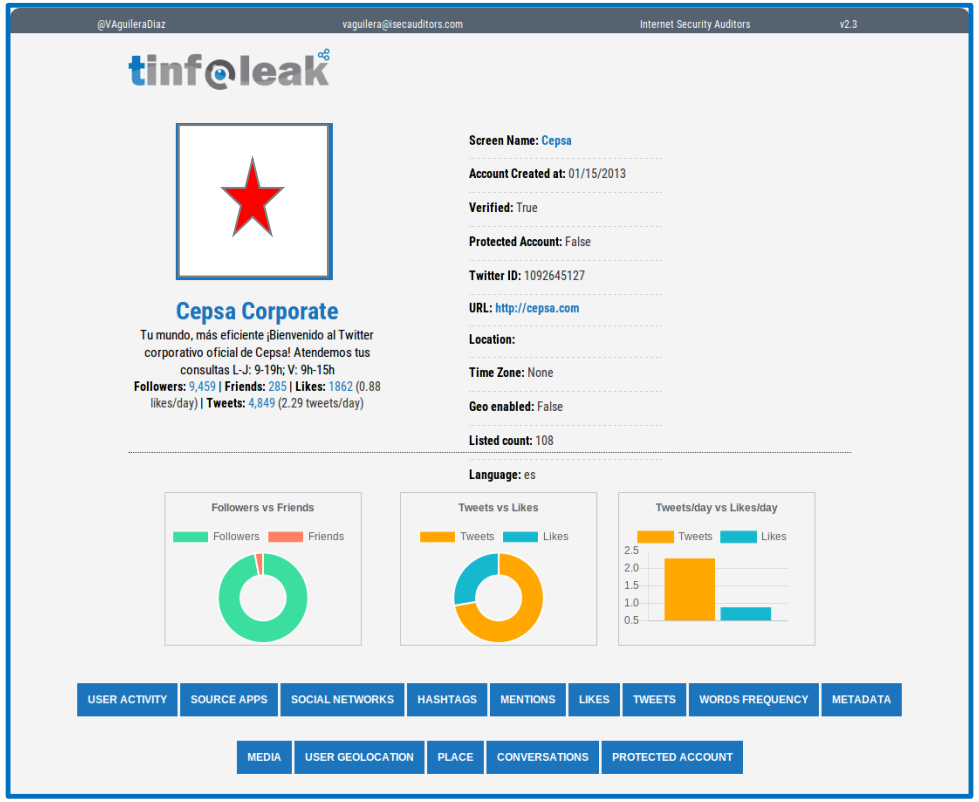
Añadir API keys a archivo de configuración de la herramienta: tinfoleak/tinfoleak.conf

Investigación Objetivo – Localizar y Analizar Perfil de Twitter

Comando:
sudo python tinfoleak/tinfoleak.py

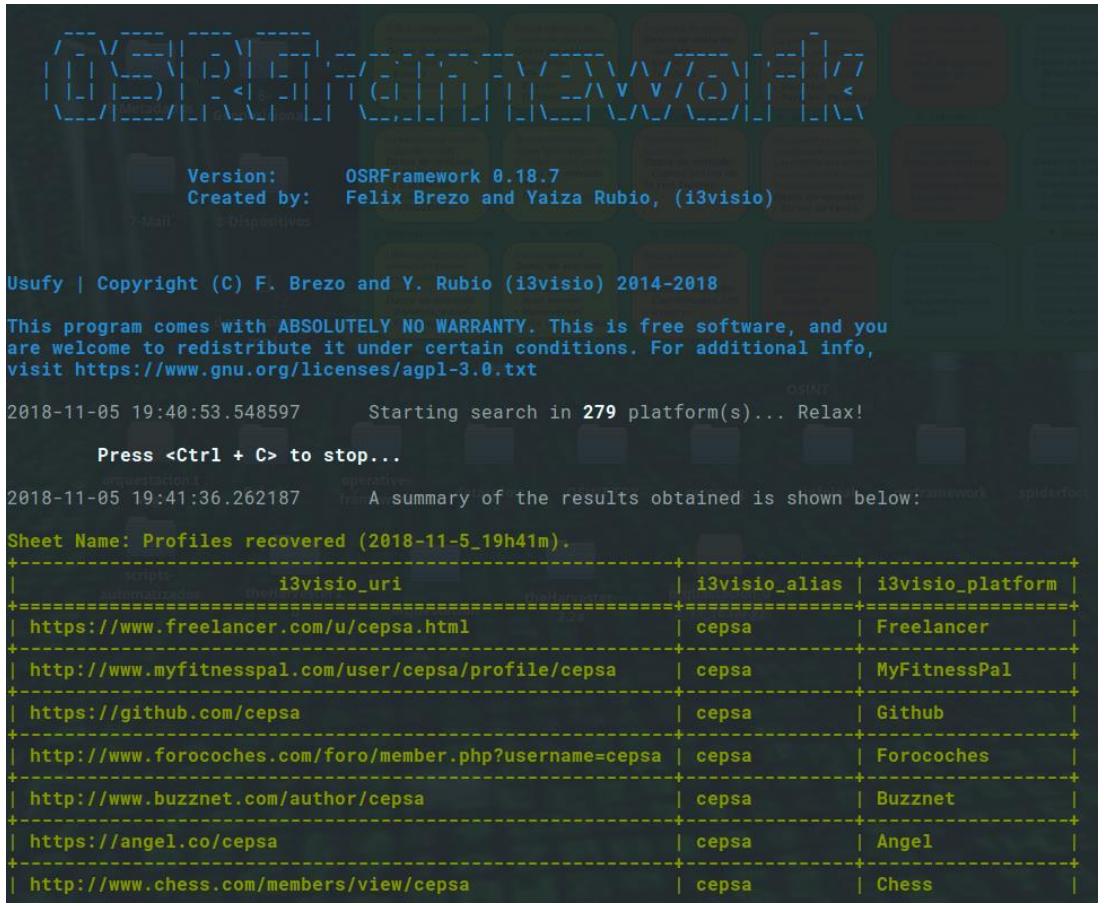


Informe:
tinfoleak/Output_Reports/tinfoleak.html



Investigación Objetivo – Localizar Perfiles de Usuarios

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



```
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

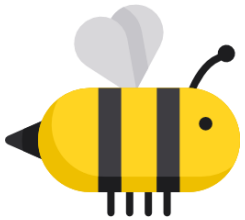
Módulo Searchfy > Permite verificar la existencia de perfiles en redes sociales a través del nombre completo de una persona.

