

Manual de usuario de la aplicación MARTA



Diciembre 2018

Edita:



CENTRO CRIPTOLOGICO NACIONAL
2.5.4.13=Qualified Certificate: AAPP-SEP-M-SW-KPSC,
ou=sello electrónico, serialNumber=S2800155J,
o=CENTRO CRIPTOLOGICO NACIONAL, cn=CENTRO
CRYPTOLOGICO NACIONAL, c=ES
2019.04.24 16:51:26 +02'00'

© Centro Criptológico Nacional, 2019

Fecha de Edición: abril de 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

SOBRE CCN-CERT, CERT GUBERNAMENTAL NACIONAL	5
1. FUNCIONALIDAD GENERAL.....	6
1.1 RECEPCIÓN DE FICHEROS Y ANÁLISIS ESTÁTICO.....	6
1.2 ANÁLISIS DINÁMICO.....	6
1.3 TRIANA	7
2. VISTA DE ACCESO	8
3. SUBIDA DE BINARIOS	10
4. PESTAÑA DE BINARIOS.....	15
4.1 LISTADO.....	15
4.2 ACCIONES SOBRE LOS FICHEROS	17
4.3 DETALLE DE UN BINARIO (ANÁLISIS ESTÁTICO).....	18
4.4 ETIQUETAS	22
4.5 ENTROPÍA.....	23
5. PESTAÑA DE ANÁLISIS.....	25
5.1 LISTADO.....	25
5.2 ESTADOS DE UN ANÁLISIS.....	26
5.3 ACCIONES SOBRE LOS ANÁLISIS.....	26
5.4 ANÁLISIS DINÁMICO	27
5.5 ANÁLISIS DINÁMICO ANDROID	32
5.6 ETIQUETAS	36
5.7 STRINGS.....	37
6. CONFIGURACIÓN	39
6.1 REGLAS YARA.....	39
6.1.1 DETALLE REGLA YARA.....	40
6.1.2 CREAR REGLA YARA.....	41
6.1.3 ELIMINAR REGLA YARA.....	41
6.1.4 ACTIVAR REGLAS SELECCIONADAS.....	42
6.1.5 DESACTIVAR REGLAS SELECCIONADAS	42
6.1.6 PUBLICAR REGLAS YARA.....	42
6.1.7 DESPUBLICAR REGLAS YARA	42

6.1.8 DESCARGAR REGLA YARA.....	42
6.2 REGLAS IOC.....	43
6.2.1 LISTADO.....	43
6.2.2 ACCIONES.....	43
6.3 ORGANISMOS.....	48
6.4 PERSISTENCIA.....	50
6.5 ETIQUETAS.....	52
6.6Listas Blancas.....	54
6.7 STRINGS.....	68
6.8 COLECTORES.....	69
7. BÚSQUEDA AVANZADA.....	72
8. INFORME PERSONALIZADO.....	75
9. ESTADÍSTICAS.....	76
10.MONITORIZACIÓN.....	77

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 el 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 con 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.

1. FUNCIONALIDAD GENERAL

MARTA es una aplicación dedicada al *análisis automatizado* de múltiples tipos de ficheros, que podrían tener un comportamiento malicioso (*malware*). Esto incluye, por supuesto, ejecutables, pero también otros tipos de ficheros, como documentos de office o PDF's.

Para facilitar el uso de la aplicación, MARTA consta de una *interfaz web*, que se puede ejecutar a través de un navegador. Preferentemente, recomendamos el uso de Mozilla Firefox y Google Chrome, en su versión más actualizada.

A través de la interfaz web se pueden utilizar todas las funcionalidades de la aplicación, las cuales se describen a lo largo de este documento. A modo de resumen, el funcionamiento general es el siguiente:

1.1 RECEPCIÓN DE FICHEROS Y ANÁLISIS ESTÁTICO

En primer lugar, la aplicación recibe un fichero sospechoso de ser malware. Este fichero puede provenir de una subida manual a través de la interfaz web, o de un colector. Los colectores recogen periódicamente malwares de páginas web dedicadas al listado de malwares, tales como VirusTotal, Malc0de, etc.

Lo primero que hace la aplicación cuando recibe un fichero, es pasarle una serie de *scripts "estáticos"*. Son llamados estáticos porque el malware no se ejecuta en ningún momento mientras se le analiza con estos scripts. Con ellos, MARTA obtiene cierta *información específica del fichero*, como su tipo (exe, dll, docx, pdf, etc), o sus hashes (MD5, SHA1, Ssdeep, etc).

En función del tipo de fichero, se obtiene más información. Por ejemplo, para ejecutables, se obtiene toda la información en la cabecera del fichero, la tabla de directorios, las secciones del binario, los recursos y librerías que utiliza, etc. En cambio, para pdfs, se obtienen sus metadatos, javascripts embebidos, objetos internos, etc.

Una vez se han pasado los scripts estáticos, el fichero queda registrado en la base de datos de MARTA, junto con todos los datos obtenidos. A través de la interfaz web, se pueden consultar todos los ficheros registrados, y, por supuesto, sus datos.

1.2 ANÁLISIS DINÁMICO

En cualquier momento, se puede pedir un *análisis dinámico* de uno de los ficheros registrados. Esta es la funcionalidad más relevante de MARTA. Un análisis dinámico consiste en *infectar una máquina virtual* que tenga instalado un sistema operativo concreto con el fichero sospechoso de ser malware. Es decir, cuando se pide un análisis dinámico de un fichero, se clona una máquina virtual, se copia el fichero en ella y se ejecuta.

En el momento de pedir el análisis, se puede elegir qué máquina virtual se desea infectar (en función del sistema operativo), junto con otras opciones, como la conexión a internet de la máquina (salida por TOR o Internet Simulado), la duración máxima del análisis, si se desea hacer una simulación humana durante la ejecución (clics, tecleo, etc), entre otras.

Cada análisis dinámico se realiza clonando una máquina virtual “limpia”. Es decir, cuando se termina un análisis, la máquina virtual que se ha utilizado se destruye. Y en el siguiente análisis, se clona nuevamente una máquina virtual del sistema operativo elegido.

Lo que hace que el análisis dinámico sea la parte más relevante de MARTA es que durante la ejecución del fichero en la máquina virtual, hay un software monitorizando un conjunto factores clave para determinar el comportamiento del fichero: conexiones de red, claves de registro, ficheros, procesos, análisis sobre la memoria, etc.

A este software lo llamamos “*sandbox*”. Actualmente, MARTA integra dos *sandbox* diferentes: *Cuckoo* y *Joe*. En el momento de pedir un análisis dinámico de un fichero, se puede elegir qué *sandbox* se desea utilizar para el análisis. Cada *sandbox* monitoriza la ejecución del fichero de una forma diferente. Gracias a la integración de ambas, se puede determinar el comportamiento de *malwares* que de forma individual, una de las *sandbox* no podría determinar.

Cada vez que se realiza un análisis dinámico de un fichero, se registra en la base de datos de MARTA, junto con todos los factores claves para determinar el comportamiento de los ficheros extraídos por la *sandbox*. A través de la interfaz web, se pueden consultar todos los análisis realizados, y todos estos factores.

1.3 TRIANA

MARTA está integrada con *Triana*, Threat Intelligent Analysis. Es una herramienta de *búsqueda de información por Internet sobre malwares*.

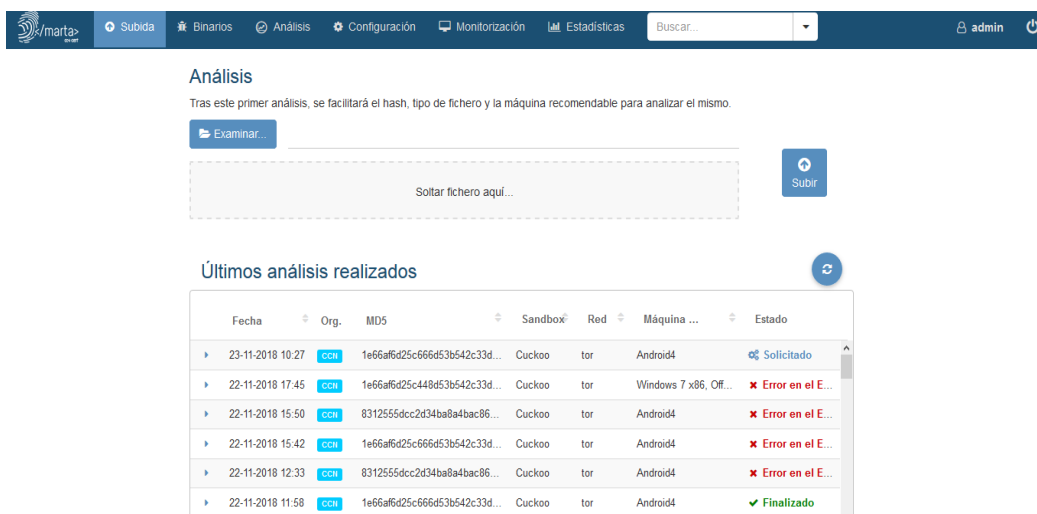
En el momento de pedir un análisis dinámico de un fichero, es posible seleccionar la opción Triana. De hacerlo, se realizará una búsqueda del MD5 del fichero en una serie de páginas de Internet dedicadas a la recopilación de información de *malwares*, tales como Virus Total o Malware (algunas de éstas páginas también son colectores). Cada una de estas páginas aporta información diversa acerca del malware correspondiente al MD5 buscado. Toda la información obtenida se almacena y se asocia al análisis dinámico.

2. VISTA DE ACCESO

Lo primero que se ve al acceder a la aplicación es una vista de acceso, en la que podemos introducir las *credenciales*:



Una vez introducidos, si son correctos, se accederá a la vista principal de la aplicación:



Además, se generará una *sesión*, de forma que no será necesario volver a introducir las credenciales si se vuelve a acceder a la aplicación, mientras esta dure, si no que accederemos directamente a la vista principal.

Mientras se esté trabajando con la aplicación, la sesión no caducará nunca, ya que se irá refrescando de forma automática. En caso de que no interactuemos con la aplicación de ninguna forma, la sesión caducará a los 15 minutos.

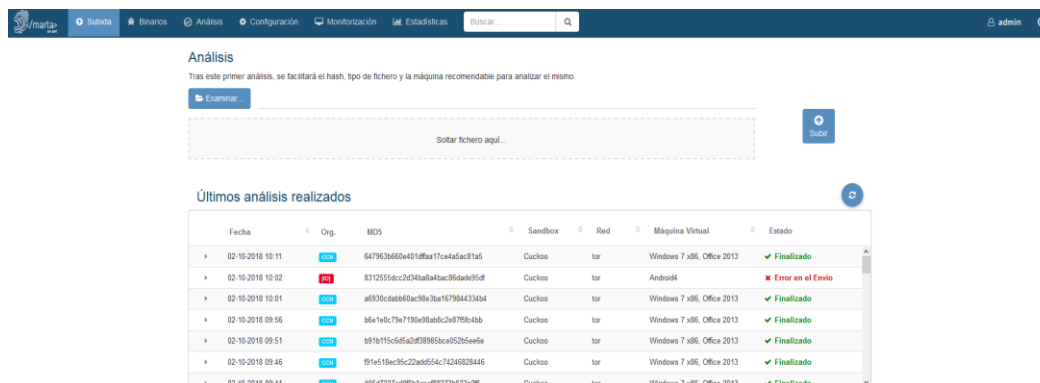
En la esquina superior derecha de la vista principal, se puede ver con qué usuario se está conectado. Además, se dispone de un *botón para desconectarse*, que anulará nuestra sesión inmediatamente:



Por seguridad, se recomienda utilizar este botón una vez hayamos terminado de utilizar la aplicación en lugar de cerrar la pestaña del navegador, aunque en caso de no hacerlo, la sesión caducará por si misma al cabo de 15 minutos.

3. SUBIDA DE BINARIOS

Esta es la vista que se muestra una vez introducidos los credenciales de acceso:

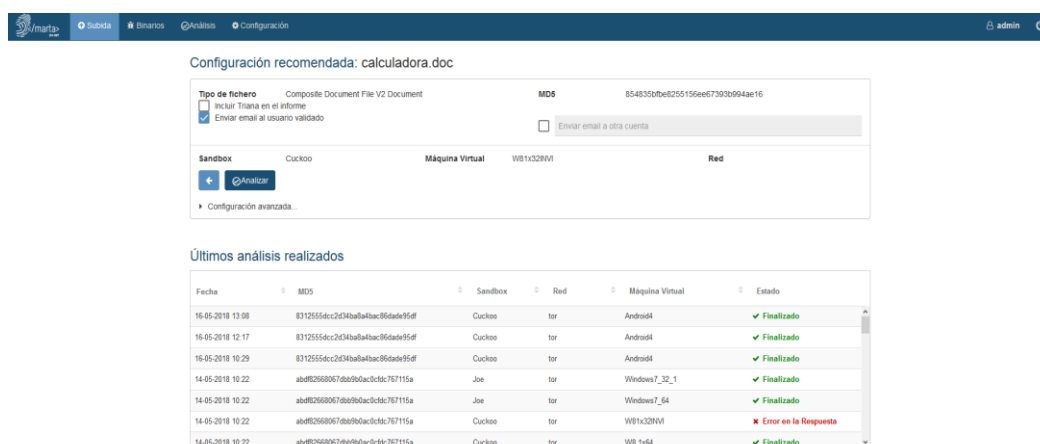


Consta de 6 pestañas:

- **Subida:** Es donde se elegirá el binario a analizar, se puede arrastrar o pulsar en el botón Examinar. Se muestra una lista con los últimos análisis realizados.
- **Binarios:** Muestra una lista con todos los ficheros subidos a MARTA. Permite hacer filtros rápidos sobre los ficheros, ver sus detalles (incluyendo los datos extraídos por los scripts estáticos), crear análisis dinámicos.
- **Análisis:** Muestra una lista con todos los análisis de ficheros realizados. Permite hacer filtros rápidos sobre los análisis, ver sus detalles (incluyendo todos los datos extraídos por la *sandbox*).
- **Configuración:** En esta pestaña se tienen las opciones de configuración de la aplicación. Reglas Yara, Organismos, Persistencia, Etiquetas, listas blancas, colectores y *Strings*. Algunas de las opciones solo serán visibles para perfiles con rol administrador.
- **Monitorización:** En esta pestaña se pueden ver los servicios y las máquinas de *Cuckoo* y *Joe*. Estas opciones solo serán visibles para perfiles con rol administrador.
- **Estadísticas:** En esta pestaña podemos ver las estadísticas que ya están configuradas por ejemplo: Uso de máquinas virtuales.

Cuando se tenga el binario seleccionado, se pulsará el botón subir y saldrá la pantalla de configuración para analizar el Binario.

Lo primero que se realiza es el análisis estático del Binario.



Configuración recomendada: calculadora.doc

Tipo de fichero Composite Document File V2 Document **MD5** 854835bfb8255156ee67393b994ae16

☐ Incluir Triana en el informe ☐ Enviar email a otra cuenta

☒ Enviar email al usuario validado

Sandbox Cuckoo **Máquina Virtual** W81x32INV **Red**

[←](#) [Analizar](#)

Configuración avanzada...

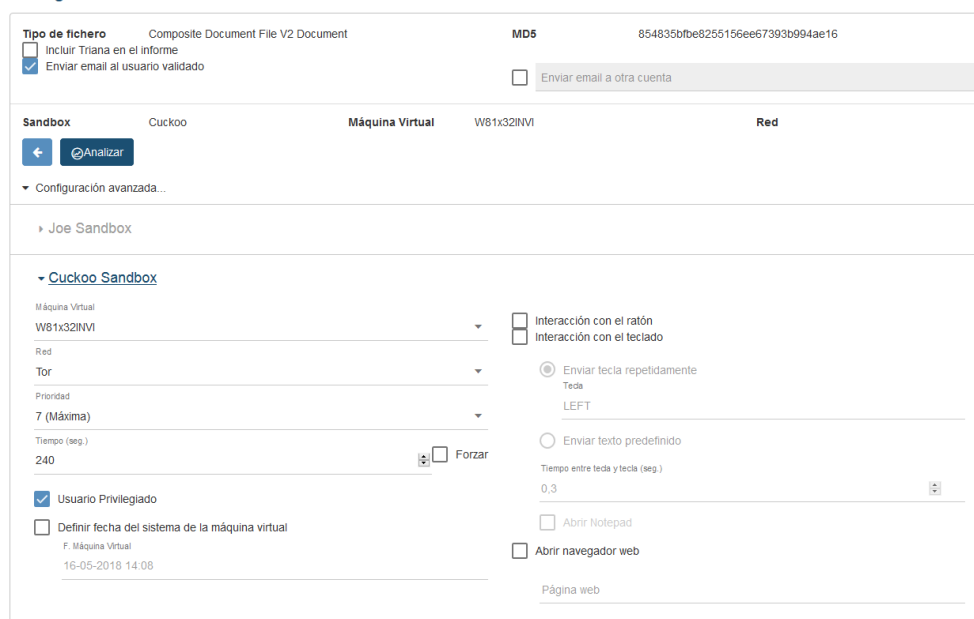
Últimos análisis realizados

Fecha	MD5	Sandbox	Red	Máquina Virtual	Estado
16-05-2018 13:08	8312555dc2d34ba8a8ac8fda95ef	Cuckoo	tor	Android4	Finalizado
16-05-2018 12:17	8312555dc2d34ba8a8ac8fda95ef	Cuckoo	tor	Android4	Finalizado
16-05-2018 10:29	8312555dc2d34ba8a8ac8fda95ef	Cuckoo	tor	Android4	Finalizado
14-05-2018 10:22	ab082668067db0b0ac8dc767115a	Joe	tor	Windows7_32_1	Finalizado
14-05-2018 10:22	ab082668067db0b0ac8dc767115a	Joe	tor	Windows7_64	Finalizado
14-05-2018 10:22	ab082668067db0b0ac8dc767115a	Cuckoo	tor	W81x32INV	Error en la Respuesta
14-05-2018 10:22	ab082668067db0b0ac8dc767115a	Cuckoo	tor	W8_1x64	Finalizado

Por defecto la aplicación elige la máquina virtual más adecuada para el análisis dinámico de ese binario.

Es importante resaltar que la máquina sugerida por defecto es la máquina que mostrará los resultados más completos y fiables puesto que no todos los sistemas soportan todas las funcionalidades de análisis ofrecidas.

Configuración recomendada: calculadora.doc



Configuración recomendada: calculadora.doc

Tipo de fichero Composite Document File V2 Document **MD5** 854835bfb8255156ee67393b994ae16

☐ Incluir Triana en el informe ☐ Enviar email a otra cuenta

☒ Enviar email al usuario validado

Sandbox Cuckoo **Máquina Virtual** W81x32INV **Red**

[←](#) [Analizar](#)

Configuración avanzada...

Joe Sandbox

Cuckoo Sandbox

Máquina Virtual W81x32INV

Red Tor

Prioridad 7 (Máxima)

Tiempo (seg.) 240 ☐ Forzar

☒ Usuario Privilegiado

☐ Definir fecha del sistema de la máquina virtual

F. Máquina Virtual 16-05-2018 14:08

☐ Interacción con el ratón

☐ Interacción con el teclado

☒ Enviar tecla repetidamente

Tecla LEFT

☐ Enviar texto predefinido

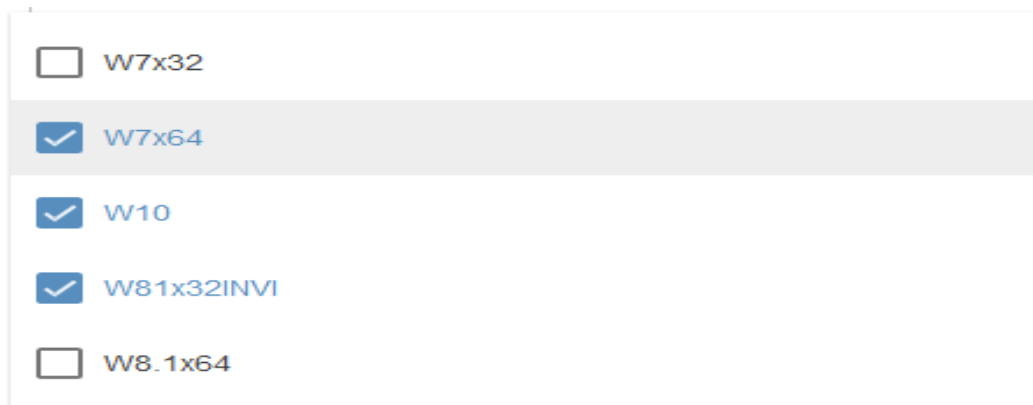
Tiempo entre tecla y tecla (seg.) 0,3

☐ Abrir Notepad

☐ Abrir navegador web

Página web

Aun así se puede elegir distintas máquinas virtuales de JOE o CUCKOO.



☐	W7x32
☒	W7x64
☒	W10
☒	W81x32INVI
☐	W8.1x64

- Tipo de Fichero: Es tipo de Fichero que se ha subido a la aplicación.
- En el campo **Enviar email a otra cuenta**, se puede indicar un correo electrónico, que recibirán el estado del análisis dinámico.
- Si marcamos el campo **Incluir Triana**, se realizará un análisis de Triana del MD5 del fichero seleccionado, y se asociará a los análisis dinámicos.
- Es posible seleccionar ambas *Sandbox* para realizar uno o varios análisis en cada una de ellas. Cada pestaña incluye todas las opciones de análisis de la *Sandbox*. Para cada *Sandbox* se debe seleccionar las máquinas virtuales sobre las que se quiere hacer análisis. Se realizará un análisis dinámico por cada máquina virtual seleccionada en cada *Sandbox*.

CUCKOO: podemos seleccionar las máquinas virtuales de *Cuckoo* sobre las que se desea realizar análisis dinámicos. Se podrá configurar la máquina virtual de las siguientes maneras.

- Tipos de Red:
 - *Internet Simulado* debe utilizarse para analizar *malwares* que para funcionar necesiten hacer conexiones a Internet, pero no se quiera que se hagan realmente. Con esta opción, la máquina estará totalmente aislada de internet, pero habrá un proceso que intentará hacer creer al malware que sí hay conexión. Resolverá correctamente las peticiones DNS que se hagan, y responderá a las peticiones a puertos conforme al protocolo estándar del puerto. Sin embargo, si el malware necesita descargarse datos de Internet o

requiere una respuesta específica a una petición, es muy posible que no funcione con Internet Simulado.

