GOBIERNO DE ESPAÑA
MINISTERIO DE LA PRESIDENCIA Y PARA LAS ADMINISTRACIONES TERRITORIALES

CCN
CENTRO CRIPTOLÓGICO NACIONAL

Guía de Seguridad de las TIC
CCN-STIC 426

REYES. MANUAL DE USUARIO

Noviembre 2017

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
CRIPTOLOGICO NACIONAL, c=ES
2017.11.30 12:10:11 +01'00'

NIPO: 785-17-039-3

Fecha de Edición: noviembre de 2017
INNOTEC SYSTEM ha participado en la realización y modificación del presente documento y sus anexos.

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

PRÓLOGO

El uso masivo de las tecnologías de la información y las telecomunicaciones (TIC), en todos los ámbitos de la sociedad, ha creado un nuevo espacio, el ciberespacio, donde se producirán conflictos y agresiones, y donde existen ciberamenazas que atentarán contra la seguridad nacional, el estado de derecho, la prosperidad económica, el estado de bienestar y el normal funcionamiento de la sociedad y de las administraciones públicas.

La Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia (CNI), encomienda al Centro Nacional de Inteligencia el ejercicio de las funciones relativas a la seguridad de las tecnologías de la información en su artículo 4.e), y de protección de la información clasificada en su artículo 4.f), a la vez que confiere a su Secretario de Estado Director la responsabilidad de dirigir el Centro Criptológico Nacional (CCN) en su artículo 9.2.f).

Partiendo del conocimiento y la experiencia del CNI sobre amenazas y vulnerabilidades en materia de riesgos emergentes, el Centro realiza, a través de su Centro Criptológico Nacional, regulado por el Real Decreto 421/2004, de 12 de marzo, diversas actividades directamente relacionadas con la seguridad de las TIC, orientadas a la formación de personal experto, a la aplicación de políticas y procedimientos de seguridad, y al empleo de tecnologías de seguridad adecuadas.

El Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica (ENS, en adelante), al que se refiere el apartado segundo del artículo 156 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, establece la política de seguridad en la utilización de medios electrónicos que permita una protección adecuada de la información.

Precisamente el Real Decreto 3/2010 de 8 de Enero, modificado por el Real Decreto 951/2015, de 23 de octubre, fija los principios básicos y requisitos mínimos así como las medidas de protección a implantar en los sistemas de la Administración, y promueve la elaboración y difusión de guías de seguridad de las tecnologías de la información y las comunicaciones (STIC) por parte de CCN para facilitar un mejor cumplimiento de dichos requisitos mínimos.

En definitiva, la serie de documentos CCN-STIC se elabora para dar cumplimiento a los cometidos del Centro Criptológico Nacional y a lo reflejado en el Esquema Nacional de Seguridad, conscientes de la importancia que tiene el establecimiento de un marco de referencia en esta materia que sirva de apoyo para que el personal de la Administración lleve a cabo su difícil, y en ocasiones, ingrata tarea de proporcionar seguridad a los sistemas de las TIC bajo su responsabilidad.

Noviembre de 2017

Félix Sanz Roldán
Secretario de Estado
Director del Centro Criptológico Nacional

ÍNDICE

1 REYES

1. REYES (REpositorio común Y EStructurado de amenazas y código dañino).
2. REYES es una herramienta desarrollada por el CCN-CERT para agilizar la labor de análisis de ciberincidentes y compartir información de ciberamenazas.
3. A través de este portal centralizado de información puede realizarse cualquier investigación de forma rápida y sencilla, accediendo desde una única plataforma a la información más valiosa sobre ciberincidentes. Una información contextualizada y correlacionada con las principales fuentes de información, tanto públicas como privadas.
4. En un primer momento, REYES se basó en la tecnología MISP (Malware Information Sharing Platform), sin embargo, en su nueva versión ha pasado a ser un portal centralizado en el que se ha integrado un metabuscador, se ha implementado un API desde cero y se ha integrado con otras herramientas del CCN-CERT.

1.1 PANTALLA DE ACCESO

5. Al acceder a la herramienta, se muestra la pantalla de acceso, cuya finalidad es que el usuario introduzca sus credenciales.