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

Input: Email, Username, Teléfono, Nombre Persona

TLP:GREEN

Manos a la obra: ya lo tenemos claro, vamos a por resultados



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 orquestra 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 NEO4J

Orquestación de herramientas relacionando datos

Noviembre 2018 | HoneyCon 4ª edición

¿Por qué son importantes las relaciones?

Fuentes

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

+

Agregación de datos

Formatos para compartir información

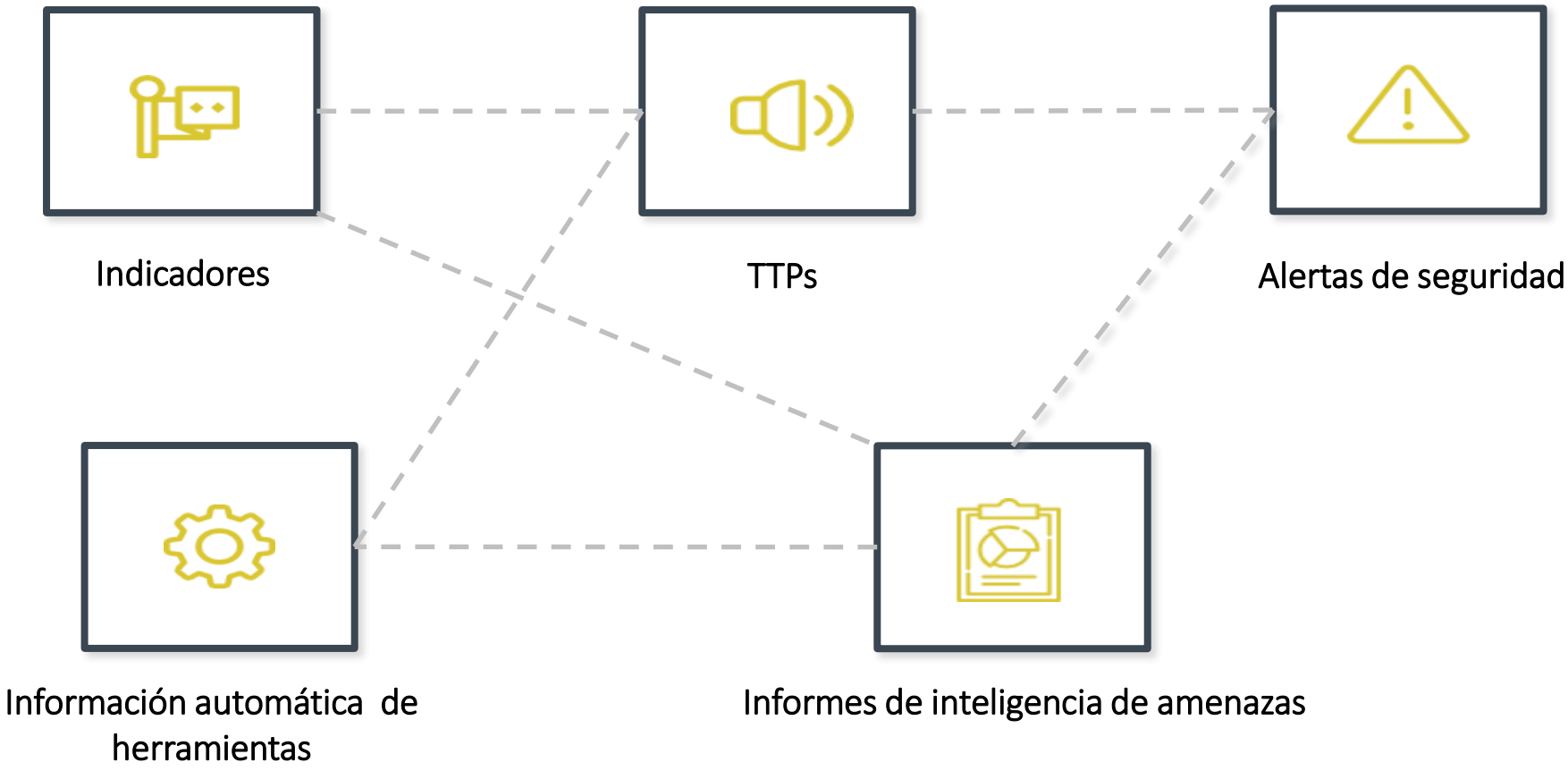
- Collective Intelligence Framework (CIF)
- Cyber Observable eXpression (CybOX)
- Incident Object Description and Exchange Format (IODEF)
- Open Indicators of Compromise (OpenIOC)
- Open Threat Exchange (OTX)
- Structured Threat Information Expression (STIX)
- Trusted Automated eXchange of Indicator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

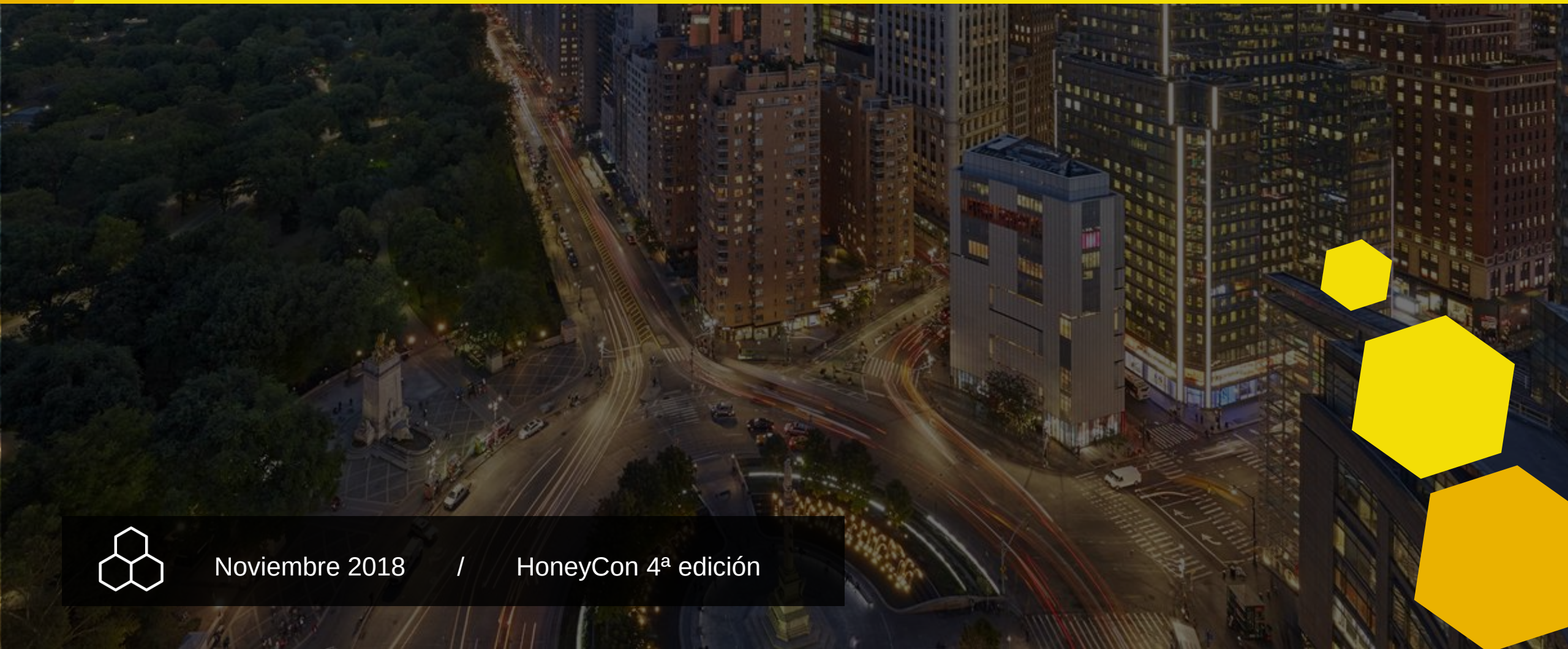
TLP:GREEN

¿Por qué son importantes las relaciones?

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

