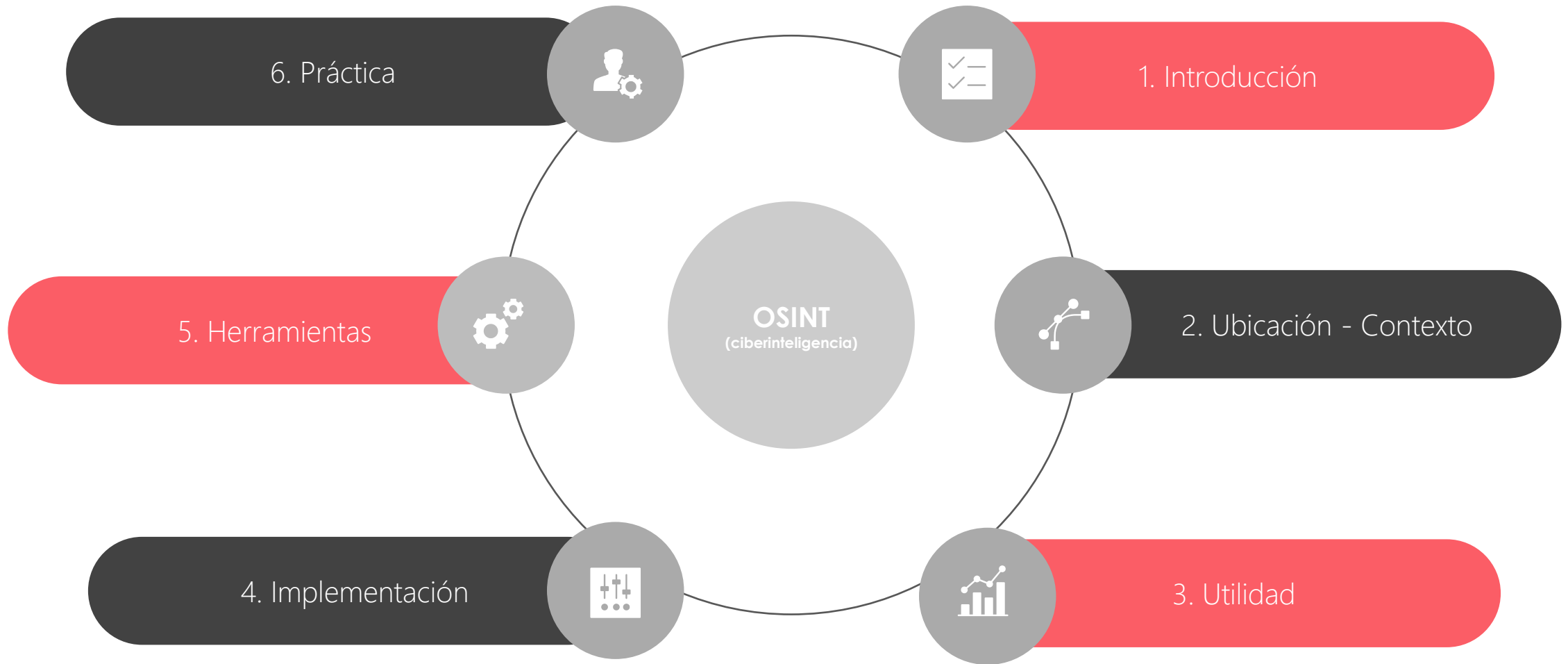


1. Recopilar información
2. Filtrar, procesar y analizar
3. Conocimiento útil

OSINT – (Ciber) Inteligencia

Conjunto de técnicas y herramientas que sirven para poder recopilar información pública acerca de nuestro objetivo: organismos, personas, páginas web, tendencias...

PLANTEAMIENTO



PLANTEAMIENTO

1. Introducción

- a) Aspectos generales
- b) Ciclo de la inteligencia
- c) Beneficios y retos del OSINT

2. Ubicación

En qué parte de la ciberseguridad se sitúa el profesional de la ciberinteligencia y el OSINT

3. Utilidad

Para qué sirve el OSINT y la ciberinteligencia

4. Implementación

- a) Securitización del entorno de trabajo
- b) Obtención de información – Objetivos

5. Herramientas

Según el objetivo

6. Práctica // exposición de resultados (informes)

Los ciberataques volverán a registrar en 2022 cifras récord

Ola de ciberataques a móviles con SMS que alertan de fallos de seguridad en cuentas bancarias

El ransomware es cada vez más sofisticado, con variantes como la doble extorsión y ataques más rápidos y dañinos

El 'phishing' y el 'malware' ponen en jaque a la empresa española a través de ataques DNS

► Ferrari sufre un ciberataque de ransomware y le roban 7GB de información privada

Alchemist, el nuevo 'framework' de ataque chino que apunta a Windows, Linux y macOS

BEC: AUMENTO DEL PHISHING CORPORATIVO

Fecha	Víctima	Grupo/Malware	Otros datos / tipo
03/01	EMCO.es	HiveLeaks	Ransomware
08/01	Amaveca Salud	Vice Society	Ransomware
17/01	Ayuntamiento de Getxo	Desconocido	Desconocido
19/01	IZO.es	LockBit 2.0	Ransomware
19/01	IB-Salut (Servicio de Salud de las Islas Baleares)	Desconocido	Desconocido
04/02	Castro Urdiales UTE	LockBit 2.0	Ransomware
26/02	Madrid Calle 30 S.A.	ALPHVM	Ransomware
21/03	OCA Global	Conti	Ransomware
24/03	Web Congreso Diputados	Desconocido	DDoS
25/03	Japauto S.L.	LockBit 2.0	Ransomware
31/03	grupodeincendios.com	LockBit 2.0	Ransomware
31/03	Iberdrola	Desconocido	Robo datos clientes

En 2020 se han producido casi a diario brechas de seguridad que han comprometido datos personales

Un ciberataque de origen ruso deja al CSIC sin conexión a internet durante dos semanas

La nueva realidad provocada por la COVID-19 centra el foco de las ciberamenazas

ASPECTOS
GENERALES

CICLO
INTELIGENCIA

1

La inteligencia de amenazas es el análisis de datos e información obtenida a través de la aplicación e implementación lógica y estructurada de herramientas y técnicas que generen patrones