- Tor, en cambio, permite la salida a Internet de forma real, pero lo hace a través de la red Tor para evitar el rastreo del análisis de forma externa.
- Prioridad: Esta opción es útil si se pretende encolar múltiples análisis al mismo tiempo. Cuando Cuckoo termine un análisis y vaya a seleccionar de la cola de análisis el siguiente, siempre seleccionará primero el más prioritario. La escala de prioridades consta de 7 niveles, siendo 1 el menos y 7 el más prioritario.
- Duración Máxima: En el campo Timeout se puede indicar el tiempo máximo en segundos que durará el análisis. Si la ejecución del malware no ha terminado una vez cumplido este tiempo, la máquina virtual se detendrá inmediatamente. Marcando la opción Forzar, la máquina virtual seguirá en ejecución y siendo monitorizada durante el tiempo indicado en Timeout, incluso si la ejecución del malware ha terminado.
- Usuario Privilegiado: Marcando esta opción, el malware se ejecutará con privilegios de administrador.
- Simulación Humana: Cuckoo dispone de una serie de opciones que permiten simular el comportamiento humano durante la ejecución del malware.
- Interacción con el ratón: Permite mover el ratón y hacer clic en las ventanas emergentes.
- Interacción con el Teclado: Permite simular la pulsación de una tecla concreta cada cierto tiempo de forma constante, o la escritura de un texto predefinido (Lorem Ipsum), durante toda la ejecución de la máquina virtual. Si no se marca el campo Abrir Notepad, la escritura se hará sobre el escritorio, o sobre las ventanas que se abran durante la ejecución del malware. En cambio, si se marca, se abrirá la aplicación Notepad y se escribirá en ella.
- Navegación web: Permite abrir el navegador web y acceder a una página web en concreto durante la ejecución de la máquina virtual.
- Fecha y Hora del Sistema de la Máquina Virtual: Permite establecer la fecha y hora del sistema operativo de la máquina virtual justo antes de ejecutar el malware. Esto es útil para analizar malwares cuya ejecución depende de la fecha y hora.

▼ Cuckoo Sandbox

Máquina Virtual	W10, W81x32INVI	☐ Interacción con el ratón
Red	Tor	☐ Interacción con el teclado
Prioridad	7 (Máxima)	☒ Enviar tecla repetidamente
Tiempo (seg.)	240	Tecla LEFT
	☐ Forzar	☐ Enviar texto predefinido
☒ Usuario Privilegiado		Tiempo entre tecla y tecla (seg.) 0,3
☐ Definir fecha del sistema de la máquina virtual		☐ Abrir Notepad
F. Máquina Virtual 16-05-2018 14:28		☐ Abrir navegador web
		Página web

JOE: se puede seleccionar las máquinas virtuales de JOE sobre las que se quiere realizar análisis dinámicos. Se puede elegir, si se pretende que sea por la red TOR o Internet Simulado y el tiempo de la máquina virtual para el análisis.

▼ Joe Sandbox

Máquina Virtual	Windows 7 x64, Office 2013
Red	Tor
Tiempo (seg.)	250

4. PESTAÑA DE BINARIOS

Esta pestaña está diseñada para facilitar todas las gestiones relativas a los ficheros subidos a MARTA.

Número total de registros: 503

Fecha	Organismo	MD5	Fichero	Tipo	A. Estático	Etiquetas	VT
16-05-2018 14:30	CCN	007a94cc8416764764b18a0484368	2016 incidents.csv	ISO-8859 text, with very long lines	En Proceso		
16-05-2018 10:30	CCN	8312555dc2d34ba8a8ac86da95df	Line.apk	Java archive data (JAR)	✓ Completo		
14-05-2018 07:24	CCN	e10e49576c4602d4a80b49f9ac3da6	RanombraMacro.docm	Microsoft OOXML	✓ Completo		
11-05-2018 14:16	CCN	c2969a0D06ac38a498a8f1252a308	828235058.docx	Microsoft Word 2007+	✓ Completo		
11-05-2018 12:17	CCN	90a9b6896a2b7c18b583295c232	816402882.docx	Microsoft Word 2007+	✓ Completo		
11-05-2018 12:04	CCN	1d2aeeedac55705d265ad779521e9	816402881.docx	Microsoft Word 2007+	✓ Completo		
11-05-2018 11:47	CCN	a83bc78178abed3837a3d24137b532	803749967.docx	Microsoft Word 2007+	✓ Completo		
11-05-2018 10:49	CCN	94e53d975081ce20b8a4362b7e5	803133090.docx	Microsoft Word 2007+	✓ Completo		
11-05-2018 10:00	CCN	929158a7b4511875e8dc7e544e109f6	803984841.docx	Microsoft Word 2007+	✓ Completo		
11-05-2018 09:57	CCN	46722c4961a6ec29e34a09b2349b7ae	802919495.docx	Microsoft Word 2007+	✓ Completo		
11-05-2018 09:50	CCN	36c5904787c1da65c4e6b7b4a4b96c4	802895137.docm	Microsoft Word 2007+	✓ Completo		
10-05-2018 17:40	CCN	157502218abfa36c555856c4688940	notepad.exe	PE32+ executable (GUI) x86-64, for MS Windows	✓ Completo		
10-05-2018 16:24	CCN	104c790af8181fa15e89716417ee422	systemd.exe	PE32+ executable (GUI) x86-64, for MS Windows	✓ Completo		

4.1 LISTADO

La pestaña muestra una *lista* a modo de resumen con *todos los ficheros* subidos a MARTA. Dado que el caso más común es que se suba una gran cantidad de binarios a la aplicación, la lista ordenada por fecha de subida del fichero, de más reciente a menos reciente.

En la lista se muestran los *atributos* más significativos de cada fichero: la fecha en la que se subió, su Organismo (solo usuario Admin) su MD5, su nombre de fichero, su tipo de fichero, el estado del Análisis Estático, sus etiquetas asociadas y su peligrosidad. Es posible *filtrar* por cualquiera de estos campos con los cuadros de filtro de cada una de las columnas:

Nº total de registros: 1

Fecha	Organismo	MD5	Fichero	Tipo	A. Estático	Etiquetas	Pelig...
29-08-2018 14:19	CCN	a3e083f601d509bcc32d9b1ce8b2...	irc.exe.binary	PE32 executable (GUI) Intel 8038...	✓ Completo	#TST #WSKI #NOPU ...	43%

En esta lista, y en todas las listas de la aplicación, es posible hacer un clic en uno de los campos para acceder a una pequeña información.

Nº total de registros: 114

Fecha: 25-09-2018 14:09

Organismo: 64ba6802903e19938c32ac3d59a4665

MD5: 64ba6802903e19938c32ac3d59a4665_sample.rf...

Fichero: Rich Text Format data

Tipo: Rich Text Format data

A. Estático: Completo

Etiquetas: #gen2 #TST #NOCPU #A-CD #Gen...

Peligrosidad: 5

Tamaño: 5 856 964 bytes

Nombre de Fichero: 64ba6802903e19938c32ac3d59a4665_sample.rf binary bin

Fuente de Peligrosidad: N/D

[virus total](#)

[Reanalizar](#)

Análisis Dinámicos Realizados (8)

Organismo	Fecha	Etiquetas	Estado	Sandbox	Cuckoo
Máquina Virtual	25-09-2018 12:11	#A-CD #TST #NOCPU	Finalizado	Sandbox	Cuckoo
Máquina Virtual	21-09-2018 13:03	#A-CD #TST #NOCPU #Gen2	Finalizado	Sandbox	Joe
Máquina Virtual	21-09-2018 13:03		Error en la Respuesta	Sandbox	Joe
Máquina Virtual	21-09-2018 13:03		Error en la Respuesta	Sandbox	Cuckoo
Máquina Virtual	21-09-2018 13:03		Finalizado	Sandbox	Cuckoo
Máquina Virtual	21-09-2018 13:03		Finalizado	Sandbox	Cuckoo
Máquina Virtual	21-09-2018 13:03		Finalizado	Sandbox	Cuckoo
Máquina Virtual	21-09-2018 13:03		Finalizado	Sandbox	Cuckoo

Al desplegar el binario se puede ver información del binario y además los análisis dinámicos realizados para dicho binario.

Se destaca que en el despliegue se dispone del botón de Reanalizar.

- **Reanalizar Binario:** Abre la vista de reanálisis del fichero seleccionado. Esta vista permite lanzar o programar uno o varios análisis dinámicos de un fichero.

Reanálisis

Configuración recomendada: icmp.exe

Tipo de fichero: PE32 executable (console) Intel 80386, for MS Windows

MD5: 190fa525529da5d7b0b13408664a9b79

Fecha y hora de inicio del primer reanálisis: 16-05-2018 15:54

Número de Análisis: 1

Intervalo (Horas): 1 h

Intervalo (Minutos): 00 m

☐ Incluir Triana en el informe

☒ Enviar email al usuario validado

☐ Enviar email a otra cuenta

Sandbox: Cuckoo

Máquina Virtual: W81x32INVI

Red:

[Reanalizar](#)

▼ Configuración avanzada...

Joe Sandbox

▼ Cuckoo Sandbox

Máquina Virtual: W81x32INVI

Red: Tor

Prioridad: 7 (Máxima)

Tiempo (seg.): 240

☐ Forzar

☐ Interacción con el ratón

☐ Interacción con el teclado

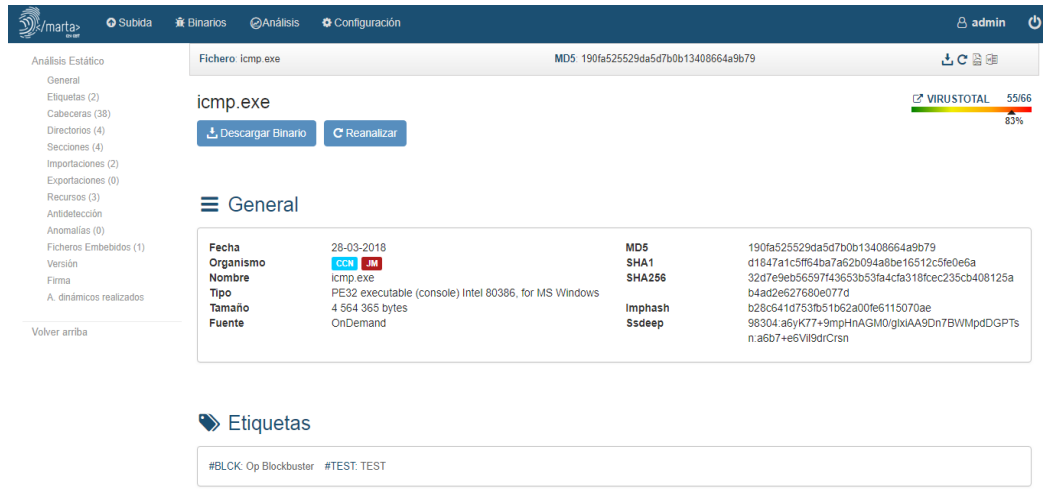
☒ Enviar tecla repetidamente

Tecla: LEFT

☐ Enviar texto predefinido

Tiempo entre tecla y tecla (seg.):

Si se pulsa sobre el MD5 se verá el detalle del análisis estático del binario.



The screenshot shows the MARTA application interface. The top navigation bar includes 'Subida', 'Binarios', 'Análisis', and 'Configuración'. The left sidebar lists various analysis categories. The main content area displays the static analysis details for the file 'icmp.exe' (MD5: 190fa525529da5d7b0b13408664a9b79). It includes a 'General' tab with fields for 'Fecha', 'Organismo', 'Nombre', 'Tipo', 'Tamaño', and 'Fuente'. A 'VirusTotal' score of 55/66 is shown. Below the general information, there is a section for 'Etiquetas' (Tags) with the value '#BLCK: Op Blockbuster #TEST: TEST'.

Desde esta pantalla o desde la anterior se podrá acceder al análisis dinámico del binario.

 A. dinámicos realizados 

Fecha	MD5	Sandbox	Máquina Virt...	Red	Estado	Etiquetas
10-05-2018 13:07	190fa525529da5d7b0b13408664a...	Cuckoo	W81x32INVI	tor	Finalizado	
09-05-2018 13:33	190fa525529da5d7b0b13408664a...	Joe	Windows7_32_1	tor	Finalizado	
09-05-2018 13:33	190fa525529da5d7b0b13408664a...	Cuckoo	W81x32INVI	tor	Finalizado	
09-05-2018 13:33	190fa525529da5d7b0b13408664a...	Cuckoo	W7x64	tor	Finalizado	
09-05-2018 13:33	190fa525529da5d7b0b13408664a...	Joe	Windows7_64	tor	Finalizado	
09-05-2018 13:33	190fa525529da5d7b0b13408664a...	Cuckoo	W8.1x64	tor	Finalizado	
09-05-2018 13:06	190fa525529da5d7b0b13408664a...	Joe	Windows7_64	tor	Finalizado	
09-05-2018 13:06	190fa525529da5d7b0b13408664a...	Cuckoo	W8.1x64	tor	Finalizado	
09-05-2018 13:06	190fa525529da5d7b0b13408664a...	Joe	Windows7_32_1	tor	Finalizado	
09-05-2018 13:06	190fa525529da5d7b0b13408664a...	Cuckoo	W81x32INVI	tor	Finalizado	

4.2 ACCIONES SOBRE LOS FICHEROS

En la parte superior de la pantalla se dispone de las siguientes acciones que se pueden realizar sobre un binario:



Permite realizar las siguientes gestiones sobre uno o varios ficheros:

- **Descargar Binario:** Descarga el fichero seleccionado. Esta acción debe realizarse con precaución ya que el fichero descargado podría ser un malware. El fichero se descarga con un nombre que está compuesto por el MD5 del fichero más el nombre de la muestra con su extensión y se le da extensión bin para evitar que lo ejecutemos por error al descargarlo.
- **Recargar:** Recarga la página por si no hubiera cargado todos los binarios.
- **Eliminar:** Elimina el fichero seleccionado, y todos sus análisis. Pide confirmación antes de eliminar.

4.3 DETALLE DE UN BINARIO (ANÁLISIS ESTÁTICO)

Esta vista contiene toda la *información* relativa a un *fichero* subido a MARTA.

Dispone de múltiples opciones de menú:

- **General:** Muestra información básica acerca del fichero.
- **Etiquetas:** Muestra y permite gestionar las etiquetas asociadas al fichero.

En función del tipo de fichero, aparecerán unas opciones u otras en el menú, diferente para cada tipo, mostrando toda la información extraída por los *scripts estáticos*.

1. **Fichero Ejecutable:** Aparece sólo si el fichero es un ejecutable, como por ejemplo un exe, un msi, un bat, etc.
 - **Cabeceras:** Muestra las cabeceras del fichero
 - **Directorios:** Muestra información sobre la tabla de directorios del ejecutable.
 - **Secciones:** Muestra las secciones del fichero.
 - **Importaciones:** Esta sección se compone de dos partes:
 - **DLLs:** Muestra información sobre las librerías importadas por el ejecutable, y las funciones de dichas librerías.
 - **Bound DLLs:** Muestra información sobre las librerías *bindeadas* al ejecutable, y las funciones de dichas librerías.

- **Exportaciones:** Muestra información sobre los *exports* del ejecutable.
- **Recursos:** Muestra información sobre los recursos del ejecutable.
- **Antidetección:** Muestra información sobre las técnicas antidetección del ejecutable.
- **Anomalías:** Muestra información sobre las anomalías del ejecutable.
- **Ficheros Embebidos:** Muestra información sobre los ficheros embebidos del ejecutable.
- **Versión:** Muestra información sobre la versión del ejecutable.
- **Firma:** Muestra información sobre la firma del ejecutable.
- **Análisis Dinámicos Realizados:** Muestra todos los análisis dinámicos realizados y programados del fichero.

2. **Fichero PDF:** Aparece sólo si el fichero es un pdf.

- **Datos:** Muestra datos generales acerca del documento pdf.
- **Versiones:** Muestra las versiones del documento pdf. Seleccionando cada versión, muestra sus datos generales, sus metadatos y sus objetos embebidos (Se permite analizar en MARTA y descargar cada uno de los objetos que lo componen de forma independiente).

3. **Fichero Office:** Aparece sólo si el fichero es un documento de Microsoft Office, como por ejemplo, un doc, un docx, un xlsx, un pptx, etc.

- **Datos:** Muestra datos generales acerca del documento, y sus metadatos.
- **Versiones:** Muestra las versiones del documento Office. Seleccionando la versión, muestra sus datos generales, sus metadatos y sus objetos (Se permite analizar en MARTA y descargar cada uno de los objetos que lo componen de forma independiente).

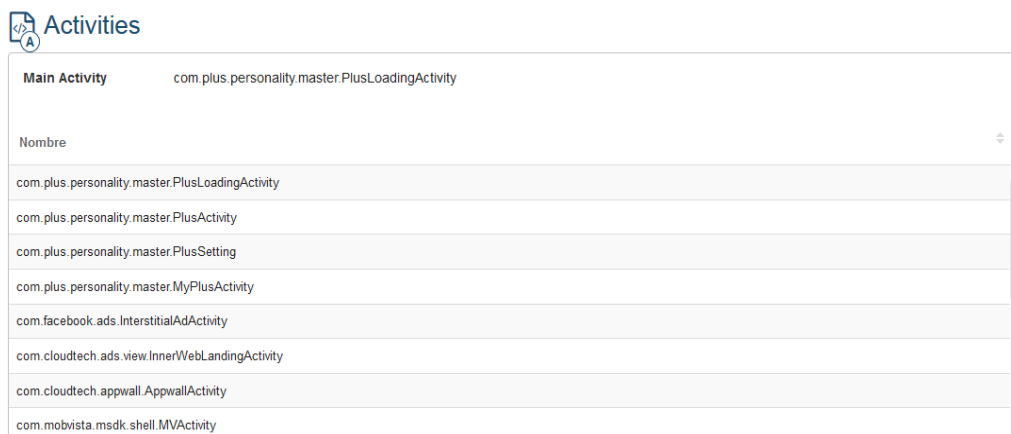
4. **Fichero OpenOffice:** Aparece sólo si el fichero es un documento de OpenOffice, como por ejemplo, un odt.

- **Datos:** Muestra datos generales acerca del documento OpenOffice

- **Ficheros:** Muestra los ficheros embebidos en el documento OpenOffice, y permite descargarlos.

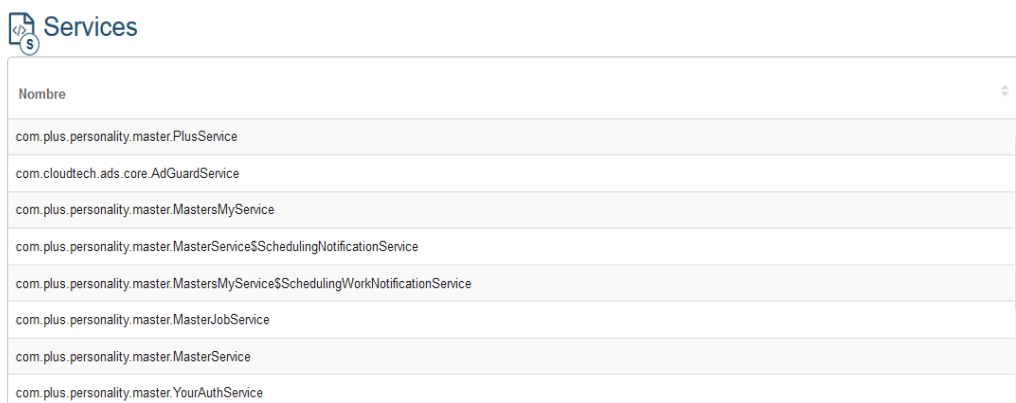
5. **Fichero Android:** Aparece sólo si el fichero es Android extensión .apk

- **Activities:** Muestra datos de todas las clases *Activities* que encuentra.



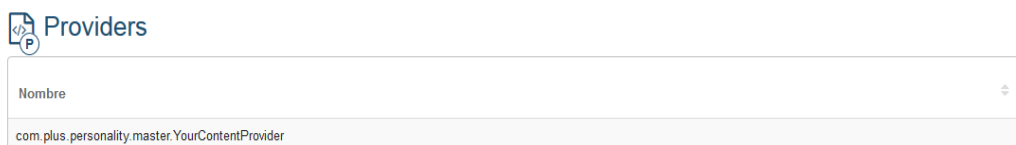
Activities	
Nombre	
Main Activity	com.plus.personality.master.PlusLoadingActivity
	com.plus.personality.master.PlusLoadingActivity
	com.plus.personality.master.PlusActivity
	com.plus.personality.master.PlusSetting
	com.plus.personality.master.MyPlusActivity
	com.facebook.ads.InterstitialAdActivity
	com.cloudtech.ads.view.InnerWebLandingActivity
	com.cloudtech.appwall.AppwallActivity
	com.mobvista.msdk.shell.MVActivity

- **Services:** Muestra datos de las clases que encuentra.



Services	
Nombre	
	com.plus.personality.master.PlusService
	com.cloudtech.ads.core.AdGuardService
	com.plus.personality.master.MastersMyService
	com.plus.personality.master.MasterService\$SchedulingNotificationService
	com.plus.personality.master.MastersMyService\$SchedulingWorkNotificationService
	com.plus.personality.master.MasterJobService
	com.plus.personality.master.MasterService
	com.plus.personality.master.YourAuthService

- **Providers:** Muestra datos de las clases que encuentra.



Providers	
Nombre	
	com.plus.personality.master.YourContentProvider

- **Receivers:** Muestra datos de las clases que encuentra.

Receivers

Nombre
com.plus.personality.master.MyPlusRecive
com.plus.personality.master.AplnInstallReceiver

- **Tipos de Fichero:** Muestra la ruta de fichero y el tipo de Fichero.

Tipos de fichero

Ruta fichero	Tipo fichero
res/drawable/mobvista_nativex_full_land_close.xml	Android binary XML
res/drawable-hdpi-v4/mobvista_cm_progress.png	PNG image data, 710 x 4, 8-bit/color RGB, non-interlaced
res/drawable/mobvista_cm_backward.xml	Android binary XML
res/drawable/mobvista_cm_forward.xml	Android binary XML
res/drawable-xxhdpi-v4/gold_shop.png	PNG image data, 86 x 86, 8-bit/color RGBA, non-interlaced
res/drawable-hdpi-v4/mobvista_wall_tab_shape.9.png	PNG image data, 12 x 12, 8-bit/color RGBA, non-interlaced
res/drawable-hdpi-v4/mobvista_cm_tail.png	PNG image data, 480 x 3, 8-bit colormap, non-interlaced
res/drawable-hdpi-v4/mobvista_wall_install_download.png	PNG image data, 48 x 48, 8-bit colormap, non-interlaced
res/layout/admob_ad.xml	Android binary XML
res/drawable/mobvista_wall_shape_bg.xml	Android binary XML

- **Permisos:** Muestra los permisos declarados y solicitados.

Permisos

Permisos declarados (0)

Permisos solicitados (0)

- **Cadena de certificados:** Muestra los siguientes campos de los certificados, Número de Serie, MD5, SHA1, Valido desde, Valido Hasta.

Cadena de Certificados

Nº de Serie	MD5	SHA1	Válido hasta	Válido desde
	248f2387daf166da09d3b69dcfdbfeda	b2a75e66e28100ab767c794cacb916ff...		

4.4 ETIQUETAS

A un binario se le pueden asignar etiquetas manualmente o se pueden ver las etiquetas asignadas por el Análisis.



Si se quiere asignar etiquetas manualmente se puede realizar de dos maneras distintas:

1.- Si se conoce la etiqueta que se quiere asignar se empieza a escribir y aparecerá una lista, se selecciona la que se quiere y automáticamente se quedara grabada.



En el caso de que se quisiera quitar del análisis la etiqueta solo se tendría que hacer clic en el aspa de la etiqueta asignada manualmente, y quedaría eliminada del binario automáticamente.



2.- La otra opción para asignar una etiqueta o varias a la vez, se realiza de la siguiente manera.