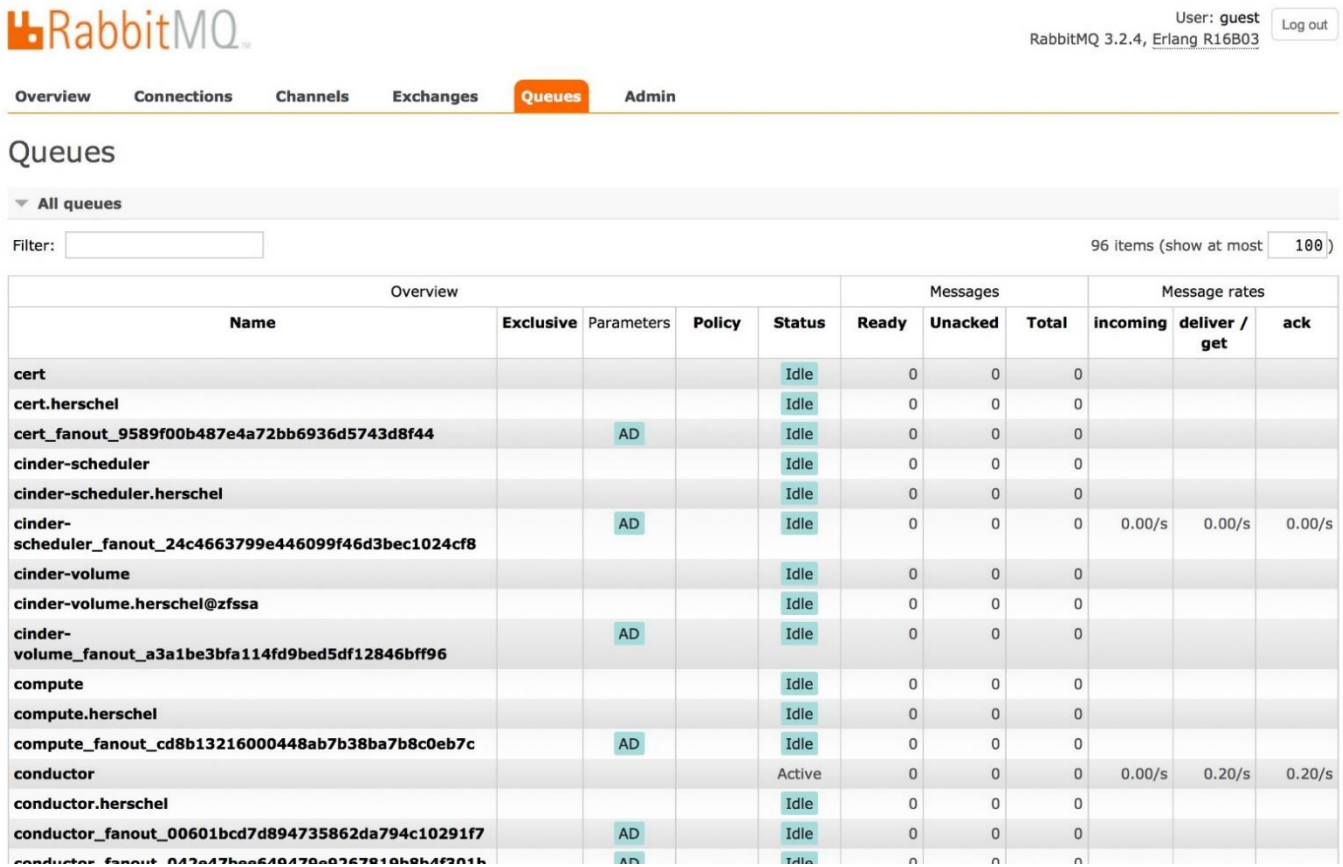
RabbitMQ

¿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



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			

Conociendo RabbitMQ

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

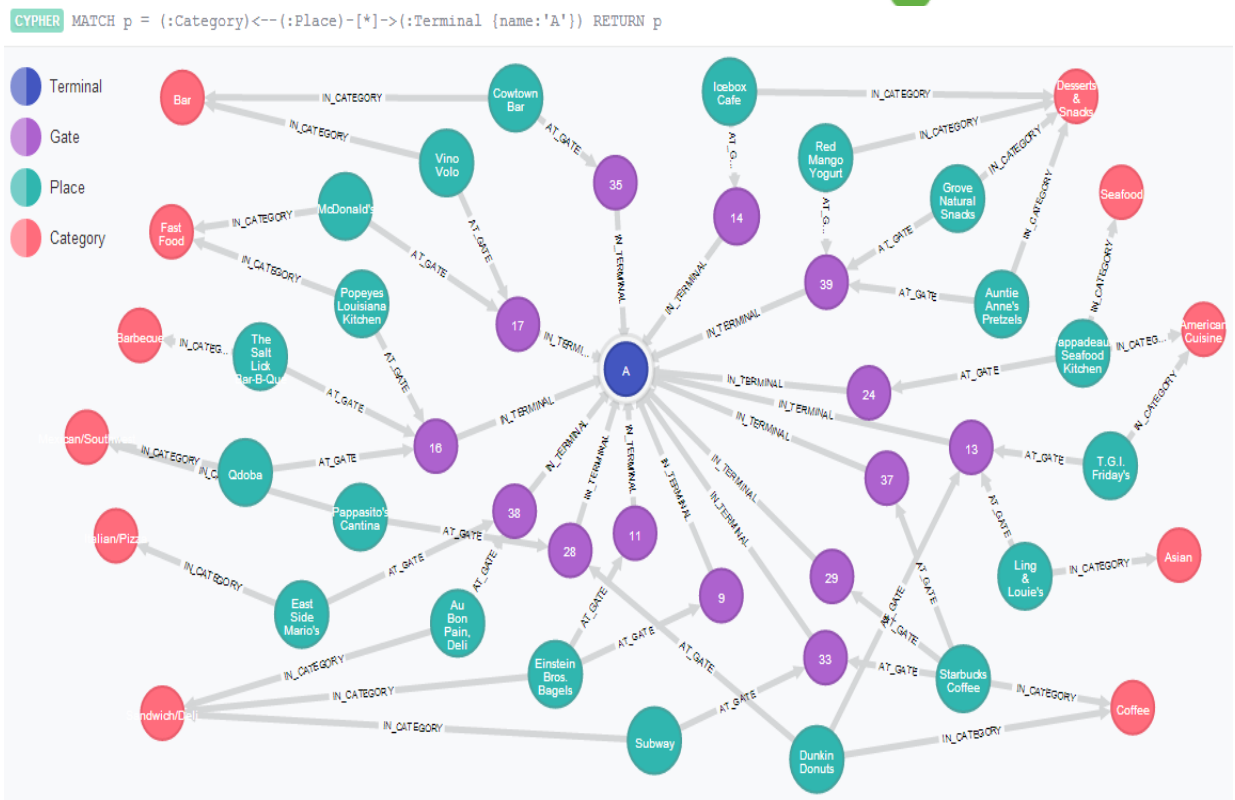
Conociendo NEO4J

¿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



Conociendo NEO4J

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

Orquestación de Herramientas relacionando datos

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