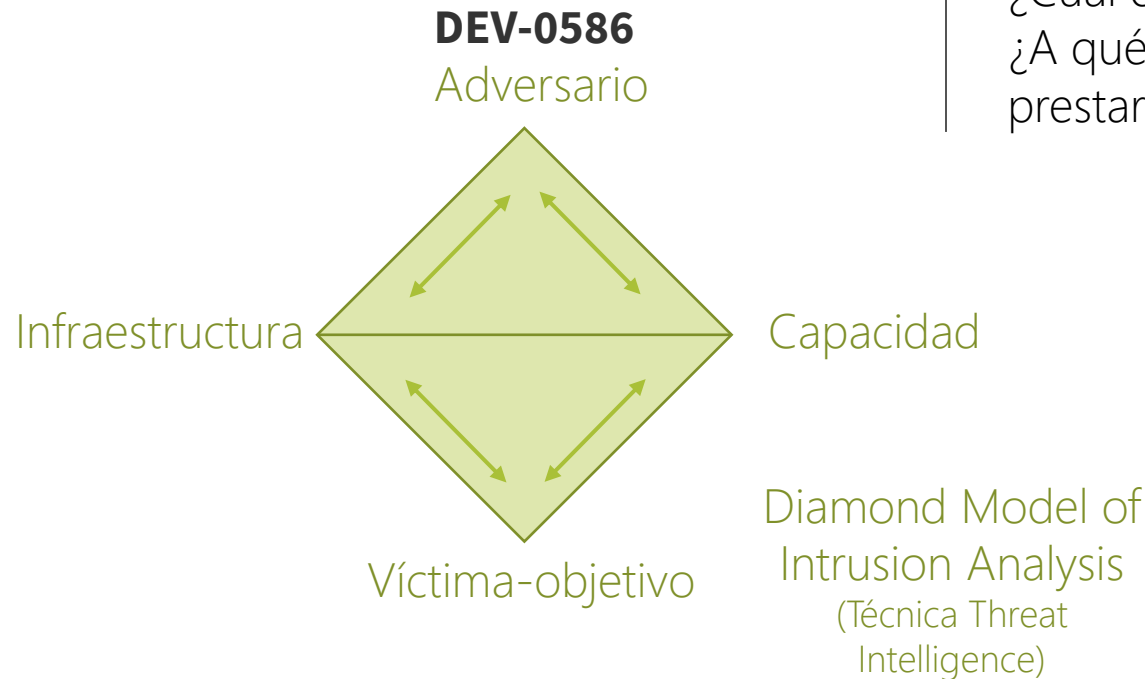
TLP:RED	Se debe utilizar TLP:RED cuando la información está limitada a personas concretas, y podría tener impacto en la privacidad, reputación u operaciones si es mal utilizada.	Los receptores no deben compartir información designada como TLP:RED con ningún tercero fuera del ámbito donde fue expuesta originalmente.
TLP:AMBER	Se debe utilizar TLP:AMBER cuando la información requiere ser distribuida de forma limitada, pero supone un riesgo para la privacidad, reputación u operaciones si es compartida fuera de la organización.	Los receptores pueden compartir información indicada como TLP:AMBER únicamente con miembros de su propia organización que necesitan conocerla, y con clientes, proveedores o asociados que deban estar al tanto para protegerse a sí mismos o evitar daños. El emisor puede especificar restricciones adicionales para compartir esta información. Nota: se debe especificar TLP:AMBER+STRICT , si la fuente desea restringir la compartición sólo a la propia organización.
TLP:GREEN	Se debe utilizar TLP:GREEN cuando la información es útil para todas las organizaciones que participan, así como con terceros de la comunidad o el sector.	Los receptores pueden compartir la información indicada como TLP:GREEN con organizaciones afiliadas o miembros del mismo sector, pero nunca a través de canales públicos.
TLP:CLEAR	Se debe utilizar TLP:CLEAR cuando la información no supone ningún riesgo de mal uso, dentro de las reglas y procedimientos establecidos para su difusión pública.	La información TLP:CLEAR puede ser distribuida sin restricciones, sujeta a controles de Copyright.

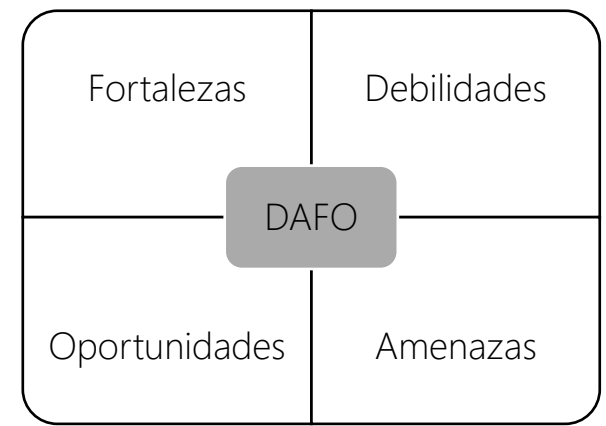
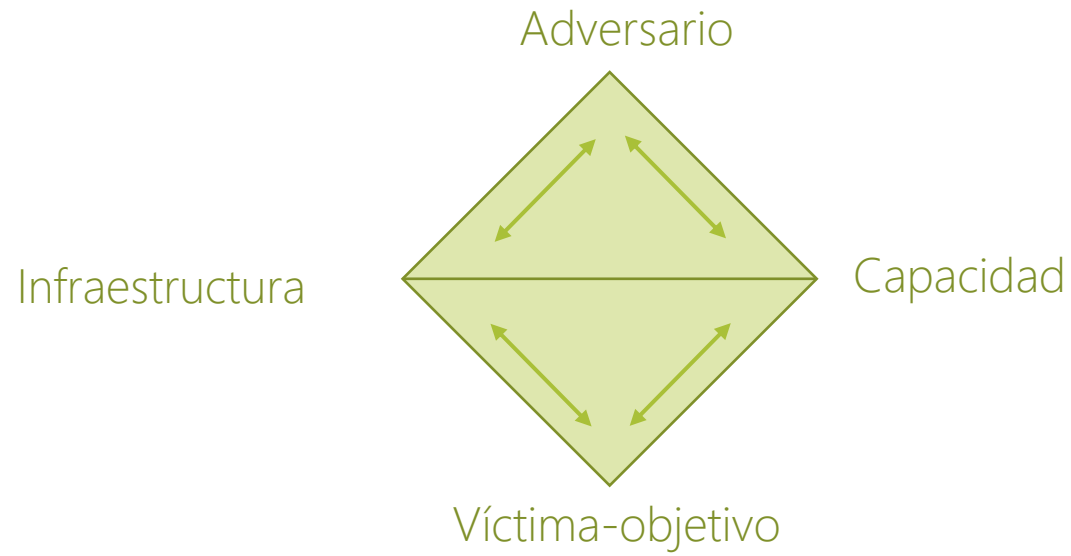
Preguntas de investigación:

- ¿Quién te ataca?
- ¿Cuál es su **motivación**?
- ¿Cuáles son sus **capacidades**?
- ¿Cuál es su **infraestructura**?
- ¿A qué signos e indicadores de compromiso (IoC's) debes prestar atención?