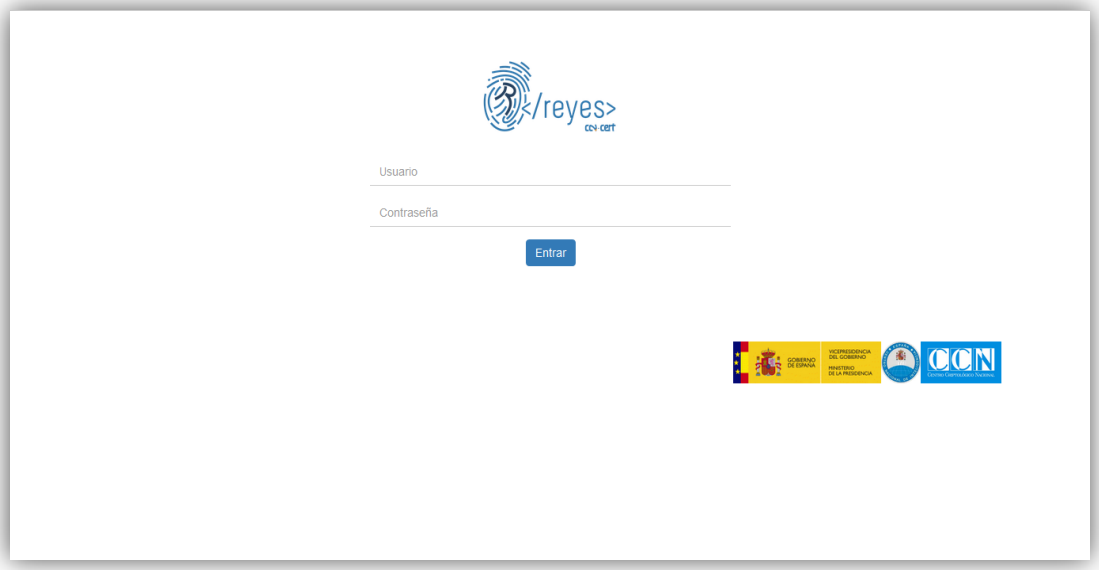


Figura 1. Pantalla de inicio de MISP

6. Una vez introducidas, si son correctas, se muestra la vista principal de la aplicación:

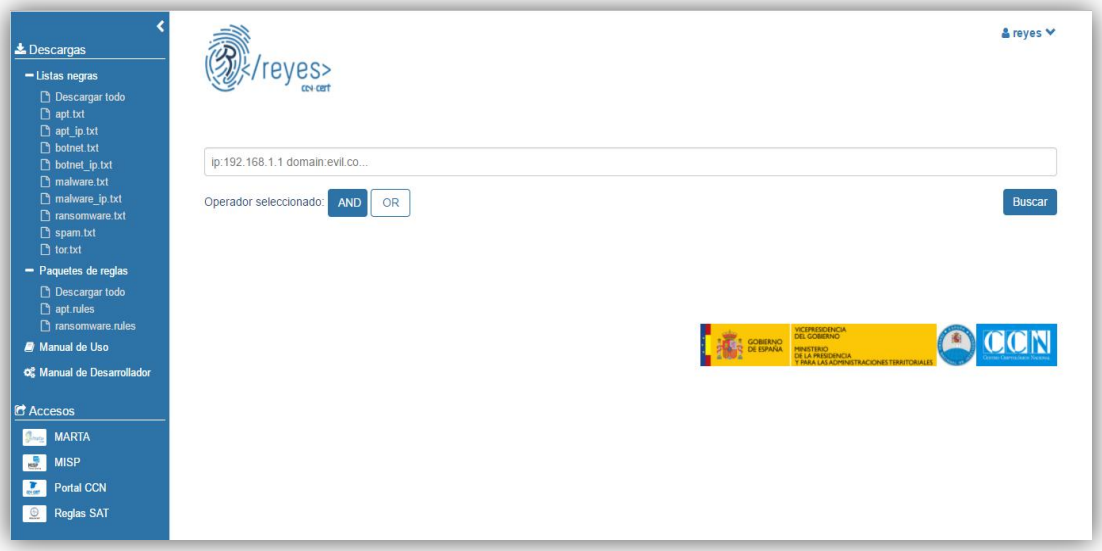


Figura 2. Vista principal de REYES

7. Al hacer login en la aplicación, se genera una sesión, que permite al usuario hacer uso de todas las funcionalidades.

8. Las sesiones caducan al cabo de dos horas y media desde la última vez que se realice una petición al servidor. Mientras el usuario esté haciendo uso de la aplicación, su sesión no caducará en ningún momento.

9. Sin embargo, un usuario puede desconectarse en cualquier momento, finalizando así su sesión, utilizando el menú de la esquina superior derecha de la vista principal:

Figura 3. Menú de usuario de REYES

10. Por seguridad, se recomienda a los usuarios utilizar este botón una vez hayan terminado de utilizar la aplicación en lugar de cerrar la pestaña del navegador, aunque en caso de no hacerlo, su sesión caducará automáticamente al cabo de 2 horas y media.

1.2 Pantalla Principal

11. Esta es la pantalla que se muestra una vez introducidas las credenciales de acceso. Por defecto, el menú lateral aparece expandido aunque se puede ocultar clicando en el siguiente botón:

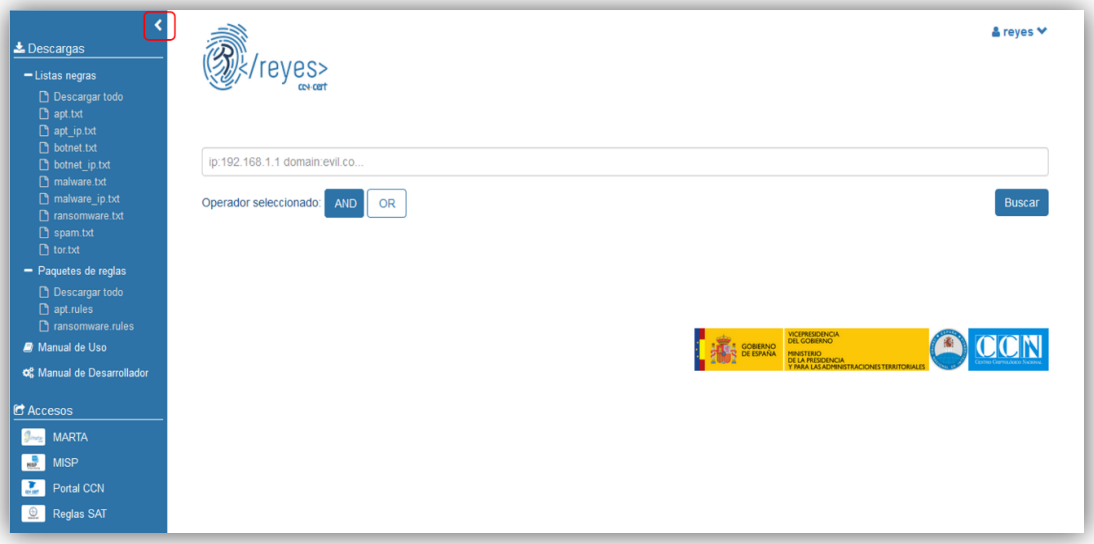


Figura 4. Pantalla principal REYES

12. La vista principal cuenta con 3 partes diferenciadas:

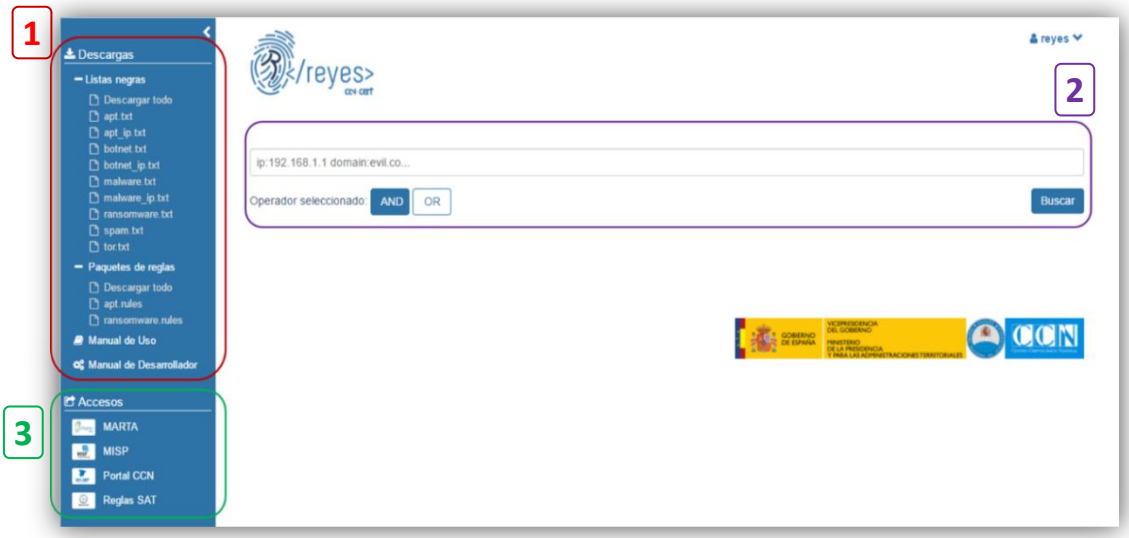


Figura 5. Partes que componen REYES

1. **Descargas**: Permiten descargar elementos independientes de las búsquedas. Actualmente: **Listas Negras**, **Paquetes de reglas**, **Manual de Uso** y el **Manual de Desarrollador**.

Figura 6. Sección de Descargas de REYES

2. Barra de Búsqueda: Permite introducir términos e iniciar búsquedas basadas en ellos.

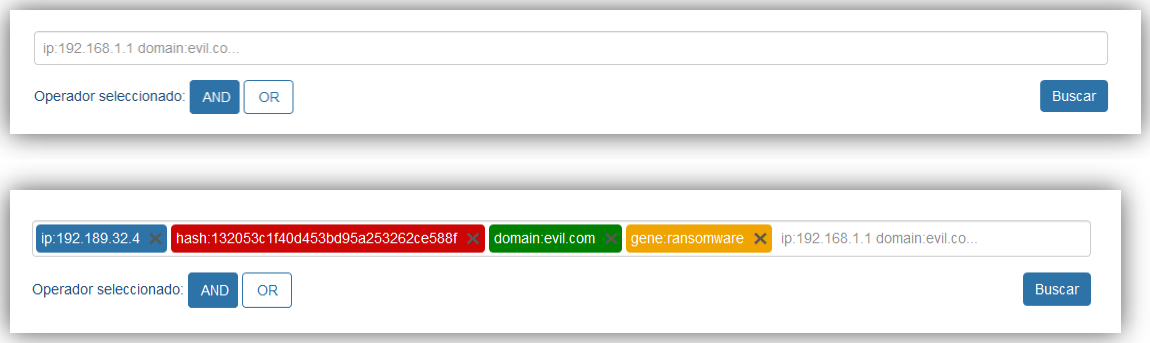


Figura 7. Barra de Búsqueda de REYES

3. Accesos Directos: Permiten acceder a las aplicaciones integradas en el single sign-on, es decir, sin necesidad de introducir credenciales de nuevo. Actualmente: **MARTA**, **MISP**, el **Portal del CCN-CERT** y el **Gestor de Reglas SAT**.

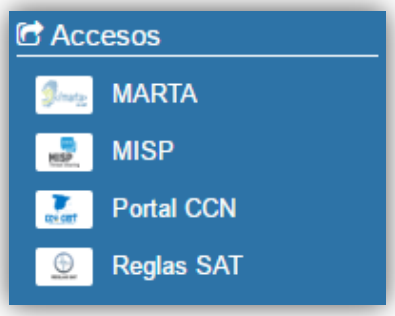


Figura 8. Sección de Accesos de REYES

1.3 DESCARGAS

13. Permiten descargar elementos independientes de las búsquedas. Actualmente: Listas Negras, Paquetes de reglas, Manual de Uso y el Manual de Desarrollador.

Figura 9. Sección de Descargas

1.3.1 LISTAS NEGRAS

14. Se trata de ficheros de texto que contienen direcciones IP y dominios que se encuentran actualmente en listas negras.

