HERRAMIENTAS

MARTA: Manual de Usuario

Motor de Análisis Remoto
de Troyanos Avanzados

https://marta.ccn-cert.cni.es

marta@ccn-cert.cni.es

Índice

1. Introducción
2. Interfaz principal de MARTA
3. Subir binario a MARTA
    3.1. Elementos de la interfaz “Subir Binario”
    3.2. Opciones de las Sandbox Cuckoo y Joe
4. Análisis Estáticos
    4.1. Pestaña General
    4.2. Pestaña de Detalles
5. Análisis Dinámicos
6. Reglas
    6.1. Reglas IOC
    6.2. Reglas YARA
7. Etiquetas
    7.1. Operaciones
    7.2. Acciones

1. Introducción

- La herramienta MARTA, desarrollada por el CCN-CERT, es una plataforma avanzada de **sandboxing**, dedicada al ***análisis automatizado*** de múltiples tipos de ficheros, que podrían tener un comportamiento malicioso y que no son detectados por los programas antivirus.

- El análisis de ficheros incluye **ejecutables**, documentos de **office** o **pdf**, entre otros.

- En una primera fase, esta herramienta está destinada a todas las organizaciones que se encuentren adheridas al **Sistema de Alerta Temprana** del CCN-CERT que pueden acceder a ella a través de la dirección: https://marta.ccn-cert.cni.es

Ventajas para el usuario

- Detección precoz de amenazas provenientes de código dañino, analizando las características de un fichero más allá de la información facilitada por un antivirus.

- Utilización de un sitio centralizado y seguro en el que albergar las muestras de malware de un modo organizado y con una herramienta de búsqueda avanzada.

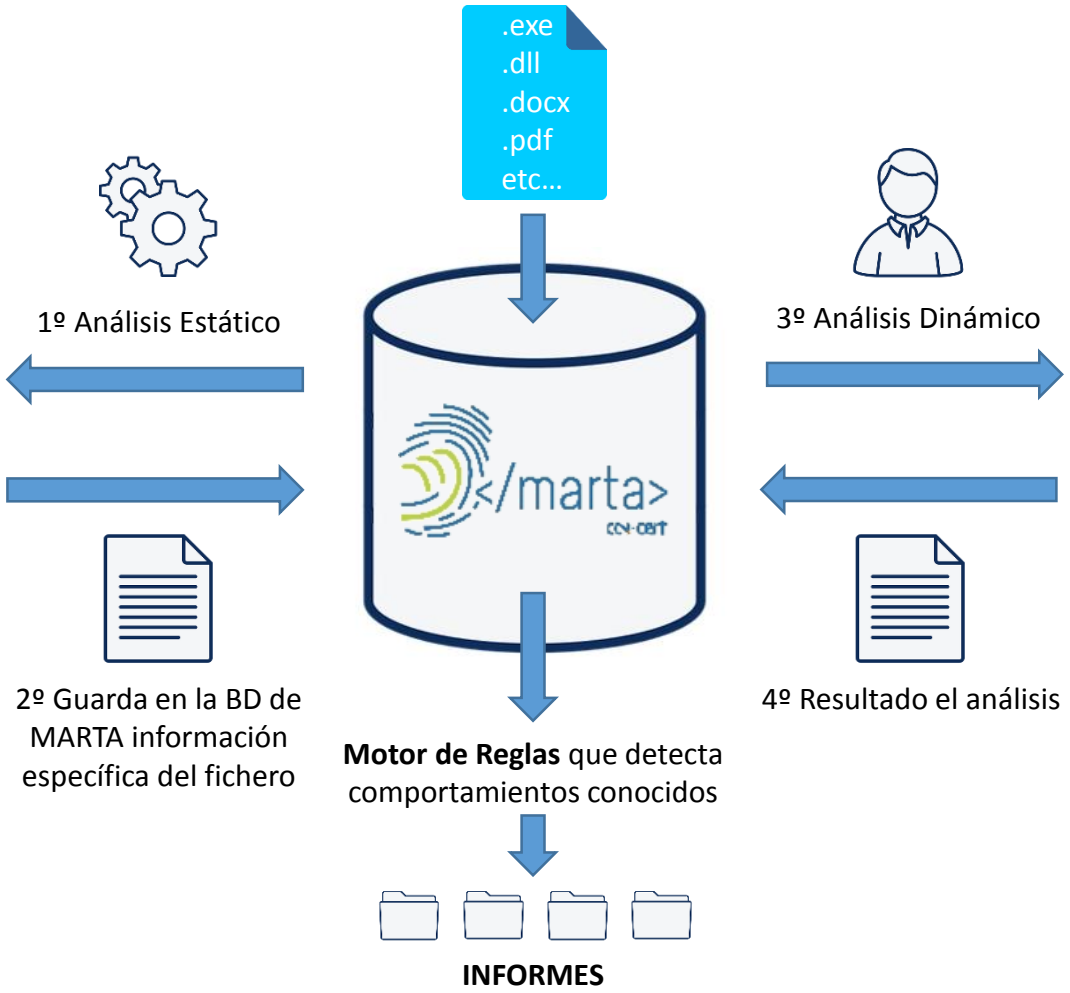
- Organización, a través de un sistema de etiquetas, de toda la información a través de un modo visual y ágil de ficheros, análisis y reglas.