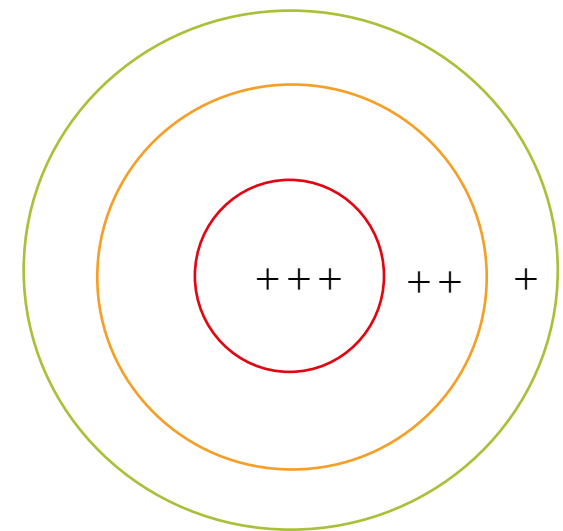
2

Ejemplo de
una técnica de
análisis de
inteligencia





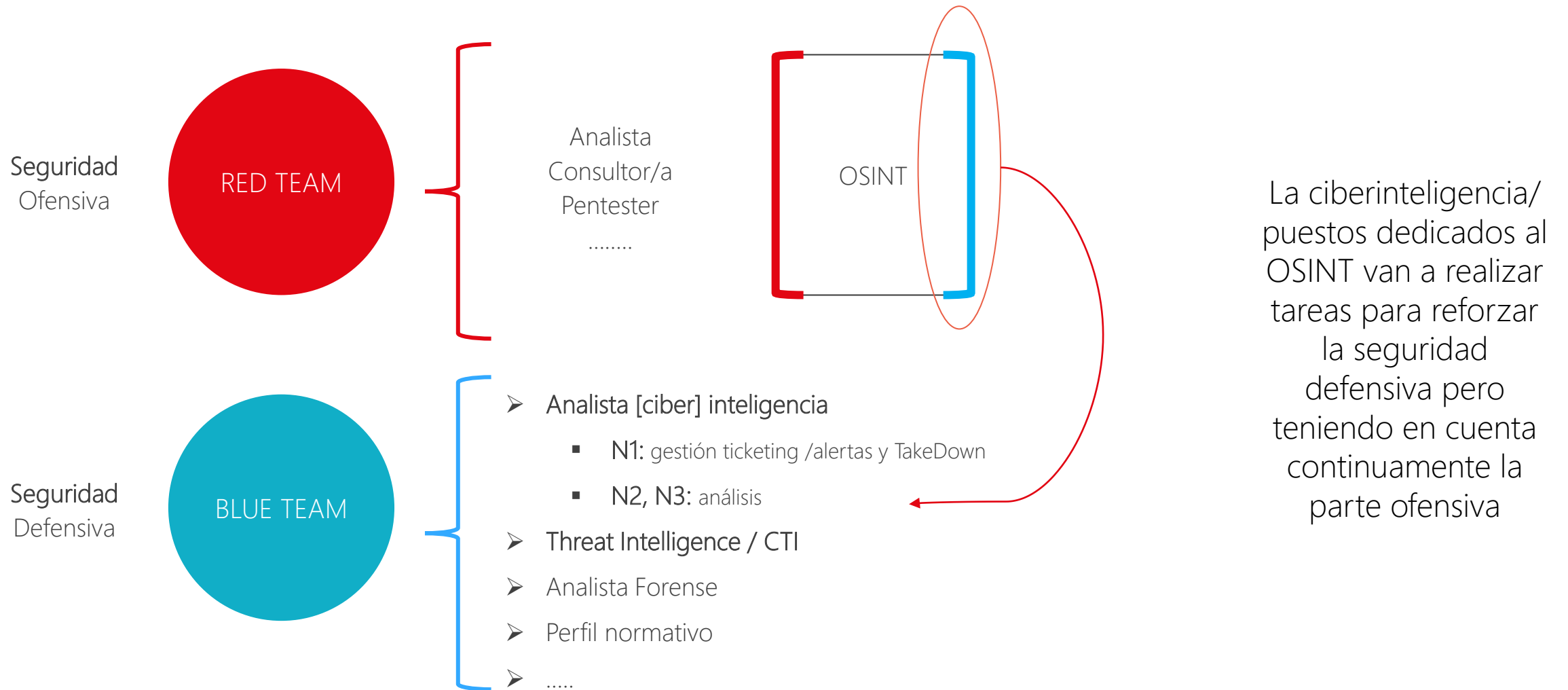
Variable	Definición	Tendencias actuales	Tendencias pasadas	Interrupción actividad



1. Fuentes de pago o sin disponibilidad → pivotar, demos, versiones gratuitas. Búsqueda activa de nuevos recursos, retroalimentación de fuentes. En muchas empresas, esta debilidad se contrarresta con la creación de automatismos propios que no dependan de herramientas de pago o desactualizadas
2. Acostumbrarse al baneado de las fuentes → creación de varias cuentas en mismos sitios
3. Desinformación → categorización de fuentes fiables
4. Falsos positivos de herramientas automáticas → filtrar la información
5. Límites legales → anonimato. Investigaciones sobre información pasiva. Protección de datos

UBICACIÓN

Mapa Cyber (desde una perspectiva de la empleabilidad)



UTILIDAD

Reconocimiento de un pentesting

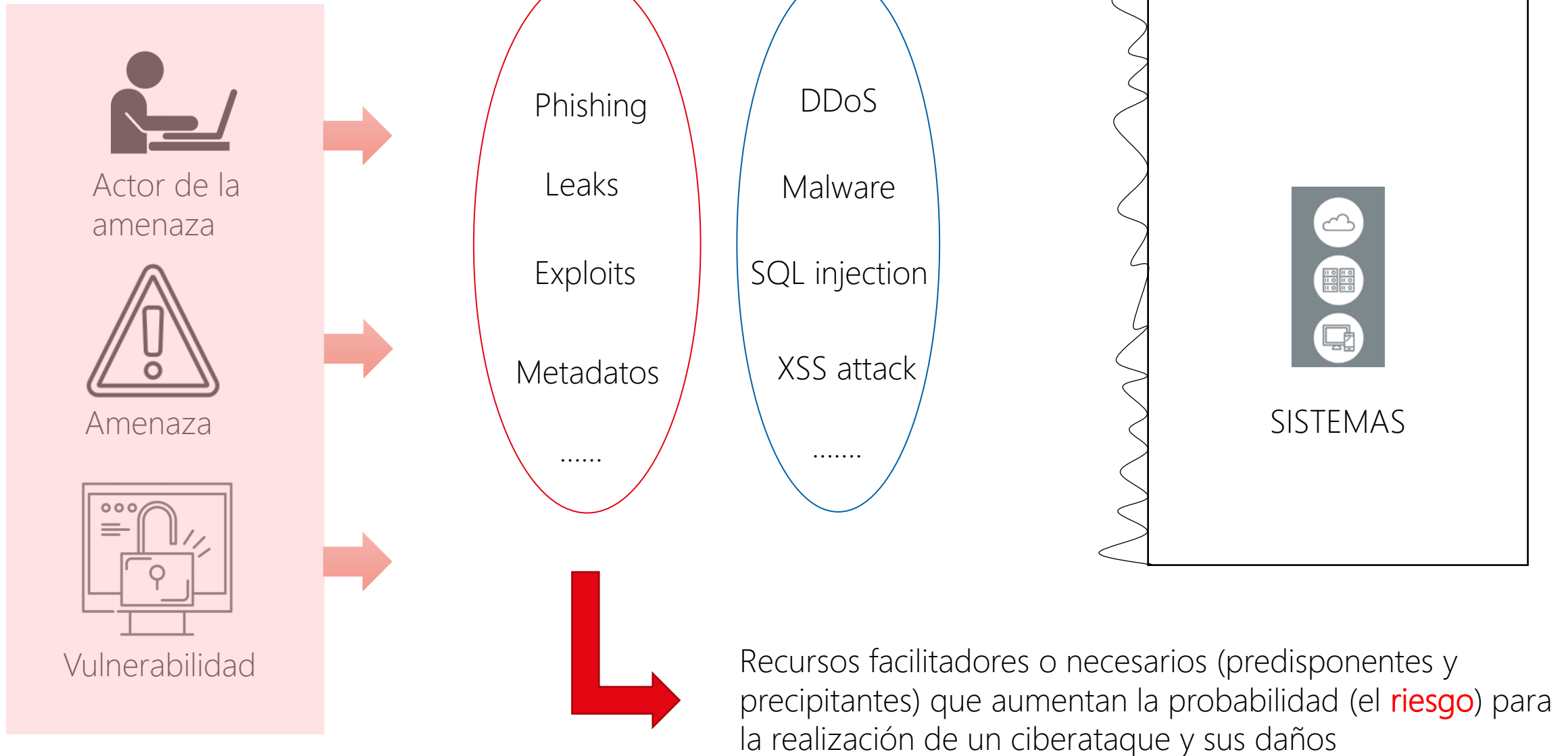
Inteligencia de amenazas → existencia de un sistema de monitorización continua y lógica que busque una DETECCIÓN, una ANTICIPACIÓN y una PREVENCIÓN sobre los Riesgos y Amenazas a los que una entidad/ institución está expuesta.