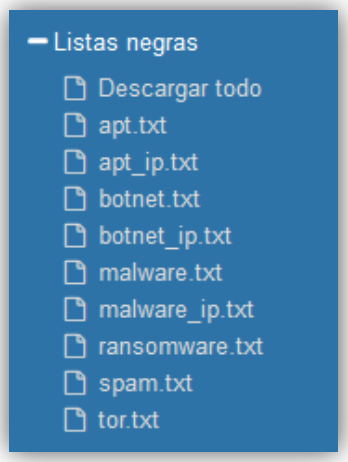


Figura 10. Listas Negras

15. Es posible descargar cualquiera de ellos clicando en su nombre:

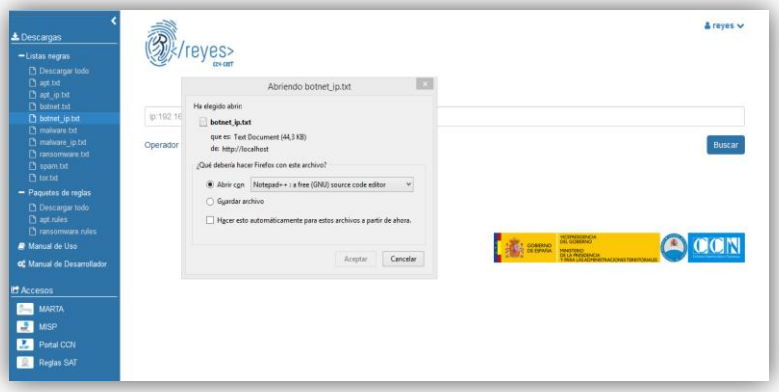


Figura 11. Descarga de listas

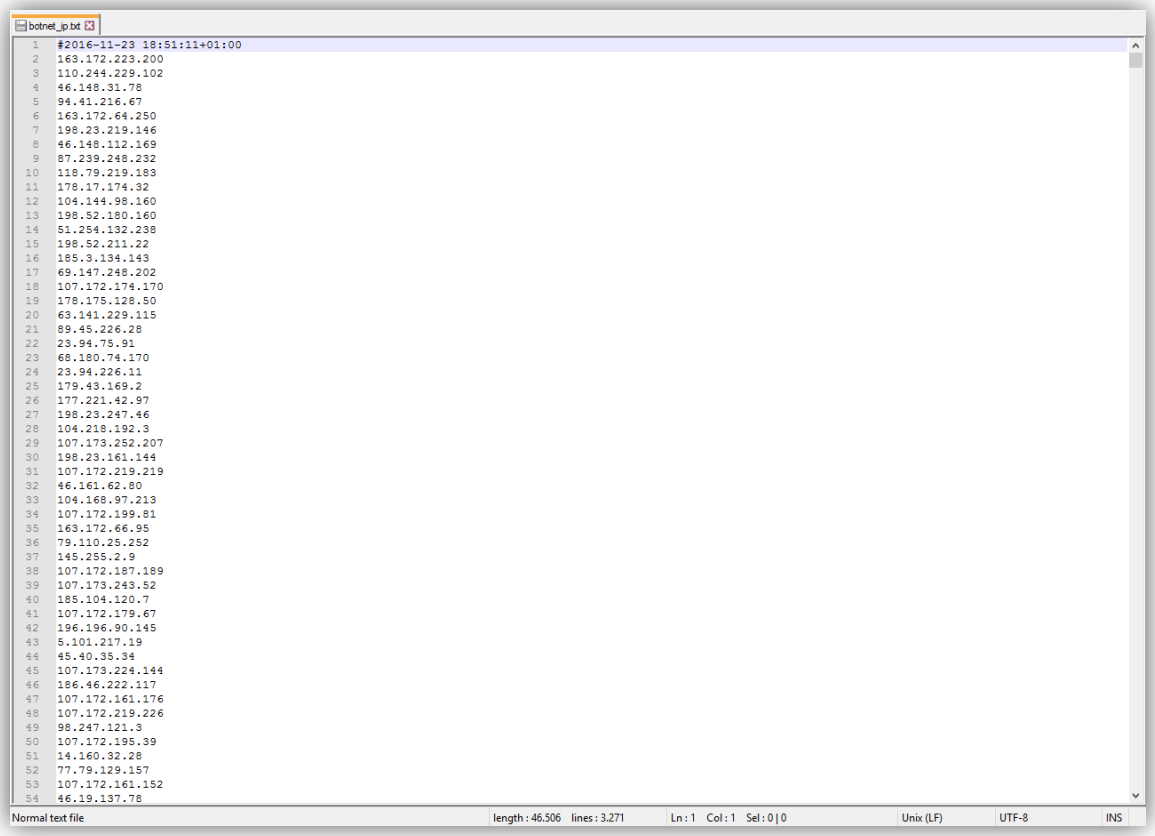


Figura 12. Fichero de listas en formato texto

16. Y también descargarlos todos en un fichero zip clicando en Descargar todo:

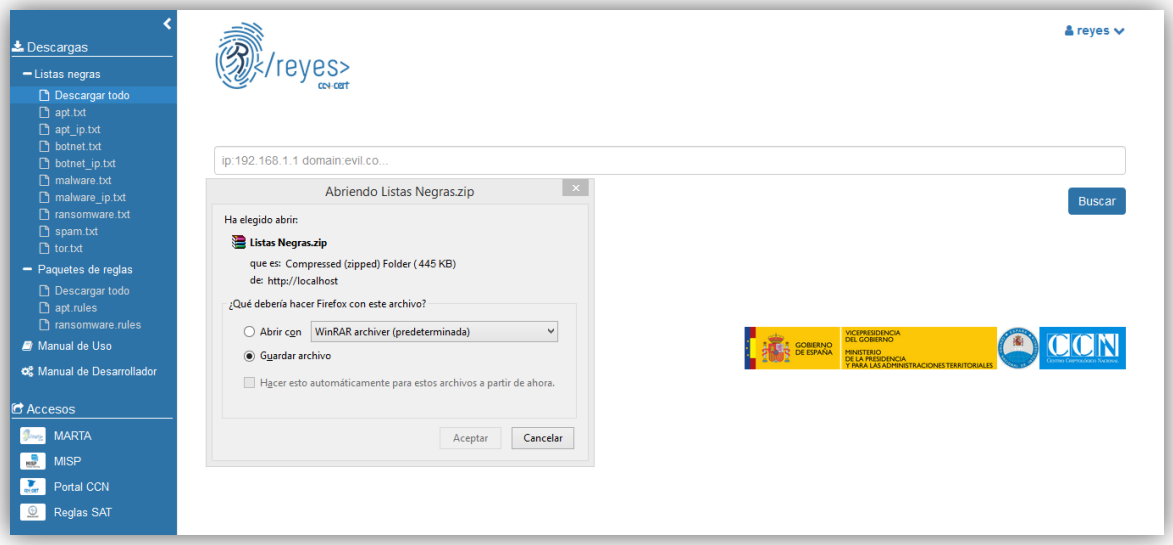


Figura 13. Fichero de listas comprimidas

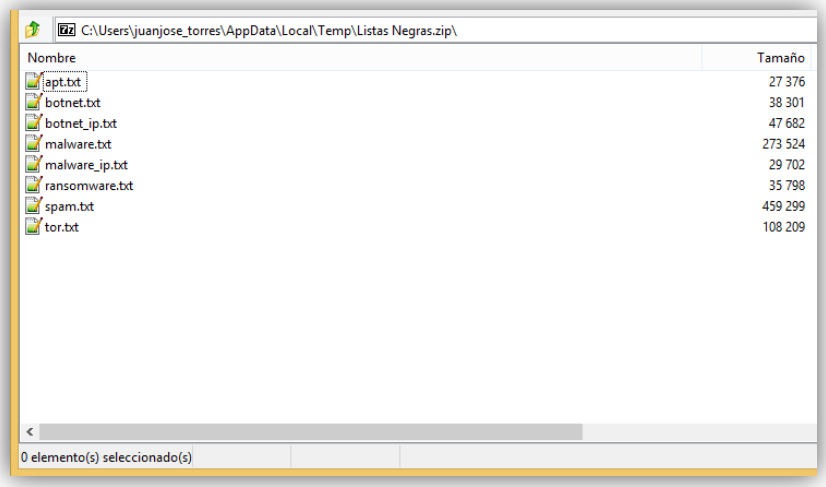


Figura 14. Fichero de listas en formato ZIP