1. Introducción

El siguiente esquema muestra las fases del análisis

Análisis Estático

Lo primero que hace la aplicación cuando recibe un fichero, es pasarle una serie de ***scripts "estáticos"*** (el código dañino no se ejecuta en ningún momento mientras se le analiza con estos scripts)



Análisis Dinámico

Consiste en ***infectar una máquina virtual*** que tenga instalado un sistema operativo concreto con el fichero sospechoso (clonado de máquina virtual, copiado del fichero y ejecución del mismo)

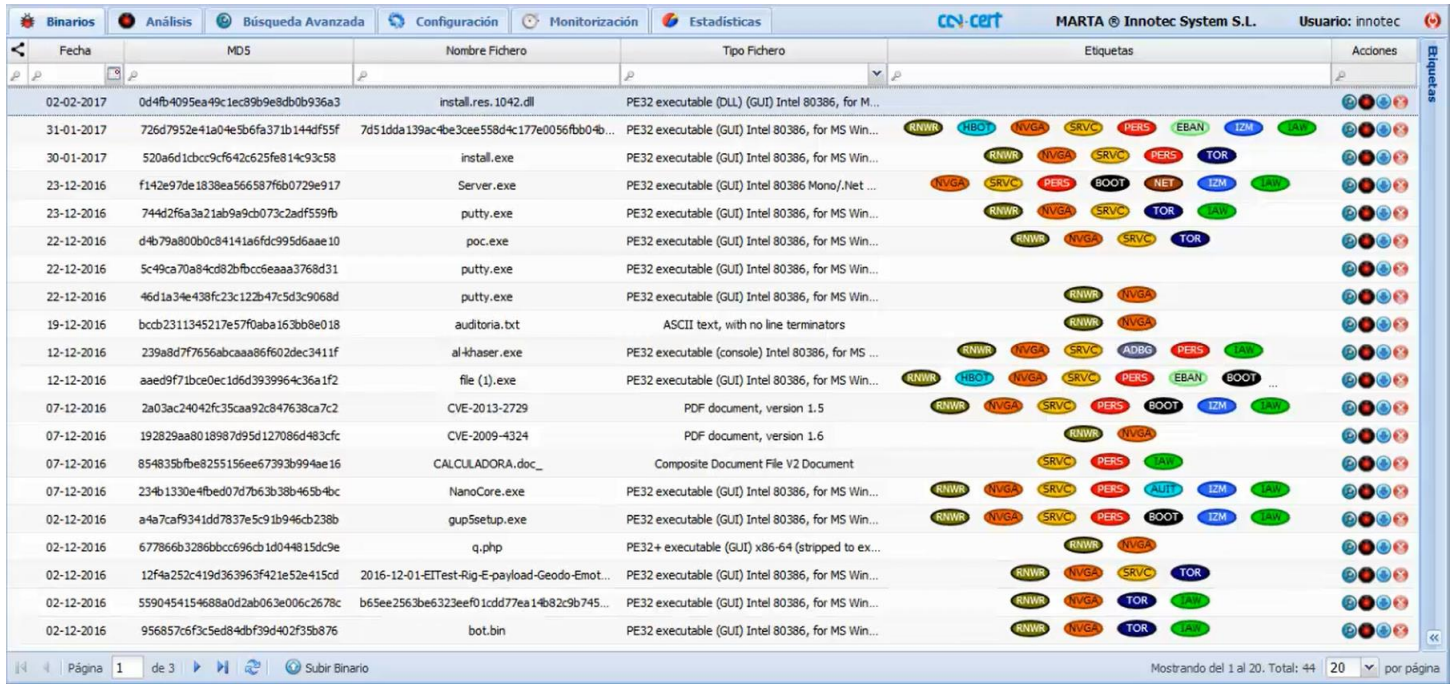
2. Interfaz principal de MARTA

Binarios: Muestra una lista con todos los ficheros subidos a MARTA. Permite subir nuevas muestras, crear análisis dinámicos y filtrar resultados.

