GOBIERNO DE ESPAÑA
MINISTERIO DE DEFENSA

CCN
centro criptológico nacional

Reyes 3.0. Manual de usuario

Marzo 2019

LIMITACIÓN DE RESPONSABILIDAD

El presente documento se proporciona de acuerdo con los términos en él recogidos, rechazando expresamente cualquier tipo de garantía implícita que se pueda encontrar relacionada. En ningún caso, el Centro Criptológico Nacional puede ser considerado responsable del daño directo, indirecto, fortuito o extraordinario derivado de la utilización de la información y software que se indican incluso cuando se advierta de tal posibilidad.

AVISO LEGAL

Quedan rigurosamente prohibidas, sin la autorización escrita del Centro Criptológico Nacional, bajo las sanciones establecidas en las leyes, la reproducción parcial o total de este documento por cualquier medio o procedimiento, comprendidos la reprografía y el tratamiento informático, y la distribución de ejemplares del mismo mediante alquiler o préstamo públicos.

Índice

1 INTRODUCCIÓN 4
2 SOBRE CCN-CERT, CERT GUBERNAMENTAL NACIONAL 4
3 ACCESO A LA APLICACIÓN 5
4 VISTA PRINCIPAL 6
4.1 Menú de usuario 7
4.1.1 Accesos a aplicaciones integradas 7
4.1.1.1 MISP 7
4.1.2 Configuración 7
4.1.3 Descargas 8
4.1.4 Acerca de 8
4.2 Barra de búsqueda 9
4.2.1 Términos 9
4.2.2 OPCIONES DE BÚSQUEDA 10
5 BÚSQUEDA 10
5.1 Inteligencia 11
5.2 Eventos 14
5.3 Información 17
5.4 Resoluciones 18
5.5 Resultado escaneo 20
5.6 Subdominios 21
5.7 Registrador 21
5.8 Muestras relacionadas 22
5.9 OSINT 22
5.10 URL 23
5.11 Incidentes 24
6 ANEXO 24

1 Introducción

Reyes es una solución del CCN-CERT que permite realizar investigación y análisis sobre ciberincidentes de forma ágil y rápida. Consiste en un metabuscador de información de diversas fuentes especializadas en ciber amenazas, que está integrado con herramientas de análisis del CCN-CERT. Permite la descarga de muestras, reglas e indicadores. Esta guía de usuario contiene información de uso de la interfaz gráfica de Reyes.

2 Sobre CCN-CERT, CERT Gubernamental Nacional

El CCN-CERT es la Capacidad de Respuesta a incidentes de Seguridad de la Información del Centro Criptológico Nacional, CCN, adscrito al Centro Nacional de Inteligencia, CNI. Este servicio se creó en el año 2006 como **CERT Gubernamental Nacional español** y sus funciones quedan recogidas en la Ley 11/2002 reguladora del CNI, el RD 421/2004 de regulación del CCN y en el RD 3/2010, de 8 de enero, regulador del Esquema Nacional de Seguridad (ENS), modificado por el RD 951/2015 de 23 de octubre.

Su misión, por tanto, es contribuir a la mejora de la ciberseguridad española, siendo el centro de alerta y respuesta nacional que coopere y ayude a responder de forma rápida y eficiente a los ciberataques y a afrontar de forma activa las ciberamenazas, incluyendo la coordinación a nivel público estatal de las distintas Capacidades de Respuesta a Incidentes o Centros de Operaciones de Ciberseguridad existentes.

Todo ello, con el fin último de conseguir un ciberespacio más seguro y confiable, preservando la información clasificada (tal y como recoge el art. 4. F de la Ley 11/2002) y la información sensible, defendiendo el Patrimonio Tecnológico español, formando al personal experto, aplicando políticas y procedimientos de seguridad y empleando y desarrollando las tecnologías más adecuadas a este fin.

De acuerdo a esta normativa y la Ley 40/2015 de Régimen Jurídico del Sector Público es competencia del CCN-CERT la gestión de ciberincidentes que afecten a cualquier organismo o empresa pública. En el caso de operadores críticos del sector público la gestión de ciberincidentes se realizará por el CCN-CERT en coordinación con el CNPIC.

3 Acceso a la aplicación

Reyes utiliza certificados de cliente expedidos por el CCN-CERT, debe incluirse en el navegador este certificado. Al acceder a la aplicación se muestra un formulario de acceso para introducir las credenciales de usuario. Debe introducirse el usuario y la contraseña en el formulario y pulsar el botón 'login'. Si las credenciales son correctas, se accederá a la aplicación o en caso contrario, se mostrará un mensaje de error al usuario.

Tras validarse el acceso se genera una sesión de usuario que permite al usuario hacer uso de las funcionalidades de Reyes. La sesión no caduca si se está haciendo uso de la aplicación. Se mantiene la sesión sólo en el navegador de la sesión actual. Mientras la sesión no caduque, no será necesario introducir de nuevo las credenciales incluso si se recarga la página. En caso de caducar redirige a la pantalla de *login* y muestra un mensaje de que ha caducado la sesión.

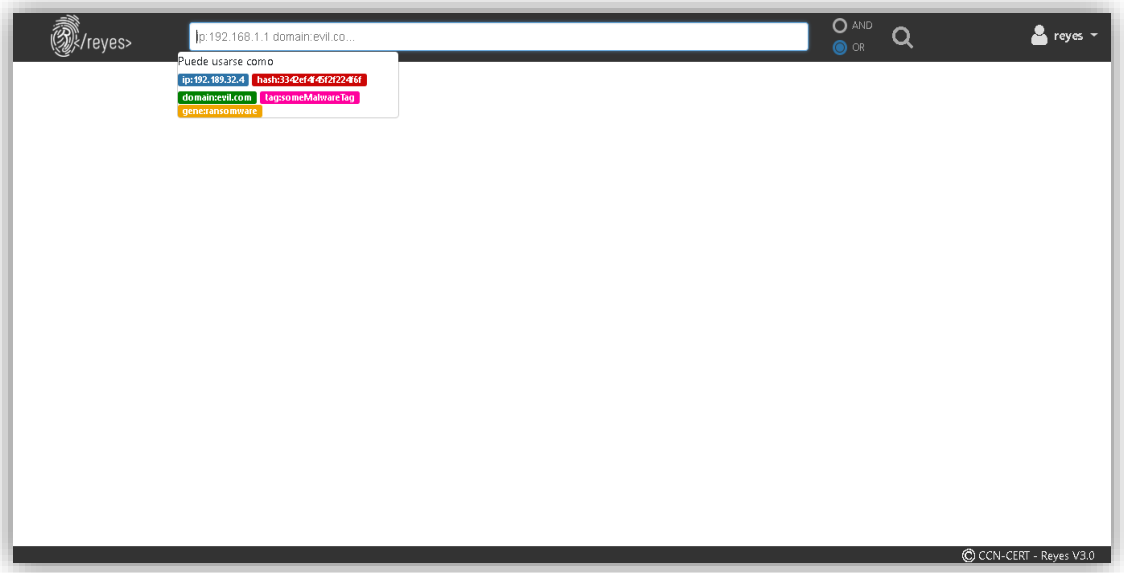
La sesión caduca en 30 minutos si no se realizan peticiones al servidor. Se puede finalizar la sesión de usuario en cualquier momento desconectándose de la aplicación con el botón 'Desconectar':

El botón está situado en el menú de usuario de la esquina superior derecha de la barra de navegación, una vez desconectado redirigirá a la vista de *login.*

Es recomendable por seguridad, utilizar este botón una vez que el usuario ha terminado de utilizar la aplicación, en lugar de cerrar la pestaña de navegación. No obstante, en caso de no desconectarse, la sesión se caduca a los 30 minutos.