1.3.2 PAQUETES DE REGLAS

17. Son ficheros de texto que contienen reglas de Snort para la detección de amenazas.

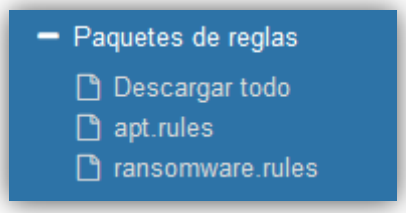


Figura 15. Fichero de reglas Snort

18. Es posible descargar cualquiera de ellos clicando en su nombre.

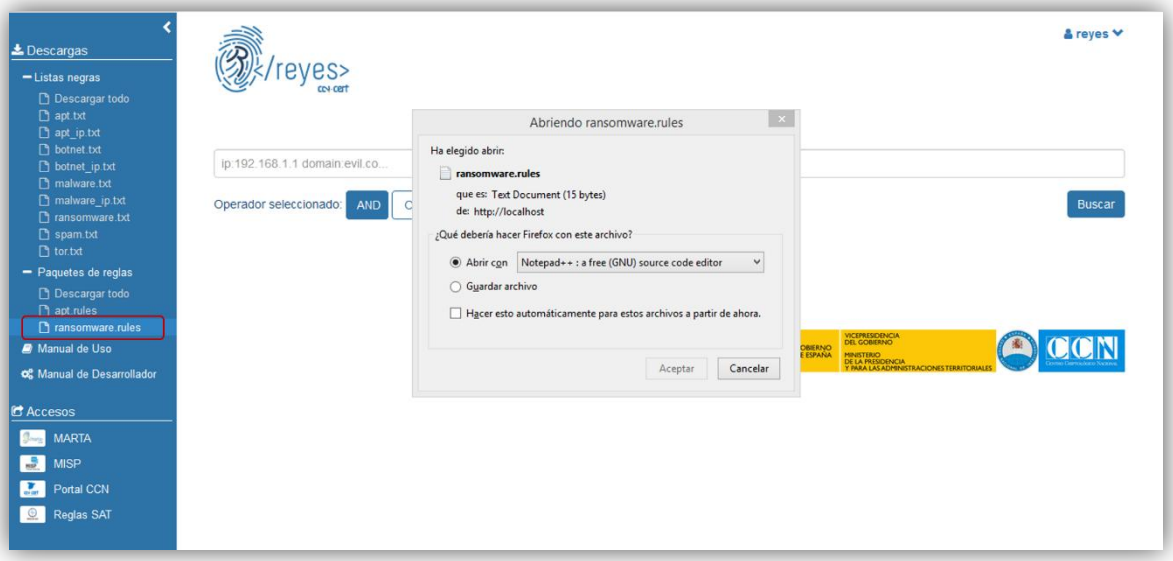


Figura 16. Descargas de reglas en formato texto

19. Y también descargarlos todos en un fichero zip clicando en Descargar todo.

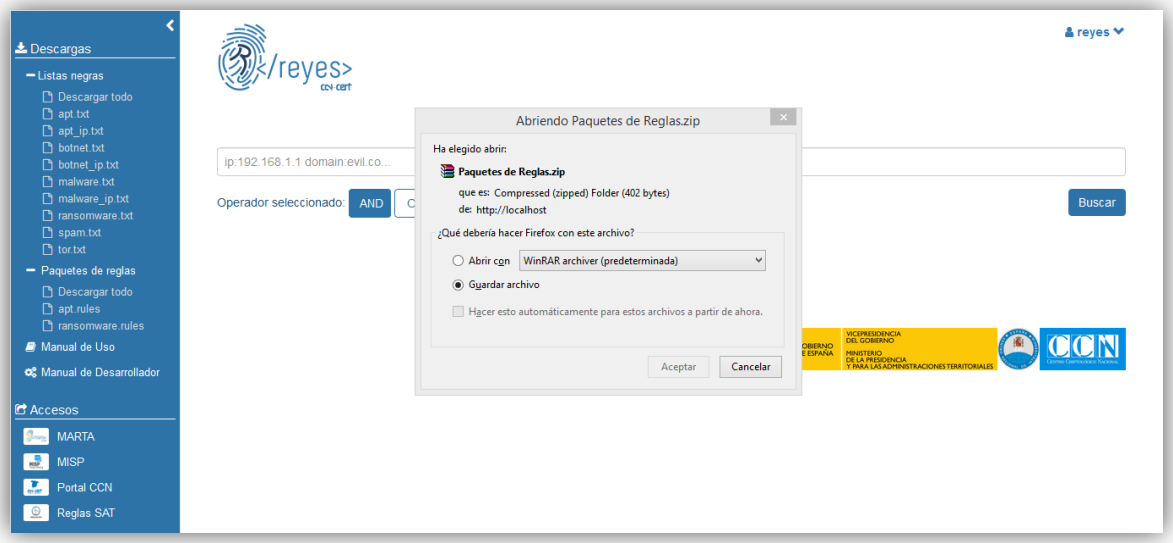


Figura 17. Descargas de reglas en formato ZIP

1.3.3 MANUAL DE USO