- Librerias para realizar peticiones a APIs
  - Requests
  - Urlib2

Modo Ejecución

Pasos a seguir

- Carpeta: /home/osintux/OSINT/orquestación
- Activar Virtualenv dentro de carpeta: source bin/actívate (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"

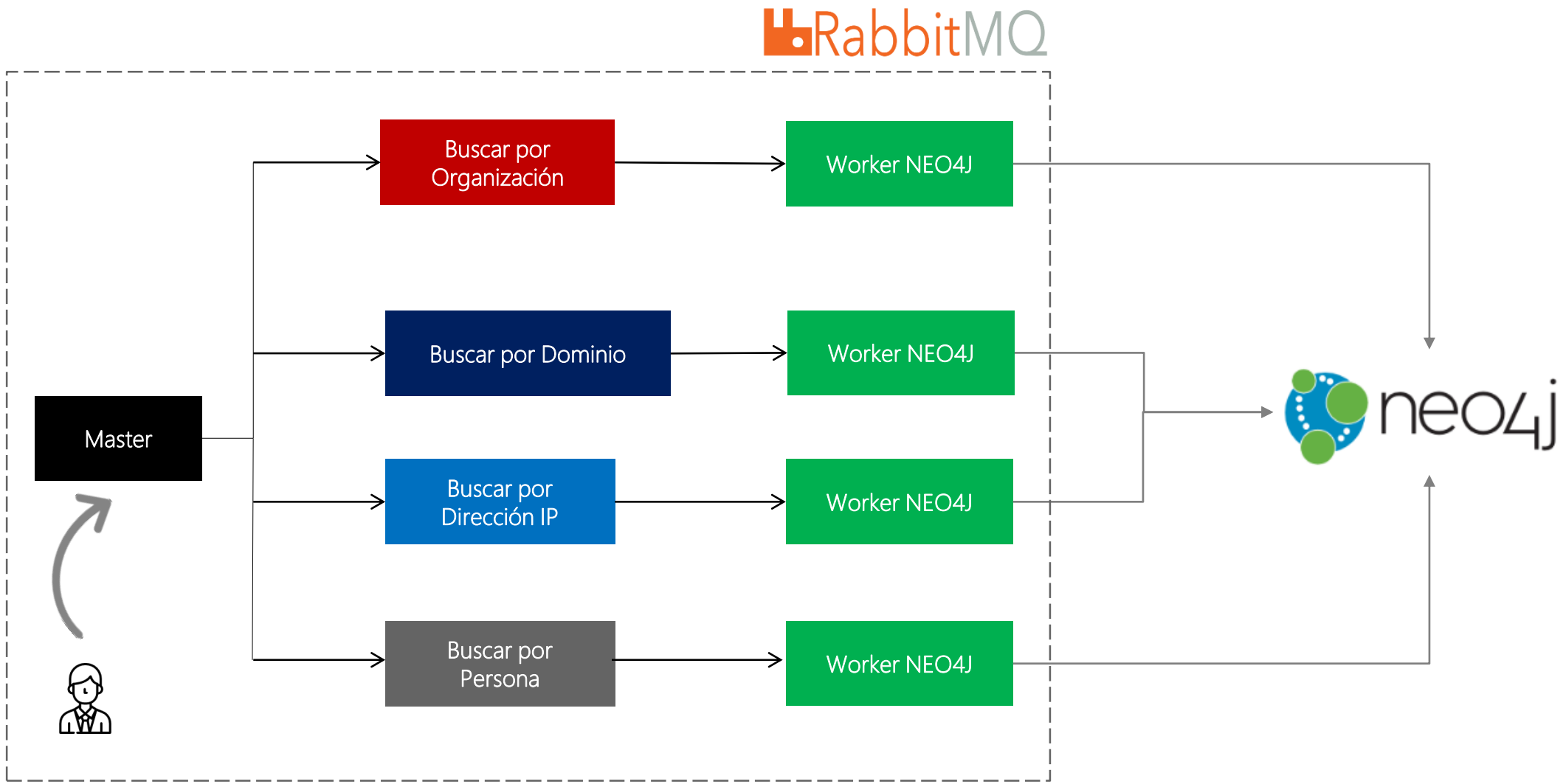
Eliminar colas existentes

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

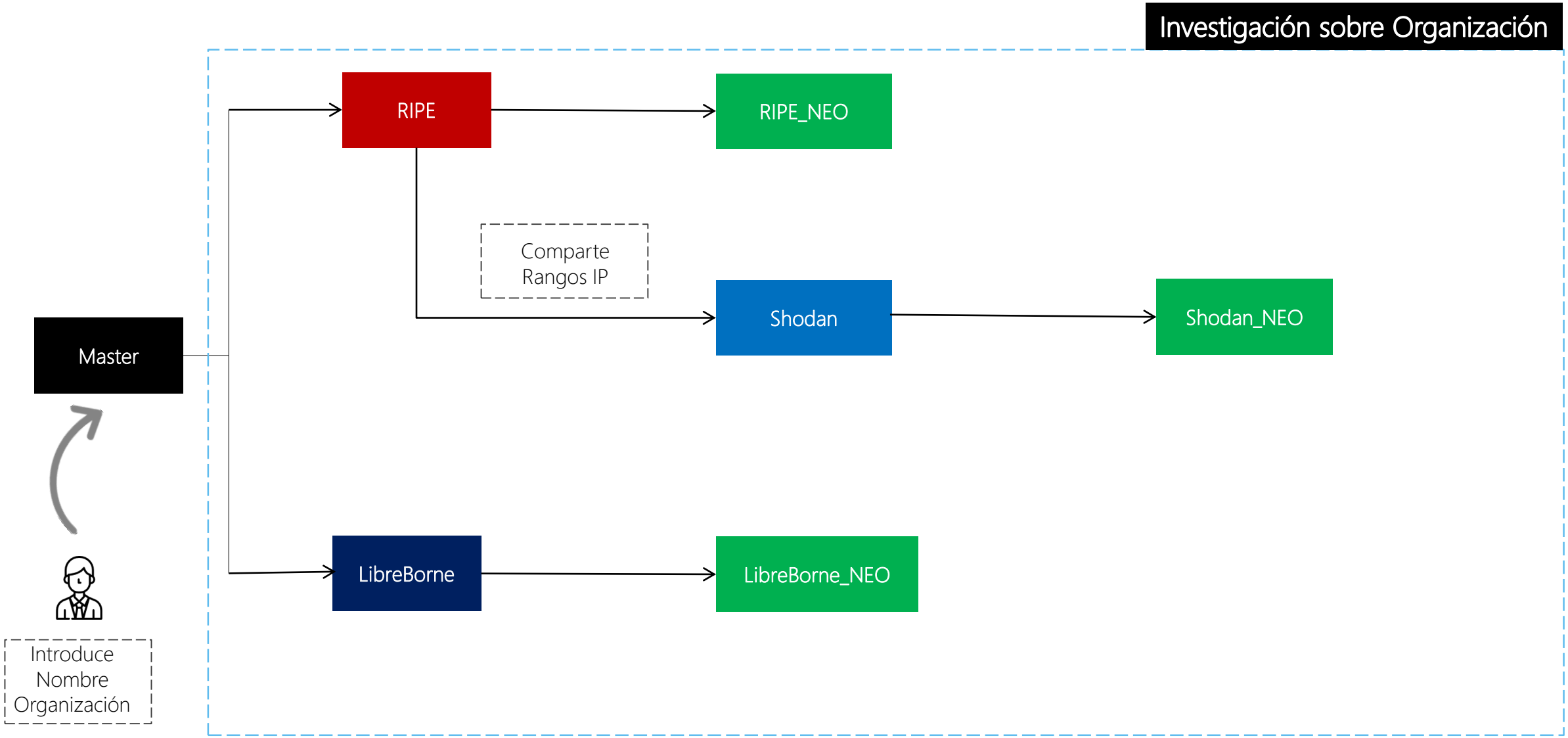
Ubicación Configuración APIs

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

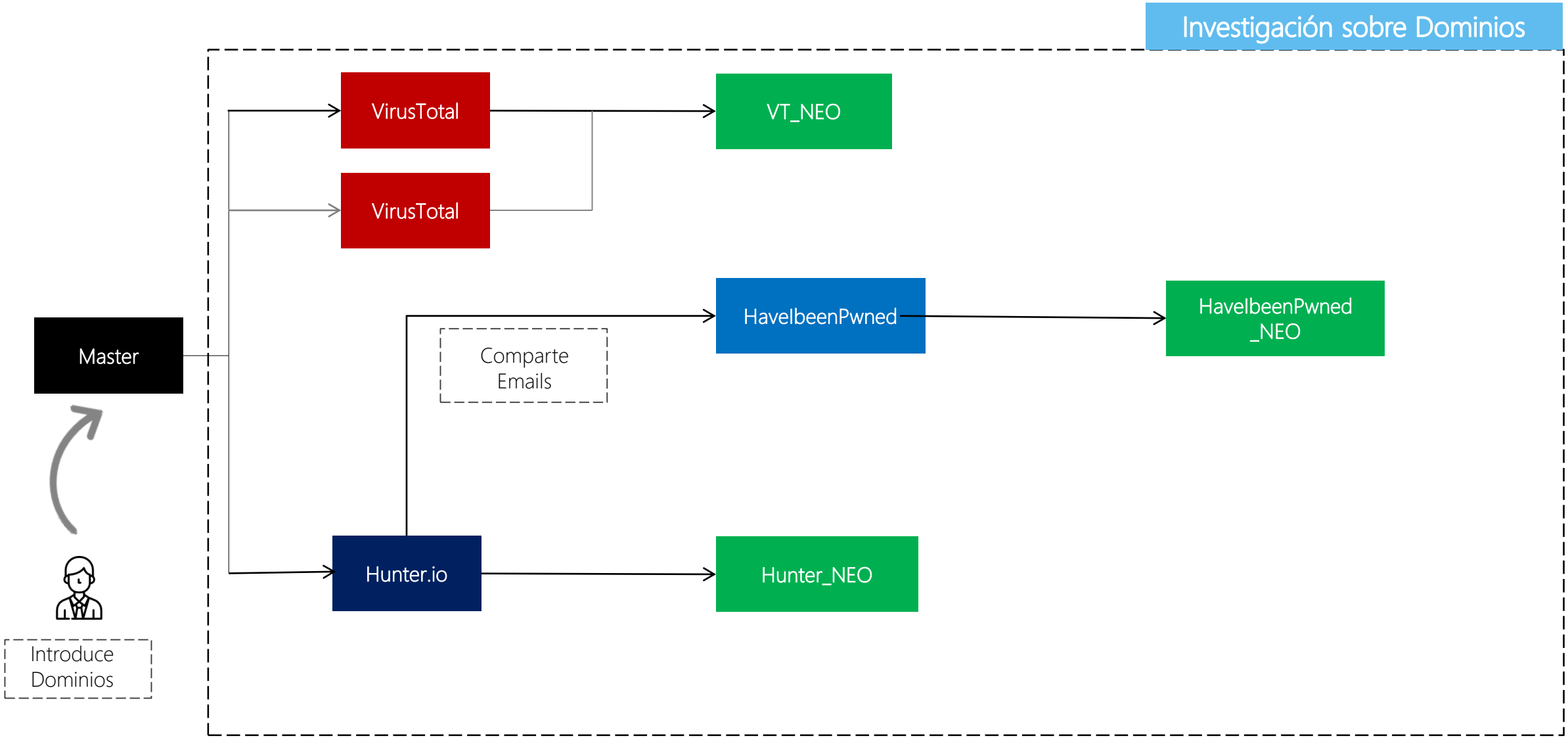