4 Vista principal

Tras realizar el registro de las credenciales de usuario con éxito, se visualiza una pantalla que contiene un botón desplegable de las opciones de usuario en el extremo superior derecho y una barra de búsqueda central para introducir los términos a analizar.



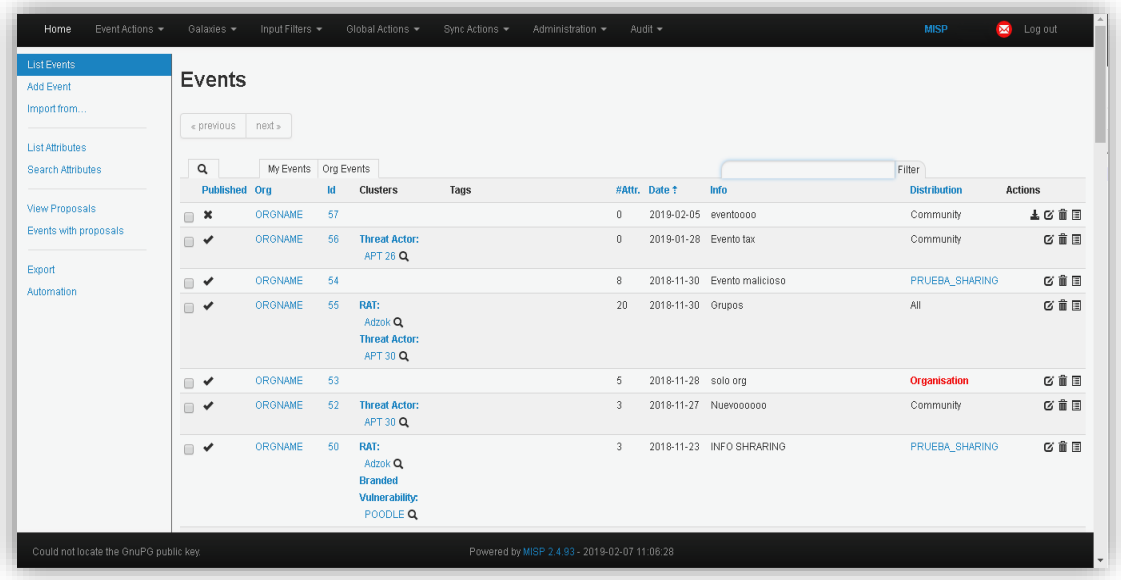
4.1 Menú de usuario

4.1.1 Accesos a aplicaciones integradas

Muestra un submenú con links de accesos a las aplicaciones integradas en el *single sign-on* del usuario sin necesidad de introducir de nuevo las credenciales.

4.1.1.1MISP

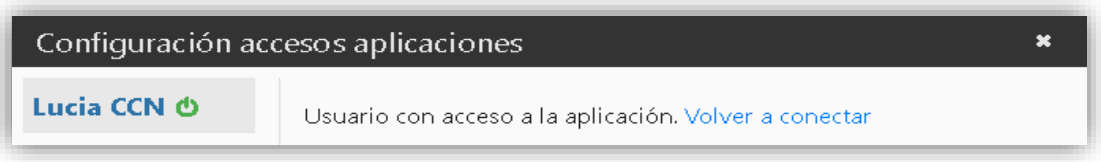
Malware Information Sharing Platform; Se trata de una plataforma *Open Source* diseñada para automatizar el intercambio de información y conocimiento sobre ciberamenazas.



4.1.2 Configuración

Para realizar las consultas de incidentes en LUCIA, deben ingresarse las credenciales en la solapa de configuración.

La configuración contiene un panel de acceso a LUCIA con usuario y contraseña, desde donde se puede hacer la conexión y desconexión.



4.1.3 Descargas

Muestra un desplegable con descargas de **listas negras** y **paquetes de reglas**.

Los primeros son ficheros de texto que contienen **IPs** y **dominios** clasificados en **listas negras**. Los **paquetes de reglas** contienen archivos de reglas de deteccion de ciberamenazas. El submenú permite seleccionar el documento a descargar y/o descargar en un único fichero *.zip* todos los ficheros de ese tipo, seleccionando Descargar todo

4.1.4 Acerca de

Al hacer *click* sobre el botón del menú se muestra una breve información sobre la versión de la aplicación.

4.2 Barra de búsqueda

Permite introducir términos, iniciar la búsqueda y borrar términos para realizar una nueva búsqueda. Dispone de una ayuda que sugiere los términos que se pueden buscar.

Los términos se introducen siguiendo el siguiente formato: **tipo**:*valor*

4.2.1 Términos

Los términos introducidos son reconocidos por el buscador según el tipo. Actualmente pueden introducirse términos de tipo ***IP***, ***dominio***, ***hash***, ***tags*** y ***términos genéricos***. Se pueden escribir múltiples términos pulsando la barra espaciadora tras escribir cada término.

4.2.2 OPCIONES DE BÚSQUEDA

Con los botones de selección de operador se puede especificar que la búsqueda se haga sobre todos los términos introducidos simultáneamente: 'AND', por ejemplo, buscando ***IP*** AND ***Tag*** o resultados relacionados con al menos uno de los términos introducidos: 'OR'.

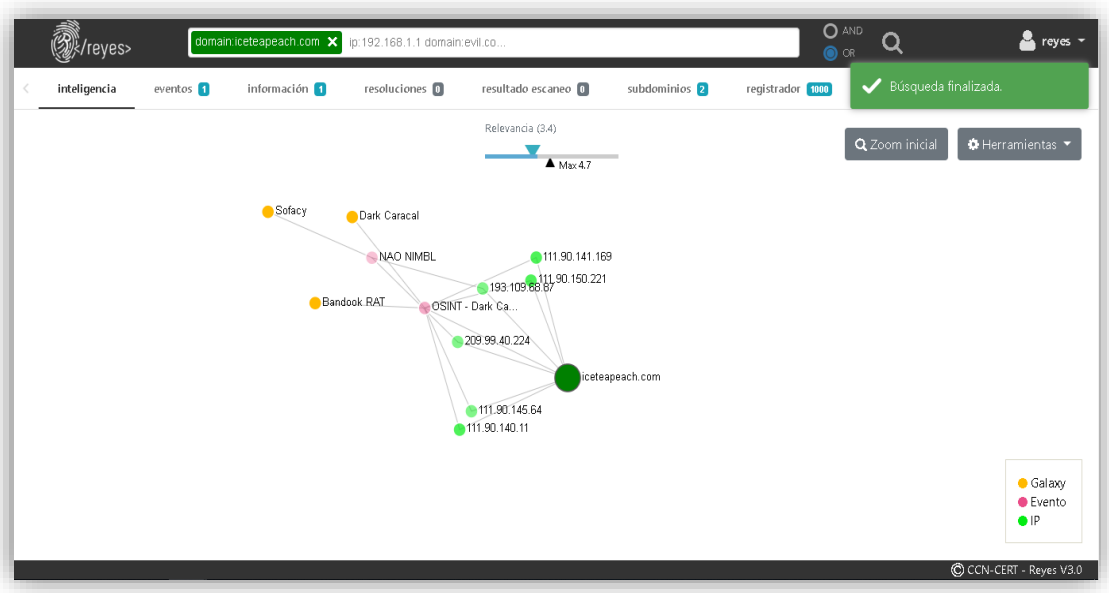
5 Búsqueda

Los resultados que devuelve la búsqueda se organizan en pestañas de contenido. Las pestañas y sus contenidos varían en función de los términos buscados. Mientras se reciben resultados se van mostrando en la pestaña que corresponde y se actualiza el grafo de inteligencia y la información de las pestañas.