Se realiza clic sobre el icono y nos aparecerá la siguiente lista de:



Etiquetas disponibles



Filtrar etiquetas...

#A-16	APT-16
#A-17	APT17 - Aurora Panda
#A-28	APT28 - Sofacy
#A-29	APT-29
#A-30	APT-30
#A-AG	APT_Agent.BTZ
#A-BT	APT - BlueTermite
#A-CD	APT - Codoso
#A-CK	APT - Carbanak
#A-CP	APT - Casper
#A-CT	APT - Careto
#A-D2	APT - Duqu2
#A-DB	APT - Derusbi

Se puede seleccionar una o varias y solo con arrastrarlas a la parte de “*Asignadas manualmente*”, se quedarían grabadas automáticamente.

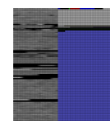
4.5 ENTROPÍA

La *entropía* de un archivo, en especial, de las secciones de un ejecutable, es el nivel de caos en la información que contiene, es decir, cuánto es de diferente. Esto es un indicativo que un fichero, o parte de él, está cifrado, comprimido o empaquetado lo que da una pista sobre las intenciones de su desarrollador para ocultar la funcionalidad del programa.

Secciones

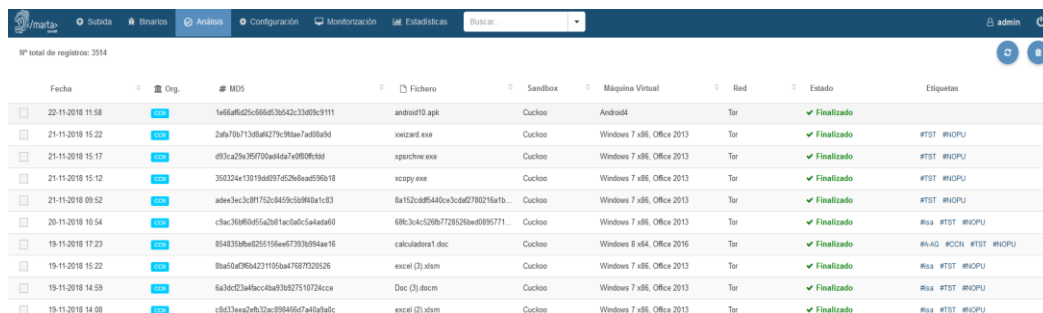
Nombre	Dirección Virtual	Tamaño Virtual	Tamaño	Entropía
CODE	0x1000	0x722c	29696	6.51167
DATA	0x9000	0x218	1024	3.1517
BSS	0xa000	0xa899	0	0
.idata	0x15000	0x864	2560	4.17386
.tls	0x16000	0x8	0	0
.rdata	0x17000	0x18	512	0.20692
.reloc	0x18000	0x5cc	1536	6.44309
.rsrc	0x19000	0x1400	5120	3.80433

Entropía



5. PESTAÑA DE ANÁLISIS

Esta pestaña está diseñada para facilitar todas las gestiones relativas a los análisis dinámicos.

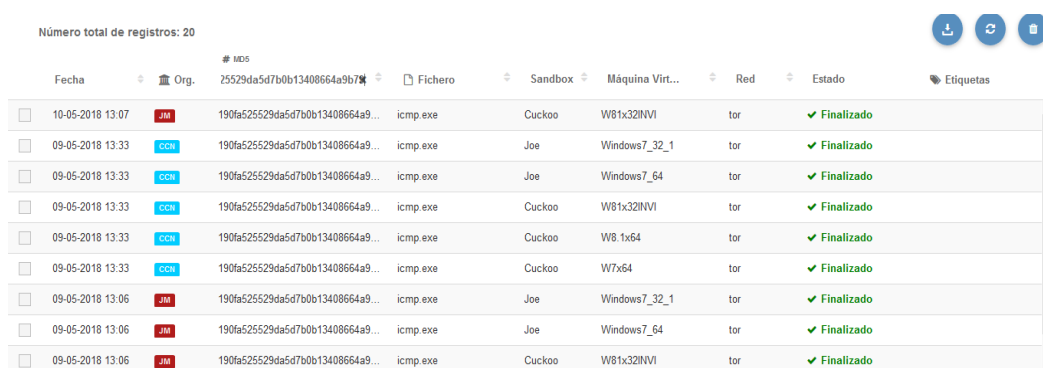


Fecha	Org.	MD5	Fichero	Sandbox	Máquina Virtual	Red	Estado	Etiquetas
22-11-2018 11:58	CCN	1e6fa625c666d3642c3369c9111	android10.apk	Cuckoo	Android	Tor	Finalizado	
21-11-2018 15:22	CCN	2afa70b713d8a4279c96aa7a08a6d	winzard.exe	Cuckoo	Windows 7 x86, Office 2013	Tor	Finalizado	#TST #NGPU
21-11-2018 15:17	CCN	d93ca29c365703a64da7c0806dd	xpsrchw.exe	Cuckoo	Windows 7 x86, Office 2013	Tor	Finalizado	#TST #NGPU
21-11-2018 15:12	CCN	36324e13615d6976c2b6ead96b18	xcopy.exe	Cuckoo	Windows 7 x86, Office 2013	Tor	Finalizado	#TST #NGPU
21-11-2018 09:52	CCN	ade33ec3c81752c845c3b9d8a1c83	8a152cd45440ca3cd42780216a1b...	Cuckoo	Windows 7 x86, Office 2013	Tor	Finalizado	#TST #NGPU
20-11-2018 10:54	CCN	c9ac368b0d5a2b1acba0c5a1a6d0	68c3c4c520b7728526ae089571...	Cuckoo	Windows 7 x86, Office 2013	Tor	Finalizado	#sa #TST #NGPU
19-11-2018 17:23	CCN	854833abae82515ee67393b994ae16	calculadora1.doc	Cuckoo	Windows 8 x64, Office 2016	Tor	Finalizado	#AAG #CCN #TST #NGPU
19-11-2018 15:22	CCN	8ba5da796b4231105b47687020526	excel (3).xlsm	Cuckoo	Windows 7 x86, Office 2013	Tor	Finalizado	#sa #TST #NGPU
19-11-2018 14:59	CCN	6a36c2e3afacc4ba93b037510724ce	Doc (3).docm	Cuckoo	Windows 7 x86, Office 2013	Tor	Finalizado	#sa #TST #NGPU
19-11-2018 14:08	CCN	c8d33ea2d6b32ac398466d7a4da8a0c	excel (2).xlsm	Cuckoo	Windows 7 x86, Office 2013	Tor	Finalizado	#sa #TST #NGPU

5.1 LISTADO

La pestaña muestra una *lista* a modo de resumen con *todos los análisis dinámicos* de MARTA. Al igual que la lista de ficheros de la pestaña de binarios, la lista esta ordenada por fecha del análisis, de más reciente a menos reciente.

En la lista se muestran los *atributos* más significativos de cada análisis: la fecha en la que realizó, la organización (solo usuario Admin) a la que pertenece el análisis, el MD5 y el nombre del fichero analizado, la *sandbox*, la máquina virtual, el tipo de red, el estado actual del análisis y sus etiquetas asociadas. Al igual que en la lista de ficheros, es posible *filtrar* por cualquiera de estos campos:



Fecha	Org.	MD5	Fichero	Sandbox	Máquina Virtual	Red	Estado	Etiquetas
10-05-2018 13:07	JM	190fa525529da5d7b0b13408664a9...	icmp.exe	Cuckoo	W81x32NVI	tor	Finalizado	
09-05-2018 13:33	CCN	190fa525529da5d7b0b13408664a9...	icmp.exe	Joe	Windows7_32_1	tor	Finalizado	
09-05-2018 13:33	CCN	190fa525529da5d7b0b13408664a9...	icmp.exe	Joe	Windows7_64	tor	Finalizado	
09-05-2018 13:33	CCN	190fa525529da5d7b0b13408664a9...	icmp.exe	Cuckoo	W81x32NVI	tor	Finalizado	
09-05-2018 13:33	CCN	190fa525529da5d7b0b13408664a9...	icmp.exe	Cuckoo	W8.1x64	tor	Finalizado	
09-05-2018 13:33	CCN	190fa525529da5d7b0b13408664a9...	icmp.exe	Cuckoo	W7x64	tor	Finalizado	
09-05-2018 13:06	JM	190fa525529da5d7b0b13408664a9...	icmp.exe	Joe	Windows7_32_1	tor	Finalizado	
09-05-2018 13:06	JM	190fa525529da5d7b0b13408664a9...	icmp.exe	Joe	Windows7_64	tor	Finalizado	
09-05-2018 13:06	JM	190fa525529da5d7b0b13408664a9...	icmp.exe	Cuckoo	W81x32NVI	tor	Finalizado	

5.2 ESTADOS DE UN ANÁLISIS

Desde que se pide o se programa un análisis dinámico hasta que finaliza, pasa por una serie de diversos estados que se describen a continuación:

- **Solicitado:** El análisis ha sido enviado a la *sandbox*, y ésta aún no ha enviado respuesta. Esto puede deberse a que el análisis se esté ejecutando (usualmente conlleva varios minutos), o a que la *sandbox* tenga otros análisis por delante.
- **Error en el Envío:** Se ha producido un error en la comunicación entre el servidor de MARTA y la *sandbox* en el momento del envío del análisis. Un análisis en este estado no llegará a ejecutarse nunca.
- **Finalizado:** El análisis se ha ejecutado correctamente y el servidor de MARTA ha recogido los datos del análisis, los cuales pueden ser consultados a través de la interfaz web.
- **Error en el Análisis:** Se ha producido un error durante la ejecución del análisis.
- **En Progreso:** El análisis está ejecutándose.
- **Error en la Respuesta:** El análisis se ha ejecutado correctamente en la *sandbox*, pero se ha producido un error en la comunicación entre el servidor de MARTA y la *sandbox* en el momento del envío de los datos del análisis.
- **Pendiente de Envío:** El análisis aún no ha sido enviado a su *sandbox* correspondiente. Esto puede deberse a que el análisis esté programado para una fecha y hora posterior a la actual, o a que el proceso que envía los análisis a las *sandbox* (el cual se ejecuta periódicamente cada poco tiempo) esté a punto de ejecutarse.
- **Anulado:** Cuando se ha anulado un análisis.

5.3 ACCIONES SOBRE LOS ANÁLISIS

Realizando un clic se puede ver las siguientes opciones del análisis:

☐	09-05-2018 13:33	CCN	190fa525529da5d7b0b13408664a...	icmp.exe	Joe	Windows7_64	tor	Finalizado
SHA256	32d7e9eb56597f43653b53fa4cfa318fcec235cb408125ab4ad2e627680e077d					Usuario	admin	
Tipo de Fichero	PE32 executable (console) Intel 80386, for MS Windows					 Reanalizar		
Descargar Informe	 PDF  DOCX							

General

Fecha	10-05-2018 13:51	Comentarios	
Organismo	CCN		
Estado	Finalizado		
Configuración del Análisis			
Sandbox	Cuckoo	Interacción con el ratón	No
Máquina Virtual	W81x32INVI	Interacción con el teclado	No
Red	tor	Enviar tecla repetidamente	No
Prioridad	7	Tecla	No
Usuario Privilegiado	Si	Enviar texto predefinido	No
Tiempo (seg.)	240	Tiempo entre tecla y tecla (seg.)	No
Forzar	No	Abrir Notepad	No
F. Máquina Virtual		Abrir navegador web	No
		Página web	

- **Etiquetas:** Aparecerán las etiquetas asociadas a ese análisis.

Etiquetas

Asignadas por los Análisis (2):

REVE reverse tcp
RWMC Ransom.WannaCry

- **Procesos:** Los procesos detectados durante el análisis, subprocessos y PID asociado a cada proceso y subprocesso.

Procesos

Process Name / Handle name	Process Path / Handle Type	PID	Parent	Arguments	Estado
lsass.exe	C:\Windows\System32\lsass.exe	536	436		✓
WINWORD.EXE	C:\Program Files\Microsoft Office\Office15\WINWORD.EXE	1556	3892		✓

- **Mutex:** Se usan en programación concurrente para evitar que ejecute más de un proceso a la vez en la sección crítica. La sección crítica es el fragmento de código donde puede modificarse un recurso compartido.

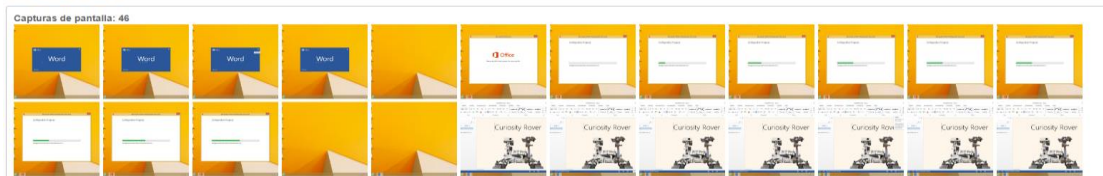
Mutex

PID	Proceso	Mutex
2168	powershell.exe	Local\ZonesCounterMutex RasPbFile Local\ZonesLockedCacheCounterMutex Local\ZoneAttributeCacheCounterMutex Local\ZonesCacheCounterMutex Global_.net clr networking

- **Evidencias:** Se verán las capturas de pantalla de las evidencias y muestra una lista con diferentes recursos obtenidos por la *sandbox* durante la ejecución del análisis.

Evidencias

Capturas de pantalla: 46



Fichero

files/141fd0137b6fe170_-516402547.dotx	📄
files/4826cd860af884d_-vrs(b39ea0a5-cc1c-4486-8059-6c3d079d9526).tmp	📄
files/b3d510ef04275ca8_excludedictionaries0c0a.lex	📄
files/b419d9625f10a3a9_-vrs(712ee564-3132-42a4-a97a-5d8fd111285e).tmp	📄
reboot.json	📄
reports/report.json	📄
reports/static_report.json	📄
shots.zip	📄

- **Red:** Muestra información acerca de las conexiones de red realizadas durante el análisis, agrupadas por protocolo TCP/UDP, DNS, HTTP, ICMP, IRC, SMTP.

Red

● IP Externa ● Simulación Humana ● Sandbox ● Gateway ● DNS Simulado

TCP / UDP (6) DNS (1) HTTP (0) ICMP (0) IRC (6) SMTP (0)

IP Origen	Puerto Origen	IP Destino	Puerto Destino	Protocolo
192.168.57.2 - Sandbox	49168	195.234.61.188 - Externa	6667	TCP
192.168.57.1 - Gateway	5353	192.168.57.2 - Sandbox	61016	TCP
192.168.57.2 - Sandbox	61016	192.168.57.1 - Gateway	53	TCP
195.234.61.188 - Externa	6667	192.168.57.2 - Sandbox	49168	TCP
192.168.57.1 - Gateway	5353	192.168.57.2 - Sandbox	61016	UDP
192.168.57.2 - Sandbox	61016	192.168.57.1 - Gateway	53	UDP

- **Geolocalización:** Muestra los dominios y direcciones IP del análisis, si se seleccionan de forma individual o múltiple los registros es posible ver en la parte derecha la geolocalización de los mismos.

Geolocalización

Dominio	IP
☐ irc.chathispano.com	
☒	195.234.61.188 - Externa

Whois

Use of the encoding pragma is deprecated at /usr/bin/whois line 80.
 Process query: '195.234.61.188'
 Query recognized as IPv4.
 Querying whois.ripe.net:43 with whois.

% This is the RIPE Database query service.
 % The objects are in RPSL format.
 %
 % The RIPE Database is subject to Terms and Conditions.



- **Strings:** Aparecerían cadenas de texto (*strings*) específicas en la memoria de la máquina durante la ejecución del análisis.

Strings

interesting (50)	all strings.txt (5000)	report.json (5000)	1824-1.dmp.txt (5000)	1824-c8f77314c9a12704.exe_bt (5000)
String				
retry_proxy_https_basic_auth				
https				
https error				
https:				
https error				
open_https				
https://				
https://				
https://				
retry_https_basic_auth				

Se puede buscar dentro del análisis y cuando encuentra la cadena que estamos buscando esta se pone de otro color por ejemplo buscaremos “*http*”, y el resultado es el siguiente:

Strings

interesting (50)	all strings.txt (5000)	report.json (5000)	1824-1.dmp.txt (5000)	1824-c8f77314c9a12704.exe_bt (5000)
String				
http				
retry_proxy_https_basic_auth				
https				
https error				
https:				
https error				
open_https				
https://				
https://				
https://				
retry_https_basic_auth				

- **Claves de Registro:** Muestra información acerca de las claves de registro con las que se interactuó durante el análisis, separadas en pestañas por acción: Abiertos, Leídos, Escritos y Eliminados.

Claves de Registro

Abiertas (160)	Leídas (209)	Escritas (0)	Eliminadas (0)
Path		Estado	
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\SafeBoot\Option\		true	
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Sip\GPI\DLL\		true	
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\		true	
HKEY_USERS\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\		true	
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\SideBySide\AssemblyStorageRoots\		true	
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Nls\Sorting\Versions\		true	
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Session Manager\		true	
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Error Message Instrument\		true	

Se indica la ruta completa de la clave de registro y el estado de la acción.

- **Ficheros:** Muestra información acerca de los ficheros con los que se interactuó durante el análisis, separado en pestañas por acción: Abiertos, Leídos, Escritos y Eliminados.

Ficheros

Abiertos (36) Leídos (5) Escritos (0) Eliminados (0)

Nombre	Full Path	MD5	Tamaño	Estado
null.exe	C:\Users\user\Desktop\null.exe			true
tzres.dll	C:\Windows\system32\tzres.dll			true
tzres.dll	C:\Windows\system32\tzres.dll			true
null.exe	C:\Users\user\Desktop\null.exe			true
null.exe	C:\Users\user\Desktop\null.exe			true
sortdefault.nls	C:\Windows\Globalization\Sorting\sortdefault.nls			true
Endpoint	\Device\NPF{Endpoint}			true
Nsi	Nsi			true

- **Hooks:** Un *hook* es un punto en el sistema de gestión de mensajes donde se puede instalar una subrutina para monitorizar determinados tipos de mensajes antes de que lleguen a la ventana encargada de procesarlos. Muestra información de los *hooks* creados por la muestra. Actualmente se detectan 4 tipos de *hooks* IDT, IRP, SSDT y KERMODO.

Hooks

IDT (0) IRP (0) SSDT (0) KERMODO (0)

Info! No existen hooks de tipo IDT.

- **Reglas:** Muestra información de las Reglas IOC y Yara que han machado en nuestro análisis.

Reglas

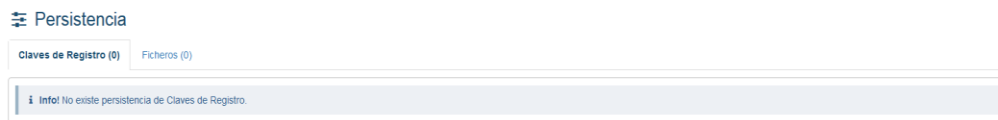
IOC (4) YARA (4)

Pública	Organi...	Nombre	Descripción	Etiquetas	
	CCN	Test 17		#WSKI	Ver detalle
	CCN	prueba_isabel		#isa	Ver detalle
✓	CCN	Prueba Jaime IOC Publica CCN		#CCN #PUBL	Ver detalle
	CCN	IOCDesarrollo	ZEUS ANALYTICDNS.COM (BACKDOOR)		Ver detalle

Desde aquí se tiene la posibilidad de volver a ejecutar las reglas IOC.

Si tenemos dos reglas IOC, se pueden unir esas dos reglas en una.

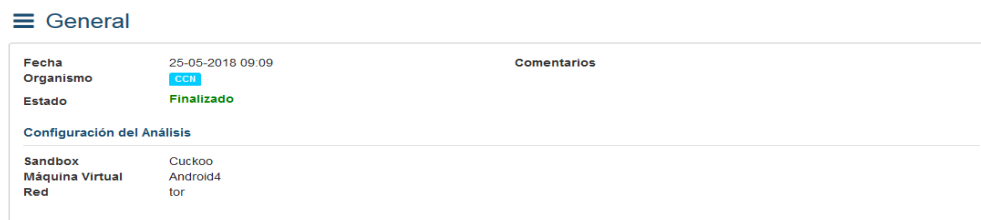
- **Persistencia:** Muestra información de los Registros y Ficheros creados por la muestra. Se divide en dos pestañas Claves de Registro y Ficheros



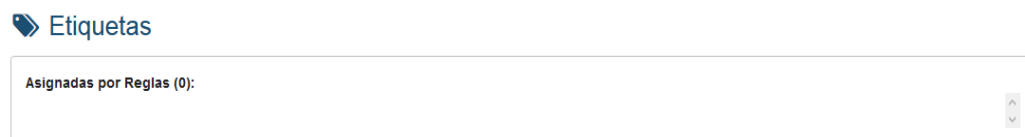
5.5 ANÁLISIS DINÁMICO ANDROID

Este análisis está diseñado para facilitar el análisis dinámico de ficheros de Android.

General: Muestra los datos generales del fichero Android.



Etiquetas: Las etiqueta que han macheado en nuestro análisis Android.



Evidencias: Las evidencias que ha encontrado, se muestran capturas de pantalla.



System Properties: Es una importante característica en android. Funciona como servicio y maneja la configuración del sistema y el status.

Todas estas configuraciones y estados son propiedades. Una propiedad es una pareja KEY/value, que son ambas del tipo cadena, que son útiles para almacenar configuraciones de depuración que están vinculadas a un dispositivo, en lugar de una aplicación o usuario en particular.

⚙ System Properties

Property
"persist.sys.timezone"
"debug.second-display.pkg"
"debug.sqlite.journalmode"
"debug.firebase.analytics.app"
"debug.sqlite.syncmode"

Content: Administra el acceso a un repositorio centra de datos. A menudo suele tener su propia IU para trabajar con datos, pero están principalmente orientados a que lo usen otras aplicaciones que acceden al proveedor de contenido.

Content

[Resolver Queries \(0\)](#)
[Enabled Settings \(0\)](#)
[Path Class Loader \(0\)](#)
[Values \(1\)](#)
[Find Resource \(0\)](#)
[Shared Preferences \(0\)](#)
[Find Library \(0\)](#)

[Load Class \(0\)](#)
[Dropped SO \(0\)](#)

Key	Value
type	0

File: Ficheros accedidos.

File

[Accessed \(6\)](#)
[Raw \(149\)](#)

Fichero
"/data/misc/keychain/pins"
"/data/data/ve.jmtecsolutiontechnologyca.veqr/shared_prefs/com.google.android.gms.appid.xml"
"/data/data/ve.jmtecsolutiontechnologyca.veqr/databases/register.db"
"/data/data/ve.jmtecsolutiontechnologyca.veqr/shared_prefs/com.google.android.gms.measurement_prefs.xml"
"/data/data/ve.jmtecsolutiontechnologyca.veqr/files/keystore"
"/proc/3683/cmdline"

Dex: Muestra varias pestañas.

File: Fichero con todas las clases.

Dropped: Clases que se escriben en disco.

Load: Clases cargadas dinámicamente.

Class Loader: Cargador dinámico de clases

Dex

File (0) Dropped (0) Load (0) Class Loader (0)

Info! Data File not found.