Análisis: Muestra una lista con todos los análisis de ficheros realizados. Permite hacer filtros rápidos sobre los análisis, ver sus detalles y también reanalizar las muestras.

Búsqueda Avanzada: Permite hacer búsquedas de binarios que cumplan una serie de directrices.

Configuración: Permite la gestión de Reglas, Fuentes, Organismos y Usuarios de la aplicación.



Monitorización: Proporciona información sobre el estado de los análisis en proceso.

Estadísticas: Proporciona información visual a través de gráficas sobre estadísticas.

3. Subir binario a MARTA

Para subir un binario hacemos clic en el botón **Subir Binario** situado en la parte inferior de la aplicación:

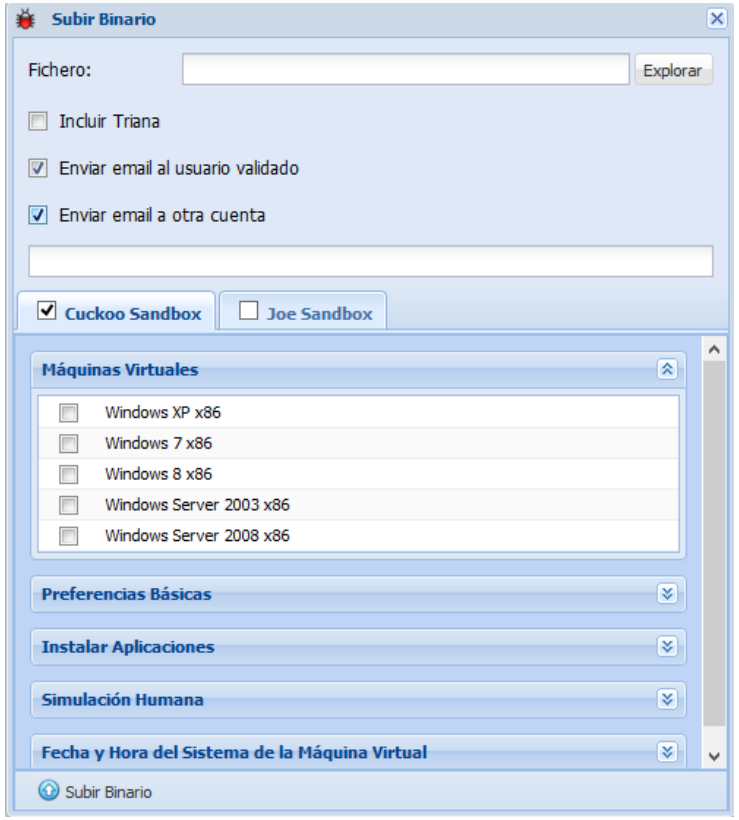
Esta vista permite **subir un fichero nuevo** a MARTA y hacerle uno o varios análisis dinámicos directamente.