DETECCIÓN






ANTICIPACIÓN

PREVENCIÓN

UTILIDAD



• Securización Entorno de trabajo •

- Para la monitorización en redes sociales → creación de avatares/identidades anónimos
- Para securizar los dispositivos y las conexiones → máquinas virtuales y VPN 
- Uso de carpetas y emails cifradas (*Kleopatra*)  **Kleopatra** Crypto Manager e incluso cifrado de disco (*Veracrypt*) 
- Gestor de contraseñas (*Keepass*) 
- Comprobar todos los archivos antes de proceder a su descarga  **VIRUSTOTAL**
- Desactivar JavaScript en Tor → para que no se ejecuten scripts al acceder a ciertas webs
- Utilizar **DuckDuckGo** en TOR
- Borrar los metadatos de los archivos que se difunden
- Estructuración del entorno de trabajo (metodológico) → no perder información

OBJETIVOS

Monitorización / investigación

Actividad dañina en internet con posible impacto para los clientes

Búsqueda manual y automatizada en feeds públicos y privados sobre actividades ilícitas en la red. **Ejemplo:** leaks, amenazas dirigidas...

Detección e investigación

Investigación y valoración de riesgos sobre las alertas y eventos detectados

Reporte

Notificación de eventos de alta criticidad.
Redacción periódica de informes con la actividad registrada.
Inteligencia de amenazas.

Registro

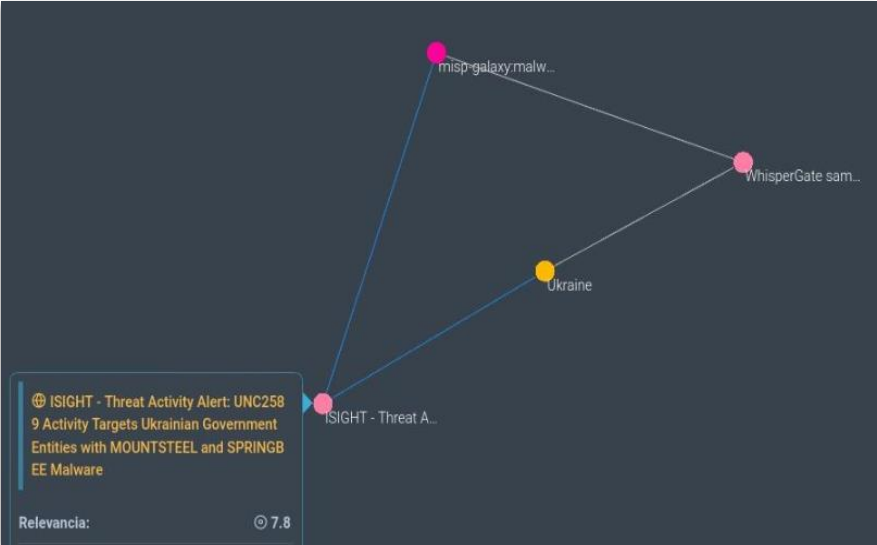
Filtro, categorización y descripción de la actividad (ciberseguridad) de los clientes



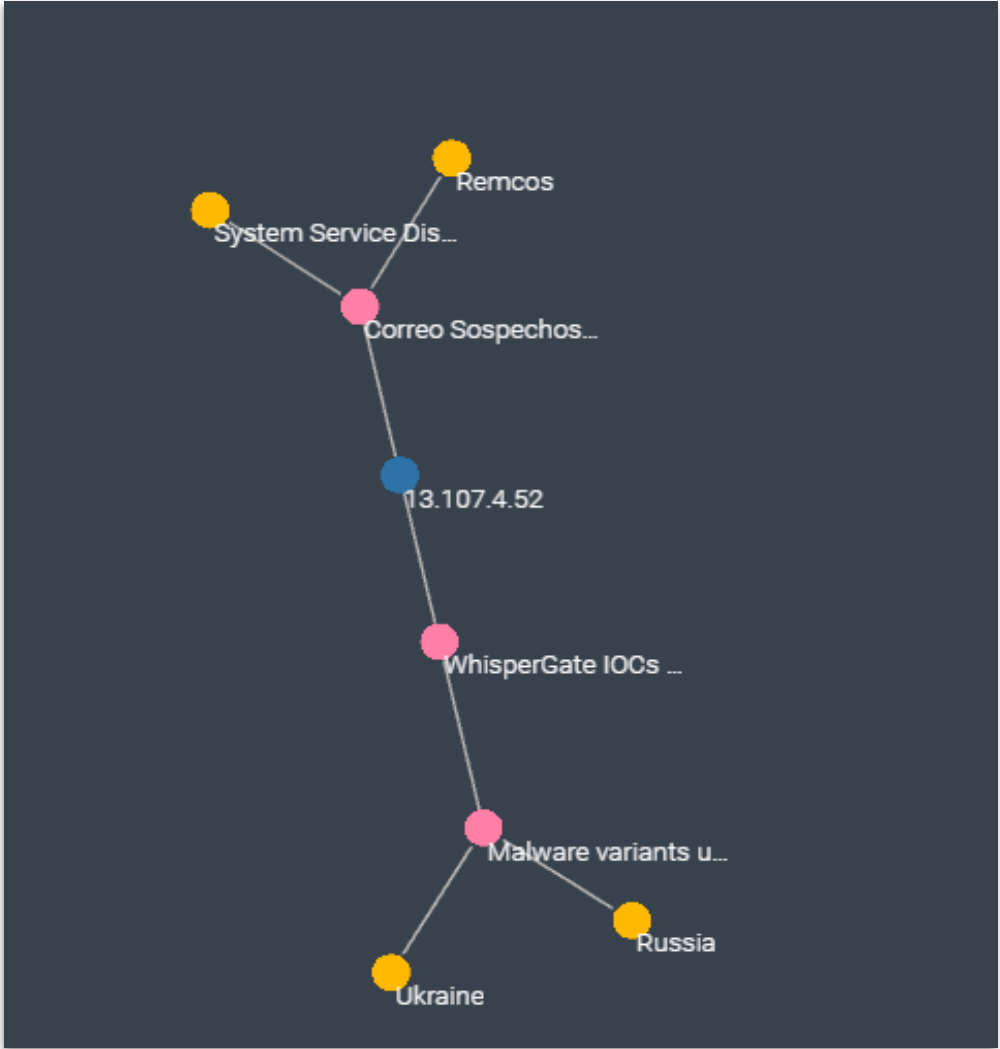
Gestión y Resolución

Eliminación de contenidos fraudulentos

Distintos IOCs asociados a **HavanaCrypt** contactan con la dirección IP **13.107.4.52**, que a su vez fue catalogada como parte de la infraestructura de varias campañas de ciberataques asociadas a las familias de malware *Remcos* y *WhisperGate*.