Refection: Sirve para determinar y supervisar el estado de conectividad, por ejemplo en Receivers se usan para obtener información. Transmite la acción `CONNECTIVITY_ACTION` ("android.net.conn.CONNECTIVITY_CHANGE") cuando se modifica la información de conectividad.

Calls: Llamadas al sistema que tiene el tipo de Reflexión.

Telephony Manager Listen: Da acceso a la información acerca de los servicios del teléfono en el dispositivo.

Reflection

Receivers (1) Calls (4) Telephony Manager Listen (0)

Value

"android.net.conn.CONNECTIVITY_CHANGE"

Network: Registra las llamadas de RED, donde vemos en la pestañas.

Network

HTTP (1) SMS (0) Mobile Data Enabled (0)

Map Key	Value
GET https://veqr.org/api/v1/config/textos/list HTTP/1.1	

Commands: Muestra varias pestañas.

Commands

Input (0) Output (0)

Info! Data Commands Input not found.

Binder: Servicio Enlazado, se debe de proporcionar un IBINDER que contenga una interfaz de programación para que los clientes puedan interactuar con el servicio y se puede realizar de la siguiente manera:

- Events → Eventos que la aplicación las maneja.
- Handle Recievers → Handles
- Started Activities → Son aquellas llamadas al sistema cuyo type: Blinder y el Method:
- Register Content Observer → Encargado de observar los cambios en los datos

Binder

Events (0)
Handle Receiver (4)
Started Activities (0)
Register Content Observer (0)

 **Info!** Data Events not found.

Fingerprint: Muestra varias pestañas.

Fingerprint

Accounts (0)
Data Leak (0)
Fingerprint (0)

 **Info!** Data Accounts not found.

Killed Process: Procesos que han sido eliminados.

Killed Process

 **Info!** Data not found.

Errors: Es el conjunto de errores que se han producido dentro de la aplicación, al intentar realizar acciones a las que no ha tenido acceso.

Errors

Value
<pre> {"timestamp":1515506631860,"result":{"mModified":{"first_open_time":1515506631829},"mClear":false},"class":"android.app.SharedPreferencesImpl\$EditorImpl","method":{"putLong"},"type":{"globals"},"args":{"first_open_time":1515506631829}}\n" </pre>
<pre> {"timestamp":1515506631873,"result":{"mModified":{"gmp_app_id":"1:732762932647:android:0665d0316dc8eb52"},"mClear":false},"class":"android.app.SharedPreferencesImpl\$EditorImpl","method":{"putString"},"type":{"globals"},"args":{"gmp_app_id":"1:732762932647:android:0665d0316dc8eb52"}}\n" </pre>
<pre> {"timestamp":1515506631874,"result":{"mModified":{"gmp_app_id":"1:732762932647:android:0665d0316dc8eb52"},"mClear":false},"class":"android.app.SharedPreferencesImpl\$EditorImpl","method":{"putLong"},"type":{"globals"},"args":{"health_monitor.start":1515506631874}}\n" </pre>
<pre> {"timestamp":1515506634319,"result":{"mModified":{"use_service":true},"mClear":false},"class":"android.app.SharedPreferencesImpl\$EditorImpl","method":{"putBoolean"},"type":{"globals"},"args":{"use_service":true}}\n" </pre>
<pre> {"timestamp":1515506634346,"result":{"mModified":{"previous_os_version":"4.4.2"},"mClear":false},"class":"android.app.SharedPreferencesImpl\$EditorImpl","method":{"putString"},"type":{"globals"},"args":{"previous_os_version":"4.4.2"}}\n" </pre>

5.6 ETIQUETAS

A un análisis se le puede asignar etiquetas manualmente o se pueden ver las etiquetas Asignadas por la regla.



Si se desea asignar etiquetas manualmente se puede realizar de dos maneras distintas:

1.- Si se conoce la etiqueta que se quiere asignar se comienza a escribir y aparecerá una lista, se selecciona la que se desea y automáticamente se quedara grabada.



En el caso de que se quisiera quitar del análisis binario la etiqueta solo se tendrá que hacer clic en el aspa de la etiqueta asignada manualmente, y quedaría eliminada del análisis automáticamente.



2.- La otra opción para asignar una etiqueta o varias a la vez, se realiza de la siguiente manera.

Se realiza clic sobre el icono  y nos aparecerá la siguiente lista de etiquetas:



Etiquetas disponibles



Filtrar etiquetas...

#A-16	APT-16
#A-17	APT17 - Aurora Panda
#A-28	APT28 - Sofacy
#A-29	APT-29
#A-30	APT-30
#A-AG	APT_Agent.BTZ
#A-BT	APT - BlueTermite
#A-CD	APT - Codoso
#A-CK	APT - Carbanak
#A-CP	APT - Casper
#A-CT	APT - Careto
#A-D2	APT - Duqu2
#A-DB	APT - Derusbi

Se puede seleccionar una o varias y solo con arrastrarlas a nuestra parte de “Asignadas manualmente”, se quedarían grabadas automáticamente.

5.7 STRINGS

Es una herramienta que facilita la búsqueda de cadenas de texto (*strings*) específicas en la memoria de la máquina durante la ejecución del análisis.

Strings

interesting (50) all strings.txt (5000) report.json (5000) 1824-1.dmp.txt (5000) 1824-c8f77314c9a12704.exe.txt (5000)

String

retry_proxy_https_basic_auth

https

https error

https:

https error

open_https

https://

https://

https://

retry_https_basic_auth

Se puede buscar dentro del análisis y cuando encuentra la cadena que se está buscando esta se nos pone de otro color por ejemplo buscaremos “[http](#)”, y el resultado es el siguiente:

Strings

interesting (50) all strings.txt (5000) report.json (5000) 1824-1.dmp.txt (5000) 1824-c8f77314c9a12704.exe.txt (5000)

String

http|

retry_proxy_https_basic_auth

https

https error

https:

https error

open_https

https://

https://

https://

retry_https_basic_auth

6. CONFIGURACIÓN

Esta pestaña engloba un conjunto de pestañas relacionadas con la configuración de MARTA:

6.1 REGLAS YARA

Facilita todas las gestiones relacionadas con el motor de reglas Yara.

En la parte superior de la pantalla en la parte derecha nos encontramos con el icono que engloba todas las opciones que componen las reglas Yara  haciendo clic sobre el icono nos aparecerán todas las opciones a las que se tienen acceso.

Pasando el ratón por encima veremos una leyenda de la acción de cada icono.



En el listado el usuario puede ver las reglas Yara que hay en el sistema. También puede filtrar los resultados por uno o varios de los campos del listado.

En la lista se pueden ver los atributos más significativos de cada regla: el nombre, la descripción, si está activa (**una regla no activa no se tendrá en cuenta para las comprobaciones de reglas coincidentes de un análisis**) y sus etiquetas asociadas. Al igual que en las listas de ficheros y de análisis, es posible *filtrar* por cualquiera de estos campos.

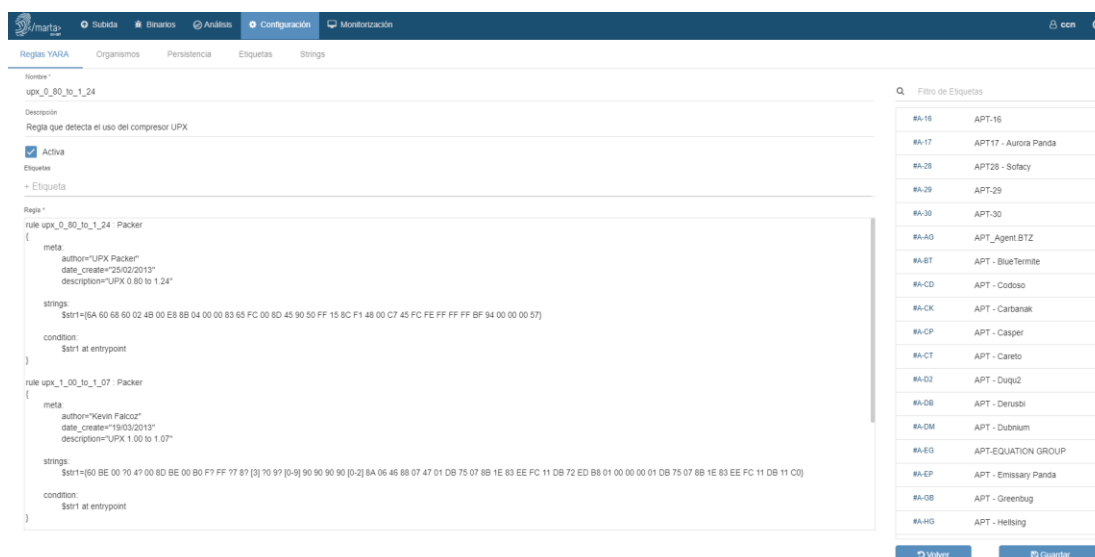
Reglas YARA						
Número total de registros: 248						
Publica	Organismo	Nombre	Descripción	Activo	Etiquetas	
☐		wpk_8_R0_3a_1_24_a	Regla que detecta el uso del compresor UPX	☐ Desactivada	#R0BR #R0VCR #R0EIP	
☐		Careto_SGH	APT - Careto	☐ Desactivada		
☐		Careto_OSI_SBD	APT - Careto	☒ Activa		
☐		Careto_CnC	APT - Careto	☒ Activa		
☐		Careto_CnC_domains	APT - Careto	☒ Activa		
☐		apt_disq2_loaders	APT - Disq 2.0	☒ Activa		
☐		apt_disq2_drivers	APT - Disq 2.0	☒ Activa		
☐		CVE_2015_1701_Talhou	Exploit - CVE 2015 1701 - Talhou	☐ Desactivada		
☐		Exploit_MS15_077_078_HackingTeam	Exploit - MS15 077 078 - Hacking Team	☒ Activa		
☐		Exploit_MS15_077_078	Exploit - MS15 077 078	☐ Desactivada		
☐		sku	Exploit - UAC elevators	☒ Activa		
☐		UACElevator	Exploit - UAC Elevator	☒ Activa		
☐		UACME_Hagi	Exploit - UAC Elevator	☒ Activa		
☐		WinTElevator2	Exploit - UAC Elevator	☒ Activa		
☐		HackingTeam_Elevator_EXE	Exploit - Hacking Team	☒ Activa		
☐		HackingTeam_Elevator_DLL	Exploit - Hacking Team	☒ Activa		
☐		bin_indisk	Exploit - Hacking Team	☒ Activa		
☐		PwDump	Hacking Tool - PwDump	☒ Activa		
☐		PScan_Portscan_1	Hack Tool - Pscan PortScan	☒ Activa		
☐		HackTool_Samples	HackTool - Samples	☒ Activa		

Las acciones disponibles desde esta pantalla son las siguientes:

- Ver detalle de una regla
- Eliminar una regla
- Crear una regla
- Activar reglas seleccionadas
- Desactivar reglas seleccionadas
- Cargar reglas desde un fichero
- Publicar reglas Yara activas en “*sandboxes*”.
- Gestionar etiquetas asociadas a las reglas Yara.

6.1.1 DETALLE REGLA YARA

Se accede al detalle de una regla realizando doble clic sobre la Regla. Desde esta opción el usuario puede ver el detalle de una regla Yara, modificar sus propiedades y etiquetas.



El usuario puede fácilmente gestionar las etiquetas asociadas a una regla Yara arrastrando de un lado a otro una o varias etiquetas seleccionadas desde cada una de las partes.

6.1.2 CREAR REGLA YARA

Se puede crear una nueva regla Yara desde el icono situado en la barra superior del menú opciones:



Se rellenan los campos y se puede crear desde cero la regla Yara o se puede arrastrar un fichero con la regla Yara que queremos crear.

Es importante resaltar *que cada vez que guardemos una regla, dicha regla se publicara automáticamente en las [Sandboxes](#).*

6.1.3 ELIMINAR REGLA YARA

Se puede eliminar una regla desde el icono situado en la barra superior del menú



opciones . La aplicación pide confirmación antes de hacer el borrado de la regla.

6.1.4 ACTIVAR REGLAS SELECCIONADAS

Se pueden activar una o varias reglas seleccionadas utilizando el icono  situado en la barra superior del menú opciones.

Es importante resaltar que *cada vez que activemos una regla, dicha regla se publicara automáticamente en las [Sandboxes](#).*

6.1.5 DESACTIVAR REGLAS SELECCIONADAS

Se pueden desactivar una o varias reglas seleccionadas utilizando el icono  situado en la barra superior del menú opciones.

6.1.6 PUBLICAR REGLAS YARA

Se pueden publicar en las distintas “[Sandboxes](#)” las reglas Yara activas utilizando el

icono  situado en la barra superior del menú opciones.

6.1.7 DESPUBLICAR REGLAS YARA

Se pueden despublicar en las distintas “[Sandboxes](#)” las reglas Yara activas utilizando el

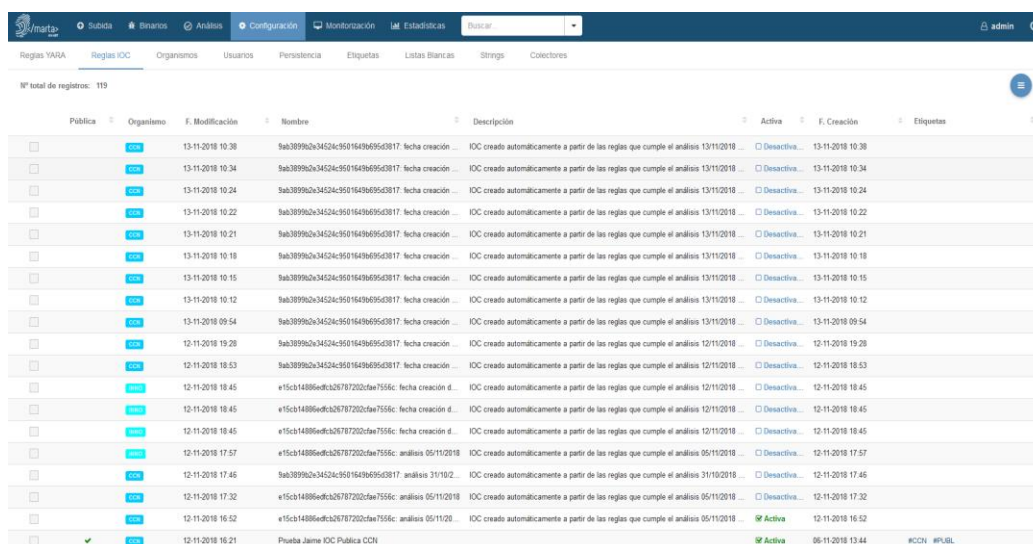
icono  situado en la barra superior del menú opciones.

6.1.8 DESCARGAR REGLA YARA

Se pueden descargar una regla Yara utilizando el icono  situado en la barra superior del menú opciones.

6.2 REGLAS IOC

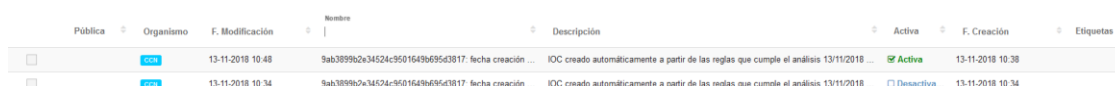
Facilita todas las gestiones relacionadas con las reglas IOC. Algunas de las opciones solo serán visibles para perfiles con rol administrador.



Publica	Organismo	F. Modificación	Nombre	Descripción	Activa	F. Creación	Etiquetas
☐	CCN	13-11-2018 10:38	9ab3899b2e34524c95016436695d3817: fecha creación ...	IOC creado automáticamente a partir de las reglas que cumple el análisis 13/11/2018 ...	☐ Desactiva...	13-11-2018 10:38	
☐	CCN	13-11-2018 10:34	9ab3899b2e34524c95016436695d3817: fecha creación ...	IOC creado automáticamente a partir de las reglas que cumple el análisis 13/11/2018 ...	☐ Desactiva...	13-11-2018 10:34	
☐	CCN	13-11-2018 10:24	9ab3899b2e34524c95016436695d3817: fecha creación ...	IOC creado automáticamente a partir de las reglas que cumple el análisis 13/11/2018 ...	☐ Desactiva...	13-11-2018 10:24	
☐	CCN	13-11-2018 10:22	9ab3899b2e34524c95016436695d3817: fecha creación ...	IOC creado automáticamente a partir de las reglas que cumple el análisis 13/11/2018 ...	☐ Desactiva...	13-11-2018 10:22	
☐	CCN	13-11-2018 10:21	9ab3899b2e34524c95016436695d3817: fecha creación ...	IOC creado automáticamente a partir de las reglas que cumple el análisis 13/11/2018 ...	☐ Desactiva...	13-11-2018 10:21	
☐	CCN	13-11-2018 10:18	9ab3899b2e34524c95016436695d3817: fecha creación ...	IOC creado automáticamente a partir de las reglas que cumple el análisis 13/11/2018 ...	☐ Desactiva...	13-11-2018 10:18	
☐	CCN	13-11-2018 10:15	9ab3899b2e34524c95016436695d3817: fecha creación ...	IOC creado automáticamente a partir de las reglas que cumple el análisis 13/11/2018 ...	☐ Desactiva...	13-11-2018 10:15	
☐	CCN	13-11-2018 10:12	9ab3899b2e34524c95016436695d3817: fecha creación ...	IOC creado automáticamente a partir de las reglas que cumple el análisis 13/11/2018 ...	☐ Desactiva...	13-11-2018 10:12	
☐	CCN	13-11-2018 09:54	9ab3899b2e34524c95016436695d3817: fecha creación ...	IOC creado automáticamente a partir de las reglas que cumple el análisis 13/11/2018 ...	☐ Desactiva...	13-11-2018 09:54	
☐	CCN	12-11-2018 19:28	9ab3899b2e34524c95016436695d3817: fecha creación ...	IOC creado automáticamente a partir de las reglas que cumple el análisis 12/11/2018 ...	☐ Desactiva...	12-11-2018 19:28	
☐	CCN	12-11-2018 18:53	9ab3899b2e34524c95016436695d3817: fecha creación ...	IOC creado automáticamente a partir de las reglas que cumple el análisis 12/11/2018 ...	☐ Desactiva...	12-11-2018 18:53	
☐	CCN	12-11-2018 18:45	e15cb14886ed32b787202dae7f556c: fecha creación d...	IOC creado automáticamente a partir de las reglas que cumple el análisis 12/11/2018 ...	☐ Desactiva...	12-11-2018 18:45	
☐	CCN	12-11-2018 18:45	e15cb14886ed32b787202dae7f556c: fecha creación d...	IOC creado automáticamente a partir de las reglas que cumple el análisis 12/11/2018 ...	☐ Desactiva...	12-11-2018 18:45	
☐	CCN	12-11-2018 17:57	e15cb14886ed32b787202dae7f556c: análisis 05/11/2018	IOC creado automáticamente a partir de las reglas que cumple el análisis 05/11/2018 ...	☐ Desactiva...	12-11-2018 17:57	
☐	CCN	12-11-2018 17:46	9ab3899b2e34524c95016436695d3817: análisis 31/10/2018	IOC creado automáticamente a partir de las reglas que cumple el análisis 31/10/2018 ...	☐ Desactiva...	12-11-2018 17:46	
☐	CCN	12-11-2018 17:32	e15cb14886ed32b787202dae7f556c: análisis 05/11/2018	IOC creado automáticamente a partir de las reglas que cumple el análisis 05/11/2018 ...	☐ Desactiva...	12-11-2018 17:32	
☐	CCN	12-11-2018 16:52	e15cb14886ed32b787202dae7f556c: análisis 05/11/2018	IOC creado automáticamente a partir de las reglas que cumple el análisis 05/11/2018 ...	☒ Activa	12-11-2018 16:52	
☒	CCN	12-11-2018 16:21	Prueba Jaime IOC Publica CCN		☒ Activa	06-11-2018 13:44	ICCN - #PUBL

6.2.1 LISTADO

En la lista se muestran los atributos más significativos de cada regla: el nombre, la descripción, si está activa (**una regla no activa no se tendrá en cuenta para las comprobaciones de reglas coincidentes de un análisis**) y sus etiquetas asociadas. Al igual que en las listas de ficheros y de análisis, es posible *filtrar* por cualquiera de estos campos.



Publica	Organismo	F. Modificación	Nombre	Descripción	Activa	F. Creación	Etiquetas
☐	CCN	13-11-2018 10:48	9ab3899b2e34524c95016436695d3817: fecha creación ...	IOC creado automáticamente a partir de las reglas que cumple el análisis 13/11/2018 ...	☒ Activa	13-11-2018 10:38	
☐	CCN	13-11-2018 10:34	9ab3899b2e34524c95016436695d3817: fecha creación ...	IOC creado automáticamente a partir de las reglas que cumple el análisis 13/11/2018 ...	☐ Desactiva...	13-11-2018 10:34	

6.2.2 ACCIONES

En la parte derecha de la pantalla tenemos el menú desplegable de todas las acciones que se pueden realizar sobre una regla IOC.



Las principales acciones son las siguientes:

- **Crear Regla:** Abre la vista de detalles de una regla, vacía, para crear una regla nueva desde cero.

Nombre

Fecha de creación

Fecha de modificación

☐ Activar Regla

Etiquetas asignadas manualmente

+ Etiqueta

Descripción

+ Añadir ✎ Modificar 🗑 Eliminar

OR

Etiquetas disponibles (Filtro)

- #A-16 APT-16
- #A-17 APT17 - Aurora Panda
- #A-28 APT28 - Sofacy
- #A-29 APT-29
- #A-30 APT-30
- #A-AG APT_Agent.BTZ
- #A-BT APT - BlueTermite
- #A-CD APT - Codoso
- #A-CK APT - Carbanak
- #A-CP APT - Casper
- #A-CT APT - Careto
- #A-D2 APT - Duqu2
- #A-D8 APT - Demosbi
- #A-D9 APT - Dubnium
- #A-E5 APT-EQUATION GROUP
- #A-EP APT - Emissary Panda
- #A-G8 APT - Greenbug

Volver Guardar

La parte de la izquierda contiene los datos básicos de la regla: el nombre, la fecha de creación y de última modificación, si está activa (**una regla no activa no se tendrá en cuenta para las comprobaciones de reglas coincidentes de un análisis**), y la descripción. Todos estos campos son editables, excepto las fechas, que se calculan de forma automática. Si una regla no tiene fecha de creación es debido a que fue importada desde un XML que no contenía esta información.

La parte del centro contiene el árbol lógico de la regla. Las reglas de MARTA tienen estructura de IOC. Es decir, están basadas en comprobaciones de términos anidados con operaciones AND y OR.