3.1 Elementos de la interfaz "Subir Binario"

Fichero: elegimos el fichero que queremos analizar.

Enviar email al usuario validado: envía un mail cuando solicitamos el análisis y otro mail cuando termina.

Enviar mail a otra cuenta: es el mail de la cuenta a la que queremos enviarle nuestra subida de binario.



3.2 Opciones de las Sandbox Cuckoo y Joe

Permite configurar las opciones de análisis tanto de Cuckoo Sandbox como de Joe Sandbox.

Una vez seleccionados todos los campos, hacemos clic en el botón **Subir Binario**. Esto hará que se suba el fichero a MARTA, se le pasen los scripts estáticos y se lance un análisis dinámico por cada máquina virtual marcada en cada sandbox.

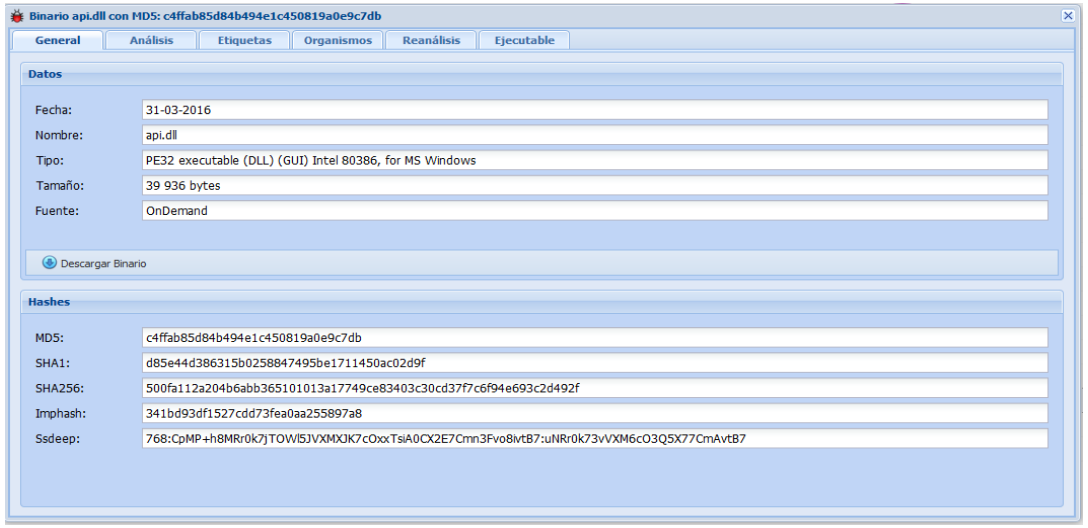
4. Análisis estáticos

Una vez subido el fichero es posible consultar diversa información del mismo, proveniente de su **análisis estático**.

4.1 Pestaña General

Muestra ***información básica acerca del fichero***:

- Fecha en la que se subió a MARTA
- Nombre
- Tipo
- Tamaño
- Fuente (esto indica si se subió manualmente, "OnDemand", o si fue recolectado por un colector)
- Hashes: MD5, SHA1, SHA256, Imphash y Ssdeep.



4.2 Pestaña de Detalles

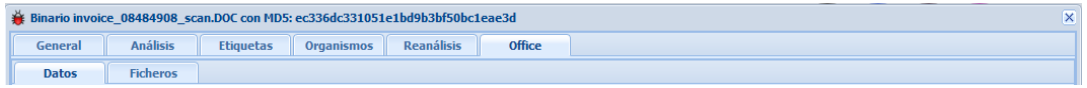
En función del fichero subido (ejecutable, .docx, .odt, .pdf, etc.), muestra toda la información extraída por los ***scripts estáticos*** acerca del fichero.