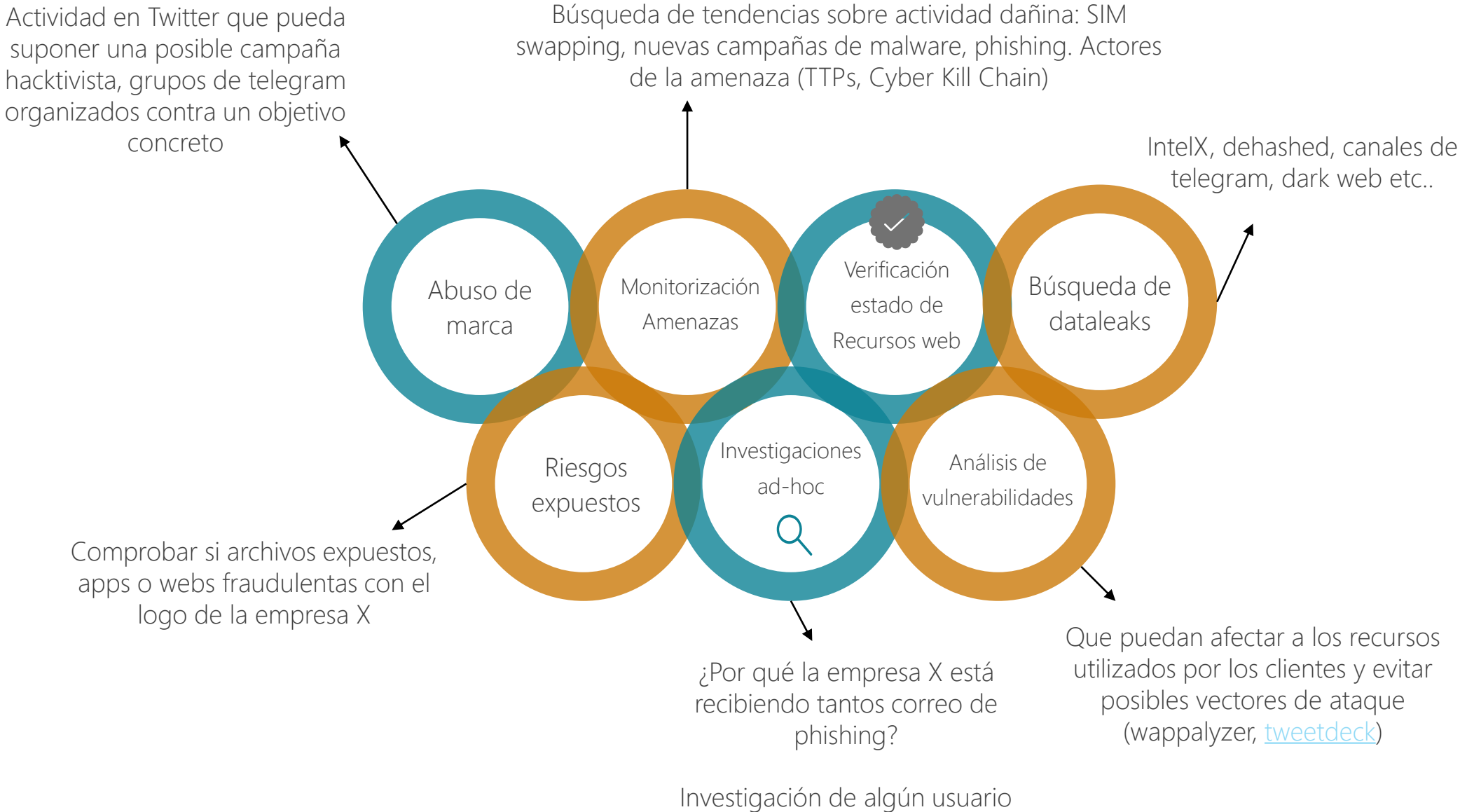


b37761715d5a2405a3fa75abccaf6bb15b7298673aaad91a158725be3c518a87			
Domain	Detections	Created	Registrar
www.microsoft.com	0 / 94	1991-05-02	MarkMonitor Inc.
Contacted IP Addresses ⓘ			
IP	Detections	Autonomous System	Country
104.97.41.163	0 / 94	16625	US
13.107.4.52	6 / 94	8068	US
20.227.128.33	5 / 94	8075	AU
20.99.132.105	0 / 94	8075	US
23.216.147.64	0 / 94	20940	US
23.216.147.76	0 / 94	20940	US



Ejemplo Caso MISP

OBJETIVOS



Según objetivo

Búsquedas manuales:

- Google dorks
- Búsqueda Surface Web (utilizando diferentes motores de búsqueda)
- Archive.org

Búsquedas RRSS:

- Twitter
- Telegram
- Facebook
- Pinterest
- WeChat
- TamTamMessenger
- Tik Tok
- Rocket.chat
- Element
- MINDS
- HoopMessenger