En la parte inferior de la vista se puede comprobar si ha finalizado la búsqueda sobre las aplicaciones externas.

Junto a los iconos de cada aplicación se muestran distintas indicaciones. Un *check* verde si ha finalizado: , un símbolo *cargando* azul si aún está recibiendo datos: , una señal amarilla de atención si ha habido un error en la búsqueda: . Si la API externa ha devuelto algún error: .

Si la búsqueda ha finalizado se muestra también un mensaje verde superpuesto en la interfaz.



En función de los tipos de términos que se indiquen en el buscador aparecerán distintas pestañas en el resultado de la búsqueda. Las pestañas que se mostrará se pueden ver en la siguiente tabla:

	Inteligencia	Eventos	Información	Resoluciones	Resultado escaneo	Subdominios	Muestras	Registrador	OSINT	URL
dominio	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
IP	✓	✓	✓	✓	✓		✓	✓	✓	✓
hash	✓	✓	✓							✓
tag	✓	✓								
genérico	✓	✓								

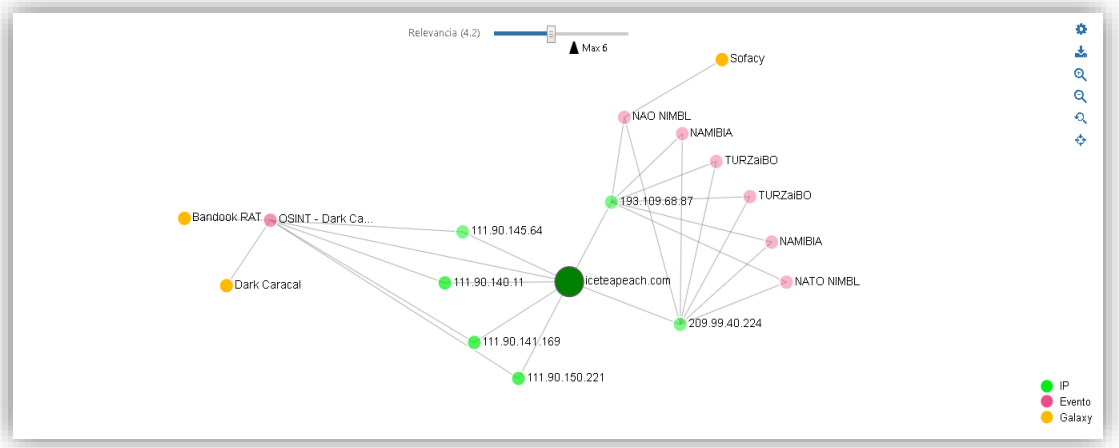
Cada pestaña muestra un número que indica la cantidad de resultados que ha devuelto la búsqueda en esa pestaña.

5.1 Inteligencia

Muestra elementos relevantes de eventos de MISP con información enriquecida tras la búsqueda contra las aplicaciones externas. Los objetos que se visualizan en el grafo son ***eventos*** de MISP, ***IP***, ***dominios***, ***URL***, ***Galaxies*** relevantes, ***hashes e incidentes de LUCIA***. Mostrará objetos de tipo ***IP***, ***dominio***, ***URL*** o ***hash*** siempre y cuando MISP devuelva algún evento.

El **enriquecimiento** se realiza buscando determinada información de las aplicaciones públicas sobre fuentes locales, como MISP, CIF y LUCIA. Se enriquecen términos de tipo ***IP***, ***dominio***, ***URL*** y ***hash***, así como datos obtenidos de las fuentes externas.

Durante el proceso de búsqueda, el grafo va dibujando los eventos directos encontrados en MISP y sus eventos relacionados.



Inicialmente el grafo contiene todos los eventos, los directos, obtenidos de MISP y el primer nivel de eventos relacionados de estos. Los elementos de la búsqueda se clasifican dependiendo de su *valor*, mediante una serie de reglas para priorizar la información que se visualiza.

Esta **ponderación** se realiza mediante una puntuación configurable de los resultados. Eventos directos y relacionados usan distintas escalas de relevancia. Los conceptos que se tienen en cuenta para calcular estas puntuaciones son:

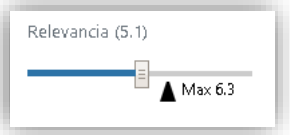
- Atributo *calidad*
- Nivel de Riesgo
- Organizaciones relevantes
- Relevancia de los términos relacionados
- Etiquetas relevantes
- *Galaxies* relevantes
- Atributos relevantes

Si se trata de un evento relacionado, se evalúa, además:

- Fechas de resolución

Una vez finalizada la búsqueda se obtiene un valor de corte en el 75 % de la puntuación de los eventos y sólo se muestran los eventos directos que tengan una puntuación mayor a ésta. También se visualizan los eventos relacionados que tengan la misma puntuación que el evento de primer nivel o la superen. A excepción de los eventos relacionados con los eventos directos que se muestran siempre.

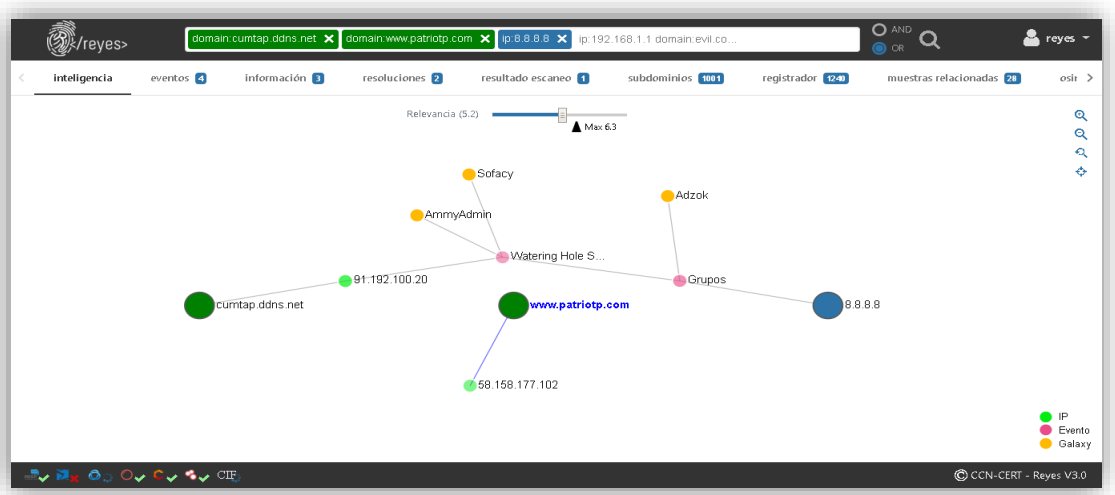
El usuario puede variar esta visualización y mostrar más eventos, moviendo el indicador de la **relevancia** hasta un máximo que es el valor de corte al que se ha hecho referencia anteriormente.