- Detalles Ejecutable:

- Detalles PDF:

- Detalles Office:

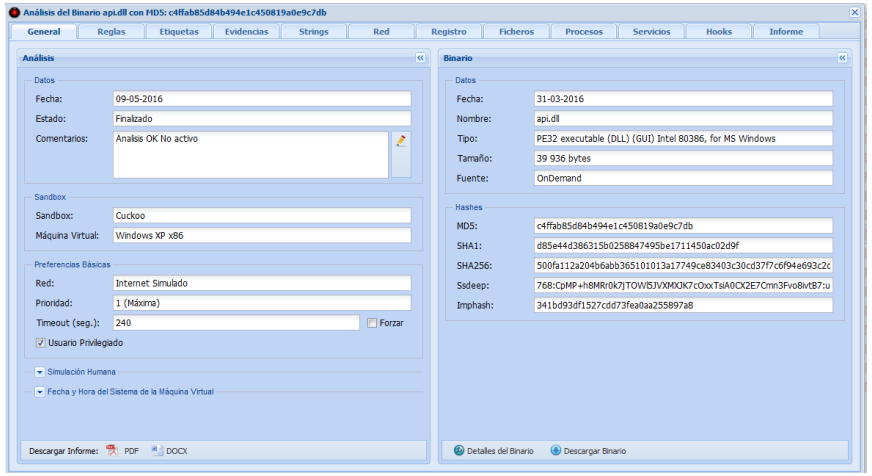
- Detalles OpenOffice:



5. Análisis dinámicos

La vista de detalle de un análisis contiene toda la ***información*** relativa a un ***análisis dinámico*** de un fichero subido a MARTA.

Se obtiene pinchando con el botón derecho del ratón sobre el fichero y seleccionando **Ver Detalle**.



Dispone de múltiples pestañas:

- **General**: Información del análisis y del fichero analizado. Permite:
  - Descargar el informe en PDF o DOCX:

  - Descargar y ver los detalles del binario:

- **Reglas**: Reglas coincidentes con el análisis y permite generar reglas a partir de él.
- **Etiquetas**: etiquetas asociadas al análisis.
- **Evidencias**: Recursos obtenidos por la sandbox durante la ejecución del análisis, como volcados de memoria o capturas de pantalla.
- **Strings**: Herramienta de búsqueda de cadenas de texto entre la memoria utilizada durante el análisis.
- **Red**: Muestra información acerca de las conexiones de red realizadas durante el análisis, agrupadas por protocolo.
- **Registro**: Claves de registro abiertas, leídas, escritas y eliminadas durante el análisis.
- **Ficheros**: Ficheros abiertos, leídos, escritos, eliminados, ejecutados, movidos y copiados durante el análisis.
- **Procesos**: Procesos creados durante el análisis.
- **Servicios:** Servicios de sistema operativo creados durante el análisis.
- **Informe**: Generación de informes a medida.

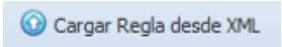
6. Reglas en MARTA

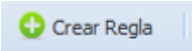
MARTA cuenta con un ***Motor de Reglas*** que permite definir ***comportamientos reconocidos***. Se puede acceder a las reglas desde la pestaña ***Configuración***.

En la barra inferior de la pestaña de reglas hay botones que permiten realizar ***gestiones*** que no están directamente ligadas a una regla:

6.1 Reglas IOC / Yara

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

- **Cargar Regla desde XML**: Abre una vista que permite cargar una regla desde un fichero XML con formato IOC (equivalente al formato en el que se descargan las reglas de MARTA). 