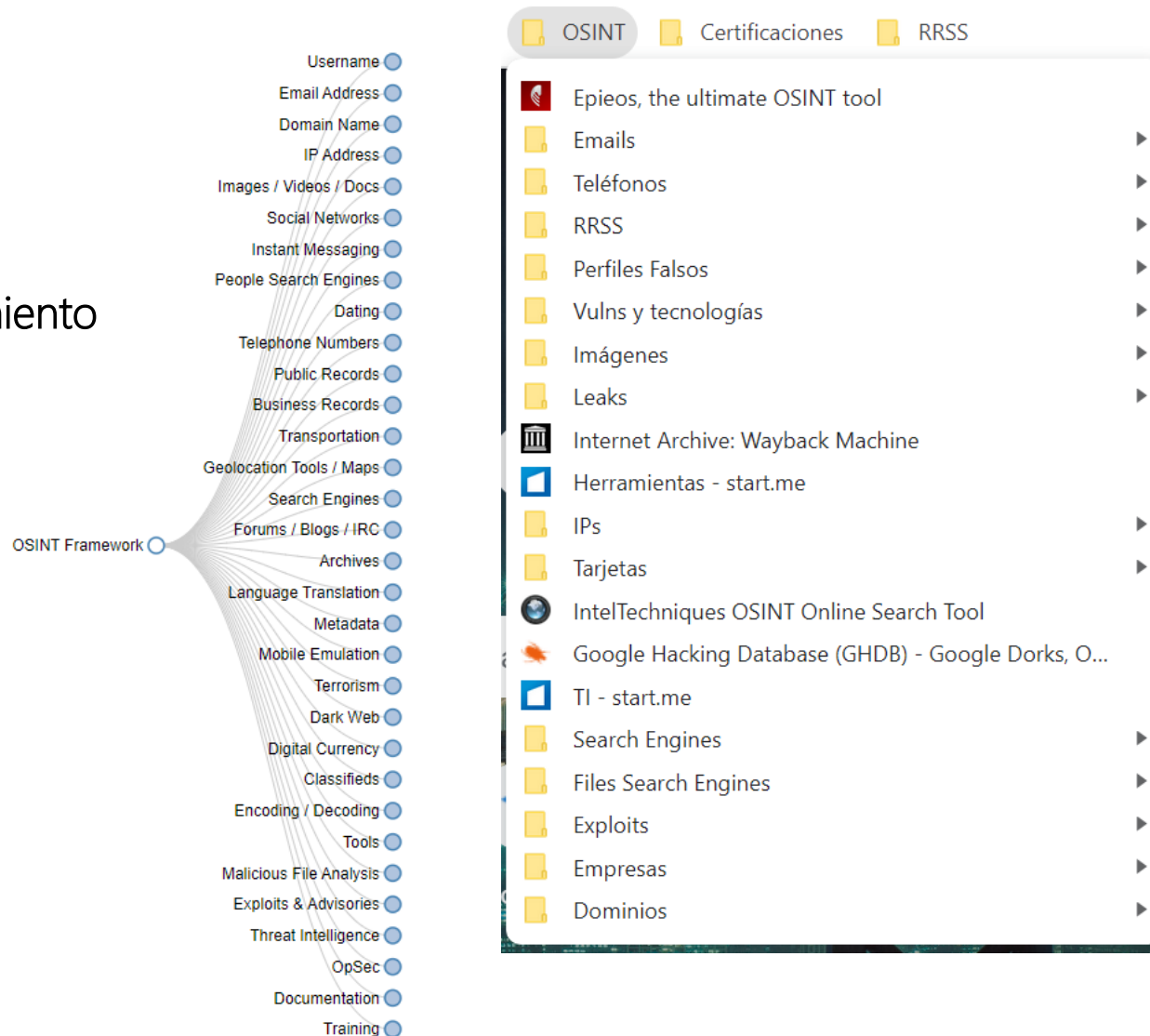
Dark Web

- TOR (hidden wiki)

Páginas de almacenamiento de archivos

- Justpasteit
- Pastebin
- Siasky.net
- Pixeldrain
- Top4top.io
- Mediafire
- Gofile
- Telegraph
- Files.fm

Herramientas:



PHOTON

web crawler

(Búsqueda de info en páginas web)

1. git clone <https://github.com/s0md3v/Photon.git>
2. pip install -r requirements.txt
3. python3 photon.py -u <https://www.thebridge.tech/> -l 3 -t 100 --wayback

} Install

```
(kali㉿kali)-[~/Tools/Photon]
$ python3 photon.py -u https://www.thebridge.tech/ -l 3 -t 100 --wayback
```



```
[~] Fetching URLs from archive.org
[+] Retrieved -1 URLs from archive.org
[+] URLs retrieved from sitemap.xml: 396
[~] Level 1: 397 URLs
[!] Progress: 397/397
[~] Level 2: 32 URLs
[!] Progress: 32/32
[~] Level 3: 30 URLs
[!] Progress: 30/30
[~] Crawling 1 JavaScript files
[!] Progress: 1/1

[+] Intel: 28
[+] Internal: 482
[+] Scripts: 1
[+] External: 3
[+] Endpoints: 100

[!] Total requests made: 460
[!] Total time taken: 0 minutes 16 seconds
[!] Requests per second: 27
[+] Results saved in www.thebridge.tech directory
```

Guía de uso:

<https://github.com/s0md3v/Photon/wiki/Usage>

La info extraída se reporta en los siguientes campos:

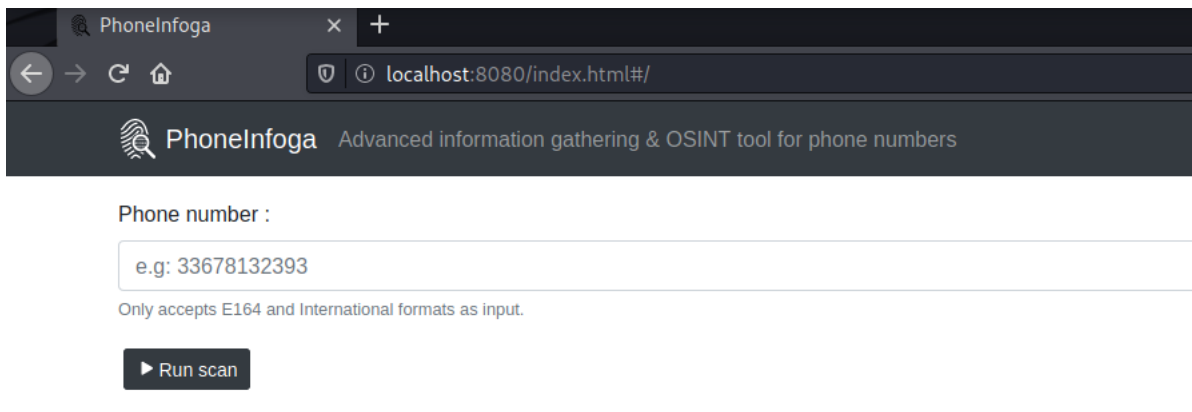
Files	Scripts
Intel	External
Robots	Fuzzable
Custom	Endpoints
Failed	keys
Internal	

Puede extraer la siguiente info:

- URL's con parámetros susceptibles de aplicar fuzzing
- Ficheros: PDF, XML, PNG, ...
- Scripts
- Enlaces

Phoneinfoga

1. `curl -L "https://github.com/sundowndev/phoneinfoga/releases/download/v2.0.8/phoneinfoga_$(uname -s)_$(uname -m).tar.gz" -o phoneinfoga.tar.gz`
2. `tar xfv phoneinfoga.tar.gz`
3. `./phoneinfoga --help`
4. `phoneinfoga serve -p 8080`
5. `localhost:8080`



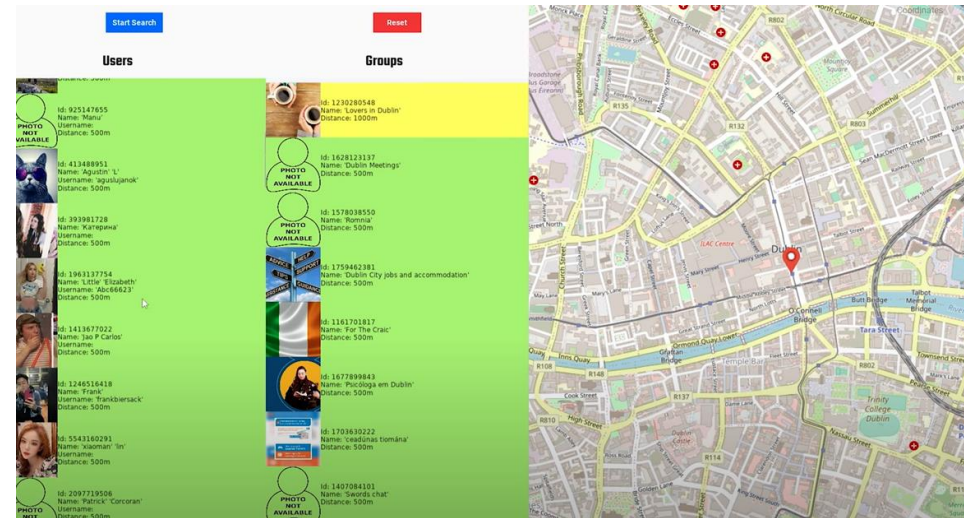
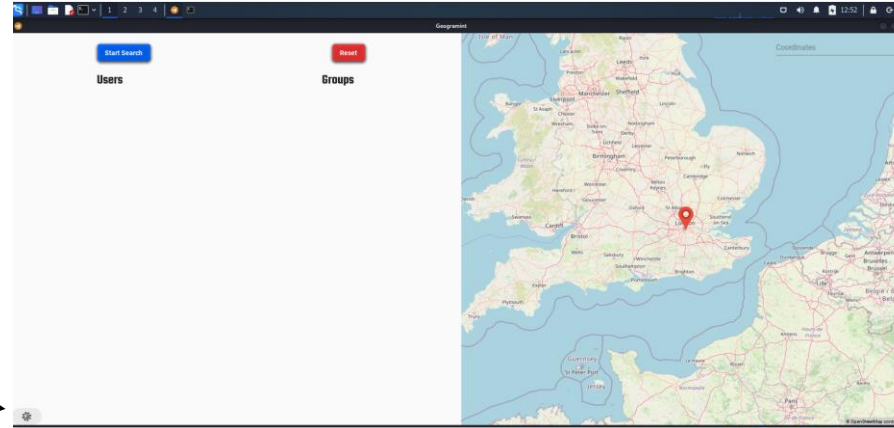
Búsqueda en terminal

```
(kali㉿kali)-[~/Tools]
└─$ phoneinfoga scan -n "+33 06 79368229"
[i] Scanning phone number +33 06 79368229
[i] Running local scan...
[+] Local format: 06 79 36 82 29
[+] E164 format: +33679368229
[+] International format: 33679368229
[+] Country found: +33 (FR)
[+] Carrier:
[i] Running Numverify.com scan...
[+] Valid: true
[+] Number: 33679368229
[+] Local format: 0679368229
[+] International format: +33679368229
[+] Country code: FR (+33)
[+] Country: France
[+] Location:
[+] Carrier: Orange France SA
[+] Line type: mobile
```