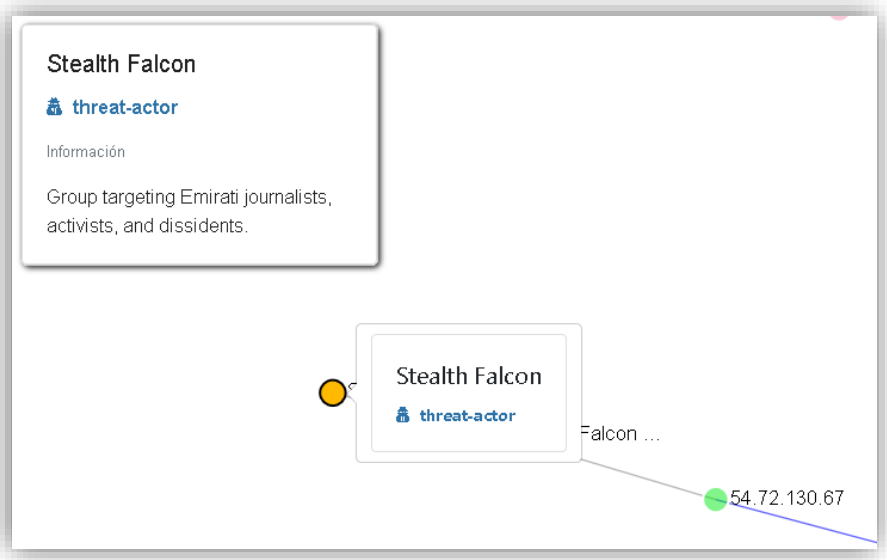
Los eventos relacionados que tienen el mismo *Galaxy* se muestran relacionados con ese *Galaxy* y agrupados y se despliegan al hacer *click* en el nodo.

Si se busca más de un término, cada uno se mostrará en un nodo y aparecerán los elementos relacionados con su término.

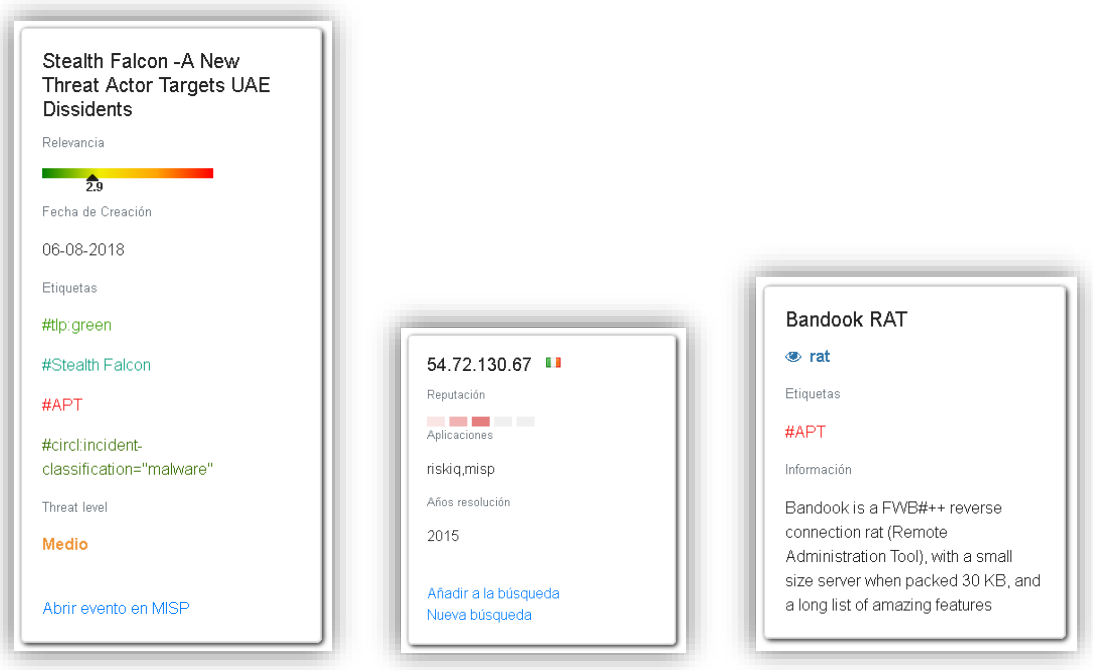
En el caso de que al buscar dos términos uno de ellos devuelva una IP con un evento relacionado que a su vez esté relacionado con un evento directo de otro término de búsqueda aparecerá una relación entre los dos eventos.



Se puede obtener una descripción de un objeto deslizando el cursor sobre el nodo, o haciendo *doble click* sobre él.

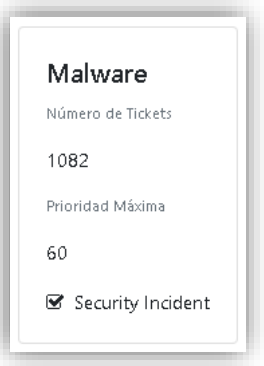


La tarjeta contiene enlaces para añadir los elementos a la búsqueda o realizar una nueva búsqueda. En los objetos ***evento*** hay un enlace para abrir el ***evento*** en MISP.



Los objetos incidente aparecen por su clasificación. Muestran el número de tickets que contienen.

Se puede obtener una descripción deslizando el cursor sobre el nodo, o haciendo *doble click* sobre él.

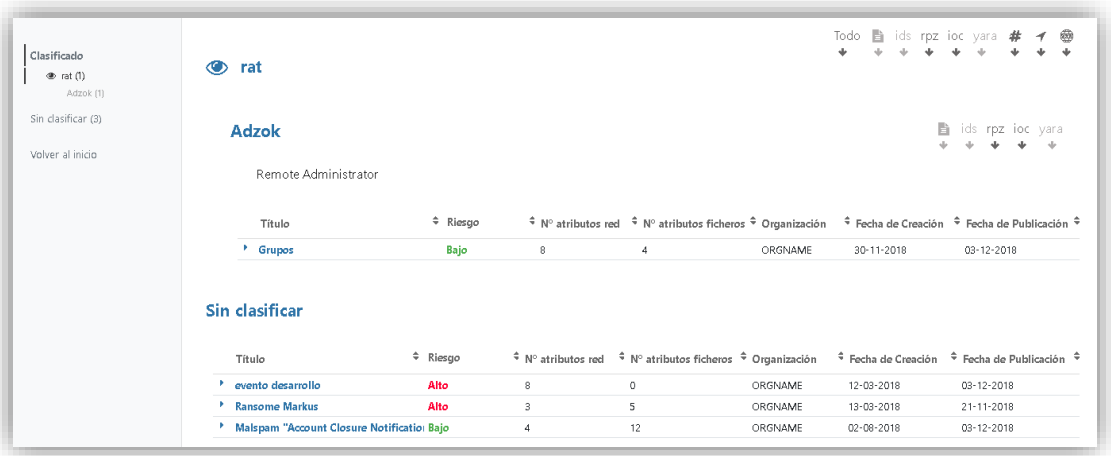


A la derecha de la vista aparecen botones de configuración, un botón para descargar el grafo en formato *.svg* o *.png* , un botón para ampliar la vista del grafo , un botón para reducir la vista , un botón para volver al tamaño inicial y un botón para centrar el grafo .

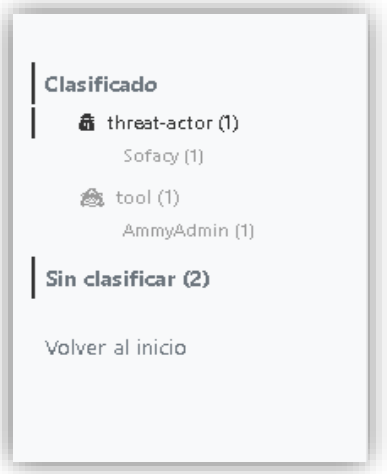
5.2 Eventos

La pestaña eventos muestra elementos de información relevante relativa a eventos sin clasificar y/o eventos clasificados por *galaxy* y taxonomía.