20. Es una guía de usuario para que se pueda hacer un uso adecuado y eficiente de la aplicación.

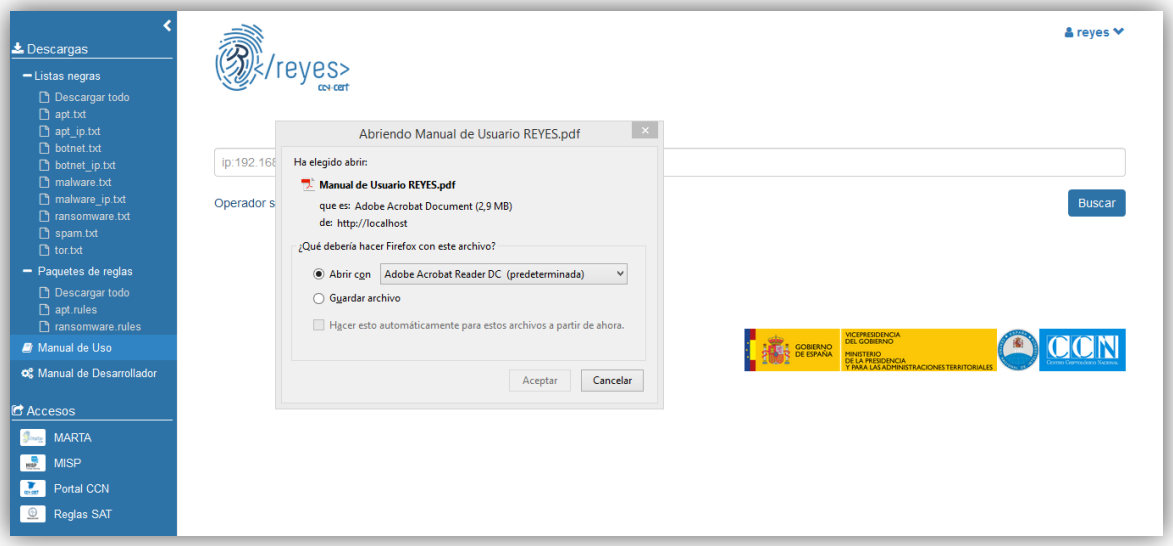


Figura 18. Descargas del Manual de Reyes

1.3.4 MANUAL DE DESARROLLADOR

21. Es una guía del API para facilitar la integración de las funciones de REYES en las aplicaciones de los organismos.

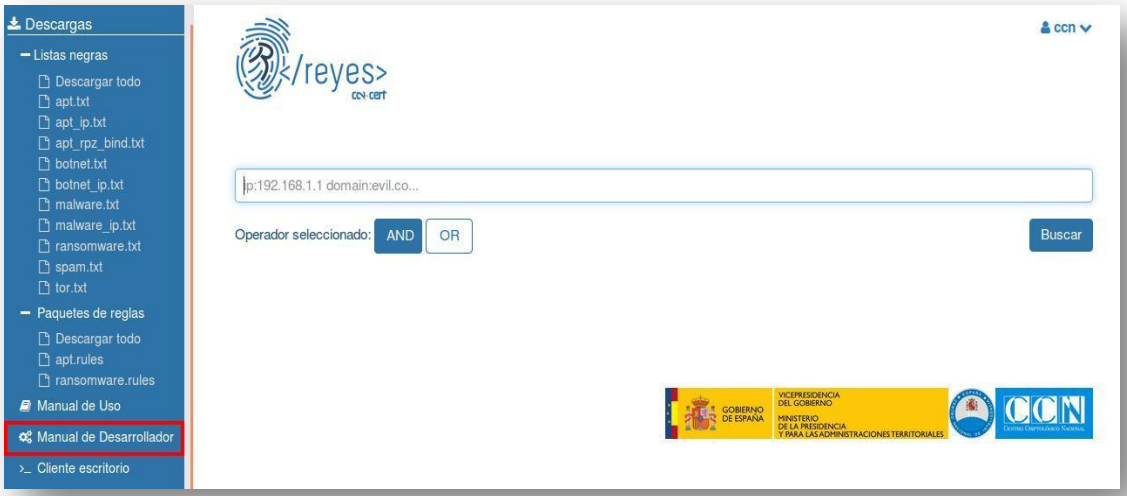


Figura 19. Descargas del Manual del Desarrollador

1.3.5 CLIENTE ESCRITORIO

22. REYES facilita el Cliente escritorio (Binario) que permite interactuar de una forma cómoda y sencilla con la API de Reyes.