Geogramint

1. `git clone https://github.com/Alb-310/Geogramint.git`
2. `cd Geogramint/`
3. `pip3 install -r requirements.txt`
4. `python3 geogramint.py` →
5. Rellenar los campos →

- a) Ponerse foto de perfil y pública (todos)
- b) Conseguir API telegram:
<https://my.telegram.org/>



PRÁCTICA

RETO 1

Necesitamos tu ayuda para **localizar** a un **conocido ciberdelincuente**. La única información que tenemos del sujeto es el **gif adjunto** que compartió recientemente en un **foro underground**.

1. **Desgranar** la pregunta de investigación y **entender** lo que nos están pidiendo
 - Hay que localizar a un individuo dedicado a la ciberdelincuencia
 - Ha compartido un **GIF** en un foro underground → foro de la dark web / hot spot (eventos delictivos)

¿QUÉ QUEREMOS SABER?

- Localización - Ubicación

¿QUÉ TENEMOS?

- GIF

¿QUÉ INFORMACIÓN CONTIENE?

¿QUÉ HA SUCEDIDO?

¿CÓMO HA SUCEDIDO?

Info: x86_64

.Uptime: 0h 27m 32s

Frequency (in MHz): 2592

Frequency (in GHz): 2.59

RAM Usage: 1.00 GiB/1.94 GiB - 51%

Swap Usage: 0 B/975 MiB - 0%

CPU Usage: 8%

File Processes: 159 Running: 1

File systems:

/ 8.24 GiB/77.3 GiB

File Actions Edit View Help

kali@kali: ~

kali@kali: ~

kali@kali: ~

kali@kali: ~

File Actions Edit View Help

kali@kali: ~

kali@kali: ~

```

1  [ ] 1157 1.35 1.17
2  [ ] 1157 1.35 1.17
Mem[ ]
Swp[ ]
Tasks: 100, 159 thr; 2 running
Load average: 0.07 0.07 0.08
Uptime: 00:27:32
850M/1.94G
0K/975M

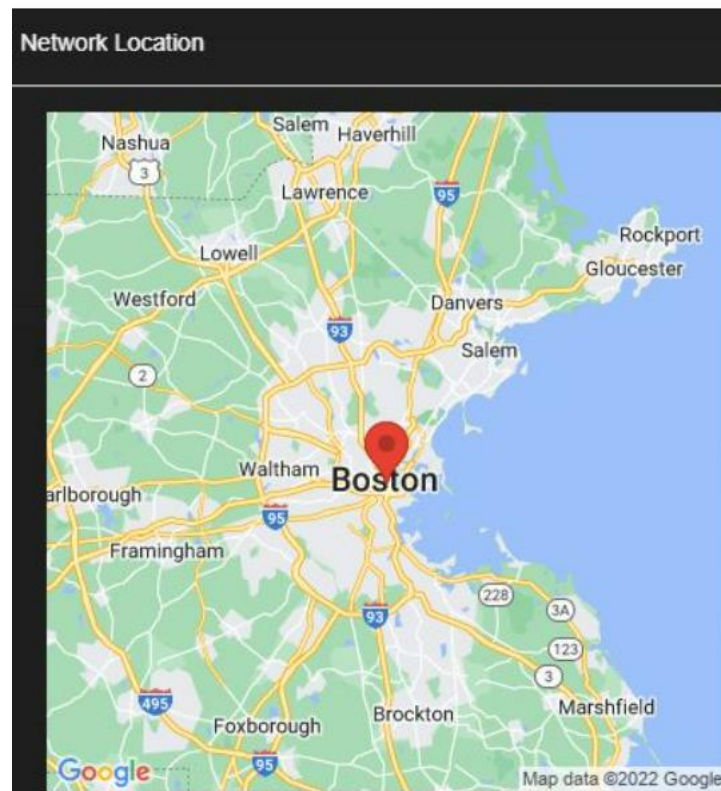
```