Orquestación de Herramientas relacionando datos – Mapa Global



Orquestación de Herramientas relacionando datos



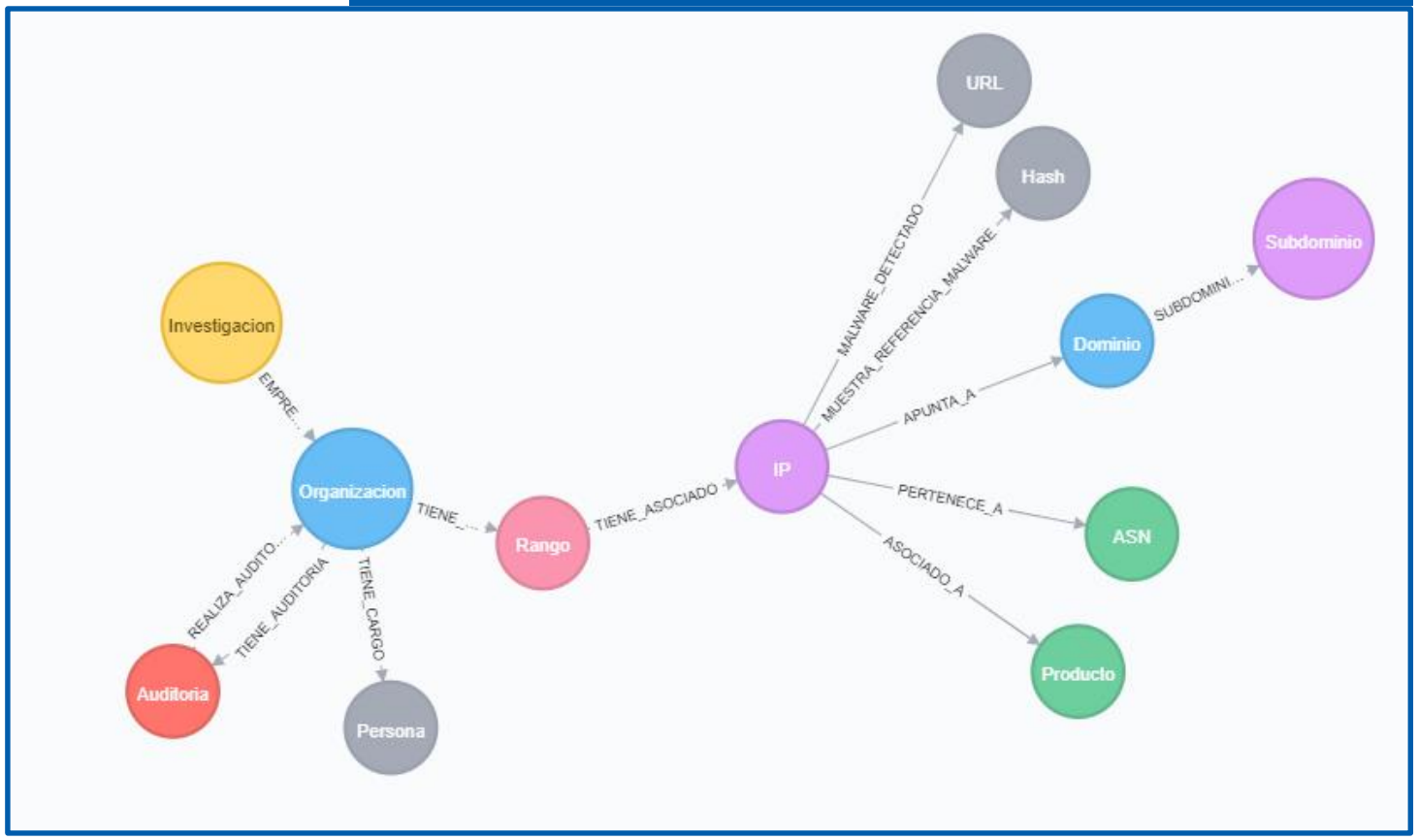
Orquestación de Herramientas relacionando datos



Comando NEO4J para grafo de Nodos y Relaciones:

call apoc.meta.graph

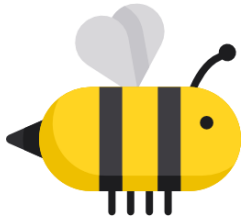
Mapa gráfico de bbdd de NEO4J



*(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)

Ya lo tenemos



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 curiosear, perdidas 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.