23. Para realizar la petición del binario personalizado pulse en el panel de la izquierda sobre cliente escritorio.

Figura 20. Cliente escritorio (Binario)

24. A continuación le aparecerá un mensaje el cual ofrece instrucciones sobre cómo descargar el Cliente escritorio.

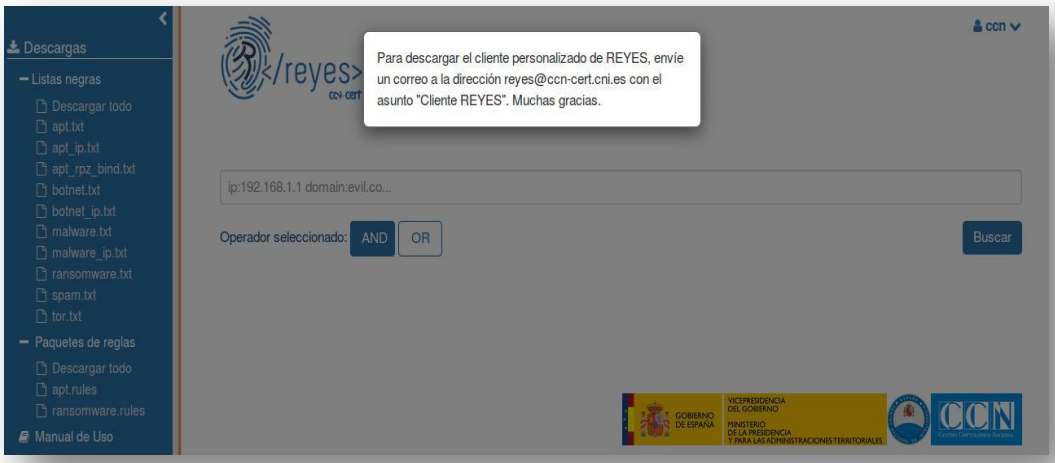


Figura 21. Descarga del Binario

25. Se puede encontrar más información de sobre uso y funcionamiento del cliente escritorio en el apartado “3. Binario” del manual de desarrollador.