PID	USER	PRI	NI	VIRT	RES	SHR	S	CPU%	MEM%	TIME+	Command
1306	root	20	0	7016	3960	3368	S	0.0	0.2	0:00.00	/bin/bash
1154	kali	20	0	7908	4844	3344	S	0.0	0.2	0:00.04	/bin/bash
1139	root	20	0	7016	3876	3316	S	0.0	0.2	0:00.02	/bin/bash
1128	root	20	0	7116	3892	3304	S	0.0	0.2	0:00.01	/bin/bash
1296	kali	20	0	8024	4924	3292	S	0.0	0.2	0:00.07	-bash
1054	root	20	0	7016	3848	3260	S	0.0	0.2	0:00.01	/bin/bash
1133	root	20	0	8696	4604	3212	R	0.0	0.2	0:12.75	htop
437	root	20	0	216M	3652	3208	S	0.0	0.2	0:00.05	/usr/sbin/rsyslogd -n -iNONE
450	root	20	0	216M	3652	3208	S	0.0	0.2	0:00.00	/usr/sbin/rsyslogd -n -iNONE
451	root	20	0	216M	3652	3208	S	0.0	0.2	0:00.00	/usr/sbin/rsyslogd -n -iNONE
452	root	20	0	216M	3652	3208	S	0.0	0.2	0:00.01	/usr/sbin/rsyslogd -n -iNONE
780	kali	20	0	80996	3324	3068	S	0.0	0.2	0:00.00	/usr/bin/gpg-agent --supervised
1283	kali	20	0	6944	3404	3044	S	0.0	0.2	0:00.00	tmux
1285	kali	20	0	8256	4580	3000	S	0.0	0.2	0:01.42	tmux
745	kali	20	0	158M	3592	2988	S	0.0	0.2	0:00.00	/usr/bin/VBoxClient --vmsvga
747	kali	20	0	158M	3592	2988	S	0.0	0.2	0:00.04	/usr/bin/VBoxClient --vmsvga
741	kali	20	0	158M	3592	2988	S	0.0	0.2	0:00.04	/usr/bin/VBoxClient --vmsvga
494	root	20	0	350M	3376	2872	S	0.0	0.2	0:00.27	/usr/sbin/VBoxService
498	root	20	0	350M	3376	2872	S	0.0	0.2	0:00.19	/usr/sbin/VBoxService
500	root	20	0	350M	3376	2872	S	0.0	0.2	0:00.01	/usr/sbin/VBoxService
497	root	20	0	350M	3376	2872	S	0.0	0.2	0:00.02	/usr/sbin/VBoxService
501	root	20	0	350M	3376	2872	S	0.0	0.2	0:00.02	/usr/sbin/VBoxService
495	root	20	0	350M	3376	2872	S	0.0	0.2	0:00.00	/usr/sbin/VBoxService
496	root	20	0	350M	3376	2872	S	0.0	0.2	0:00.00	/usr/sbin/VBoxService
499	root	20	0	350M	3376	2872	S	0.0	0.2	0:00.00	/usr/sbin/VBoxService
502	root	20	0	350M	3376	2872	S	0.0	0.2	0:00.00	/usr/sbin/VBoxService
615	rtkit	20	0	149M	2884	2644	S	0.0	0.1	0:00.00	/usr/libexec/rtkit-daemon
616	rtkit	RT	1	149M	2884	2644	S	0.0	0.1	0:00.00	/usr/libexec/rtkit-daemon
611	rtkit	21	1	149M	2884	2644	S	0.0	0.1	0:00.02	/usr/libexec/rtkit-daemon
429	root	20	0	6592	2744	2540	S	0.0	0.1	0:00.00	/usr/sbin/cron -f
735	kali	20	0	155M	2932	2476	S	0.0	0.1	0:03.09	/usr/bin/VBoxClient --draganddrop
743	kali	20	0	155M	2932	2476	S	0.0	0.1	0:03.05	/usr/bin/VBoxClient --draganddrop
738	kali	20	0	155M	2932	2476	S	0.0	0.1	0:00.00	/usr/bin/VBoxClient --draganddrop
739	kali	20	0	155M	2932	2476	S	0.0	0.1	0:00.01	/usr/bin/VBoxClient --draganddrop
729	kali	20	0	154M	2872	2420	S	0.0	0.1	0:00.00	/usr/bin/VBoxClient --seamless
740	kali	20	0	154M	2872	2420	S	0.0	0.1	0:00.00	/usr/bin/VBoxClient --seamless
726	kali	20	0	154M	2872	2420	S	0.0	0.1	0:00.00	/usr/bin/VBoxClient --seamless
427	root	20	0	8104	7544	1660	S	0.0	0.4	0:00.59	/usr/sbin/haveged --Foreground --verbose=1 -w 1024
523	root	20	0	5624	1692	1580	S	0.0	0.1	0:00.00	/sbin/agetty -o -p -- \u --noclear tty1 linux
895	kali	20	0	20764	1896	1536	S	0.0	0.1	0:00.20	xcap -e Super_L Control_L Escape
1132	root	20	0	2156	688	624	S	0.0	0.0	0:00.00	./airodump-ng -c 11 --bssid f0:ab:54:50:1d:27 -w dump wlan0mon

F1Help F2Setup F3Search F4Filter F5Free F6SortByF7Nice F8Nice F9Kill F10Quit

Showing records 1 to 1 of 1

Map	Net ID	SSID	Type	First Seen	Most Recently	Crypto	Est. Lat
Map	F0:AB:54:50:1D:27	WiFi Hotspot 5725	infra	2016-05-15T12:00:00.000Z	2016-05-15T14:00:00.000Z		42.35916519



PRÁCTICA

Threat Intelligence

1

The bridge ha sido recientemente víctima de un ciberataque. Parece que no hay daños importantes, y no parece haber otros indicadores significativos de compromiso en cualquiera de nuestros sistemas. Sin embargo, durante el análisis forense nuestros administradores encontraron una imagen dejada por los ciberdelincuentes.

¿Quizás contenga alguna pista que nos permita determinar quiénes fueron los atacantes?

<https://raw.githubusercontent.com/OsintDojo/public/3f178408909bc1aae7ea2f51126984a8813b0901/sakurapwnedletter.svg>

¿Qué podemos hacer con este nombre de usuario?

Vamos a buscar el nombre completo y el mail

¿De qué criptomoneda es dueño el atacante?

¿Cuál es la dirección de la cartera de criptomonedas del atacante?

¿Cuál es el nombre actual del atacante en Twitter?

¿Cuál es el BSSID del WiFi del atacante?

Subrayar palabras o frases importantes

#Plan de ataque



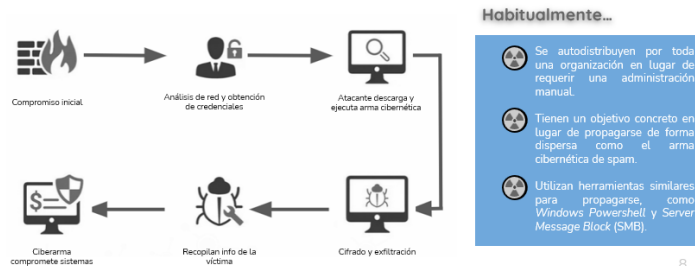
OPERADORES HUMANOS

Dado que el ransomware no posee altas capacidades para propagarse a través de Internet, el proceso de compromiso inicial es llevado a cabo por operadores humanos. De esta forma, el operador debe encargarse de desplegarlo a través de la red interna. Deben tenerse en cuenta todas las opciones que puedan terminar derivando en una ejecución de código malicioso, como la explotación de vulnerabilidades, el envío de correos con adjuntos maliciosos o el uso de exploit kits.

En teoría, **HavanaCrypt** es un ransomware, pero los investigadores aún **no sabemos si ha sido diseñado con esa finalidad o no**. Por ahora, esta arma cibernética está en fase de desarrollo y se desconoce si, hasta el momento, ha habido algún incidente o alguna víctima.

Teniendo en cuenta este dato y que no hay nota de rescate, **no podemos decir que se esté utilizando para extorsionar**. Por lo que sabemos hasta el momento, hoy por hoy **podríamos definirlo más como un wiper** (un ciberarma que borra datos sin que exista la posibilidad de que estos sean recuperados), que como un ransomware, cuya finalidad es cifrar los datos para extorsionar y conseguir un rédito económico.

Teniendo en cuenta esta peculiaridad, veamos **cómo se suele desplegar habitualmente** un ataque de ransomware:



Gráficos

Cuadros destacados con la información más relevante



Comprensión de aquello que se solicita (QUÉ), (CUÁL) alcance y objetivo, (CUÁNTO) tiempo



(CÓMO) conseguir datos → Herramientas, recursos, metodología



Recolección de evidencias, filtrar la información (desinformación), redacción lógica, plasmar la información obtenida en un informe → conocimiento útil

ENLACES

Grupo Telegram Herramientas OSINT

- https://t.me/osint_anatomy

Retos OSINT TryHackMe:

- <https://tryhackme.com/room/ohsint>
- <https://tryhackme.com/room/sakura>

Aquí os dejo un enlace de un reto en el que se incluye el análisis de emails (muy interesante) y alguna que otra herramienta más!!

- <https://tryhackme.com/room/threatinteltools>

Cualquier pregunta: goranemendi@hotmail.com