Ya lo tenemos

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.

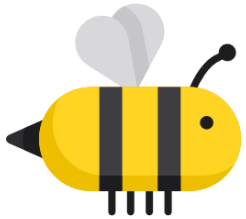
Diego

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.

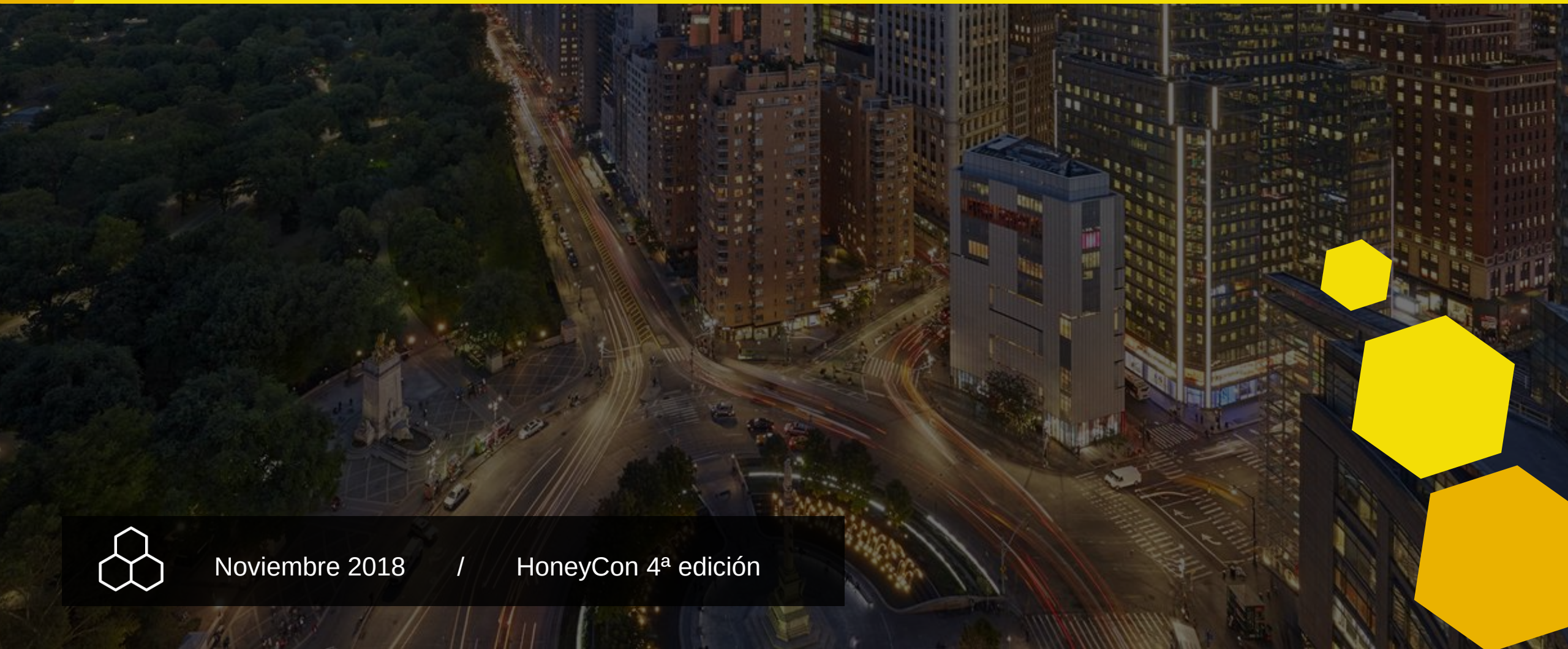
Conclusiones



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



Agradecimientos a:

Wiktor Nykiel | Cyber Intelligence & Security Senior Manager

#Creative and #innovative in #cyberintelligence.
IT enthusiast, ɹəɥɔɹɐǝsǝɹ ʎʇıɹnɔǝs, #entrepreneur.

wiktornykiel wiktornykiel

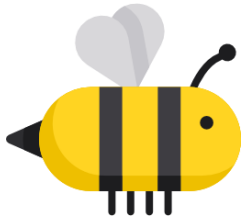
Gonzalo Espinosa | Cybersecurity Consultant

#Vulnerabilities #Incident&Response #Cyberintelligence

gonzaloespinosa

Recursos y referencias