Reglas YARA **Reglas IOC** Organismos Persistencia Etiquetas Listas Blancas Strings Colectores

Organismo
CCNCERT

Nombre
Ransom.CryptXXX

Fecha de creación
21-02-2017

Fecha de modificación
31-10-2018

☒ Activar Regla

Etiquetas asignadas manualmente

#RWC Ransomware CryptXXX

+ Etiqueta

Descripción
IOC para detectar el código Ransom.CryptXXX

+ Añadir ✎ Modificar 🗑 Eliminar

OR

- Port Remote IP is 188.0.236.7
- File MD5 is d01fd2bb8c6296d51be297978af8b3a1
- File MD5 is ae06248ab3c02e1c2ca9d53b9a155199
- Process Handle Name is FX1112

AND

- Process Handle Name is FX1114

Etiquetas disponibles (Filtro)

- #A-16 APT-16
- #A-17 APT17 - Aurora Panda
- #A-28 APT28 - Sofacy
- #A-29 APT-29
- #A-30 APT-30
- #A-AG APT_Agent.BTZ
- #A-BT APT - BlueTermite
- #A-CD APT - Codoso
- #A-CK APT - Carbanak
- #A-CP APT - Casper

Volver al listado Ejecutar Regla Guardar

https://172.20.40.213/MartaWeb/#/unload

Hay una gran cantidad de términos diferentes, Valor de Registro (Registry Value), Nombre de Proceso (Process Name), URI, Extensión de Fichero (File Extension), Servidor DNS (DNS Host), Nombre de Servicio (Service Name), Puerto Remoto (Remote Port), y un largo etcétera. Entre todos ellos, se puede definir cualquier comportamiento que MARTA pueda analizar. Y las reglas se pueden hacer tan complicadas como sea necesario, anidando términos con operadores lógicos. Es decir, es posible definir reglas que detecten comportamientos muy complejos o muy concretos.

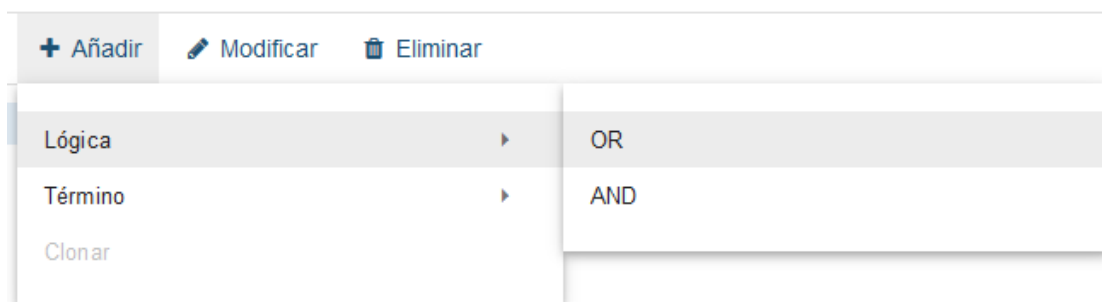
Tenemos tres botones para crear una regla:

Añadir

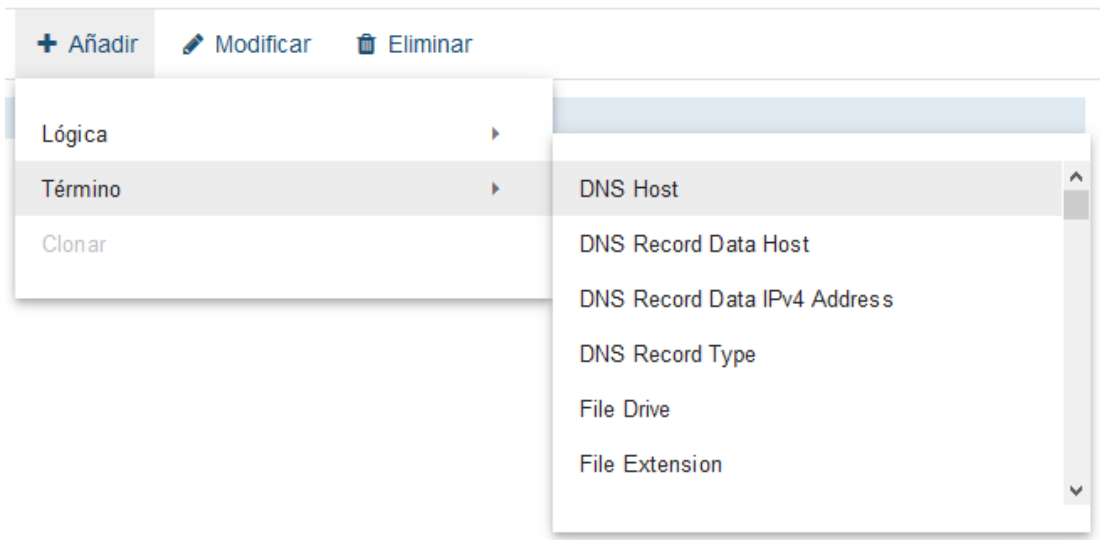


Se puede añadir una Lógica o un Término:

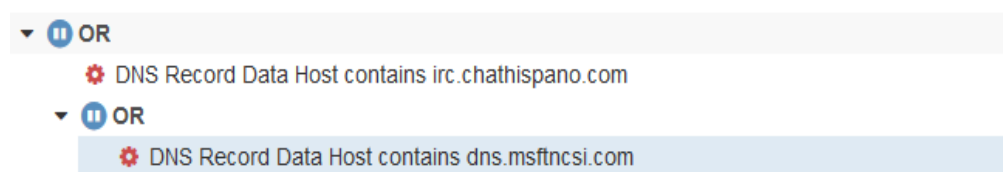
Lógica



Término

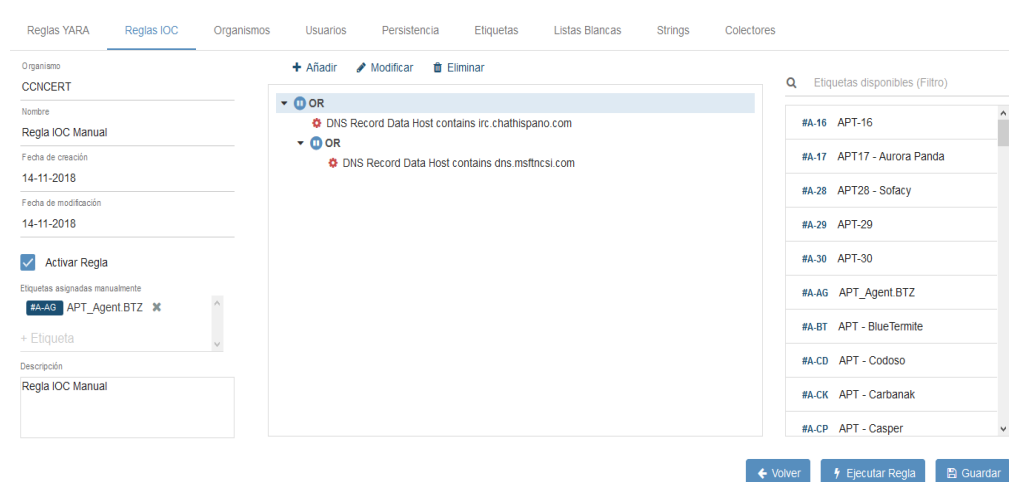


Ejemplo de una regla IOC:



Si en el análisis se cumplieran una de las dos condiciones la regla IOC se macheara en el análisis.

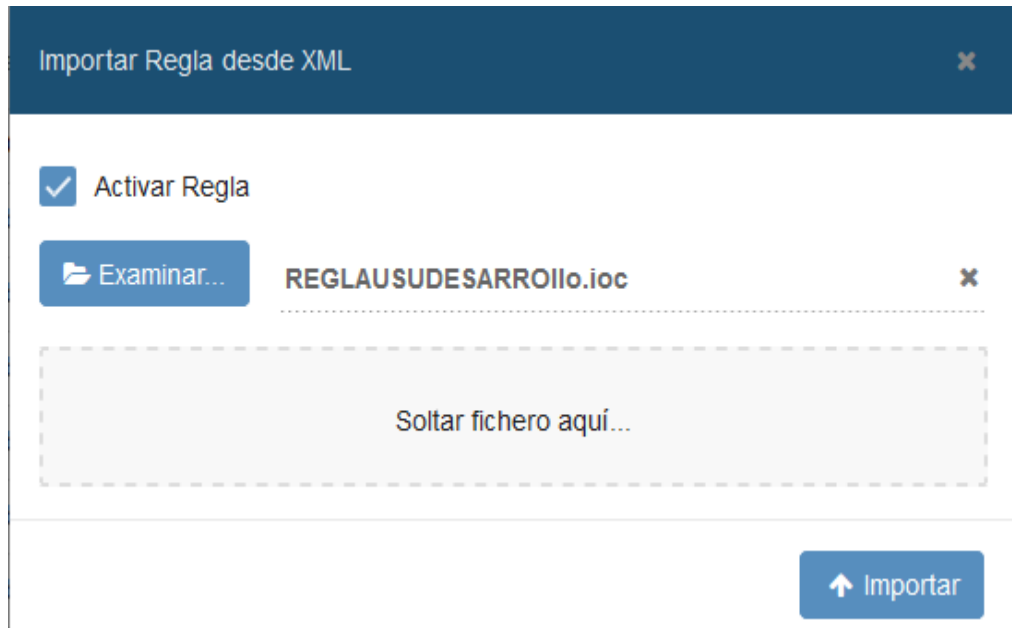
- **Ver Detalle:** Se realiza doble clic sobre la regla que se quiere ver. Abre la vista de detalles de una regla, para modificar una regla ya existente.



Desde esa pantalla se puede modificar la regla IOC. Si se quiere ejecutar esta regla sobre nuestros análisis se deberá de hacer clic sobre el botón “Ejecutar Regla”.



- **Importar:** Abre una vista que permite cargar una regla desde un fichero XML con formato IOC.



The dialog box titled "Importar Regla desde XML" contains a checked checkbox "Activar Regla", an "Examinar..." button, and a text field containing "REGLAUSUDEDESARROLLO.ioc". Below these is a dashed box with the text "Soltar fichero aquí...". At the bottom right is an "Importar" button with an upward arrow icon.

- **Descargar Reglas:** Seleccionamos las reglas que se quieran descargar y se hace clic en el botón “Descargar Reglas” .
- **Publicar Reglas:** Seleccionamos las reglas que se quieran publicar y se hace clic en el botón “Publicar Reglas” .
- **Despublicar Reglas:** Seleccionamos las reglas que se quieran despublicar y se hace clic en el botón “DesPublicar Reglas” .
- **Activar Reglas:** Seleccionamos las reglas que se quieran activar y se hace clic en el botón “Activar Reglas” .
- **Desactivar Reglas:** Seleccionamos las reglas que se quieran desactivar y se hace clic en el botón “Desactivar Reglas” .
- **Eliminar Reglas:** Seleccionamos las reglas que se quieran eliminar y se hace clic en el botón “Eliminar” .

6.3 ORGANISMOS

Facilita todas las gestiones relacionadas con los organismos. Algunas de las opciones solo serán visibles para perfiles con rol administrador.

Nombre	Etiqueta	Descripción
☐ AEAT	AEAT	AEAT
☐ AENA	AENA	Aeropuertos Españoles y Navegación Aérea
☐ AIRBUS	AIRBUS	Airbus
☐ ALESTIS	ALESTIS	Alestis
☐ Almendralejo	Almendralejo	Almendralejo
☐ ARAGON	ARAGON	Aragón
☐ ASTURIAS	ASTURIAS	Asturias
☐ AytoAlicante	AytoAlicante	Ayuntamiento de Alicante
☐ AytoBenidorm	AytoBenidorm	Ayuntamiento de Benidorm
☐ AytoCórdoba	AytoCórdoba	Ayuntamiento de Córdoba
☐ AytoMálaga	AytoMálaga	Ayuntamiento de Málaga
☐ AytoOurense	AytoOurense	Ayuntamiento de Ourense
☐ AytoPalma	AytoPalma	Ayuntamiento de Palma
☐ BALEARIS	BALEARIS	Baleares
☐ BancoPopular	BancoPopular	Banco Popular
☐ BCC	BCC	BCC
☐ BNE	BNE	Biblioteca Nacional Española
☐ BOE	BOE	Boletín Oficial del Estado
☐ CabTenerife	CabTenerife	Cabildo de Tenerife

La pestaña consta de un listado, donde se puede modificar o eliminar una Organización y se dispone de la opción de crear una Organización nueva.

Nueva Organización: En la barra de herramientas de la parte superior, está el botón



Crear Organismo, que permite crear organismos nuevos.

Creación de Organismo

Nombre *

Alias *

Color * Vista Previa

Descripción

+ CREAR

Se rellenan los campos y se hace clic en el botón CREAR. Se crea un nuevo Organismo que aparecerá en el listado de Organismos.

Modificar Organización: Se realiza doble clic sobre la organización que se desea Modificar.

The screenshot shows a web form titled "Edición de Organismo" with a close button (X) in the top right corner. The form contains the following fields and elements:

- Nombre ***: A text input field containing "CCNCERT".
- Fecha de Alta**: A text input field containing "06-06-2018 18:23".
- Alias ***: A text input field containing "CCN".
- Color ***: A color selection interface with a large color palette and a row of smaller color swatches below it.
- Vista Previa**: A small preview of the CCN logo.
- Descripción**: A text area containing "Organismo administrador".
- GUARDAR**: A blue button with a save icon and the text "GUARDAR" at the bottom right.

En esta pantalla aparece la fecha de cuando se dio de alta el Organismo (Fecha de Alta). Se modifican los campos necesarios y se hace clic en GUARDAR.

Eliminar Organización: Elimina el organismo seleccionado. Pide confirmación antes de eliminar.



6.4 PERSISTENCIA

Esta pestaña está diseñada para facilitar todas las gestiones relativas a las reglas de Persistencia. Algunas de las opciones solo serán visibles para perfiles con rol administrador.

Organismos		Persistencia
Número total de registros: 69		    
Nombre	Tipo de Persistencia	Activo
☐ "SYSTEM\CurrentControlSet\Control\Lsa\Notification Packages"	Ficheros de sistema modificados	 Activa
☐ "SYSTEM\CurrentControlSet\Control\Lsa\Notification Packages"	Ficheros tras reinicio	 Activa
☐ "SYSTEM\CurrentControlSet\Control\Lsa\Notification Packages"	Claves de registro	 Activa
☐ "SYSTEM\CurrentControlSet\Control\Lsa\Notification Packages1"	Claves de registro	 Activa
☐ "SYSTEM\CurrentControlSet\Control\Lsa\Notification Packages12"	Claves de registro	 Activa
☐ "SYSTEM\CurrentControlSet\Control\Lsa\Notification Packagesss4"	Ficheros de sistema modificados	 Activa
☐ 107-TRIAL-system\autoexec.nt 181	Ficheros de sistema modificados	 Activa
☐ 186-TRIAL-system.ini 214	Ficheros de sistema modificados	 Activa
☐ 19-TRIAL-dosstart.bat 105	Ficheros de sistema modificados	 Activa
☐ 218-TRIAL-system\config.nt 30	Ficheros de sistema modificados	 Activa
☐ c:\autoexec.bat	Ficheros de sistema modificados	 Activa

Muestra una lista con todas las reglas registradas en MARTA, Nombre, el tipo de Persistencia y si esta activa la regla de Persistencia.

Ver Detalle: Con doble clic abre la vista de detalle de la regla de persistencia elegida. Esta vista muestra el Nombre, Activa, Descripción, Tipo de Resistencia, y permite modificarlos haciendo clic fuera de la pantalla.

Guardar Cambios: Se selecciona fuera para grabar los cambios.

Edición de regla de Persistencia

Nombre *

"SYSTEM\CurrentControlSet\Control\Lsa\Notification Packages"

Descripción

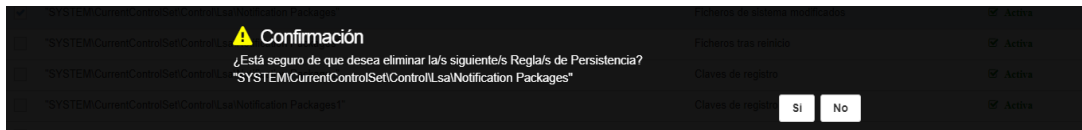
Tipo de Persistencia *

Ficheros sistema modificados

☒ Activa

GUARDAR

Eliminar: Elimina la regla de Persistencia elegida. Pide confirmación antes de eliminar.



En la barra de herramientas de la parte superior de la pestaña, está el botón **Crear Regla de Persistencia**, que permite crear reglas de persistencia nuevas, Activar/Desactivar Reglas, Actualizar y Borrar.



Crear Regla

Nueva regla de Persistencia

Nombre *

Descripción

Tipo de Persistencia *

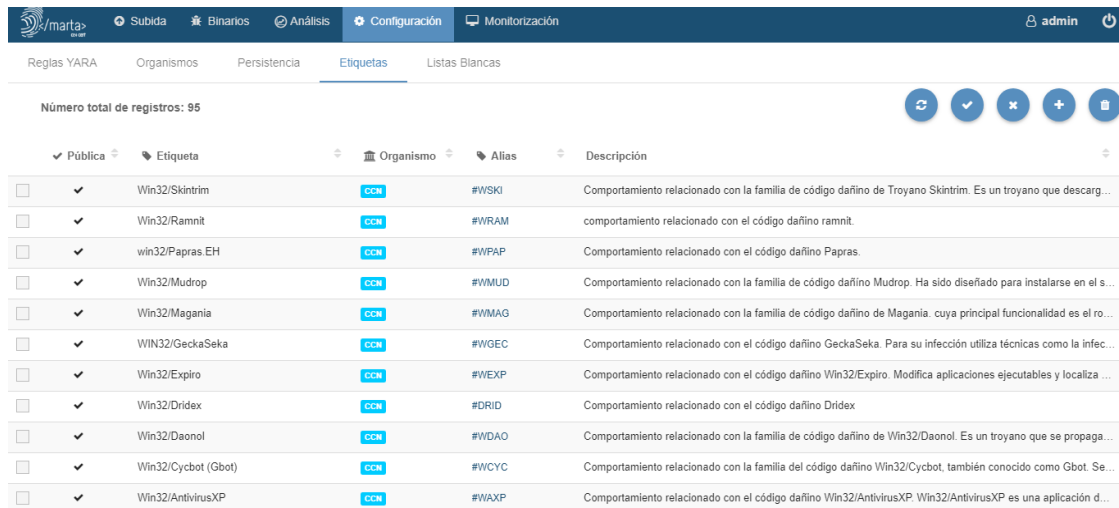
☐ Activa

+ CREAR

Esta pantalla abre la vista de detalle de una regla de persistencia, vacía para que se rellene el nombre, si la vamos a activar, descripción, tipo de Persistencia y se cree al hacer clic fuera de la pantalla.

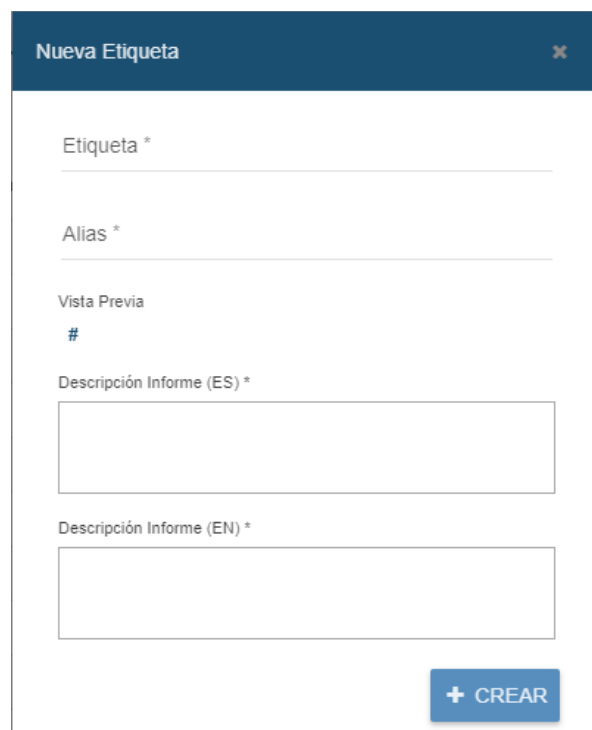
6.5 ETIQUETAS

En la pestaña de configuración se tiene la parte de etiquetas. Desde aquí se puede Crear, Modificar, Eliminar y Publicar (Solo CCN) etiquetas.



✓ Pública	Etiqueta	Organismo	Alias	Descripción
☐	Win32/Skintrim	CCN	#WSKI	Comportamiento relacionado con la familia de código dañino de Troyano Skintrim. Es un troyano que descarg...
☐	Win32/Ramnit	CCN	#WRAM	comportamiento relacionado con el código dañino ramnit.
☐	win32/Papras.EH	CCN	#WPAP	Comportamiento relacionado con el código dañino Papras.
☐	Win32/Mudrop	CCN	#WMUD	Comportamiento relacionado con la familia de código dañino Mudrop. Ha sido diseñado para instalarse en el s...
☐	Win32/Maganla	CCN	#WMAG	Comportamiento relacionado con la familia de código dañino de Magania. cuya principal funcionalidad es el ro...
☐	WIN32/GeckaSeka	CCN	#WGEC	Comportamiento relacionado con el código dañino GeckaSeka. Para su infección utiliza técnicas como la infec...
☐	Win32/Expiro	CCN	#WEXP	Comportamiento relacionado con el código dañino Win32/Expiro. Modifica aplicaciones ejecutables y localiza ...
☐	Win32/Dridex	CCN	#DRID	Comportamiento relacionado con el código dañino Dridex
☐	Win32/Daonol	CCN	#WDAO	Comportamiento relacionado con la familia de código dañino de Win32/Daonol. Es un troyano que se propaga...
☐	Win32/Cycbot (Gbot)	CCN	#WCYC	Comportamiento relacionado con la familia del código dañino Win32/Cycbot, también conocido como Gbot. Se...
☐	Win32/AntivirusXP	CCN	#WAXP	Comportamiento relacionado con el código dañino Win32/AntivirusXP. Win32/AntivirusXP es una aplicación d...

Para crear una etiqueta se pulsa sobre el icono  y aparecerá una pantalla con los campos que se tienen que rellenar.



Nueva Etiqueta

Etiqueta *

Alias *

Vista Previa
#

Descripción Informe (ES) *

Descripción Informe (EN) *

+ CREAR

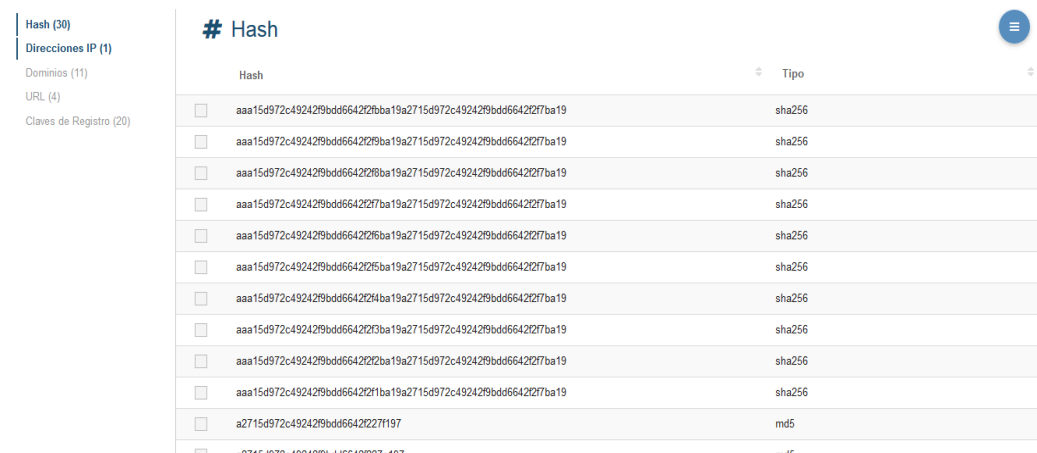
Se rellenan los campos y se hace clic en el botón CREAR, creará una etiqueta nueva que aparecerá en el listado.