La vista se estructura en dos partes: el menú de navegación y el contenido.



En la izquierda está el menú lateral que permite la navegación entre los datos:



Organiza los eventos en *Clasificados* y eventos *Sin clasificar*. Los eventos clasificados se organizan por el *galaxy* Sofacy (1) al que pertenecen indicando el número de eventos que contienen y en un nivel superior de organización se clasifican por la taxonomía del *galaxy* threat-actor (1) indicando el número de *galaxies* que contienen.

Haciendo *click* en cualquier elemento de este menú se puede navegar entre el contenido de los eventos en la derecha en la vista principal de la pestaña.

En la parte derecha de la vista, ocupando la mayor parte de la vista se muestran los eventos agrupados en taxonomía y galaxy.

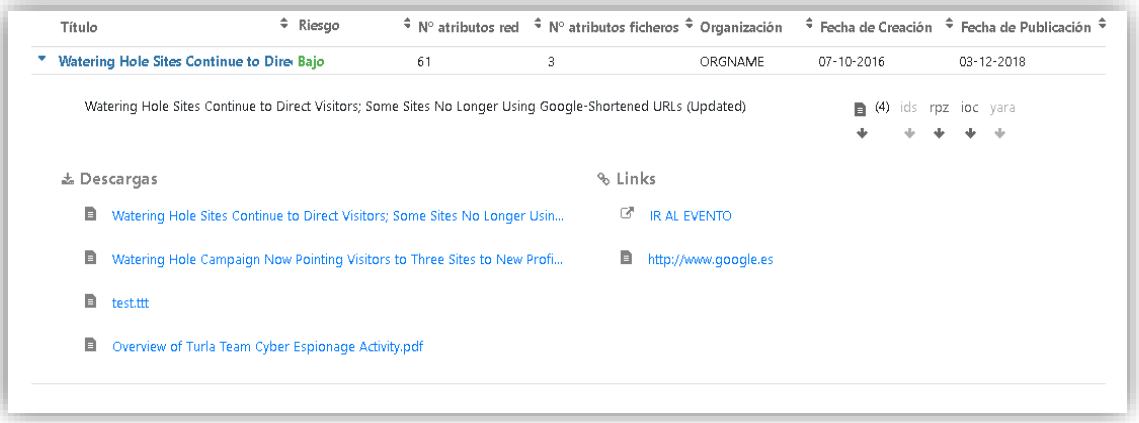
En la esquina superior derecha hay botones (de izquierda a derecha) el primero descarga en un fichero .zip **todos los archivos de la búsqueda** Todo, hay un botón para descargar los **documentos de la búsqueda** (1) cuatro botones distintos para descargar **indicadores** ids rpz ioc yara, un botón para descargar todas las **muestras** relacionadas con la búsqueda #, otro para descargar las ***IPs*** relacionadas con la búsqueda y un botón para descargar listados de ***dominios*** relacionados

Los eventos *Clasificados* por taxonomía y *galaxy* se sitúan primero y en la parte inferior los eventos *Sin clasificación*.

Vista de un *galaxy* conteniendo un evento:

Al hacer *click* sobre un evento, este se despliega.

Vista de un evento con su detalle desplegado:



La vista del evento muestra información descriptiva. Hay enlaces individuales para descargar cada documento relacionado con el evento.

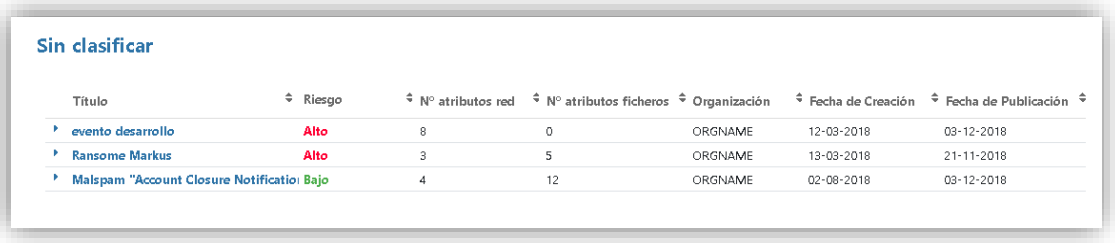
Un enlace de navegación que permite navegar al evento en MISP en una nueva pestaña del navegador.

También existen enlaces de navegación a sitios con información relacionada con el evento.

La sección *de eventos clasificados por su galaxy* contiene un botón para descargar los **documentos** (1) en un fichero *.zip* y cuatro botones distintos para descargar **indicadores** ids rpz ioc yara. Cada evento también dispone de un botón de

descarga de documentos en un fichero *.zip*, y cuatro botones para descargar indicadores.

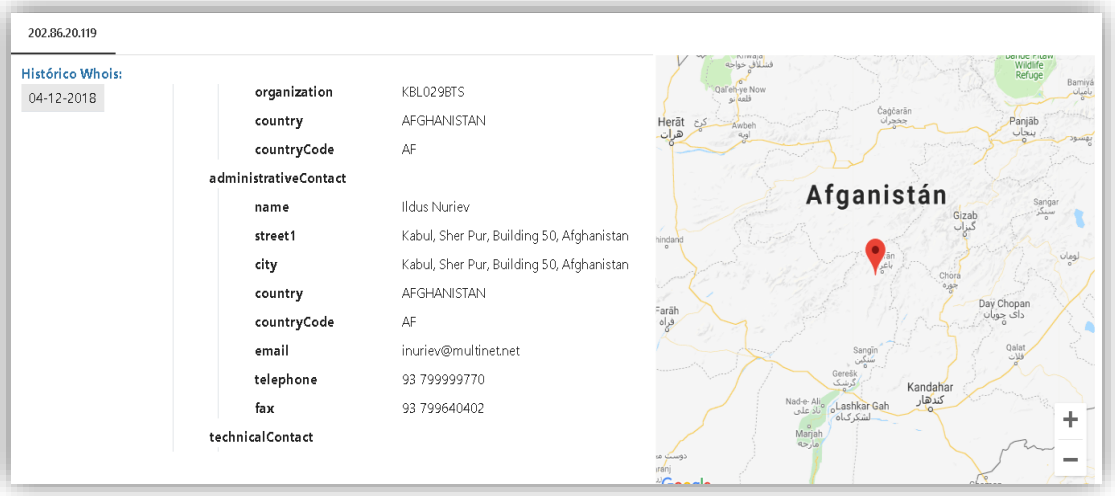
Vista de los eventos sin clasificación:



5.3 Información

Se mostrará cuando se buscan ***dominios***, ***IPs*** y ***hashes***. ***Dominio*** e ***IP*** muestran sus datos de registro, histórico y un mapa de geolocalización.

Por cada término de búsqueda aparecerá una subpestaña.



A la izquierda de la vista se muestra el histórico de WHOIS, siendo el primero de ellos el registro actual. Haciendo *click* en cada fila del histórico aparece información del registro de WHOIS a su derecha.

En la parte derecha de la vista se muestra la geolocalización de todos los ***dominios*** e ***IPs*** que se hayan buscado.

Hay un botón para exportar el JSON, el cual contendrá un fichero con el histórico y un fichero con el WHOIS.

Si el término buscado es ***hash***, muestra información de los escaneos y las detecciones.

Se muestran unos botones de subsecciones de la búsqueda, como: .

Arriba, si el hash contiene ficheros embebidos aparecerá el icono de ficheros embebidos: , de la misma forma si contiene macros, aparecerá el icono:

En la esquina superior derecha se mostrarán las detecciones para esa muestra.