Sigue investigando y aprendiendo



Bee You

Usa los recursos para educación

- 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

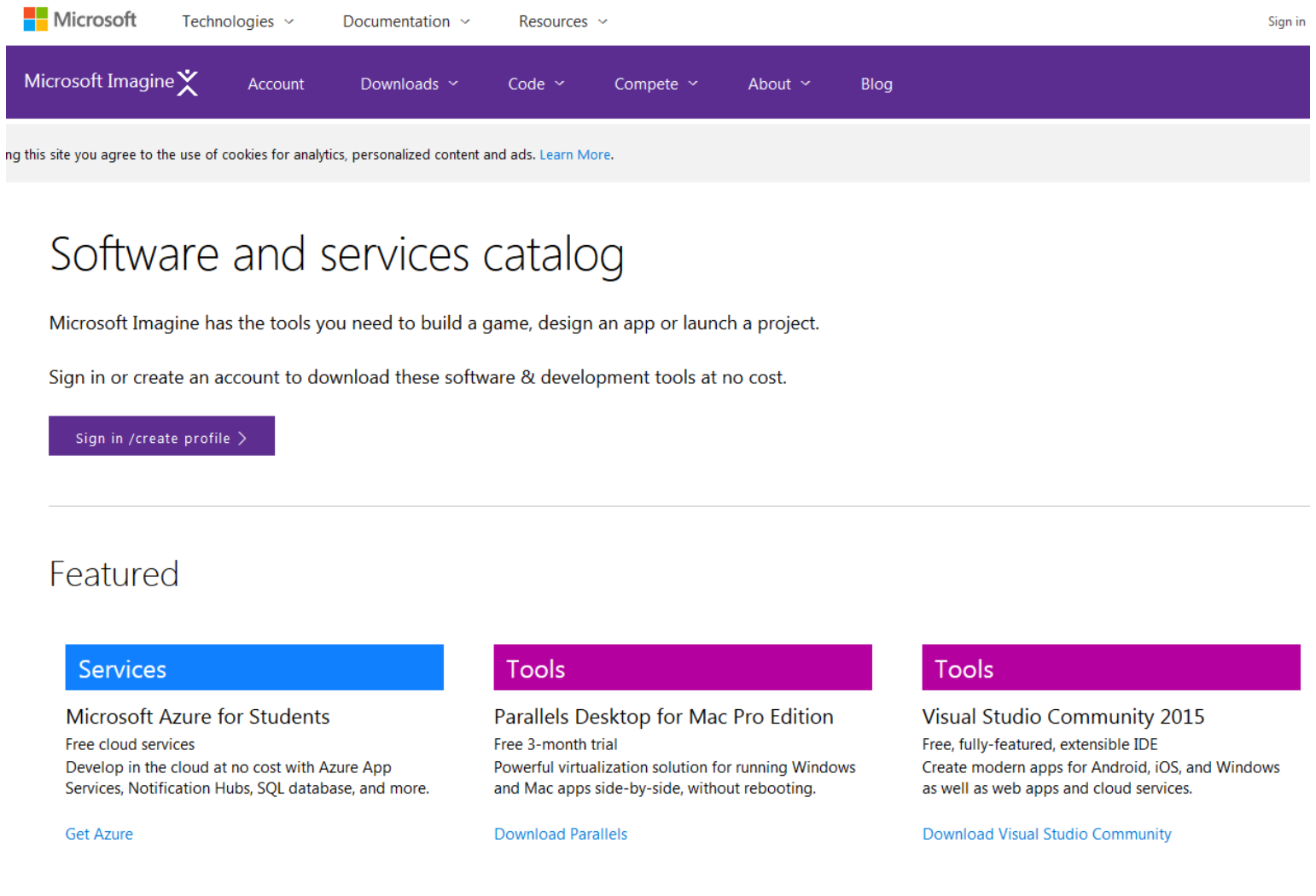
Recursos para estudiantes

https://education.github.com/pack

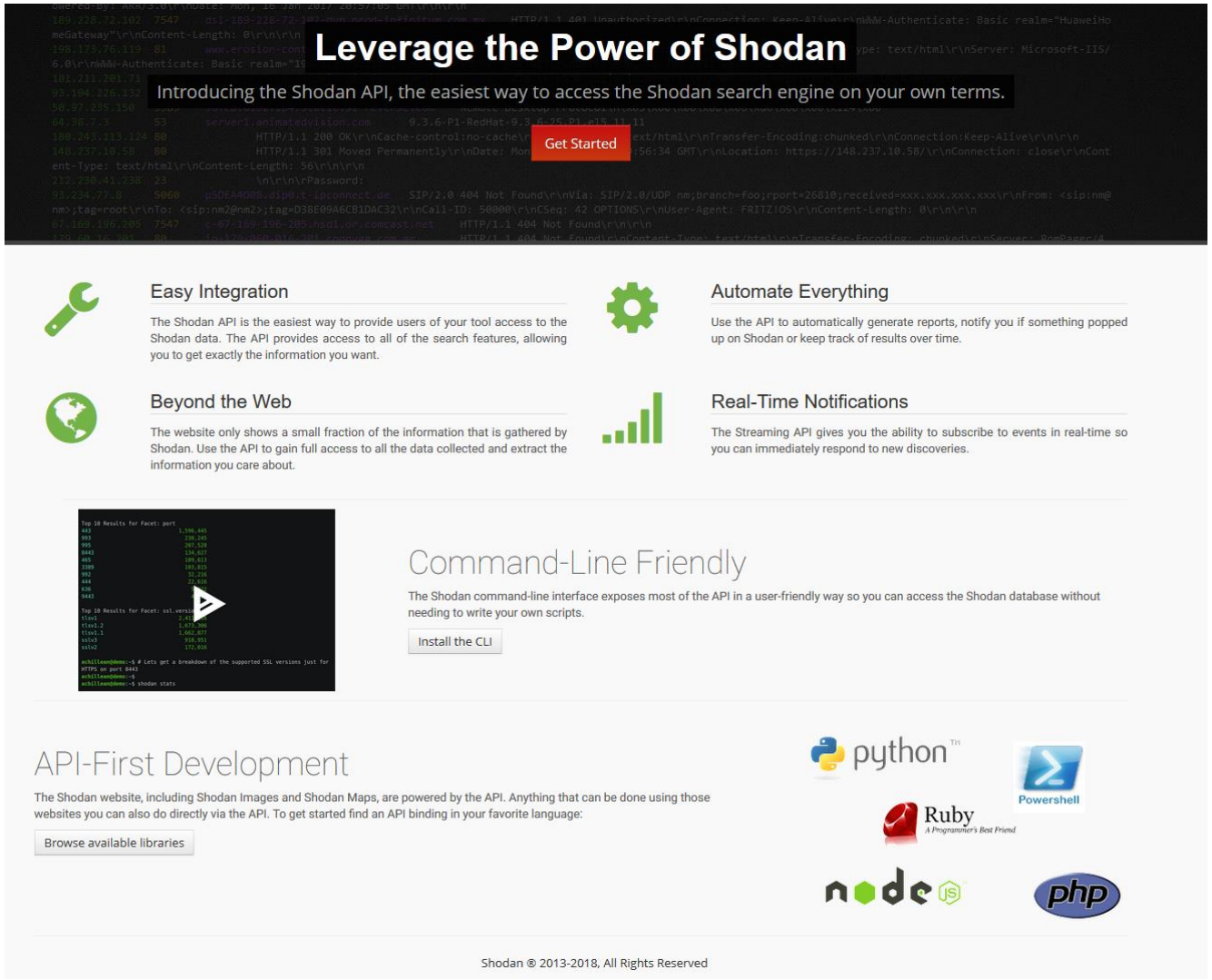
TLP:GREEN

Recursos para estudiantes

https://imagine.microsoft.com



Recursos para estudiantes



Referencias

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://hailataxii.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/cisoplatform7/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...

HoneyCON
By HoneySec

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