6.6 Listas Blancas

Es un listado dividido en Hash, Direcciones IP, Dominios, URL y Claves de Registro. Esta opción solo será visible para perfiles con rol administrador.

Desde esta pantalla se crearan, modificaran y eliminaran los datos de nuestra Listas Blancas.

1. Hash: Se dispone de un listado de Hashes.



Hash	Tipo
☐ aaa15d972c49242f9bdd6642f2fba19a2715d972c49242f9bdd6642f2fba19	sha256
☐ aaa15d972c49242f9bdd6642f2fba19a2715d972c49242f9bdd6642f2fba19	sha256
☐ aaa15d972c49242f9bdd6642f2fba19a2715d972c49242f9bdd6642f2fba19	sha256
☐ aaa15d972c49242f9bdd6642f2fba19a2715d972c49242f9bdd6642f2fba19	sha256
☐ aaa15d972c49242f9bdd6642f2fba19a2715d972c49242f9bdd6642f2fba19	sha256
☐ aaa15d972c49242f9bdd6642f2fba19a2715d972c49242f9bdd6642f2fba19	sha256
☐ aaa15d972c49242f9bdd6642f2fba19a2715d972c49242f9bdd6642f2fba19	sha256
☐ aaa15d972c49242f9bdd6642f2fba19a2715d972c49242f9bdd6642f2fba19	sha256
☐ aaa15d972c49242f9bdd6642f2fba19a2715d972c49242f9bdd6642f2fba19	sha256
☐ aaa15d972c49242f9bdd6642f2fba19a2715d972c49242f9bdd6642f2fba19	sha256
☐ aaa15d972c49242f9bdd6642f2fba19a2715d972c49242f9bdd6642f2fba19	sha256
☐ a2715d972c49242f9bdd6642f2fba19a2715d972c49242f9bdd6642f2fba19	md5
☐ a2715d972c49242f9bdd6642f2fba19a2715d972c49242f9bdd6642f2fba19	md5

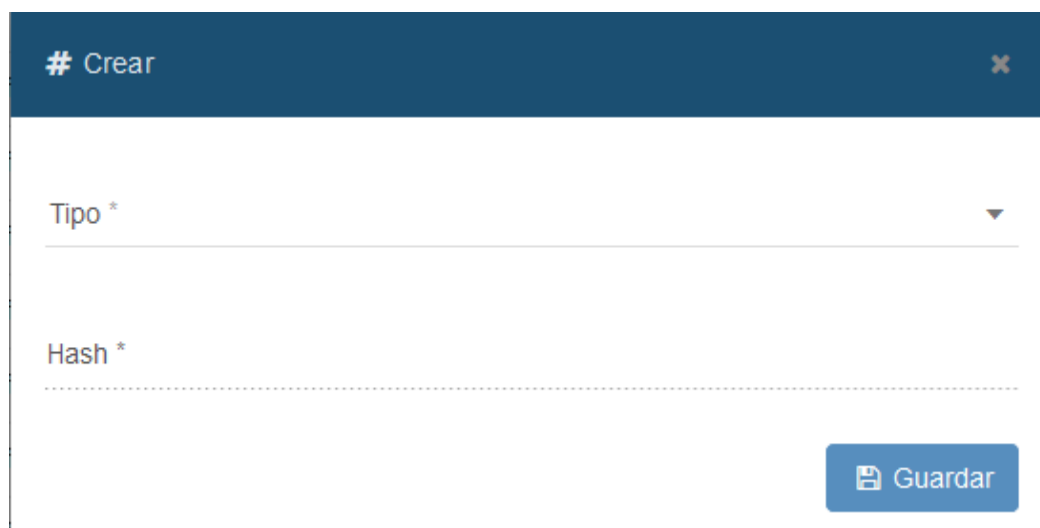
En la parte superior se dispone de las siguientes opciones.



Se podrán crear, importar o eliminar un Hash.



Crear Hash: Desde esta pantalla crearemos un Hash para nuestra Lista Blanca.



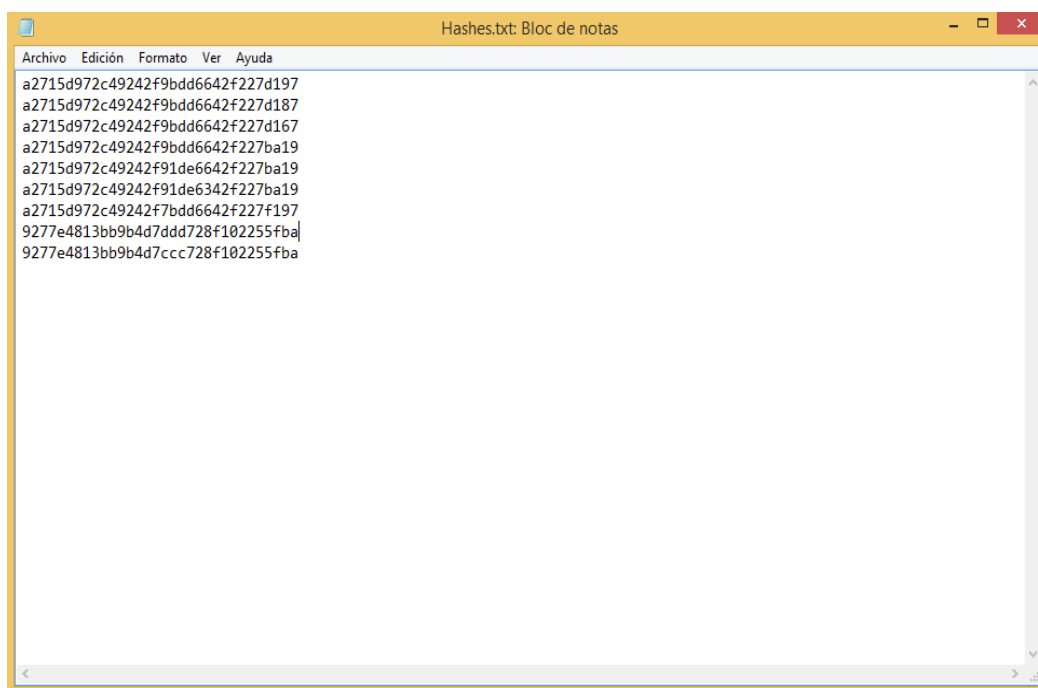
Elegimos el tipo “MD5, SHA256” y ponemos el Hash que queremos que este en nuestra Lista Blanca.



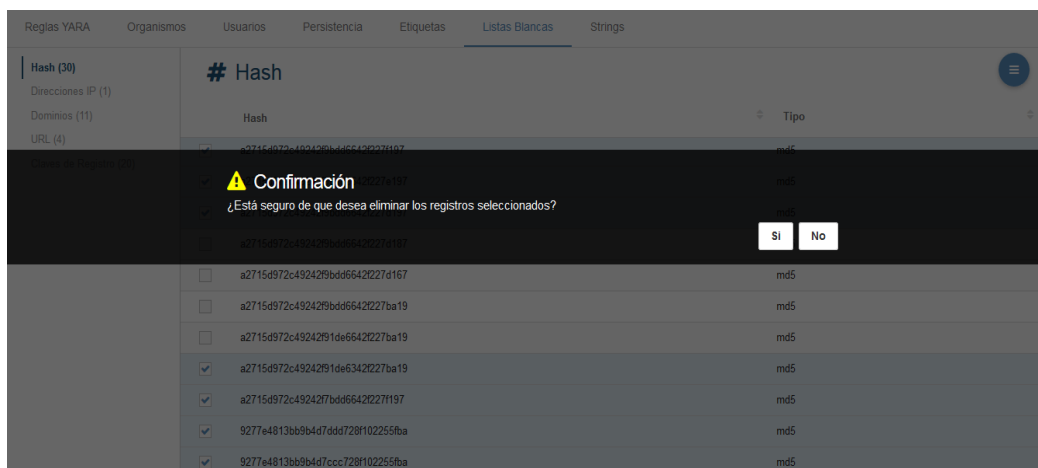
Importar Hash: Desde esta pantalla se importan Hashes, solo se tendrán que elegir el tipo de dato “MD5, SHA256” y elegir nuestro fichero que debe de ser con extensión .txt.



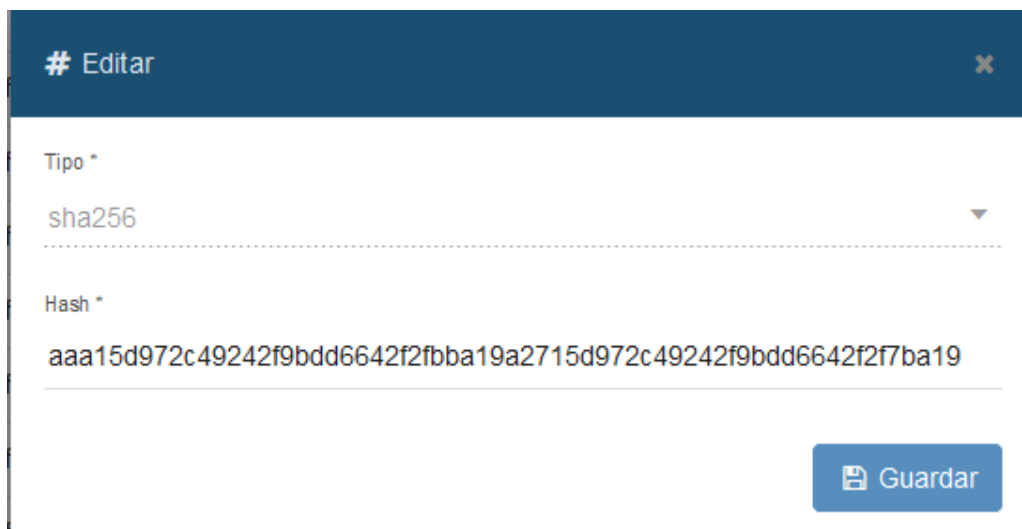
Se pueden importar un solo Hash o varios, el formato del fichero seria el siguiente:



Eliminar Hash: Se selecciona el Hash o Hashes que se quieren eliminar.

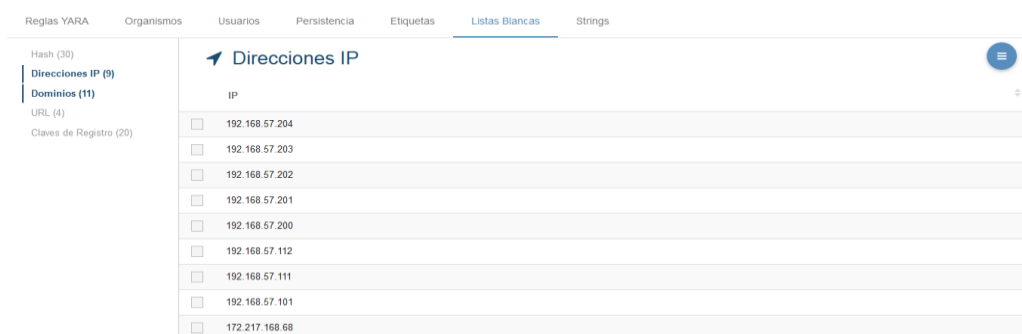


Editar Hash: Para modificar un Hash doble clic sobre el Hash a modificar.



El tipo no es modificable.

2. Direcciones IP: Se dispone de un listado de Direcciones IP.



Direcciones IP	
	IP
☐	192.168.57.204
☐	192.168.57.203
☐	192.168.57.202
☐	192.168.57.201
☐	192.168.57.200
☐	192.168.57.112
☐	192.168.57.111
☐	192.168.57.101
☐	172.217.168.68

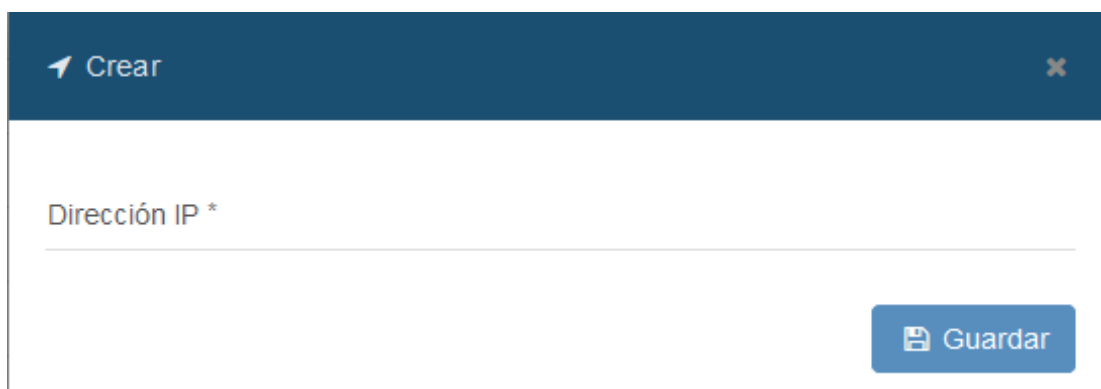
En la parte superior se dispone de las siguientes opciones.



Se podrán crear, importar o eliminar una Dirección IP.



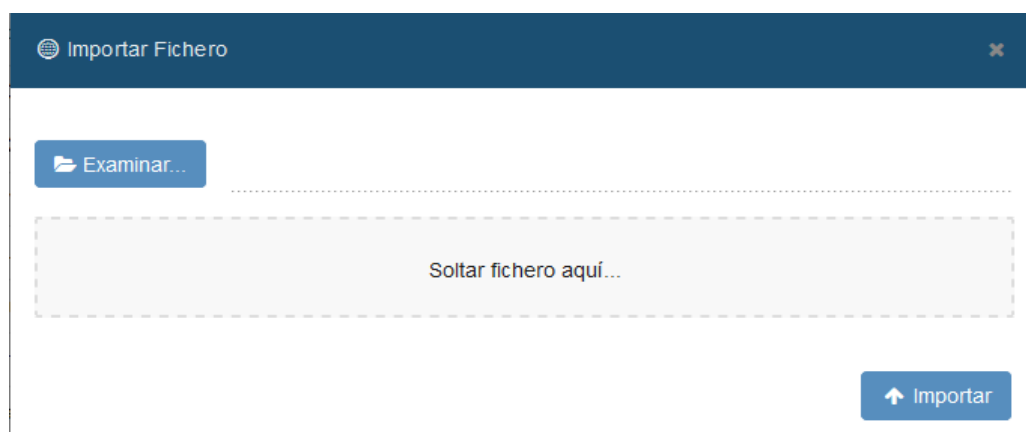
Crear Dirección IP: Desde esta pantalla incluiremos una Dirección IP para nuestra Lista Blanca.



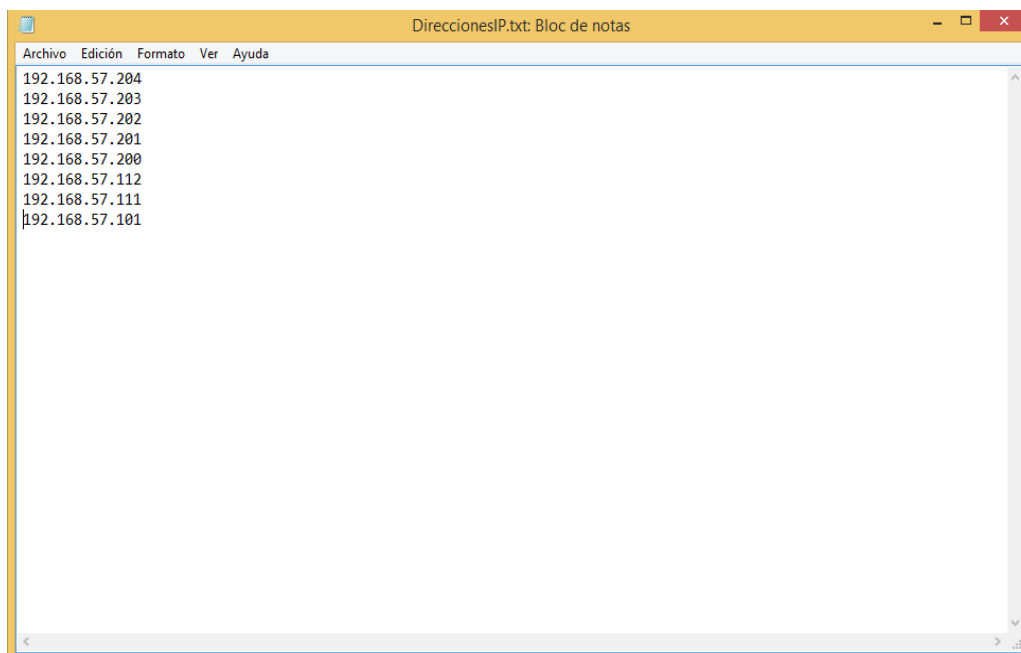
Se elige la Dirección IP que queremos que este en nuestra Lista Blanca.



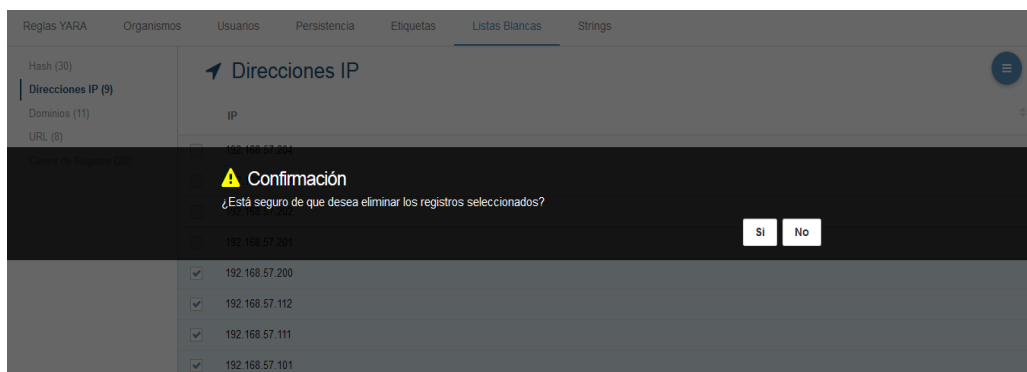
Importar Dirección IP: Desde esta pantalla se importan las direcciones IP, se elige nuestro fichero que debe de ser con extensión .txt.



Se pueden importar un solo Hash o varios, el formato del fichero seria el siguiente:

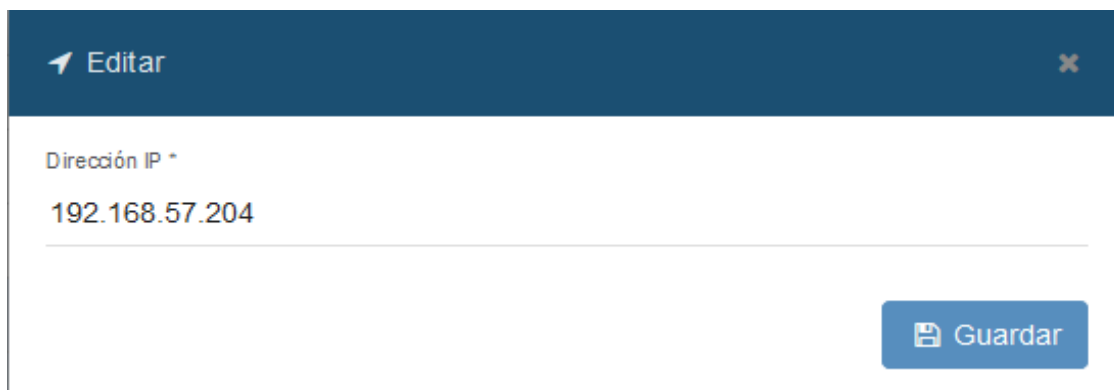


Eliminar Dirección IP: Se selecciona la dirección IP o las direcciones IP que se quieren eliminar.



Para modificar una Dirección IP doble clic sobre la dirección IP a modificar.

Editar Direcciones IP: Para modificar una dirección IP doble clic sobre la dirección IP a modificar.



3. **Dominios:** Se muestra un listado de Dominios, se pueden modificar o eliminar dichos dominios.



	Dominio
☐	www.sisi3.de
☐	www.sisi2.de
☐	www.sisi1.de
☐	www.sisi.de
☐	www.nnnn.com
☐	www.marca.es
☐	www.hola.com
☐	www.globo.com
☐	www.bing.com
☐	www.abcd.es
☐	time.windows.com

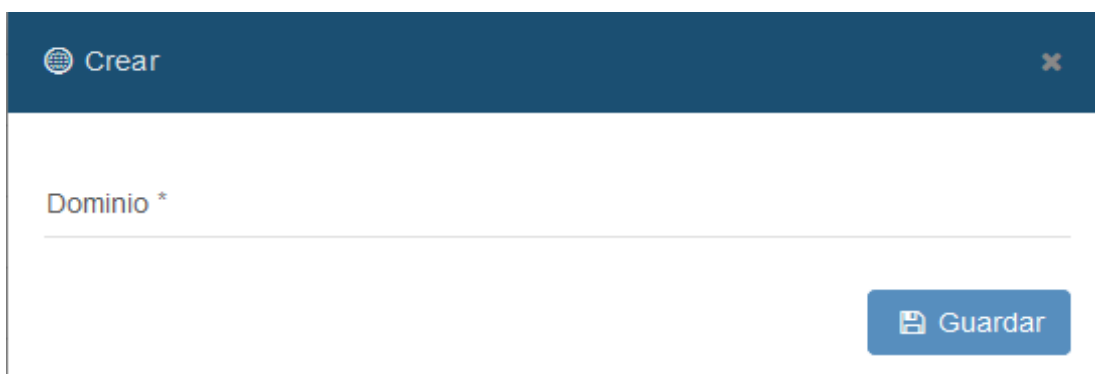
En la parte superior existen las siguientes opciones.



Se podrán crear, importar o eliminar un Dominio.



Crear Dominios: Desde esta pantalla crearemos un Dominio para nuestra Lista Blanca.



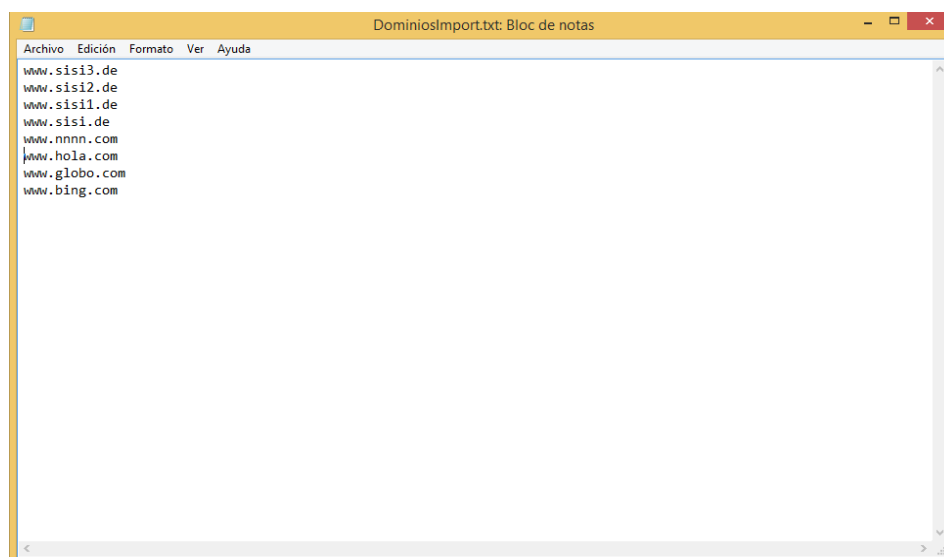
Elegimos el Dominio que queremos que este en nuestra Lista Blanca.