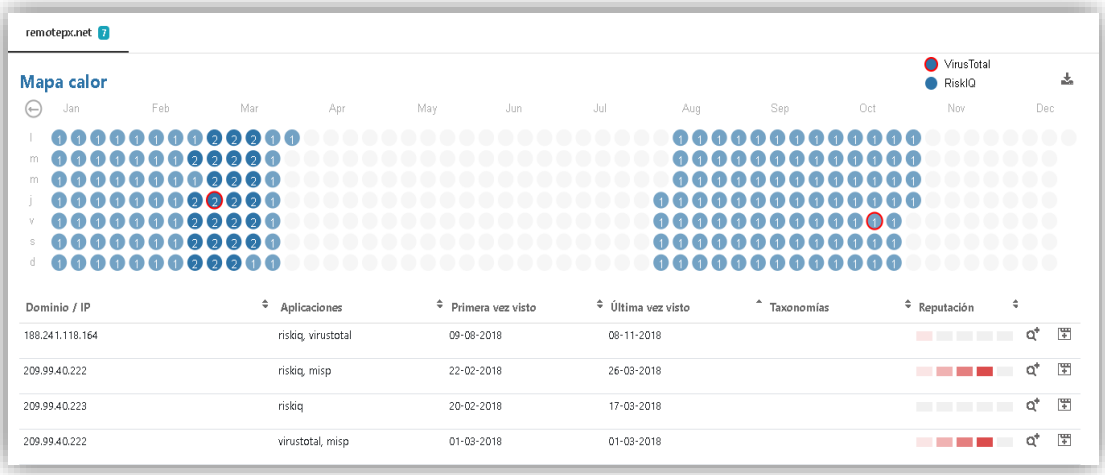
Hay un botón para descargar el JSON con el contenido del ***hash***.

5.4 Resoluciones

Esta pestaña muestra resultados de las resoluciones de la búsqueda para los términos ***IP***, ***dominio***.

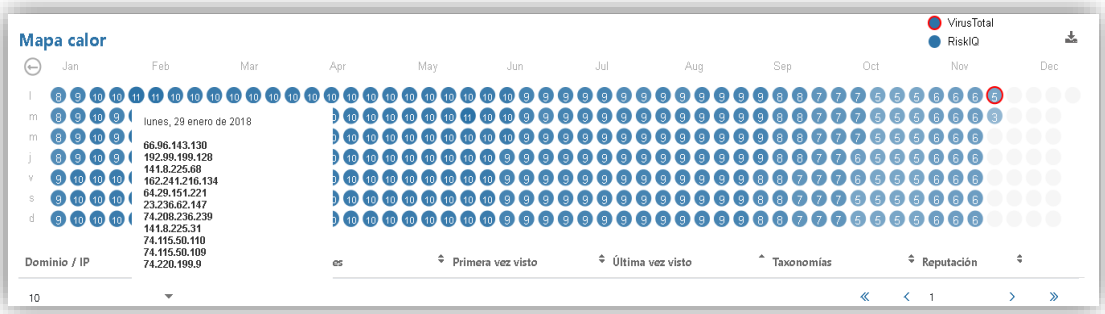
Por cada término de búsqueda aparecerá una subpestaña.

En la parte de arriba se puede ver un mapa de calor que muestra el histórico de resoluciones DNS relacionadas con el término. Si hay detecciones, se indica el número de dominios que apuntaban a la IP en esa fecha.

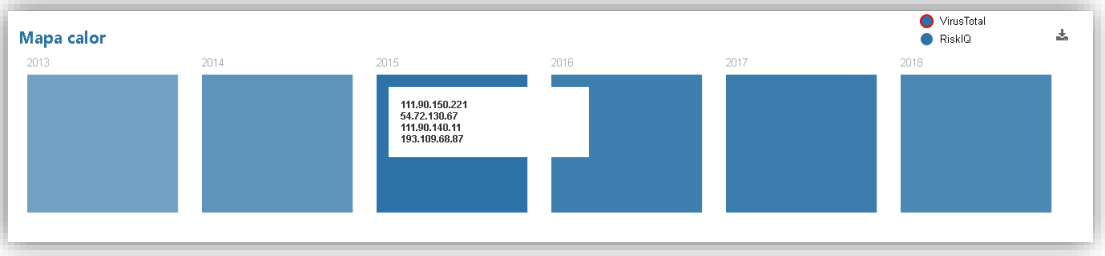


El mapa de calor tiene dos formatos de visualización:

- Visualización de todos los días del año. En esta vista, al superponer el ratón sobre los números de detecciones del mapa se ven las ***IPs*** o ***dominios*** de resolución. Se puede acceder a la visualización de todos los años haciendo *click* en el botón situado en el extremo izquierdo superior del mapa de calor.



- Visualización de todos los años en los que se han encontrado datos. En esta vista, si hacemos *click* sobre un año, se mostrará una visualización de todos los días del año.



En el extremo superior derecho hay un botón para la descarga de un fichero *.txt* con el listado de ***IP*** y ***dominios***.

Además contiene una tabla de resoluciones de ***IPs*** y ***dominios*** relacionados con el término buscado y el detalle del rango de fechas de resolución desde el que hay información.

En caso de haberse encontrado en Misp aparecerán las taxonomías si las tiene.

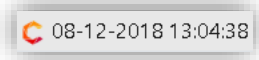
En cada fila de la tabla hay un botón para lanzar una nueva búsqueda con ese resultado o para añadirlo a la búsqueda .

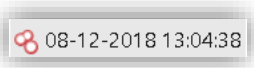
5.5 Resultado escaneo

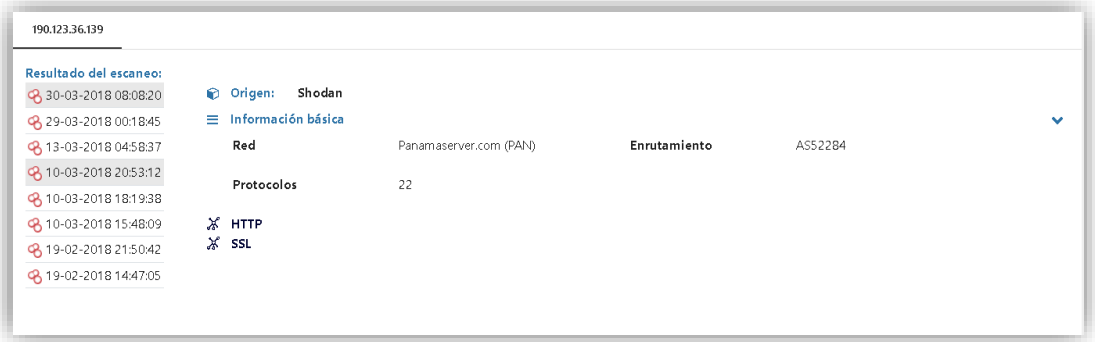
Esta pestaña contiene la información obtenida de los escaneos realizados al término buscado, si este es una dirección ***IP dominio***.

Por cada término de búsqueda aparecerá una subpestaña.

En la parte izquierda podemos ver un histórico de fechas, sobre el que se puede hacer *click* para ver información en detalle de la fecha seleccionada.