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

- **Activar / Desactivar**: Activa / Desactiva todas las reglas seleccionadas de la lista de reglas

Una vez creada una regla, se pueden hacer varias operaciones con ella:

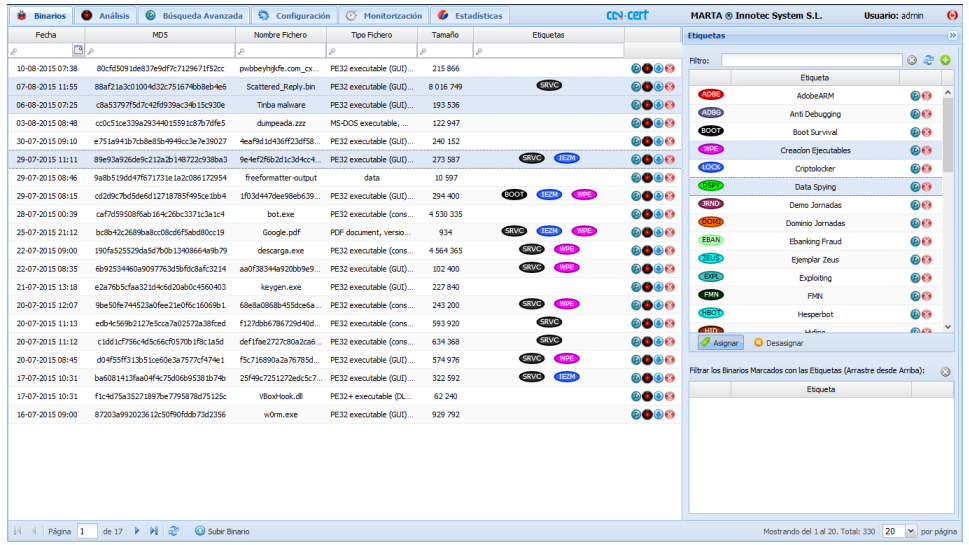
- **Ver Detalle**: Abre la vista de detalles de la regla seleccionada. Esta vista contiene toda la información relativa a la regla.
- **Descargar Regla como XML**: Permite exportar la regla a un fichero con formato XML y descargarlo.
- **Eliminar**: Elimina la regla seleccionada. Pide confirmación antes de eliminar.

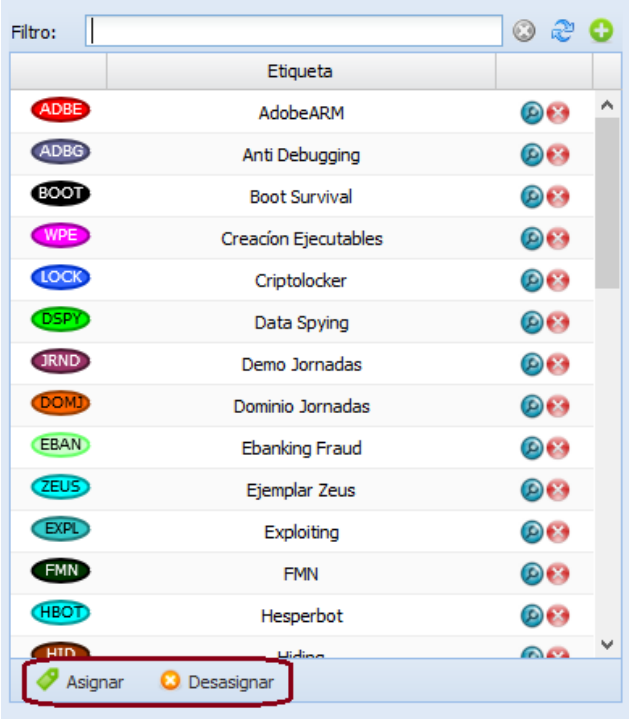
7. Etiquetas en MARTA

MARTA dispone de un ***Sistema de Etiquetas*** que permite una organización rápida y sencilla.

Acciones:

- **Asignar**: Permite asignar todas las etiquetas seleccionadas a todos los ficheros seleccionados. Solo se podrán asignar etiquetas creadas por nuestra organización.





- **Desasignar**: Permite desasignar todas las etiquetas seleccionadas de todos los ficheros seleccionados.

- **Acceso a MARTA**
  - https://marta.ccn-cert.cni.es
- **Correo electrónico**
  - marta@ccn-cert.cni.es
- **Más información**
  - https://www.ccn-cert.cni.es/herramientas-de-ciberseguridad/marta.html
- **Síguenos en**