Importar Dominio: Desde esta pantalla se importan los Dominios, se elige el fichero que debe de ser con extensión .txt.

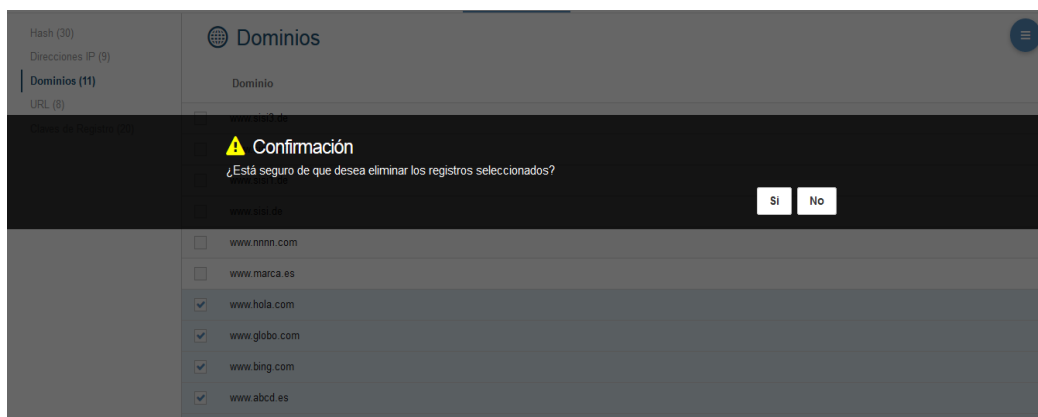


Se pueden importar un solo Dominio o varios, el formato del fichero seria el siguiente:

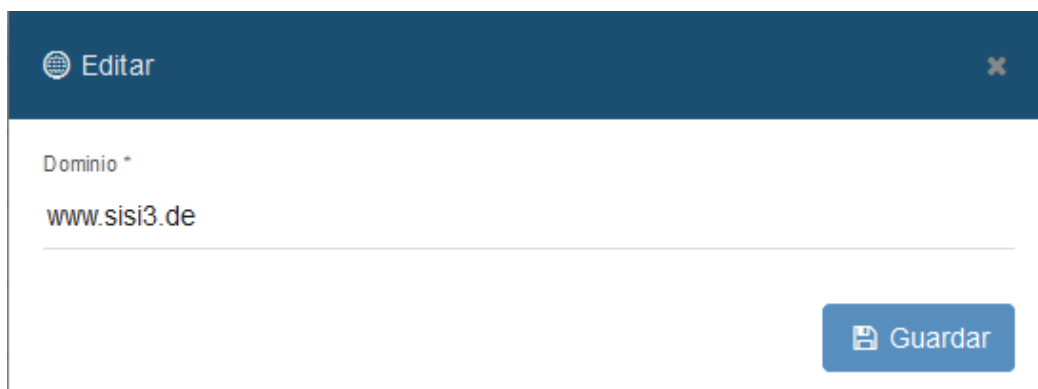




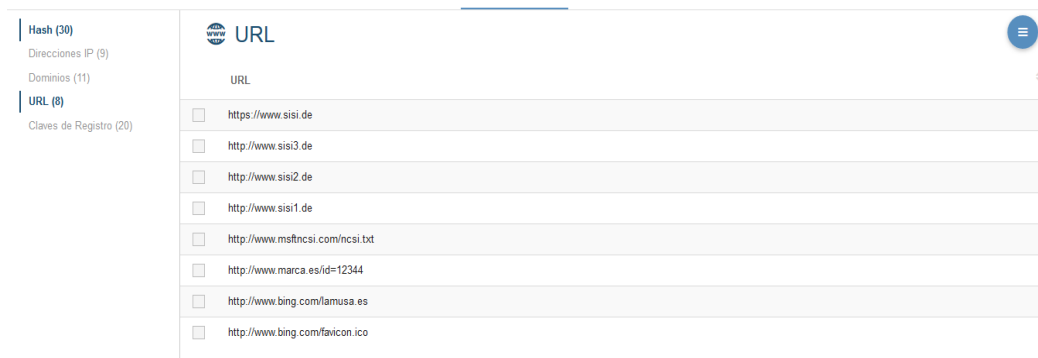
Eliminar Dominio: Seleccionamos el Dominio o Dominios que se quieren eliminar.



Editar Dominios: Para modificar un Dominio doble clic sobre el Dominio a modificar.



4. **URL:** Se muestra un listado de direcciones URL, se pueden modificar o eliminar dichas direcciones URL.



En la parte superior existen las siguientes opciones.



Se podrán crear, importar o eliminar un Dominio.



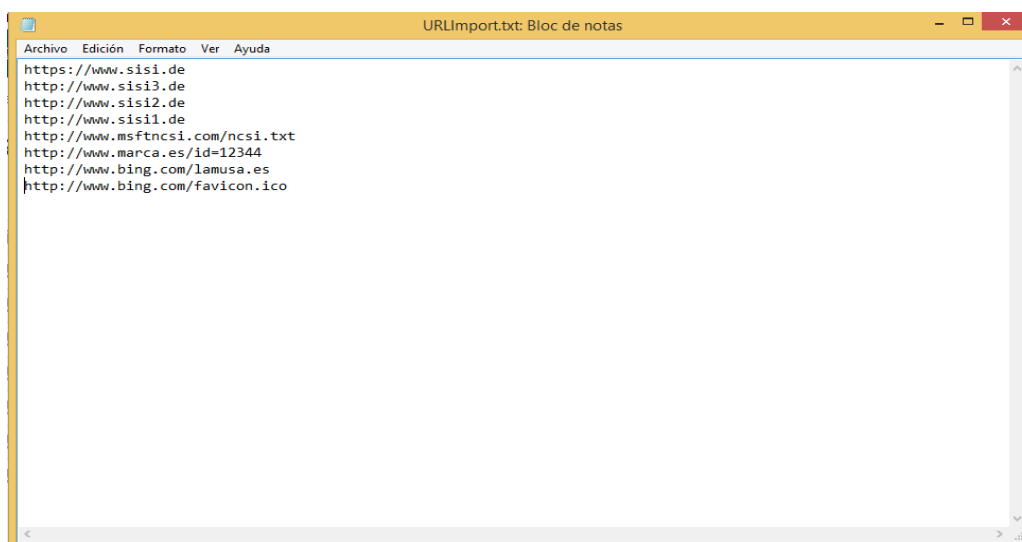
Crear Dominio: Desde esta pantalla crearemos un Dominio para nuestra Lista Blanca.

Elegimos el Dominio que queremos que este en nuestra Lista Blanca.

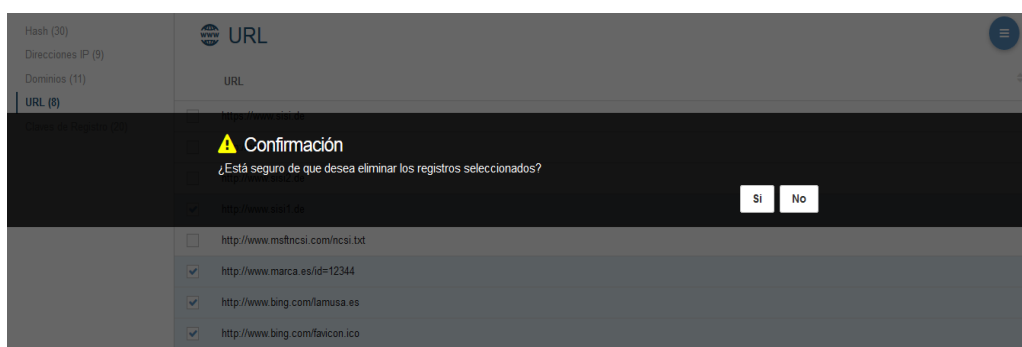


Importar Dominio: Desde esta pantalla se importan dominios, elegimos nuestro fichero que debe de ser con extensión .txt.

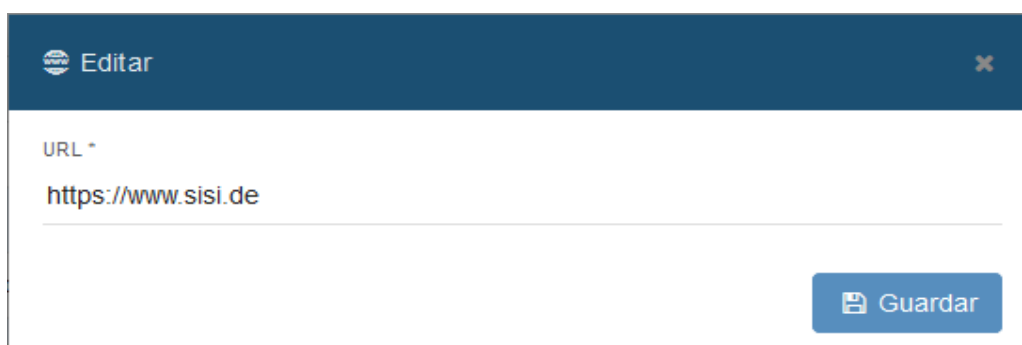
Se pueden importar solo una dirección URL o varias a la vez, el formato del fichero seria el siguiente:



Eliminar URL: Seleccionamos la dirección URL o las direcciones URL que se quieran eliminar.



Editar URL: Para modificar una dirección URL doble clic sobre la dirección URL a modificar.



5. Claves de Registro: Se dispone de un listado de Claves de Registro.

Hash (30) Direcciones IP (9) Dominios (11) URL (8) Claves de Registro (20)	Claves de Registro Clave <table> <tr><td>☐</td><td>HKLM\Software\Python\PythonCore\bot\Modules\functools42</td></tr> <tr><td>☐</td><td>HKLM\Software\Python\PythonCore\bot\Modules\functools4</td></tr> <tr><td>☐</td><td>HKLM\Software\Python\PythonCore\bot\Modules\functools1</td></tr> <tr><td>☐</td><td>HKLM\Software\Python\PythonCore\bot\Modules\functools\</td></tr> <tr><td>☐</td><td>HKEY_USERS\Software\Microsoft\Windows\CurrentVersion\Explorer\StartPage2\</td></tr> <tr><td>☐</td><td>HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\SafeBoot\Option\</td></tr> <tr><td>☐</td><td>HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Error Message Instrument\</td></tr> <tr><td>☐</td><td>HKEY_LOCAL_MACHINE\Software\Python\PythonCore\bot\Modules\linecache\</td></tr> <tr><td>☐</td><td>HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\Windows Error Reporting\WMR\</td></tr> <tr><td>☐</td><td>HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\Windows Error Reporting\WMR\</td></tr> <tr><td>☐</td><td>HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\Windows Error Reporting\WMR\</td></tr> </table>	☐	HKLM\Software\Python\PythonCore\bot\Modules\functools42	☐	HKLM\Software\Python\PythonCore\bot\Modules\functools4	☐	HKLM\Software\Python\PythonCore\bot\Modules\functools1	☐	HKLM\Software\Python\PythonCore\bot\Modules\functools\	☐	HKEY_USERS\Software\Microsoft\Windows\CurrentVersion\Explorer\StartPage2\	☐	HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\SafeBoot\Option\	☐	HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Error Message Instrument\	☐	HKEY_LOCAL_MACHINE\Software\Python\PythonCore\bot\Modules\linecache\	☐	HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\Windows Error Reporting\WMR\	☐	HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\Windows Error Reporting\WMR\	☐	HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\Windows Error Reporting\WMR\
☐	HKLM\Software\Python\PythonCore\bot\Modules\functools42																						
☐	HKLM\Software\Python\PythonCore\bot\Modules\functools4																						
☐	HKLM\Software\Python\PythonCore\bot\Modules\functools1																						
☐	HKLM\Software\Python\PythonCore\bot\Modules\functools\																						
☐	HKEY_USERS\Software\Microsoft\Windows\CurrentVersion\Explorer\StartPage2\																						
☐	HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\SafeBoot\Option\																						
☐	HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Error Message Instrument\																						
☐	HKEY_LOCAL_MACHINE\Software\Python\PythonCore\bot\Modules\linecache\																						
☐	HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\Windows Error Reporting\WMR\																						
☐	HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\Windows Error Reporting\WMR\																						
☐	HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\Windows Error Reporting\WMR\																						

En la parte superior se dispone de las siguientes opciones.



Se podrán crear, importar o eliminar un Hash.



Crear Clave de Registro: Desde esta pantalla se puede crear una Clave de Registro para nuestra Lista Blanca.

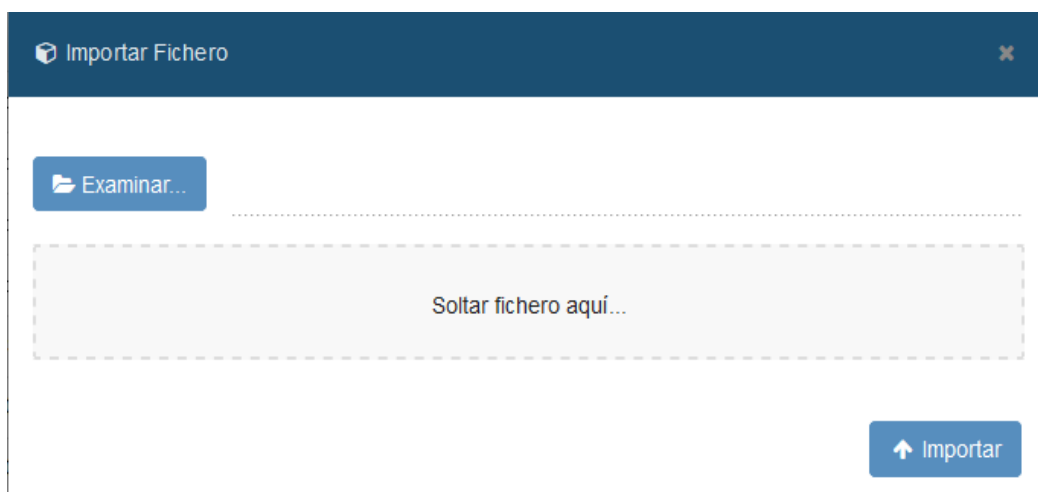
Crear

Clave de Registro *

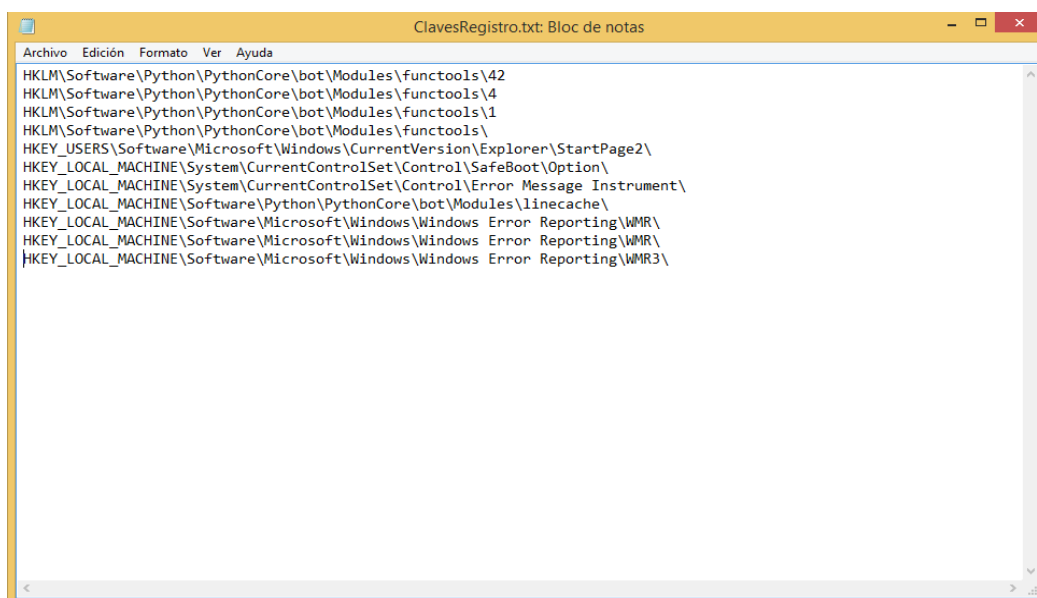
Elegimos la Clave de Registro que queremos incluir en nuestra Lista Blanca.



Importar Clave de Registro: Desde esta pantalla se importan Claves de Registro, elegimos el fichero que debe de ser con extensión .txt.

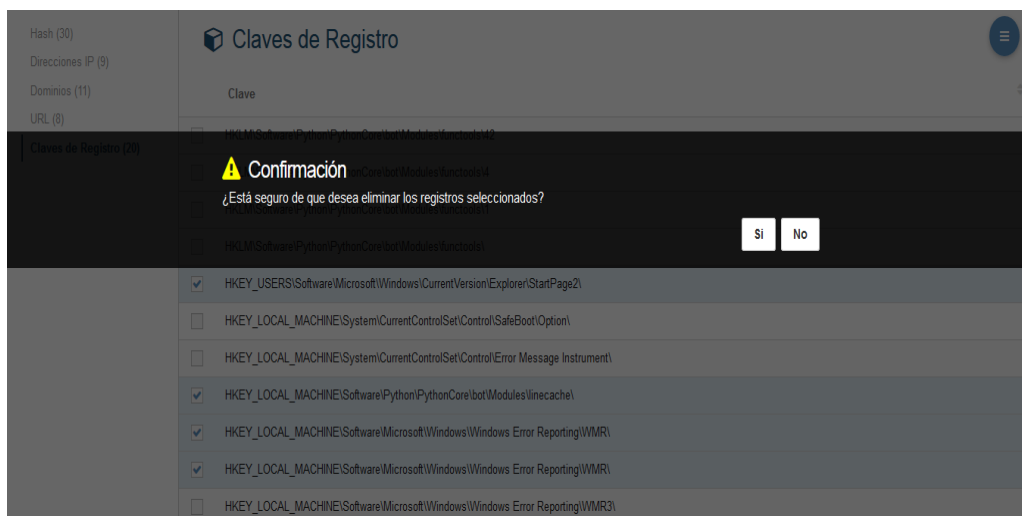


Se pueden importar solo una Clave o varias a la vez, el formato del fichero debe ser el siguiente:

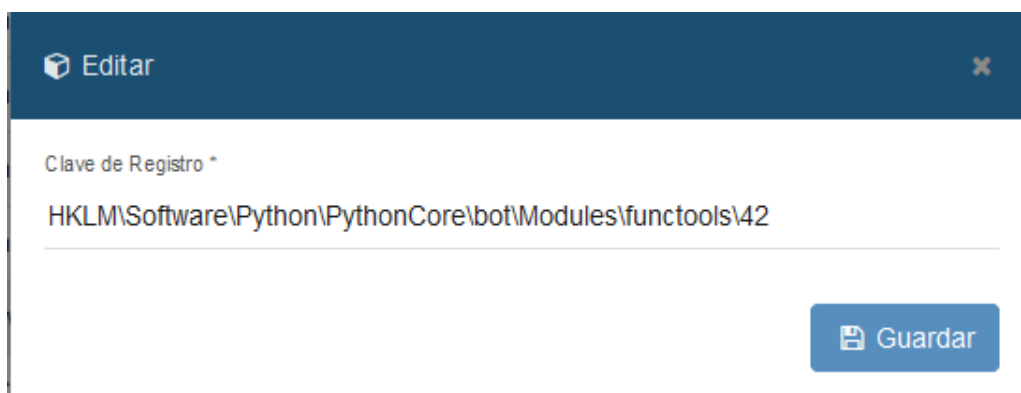




Eliminar Clave de Registro: Se seleccionan la Clave o Claves de Registro que se quieren eliminar.

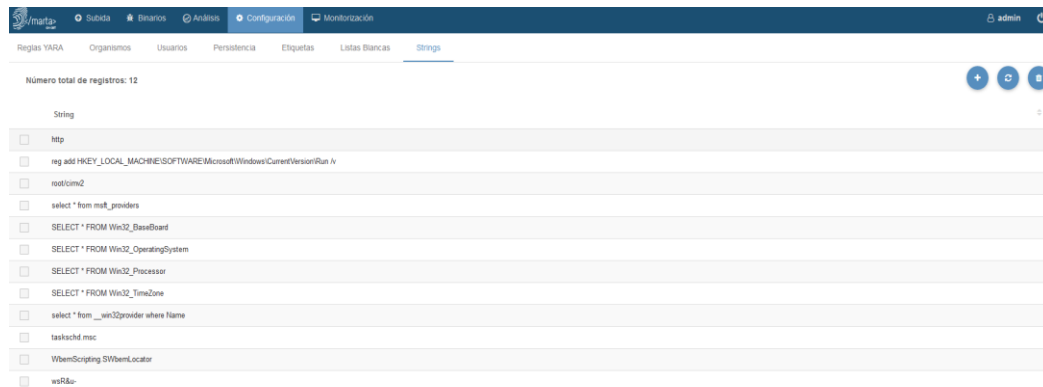


Editar Clave de Registro: Para modificar una Clave de Registro doble clic sobre la Clave a modificar.

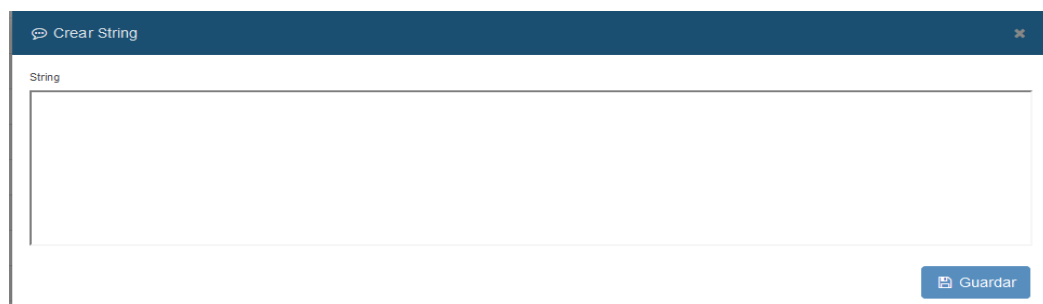


6.7 STRINGS

Esta pestaña es una herramienta que facilita la búsqueda de cadenas de texto (*strings*) específicas en la memoria de la máquina durante la ejecución del análisis.