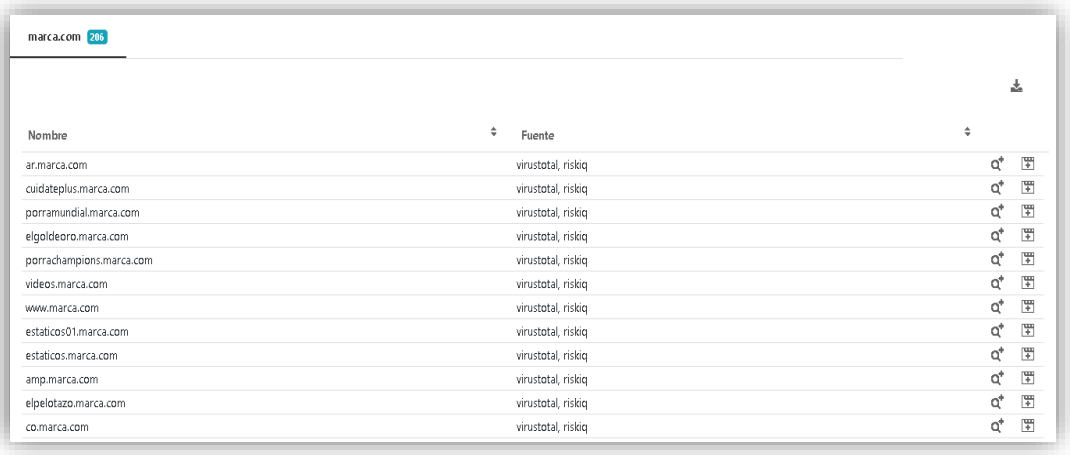




5.6 Subdominios

Esta pestaña muestra una tabla con la lista de subdominios cuando se busca un ***dominio***.

Por cada término de búsqueda aparecerá una subpestaña.



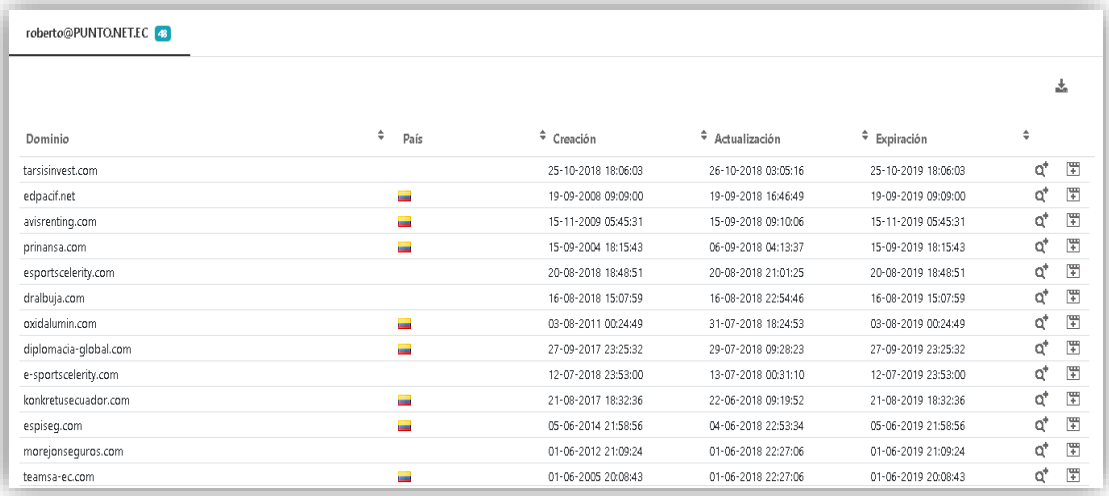
En el extremo superior derecho hay un botón para la descarga de un fichero .txt con el listado de ***dominios.***

En cada fila de la tabla hay un botón para lanzar una nueva búsqueda con ese resultado o para añadirlo a la búsqueda .

5.7 Registrador

Se muestra cuando se busca un ***dominio*** y contiene los datos de los ***dominios*** obtenidos a partir del registrador de su WHOIS.

Por cada término de búsqueda aparecerá una subpestaña.



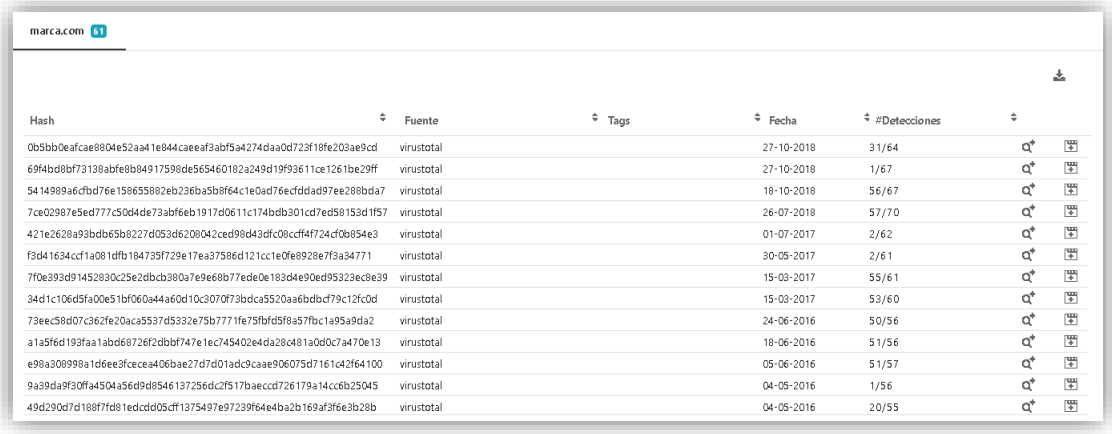
En el extremo derecho superior hay un botón para la descarga de un fichero .txt con el listado de ***dominios***.

En cada fila de la tabla hay un botón para lanzar una nueva búsqueda con ese resultado o para añadirlo a la búsqueda .

5.8 Muestras relacionadas

Contiene un listado de muestras relacionadas obtenidas de la búsqueda de ***IPs*** y ***dominios***.

Por cada término de búsqueda aparecerá una subpestaña.



En la columna de detecciones, se encuentra a la derecha el número de detecciones positivas y a la izquierda el total de detecciones 31/64 .

En el extremo derecho superior hay un botón para la descarga de un fichero formato .txt con el listado de muestras relacionadas.

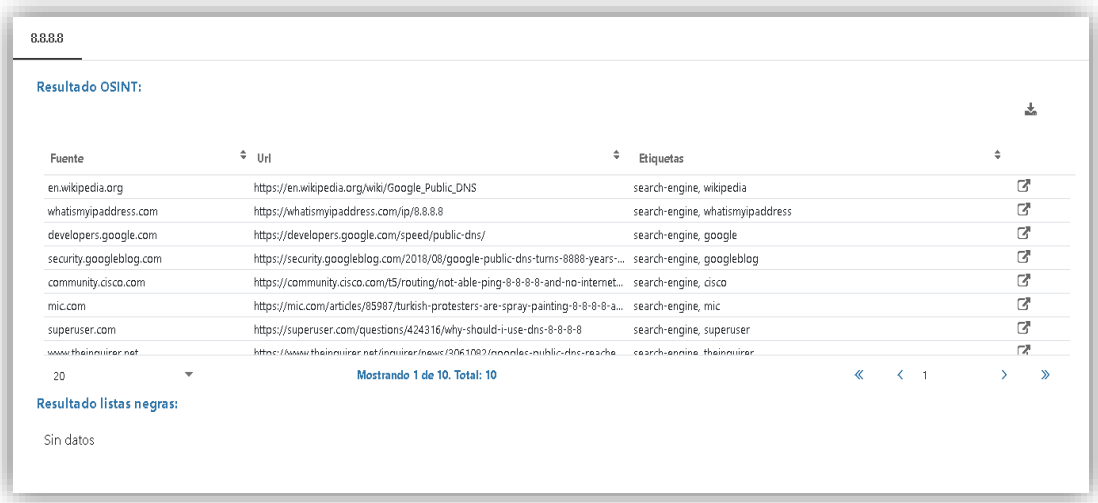
En cada fila de la tabla hay un botón para lanzar una nueva búsqueda con ese resultado o para añadirlo a la búsqueda