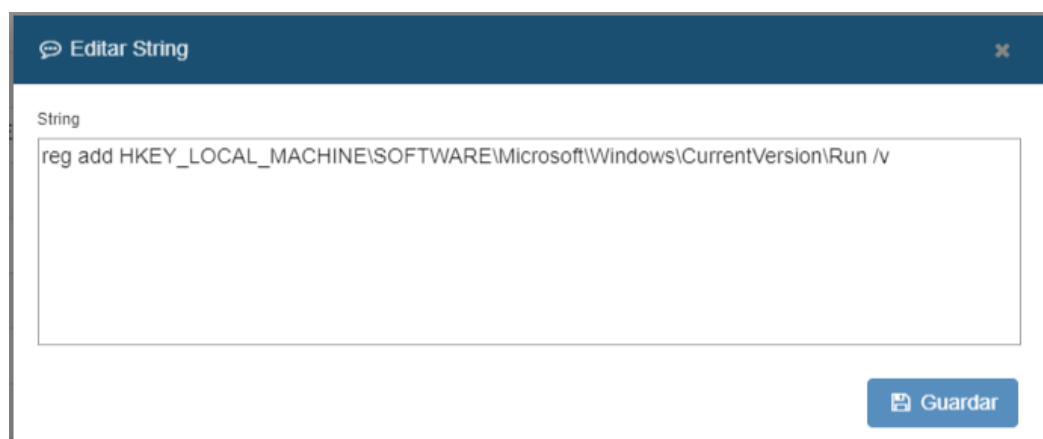


Si se quiere Crear una *String* nueva, se hace clic en el botón  y saldrá la siguiente pantalla.



Se escribe el *String* que se quiere buscar en los análisis y se pulsa el botón Guardar.

Para Modificar realizamos doble clic sobre el *String* que deseamos Modificar.



Se Modifica el *String* y se pulsa el botón Guardar.

Para eliminar se dispone de la opción de eliminar varias *Strings* a la vez, se seleccionan



y hace clic en el botón



Se hace clic en Si y se borra el *String* seleccionado o seleccionados. Si se realiza esta operación desaparecerán de nuestros análisis los *strings* a los que se hacía referencia.

6.8 COLECTORES

Esta pestaña está diseñada para facilitar todas las gestiones relativas a los colectores de MARTA. Esta opción solo será visible para perfiles con rol administrador.

Reglas YARA	Organismos	Usuarios	Persistencia	Etiquetas	Listas Blancas	Strings	Colectores
Nº total de registros: 7							
Nombre			Activo		Ficheros subidos		Última subida
☐	VirusTotal		✓		10		14-09-2018
Configuraciones: (6)							
Sandbox		Máquina Virtual		Red	Conf. activa		
	Cuckoo	Windows 10, Office 2016		Tor	✓		/ ✖
	Joe	Windows 7 x64, Office 2013		InetSim	✗		/ ✖
	Cuckoo	Windows 7 x64, Office 2013		Tor	✓		/ ✖
	Cuckoo	Windows 8 x64, Office 2013		Tor	✓		/ ✖
	Cuckoo	Windows 7 x86, Office 2013		Tor	✓		/ ✖
	Cuckoo	Windows 8 x86, Office 2013		Tor	✓		/ ✖
☐	ZeusTracker		✓		100		14-09-2018
☐	Sophos		✓		34		14-09-2018
☐	OnDemand		✓		78		14-09-2018
☐	MalCide		✗		45		14-09-2018
☐	FileOnDemand		✓		65		14-09-2018
☐	CyberCrime		✗		23		14-09-2018

Los colectores son procesos que recogen periódicamente *malwares* de páginas web dedicadas al listado de *malwares*. Es decir, cada cierto tiempo (por lo general, una vez al día), cada colector se baja de su página web todos los *malwares* nuevos registrados, los sube a MARTA y les realiza uno o varios análisis.

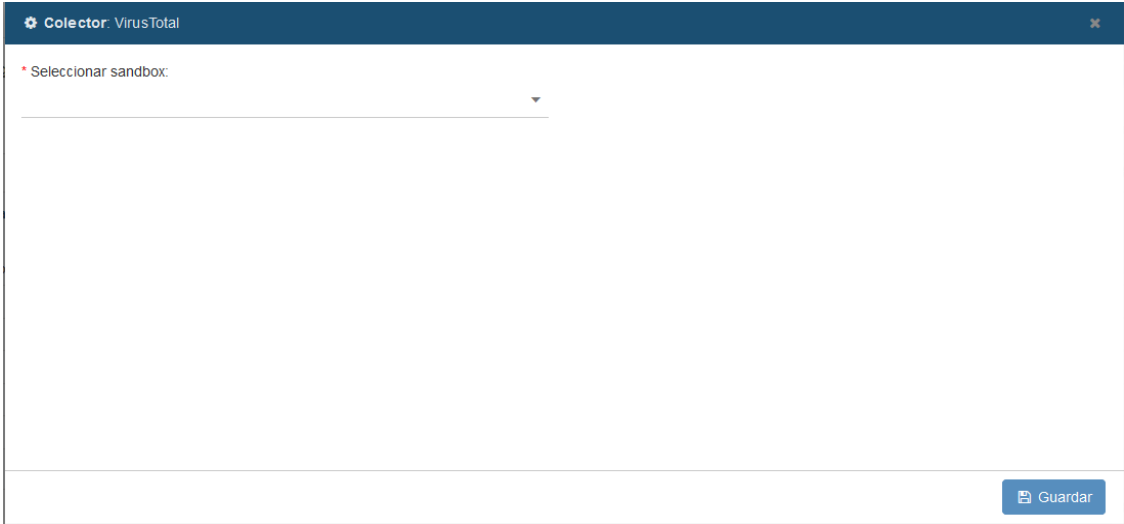
Cada colector es una fuente. Las fuentes son las diferentes formas a través de las cuales pueden subirse ficheros a MARTA. Además de los colectores, existe la

fuelle OnDemand, es decir, subida manual de ficheros a MARTA a través de la interfaz web.

Si una fuente sube a MARTA un fichero que ya había subido anteriormente (distinción por MD5), el fichero se ignora. No se le vuelven a pasar los scripts estáticos, ni se le realiza un análisis nuevo, ya que es muy posible que varias páginas web dedicadas al listado de *malwares* listen el mismo malware, o listen un malware antiguo como nuevo. La única excepción a esto es la fuente OnDemand. Si a través de la interfaz web de MARTA se sube un fichero que ya había sido subido anteriormente, no se le vuelven a pasar los scripts estáticos, pero sí que se realizan los análisis dinámicos que se marquen en el formulario de subida.

Se puede editar una configuración, crear o eliminar una configuración nueva.

Crear Configuración: Primero se selecciona la *sandBox*.



Después de elegir la *sandBox* se debe de configurar.

Colector: VirusTotal

* Seleccionar sandbox:

Cuckoo

☒ Configuración activa

▼ Cuckoo Sandbox

Máquina Virtual
Red
Tor
Prioridad
7 (Máxima)
Tiempo (seg.)
240

☐ Forzar

☐ Interacción con el ratón
☐ Interacción con el teclado

☒ Enviar tecla repetidamente
Tecla
LEFT

☐ Enviar texto predefinido

Guardar

Si se quiere Editar se hace clic en el icono .

Colector: VirusTotal

☒ Configuración activa

▼ Cuckoo Sandbox

Máquina Virtual
Windows 10, Office 2016
Red
Tor
Prioridad
7 (Máxima)
Tiempo (seg.)
540

☒ Forzar

☒ Interacción con el ratón
☒ Interacción con el teclado

☒ Enviar tecla repetidamente
Tecla
DELETE

☐ Enviar texto predefinido

Usuario Privilegiado

Definir fecha del sistema de la máquina virtual

Tiempo entre tecla y tecla (seg.)
4

Guardar

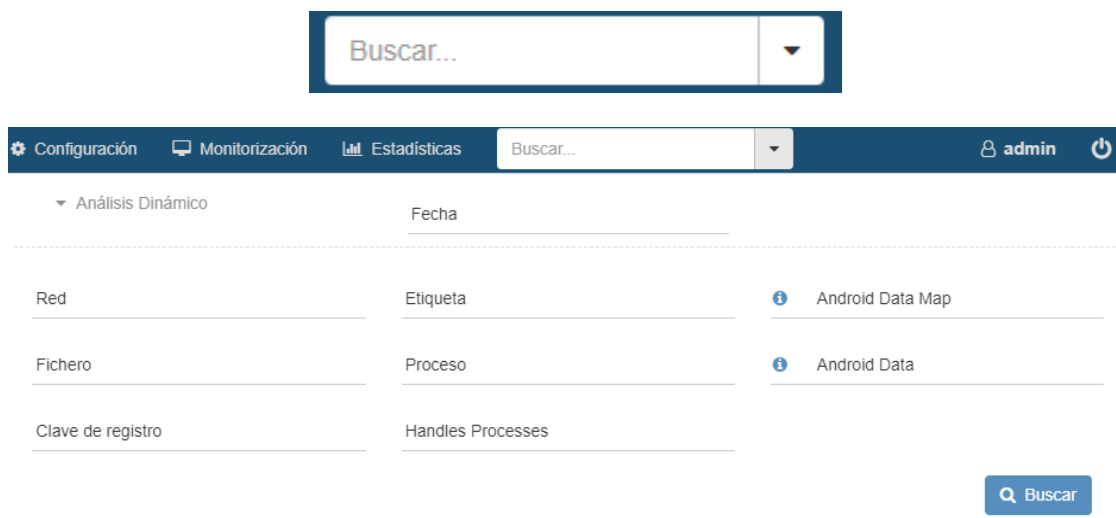
7. BÚSQUEDA AVANZADA

MARTA cuenta con una herramienta de *búsqueda avanzada*, que permite buscar ficheros *filtrando por cualquier dato* que pudiera obtenerse tanto de los resultados de los scripts estáticos como de los análisis dinámicos. Por ejemplo, es posible buscar todos los ficheros que crean un fichero .exe y sobrescriben la clave de registro Software\Microsoft\Windows\CurrentVersion\Run.

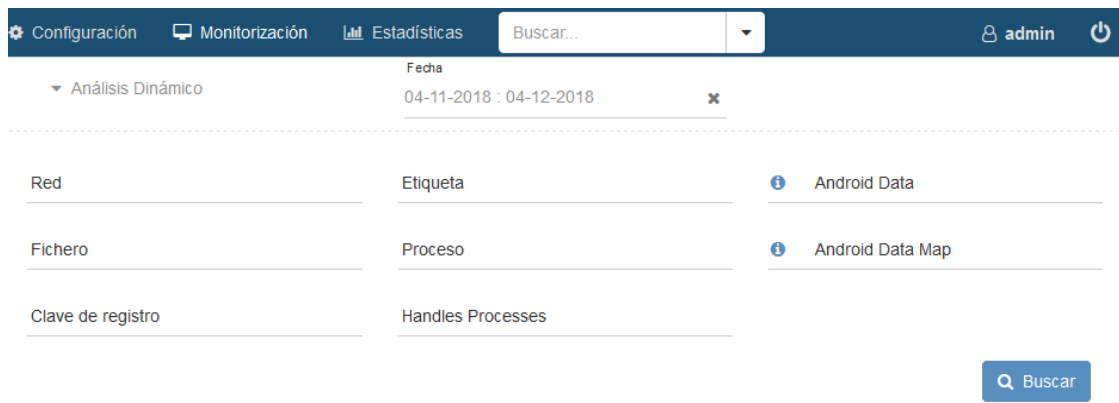
Para poder realizar búsquedas por varios campos se deberá de poner el campo seguido de dos puntos. Estos son los campos por los que se puede filtrar:

Red, fichero, clave, etiqueta, manejador, proceso, androidData, androidDataMap, androidRaw, Hash, dll, functiondll, anomalía, bounddll, boundfunctiondll, macro, embebido, exports, packer, Objetopdf, firma, firmacert, versión, Android, androidActivity, androidResource, androidProvider androidReceiver, androidPermission, androidService.

Se puede filtrar desde cualquier parte de nuestra aplicación MARTA.



Para poder ver su funcionalidad realizaremos el siguiente ejemplo con una búsqueda múltiple:



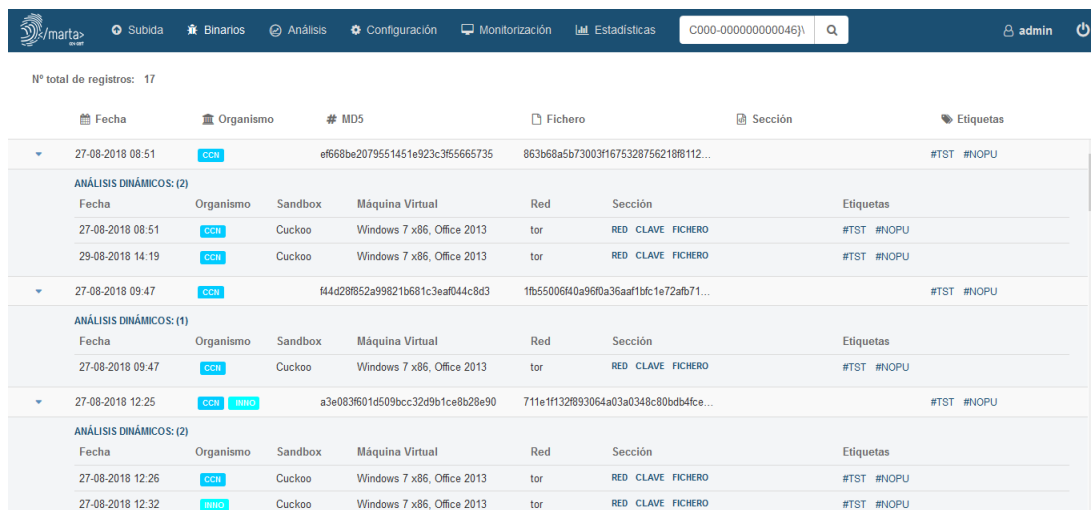
Se rellenan varios campos en los que se encontraran resultados dentro de los binarios

Fichero:C:\Program Files\Adobe\Reader 9.0\Reader\plug_ins\Accessibilit

Red: 103

Clave de Registro: HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Interface\{00000134-0000-0000-C000-000000000046}\

Es importante resaltar que *la fecha va predefinida en los últimos 30 días, por lo que sacara resultados de los últimos 30 días, si queremos una búsqueda mayor o menor en tiempo podemos cambiarla en el campo fecha.*



Fecha	Organismo	# MD5	Fichero	Sección	Etiquetas
27-08-2018 08:51	CCN	e1668be2079551451e923c3f55665735	863b68a5b73003f1675328756218b112...		#TST #NOPU
ANÁLISIS DINÁMICOS: (2)					
27-08-2018 08:51	CCN	Cuckoo	Windows 7 x86, Office 2013	tor	RED CLAVE FICHERO #TST #NOPU
29-08-2018 14:19	CCN	Cuckoo	Windows 7 x86, Office 2013	tor	RED CLAVE FICHERO #TST #NOPU
27-08-2018 09:47	CCN	f44d28852a99821b681c3eaf044c8d3	1fb55006f40a960a36aaf1bfc1e72afb71...		#TST #NOPU
ANÁLISIS DINÁMICOS: (1)					
27-08-2018 09:47	CCN	Cuckoo	Windows 7 x86, Office 2013	tor	RED CLAVE FICHERO #TST #NOPU
27-08-2018 12:25	CCN	a3e083f601d509bcc32d9b1ce8b28e90	711e1f132f893064a03a0348c80bdb4fce...		#TST #NOPU
ANÁLISIS DINÁMICOS: (2)					
27-08-2018 12:26	CCN	Cuckoo	Windows 7 x86, Office 2013	tor	RED CLAVE FICHERO #TST #NOPU
27-08-2018 12:32	IRMO	Cuckoo	Windows 7 x86, Office 2013	tor	RED CLAVE FICHERO #TST #NOPU

En esta pantalla en la parte **SECCIÓN** es donde vemos que nuestra Búsqueda ha encontrado los datos que estamos buscando. **Red, Clave Fichero**

8. INFORME PERSONALIZADO

MARTA permite la generación de *informes* a partir de un análisis dinámico. Estos informes incluyen por defecto toda la información extraída del análisis, y también toda la información de los scripts estáticos. Sin embargo, es posible generar informes personalizados con sólo algunas partes de esta información.

Para acceder a esta opción, debemos de estar dentro de un análisis, y en la parte superior derecha hacemos clic en  “Informe Personalizado”.

Se elige con un *check* las partes que queremos que salgan en el análisis, después pulsamos sobre PDF o DOC para elegir el formato.



Informe Personalizado

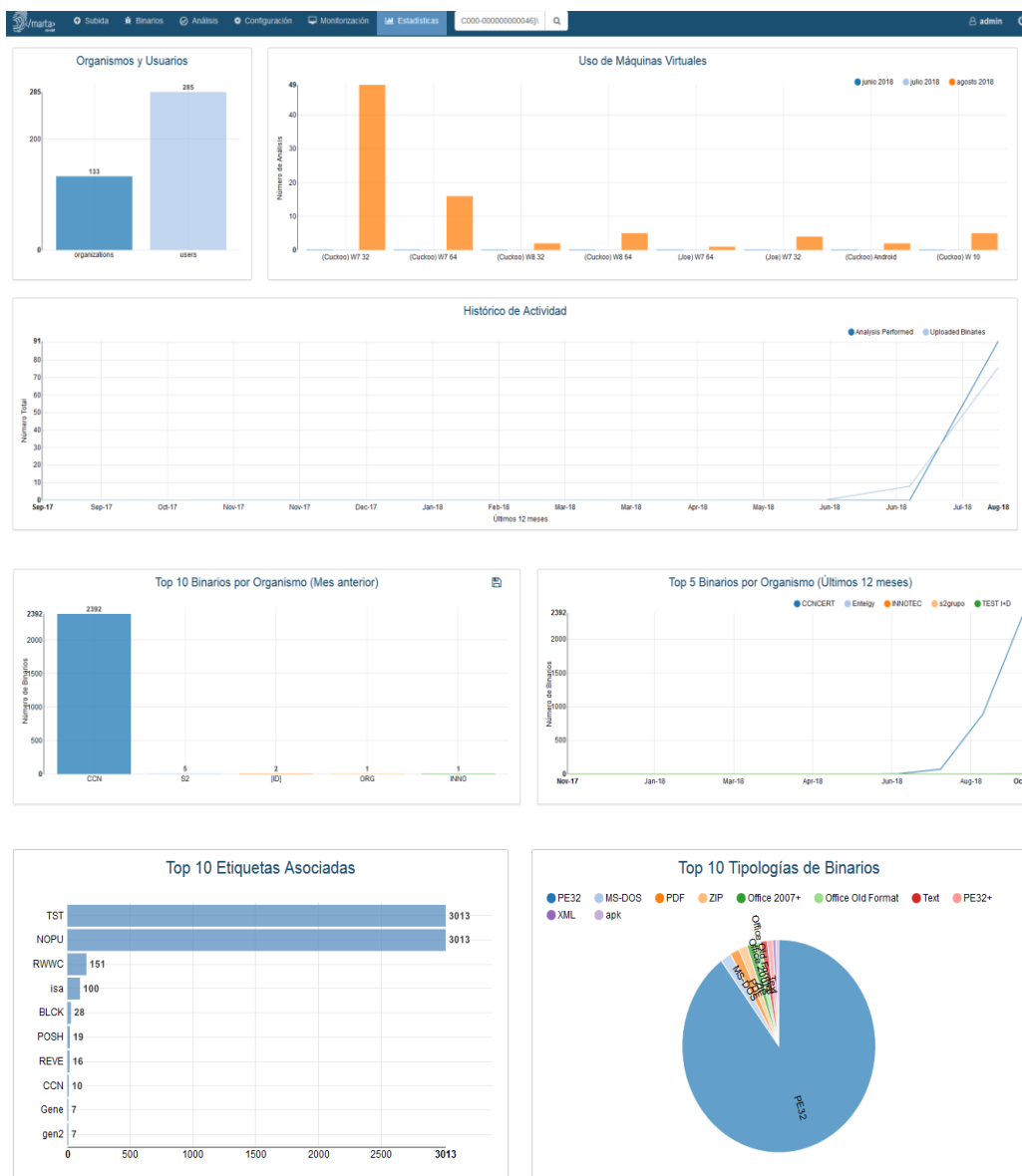


Fichero: excel (3).xlsm

- ☒ RESUMEN EJECUTIVO
- ☒ CARACTERÍSTICAS DEL CÓDIGO DAÑINO
- ☒ DETALLES GENERALES
- ☒ CARACTERÍSTICAS TÉCNICAS
 - ☒ PROCESOS DETECTADOS
 - ☒ MUTEX
 - ☒ FICHEROS
 - ☒ REGISTRO
 - ☒ HOOKS
 - ☒ SERVICIOS
- ☒ PERSISTENCIA EN EL SISTEMA
- ☒ CONEXIONES DE RED
 - ☒ TRÁFICO DNS
 - ☒ TRÁFICO HTTP
 - ☒ ICMP
 - ☒ IRC
 - ☒ SMTP
 - ☒ TRÁFICO
 - ☒ USER-AGENT
- ☒ ARCHIVOS RELACIONADOS
- ☒ INFORMACIÓN DEL ATACANTE
- ☒ ANEXO TRIANA
 - ☒ VirusTotal
 - ☒ Malekal

9. ESTADÍSTICAS

MARTA dispone de una sección de *estadísticas*, en la que se pueden consultar las etiquetas más comunes, Uso de Máquinas Virtuales, Histórico de Actividad, Top 10 Binarios por Organismo, etc.



10. MONITORIZACIÓN

Esta pestaña permite monitorizar todos los procesos y *sandbox* de MARTA, y visualizar rápidamente si hay algún problema con alguno de ellos. Esta opción solo será visible para perfiles con rol administrador.



Consta de 3 paneles:

- **Procesos:** Monitoriza los procesos de MARTA. Contiene un subpanel por cada proceso, que muestra el estado del proceso con un *check* verde (bien), o roja (mal) y la fecha de la última monitorización.

Servicios



- **Proceso de los Análisis Pendientes de Envío:** Este proceso se encarga de gestionar los análisis pedidos y programados y enviárselos a las *sandbox*.
- **Proceso de los Análisis Solicitados a las Sandbox:** Este proceso se encarga de recoger los análisis terminados de las *sandbox*.
- **Proceso de Ejecución de Reglas:** Este proceso se encarga de pasar las reglas activas sobre los análisis terminados para comprobar las reglas coincidentes.

Estos procesos se ejecutan periódicamente cada poco tiempo (minutos). Si alguno de ellos tuviera un error, su check se pondría en rojo.

- **Cuckoo:** Monitoriza la *sandbox Cuckoo*. Muestra su estado con un *check* verde (bien), o roja (mal), la fecha de la última monitorización, y la cantidad de tareas (análisis) que tiene en ejecución y pendientes. Es posible reiniciar la *sandbox* haciendo clic en el botón  **Reiniciar máquina**.
Nota Importante: En el caso de que hubiera análisis pendientes estos análisis desaparecerían.

Cuckoo



Fecha de última monitorización:
02-10-2018 12:07

Tareas

Análisis en ejecución: 0

Análisis pendientes: 0

 Reiniciar máquina

- **Joe:** Monitoriza la *sandbox Joe*. Muestra su estado con un *check* verde (bien), o roja (mal), la fecha de la última monitorización, y la cantidad de tareas (análisis) que tiene pendientes.

Joe



Fecha de última monitorización:
02-10-2018 12:09

Tareas

Análisis pendientes: 0