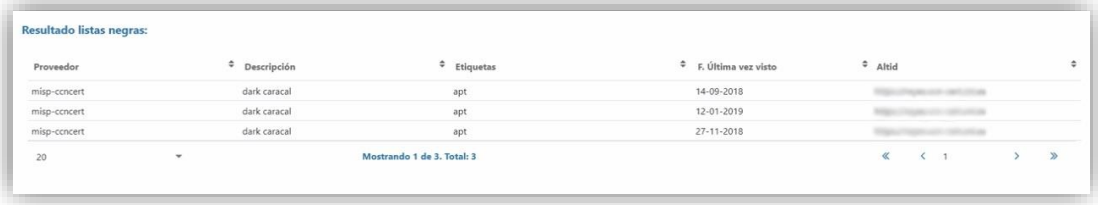
5.9 OSINT

Contiene dos listados, obtenidos de la búsqueda de ***IPs*** y ***dominios***, uno con resultados OSINT y otro con listas negras.

Por cada término de búsqueda aparecerá una subpestaña.

En la parte superior se encontrarán los resultados OSINT y en la parte inferior, las listas negras si CIF devuelve resultados.



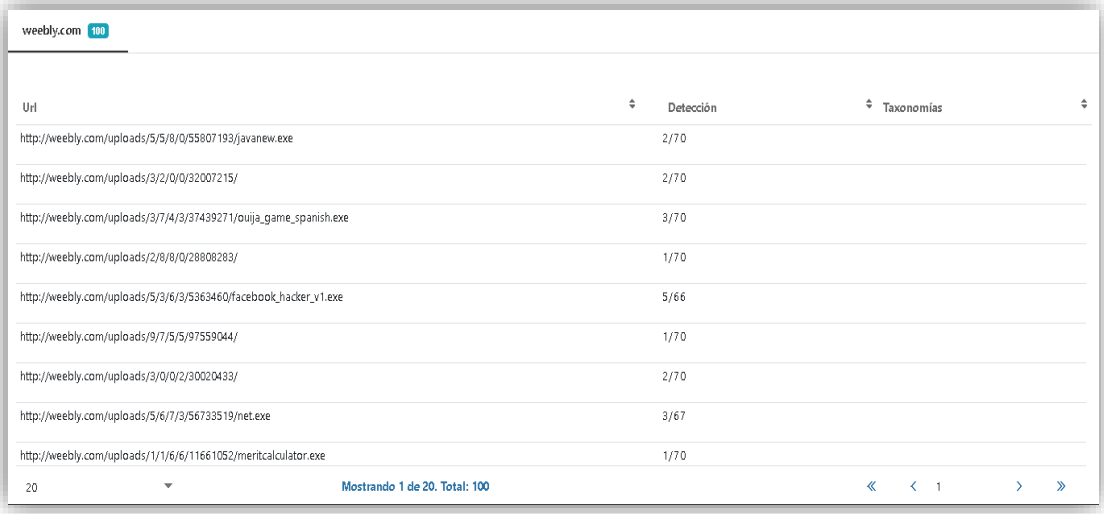


En el extremo derecho superior hay un botón para la descarga de un fichero .txt con el listado de muestras relacionadas.

En cada fila hay un botón de enlace hacia la ***URL*** especificada

5.10 URL

Muestra las ***URL*** detectadas del ***dominio*** o de la dirección ***IP***.
Por cada término de búsqueda aparecerá una subpestaña.



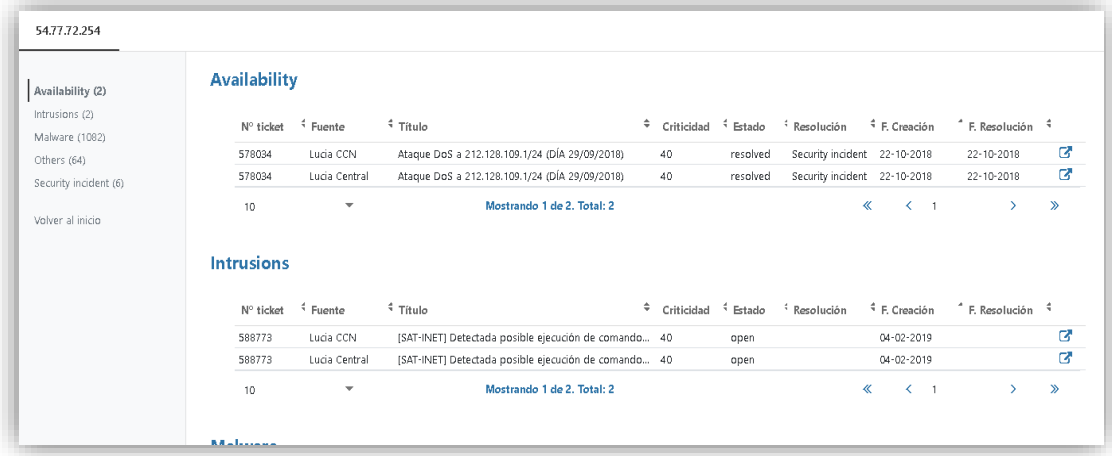
En la columna de detecciones aparecen a la derecha, el número de detecciones positivas y a la izquierda el total de detecciones: 31/64 .

En caso de haberse encontrado en Misp, aparecerán las taxonomías, si las tiene.

5.11 Incidentes

La pestaña Incidentes muestra los tickets de incidentes en LUCIA relacionados con los términos buscados cuando son de tipo ***IP*** y ***dominio***. Se agrupan por 'CF' (*Cyber Incident Classification*).

La vista se estructura en dos partes: el menú de navegación y el contenido.



6 Anexo

Las fuentes de datos de Reyes son de dos tipos:

- Aplicaciones integradas que son fuentes privadas de la organización como MISP y CIF.
- Fuentes públicas especializadas en ciberamenazas: RiskIQ, VirusTotal, Whois, Censys, Shodan

Fuentes privadas:

Todos los tipos de términos se buscan en MISP.

En MISP también se busca información adicional sobre los datos obtenidos de las fuentes públicas. Para datos de tipo ***IP***, ***dominio***, ***URL*** y ***hash*** se hacen nuevas búsquedas en MISP.

En CIF se consultan los términos de búsqueda en listas negras.

Fuentes públicas:

Para los términos ***IP***, ***dominio***, se obtienen las resoluciones DNS de Virus Total y RiskIQ, muestras de malware, informes, OSINT, subdominios si la búsqueda se hace sobre un ***dominio***. En Whois se obtiene la geolocalización y los datos de registro e

histórico Whois. De Censys se obtiene información de los escaneos de ***IP*** y ***dominio*** y de Shodan, los escaneos de ***IP***.

Las búsquedas de término tipo ***URL*** son similares a las de tipo ***dominio***.

Si el término buscado es ***hash***, la búsqueda se hace sobre Virus Total y obtenemos información de los escaneos y las detecciones de Virus Total.

En la siguiente tabla se esquematiza la búsqueda de tipos de términos en las aplicaciones

	MISP	CIF	Whois	virustotal	RiskIQ	Censys	SHODAN	LUCIA
dominio	✓	✓	✓	✓	✓	✓	✓	✓
IP	✓	✓	✓	✓	✓	✓	✓	✓
URL	✓			✓				
hash	✓			✓				