1.4 Barra de Búsqueda

26. Permite introducir términos e iniciar búsquedas basadas en ellos.

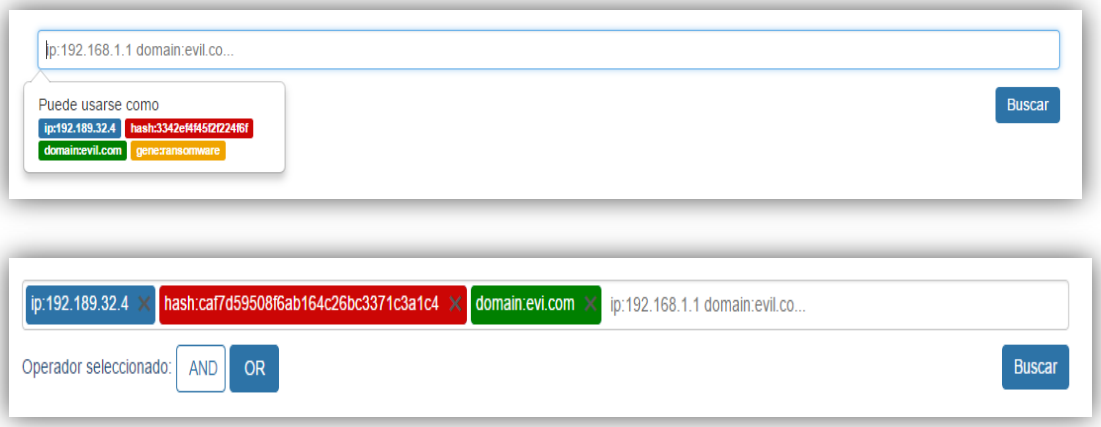


Figura 22. Barra de Búsqueda

27. Los términos se introducen siguiendo el siguiente formato:

tipo:valor

28. Actualmente existen 3 tipos de término: **ip, domain y hash**.

1.4.1 IP

29. Dirección IP v4 ó v6. Ejemplo:

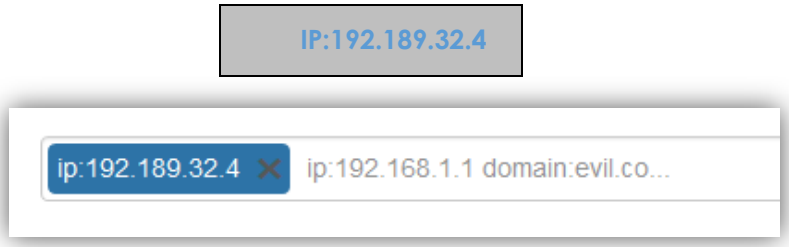


Figura 23. Ejemplo de una IPv4

1.4.2 DOMAIN

30. Dominio. Ejemplo:

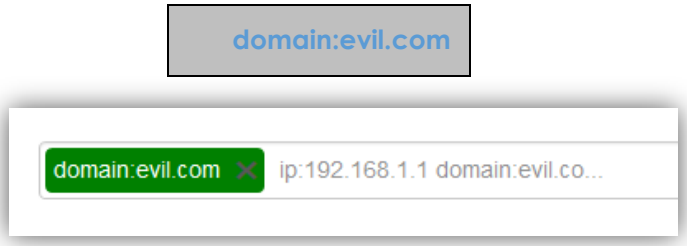


Figura 24. Ejemplo de un Dominio

1.4.3 HASH

31. Hash (normalmente identificativo de un fichero) MD5, SHA1 o SHA256. Ejemplos:

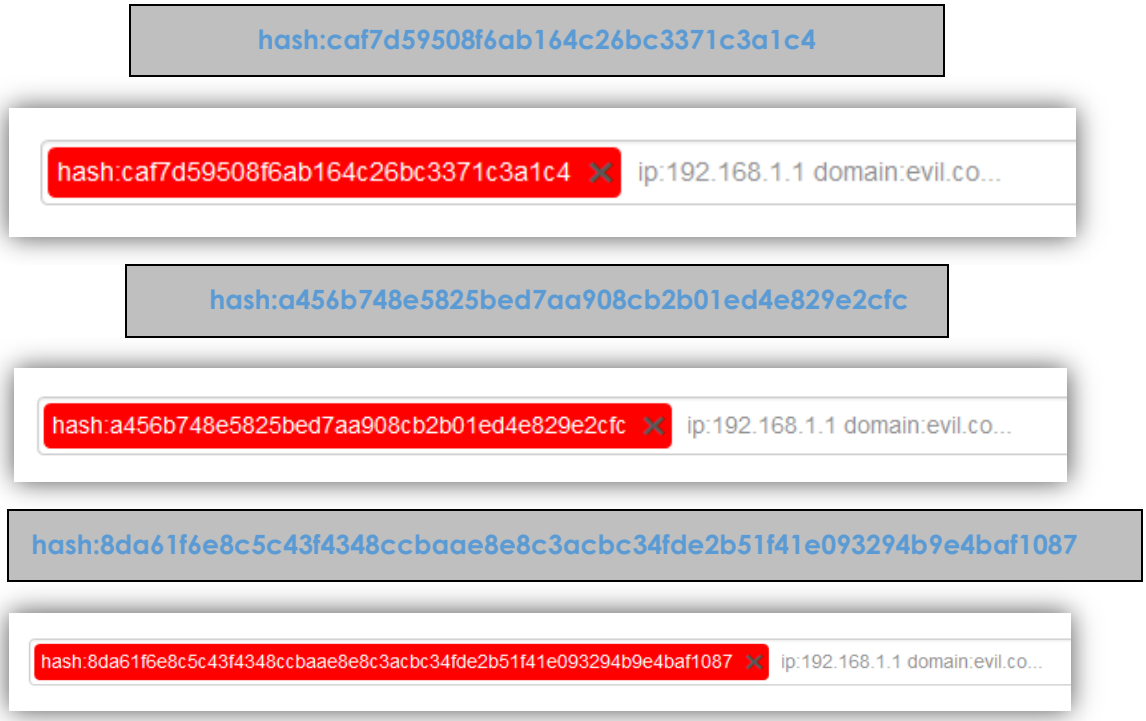


Figura 25. Ejemplo de HASH MD5,SHA1,SHAS256

32. Los términos son aceptados por la barra de búsqueda al pulsar la barra espaciadora, o al salir de la barra:

Figura 26. Ejemplo Búsqueda I

33. No es estrictamente necesario escribir el tipo de término. La barra de búsqueda tiene la capacidad de reconocerlos:

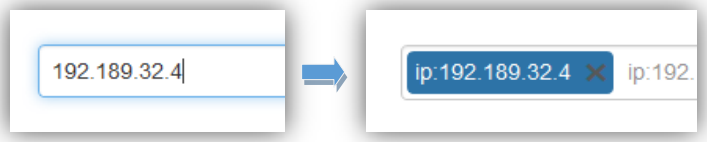


Figura 27. Ejemplo Búsqueda II

Figura 28. Ejemplo Búsqueda III

Figura 29. Ejemplo Búsqueda IV

34. Es posible introducir tantos términos como se desee:

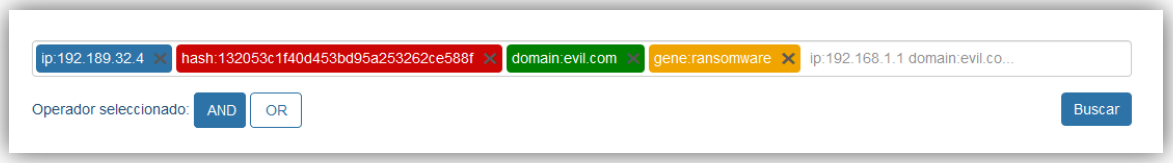


Figura 30. Ejemplo Búsqueda V

35. **Operador seleccionado:** se puede elegir que la búsqueda se realice por "**AND**", es decir, que se busquen resultados que estén relacionados con todos los términos introducidos simultáneamente, o por "**OR**", es decir, que se muestren resultados que estén relacionados con al menos uno de los términos introducidos.

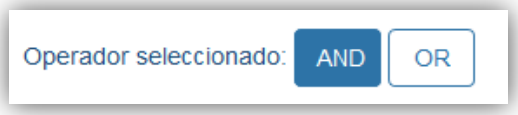


Figura 31. Operadores disponibles

36. Las búsquedas se inician haciendo clic en el botón de Buscar, o pulsando la tecla *enter* en la barra de búsqueda.

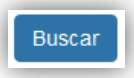


Figura 32. Botón de Búsqueda

37. Conforme REYES vaya encontrando resultados, se irán mostrando en cajas de contenido.

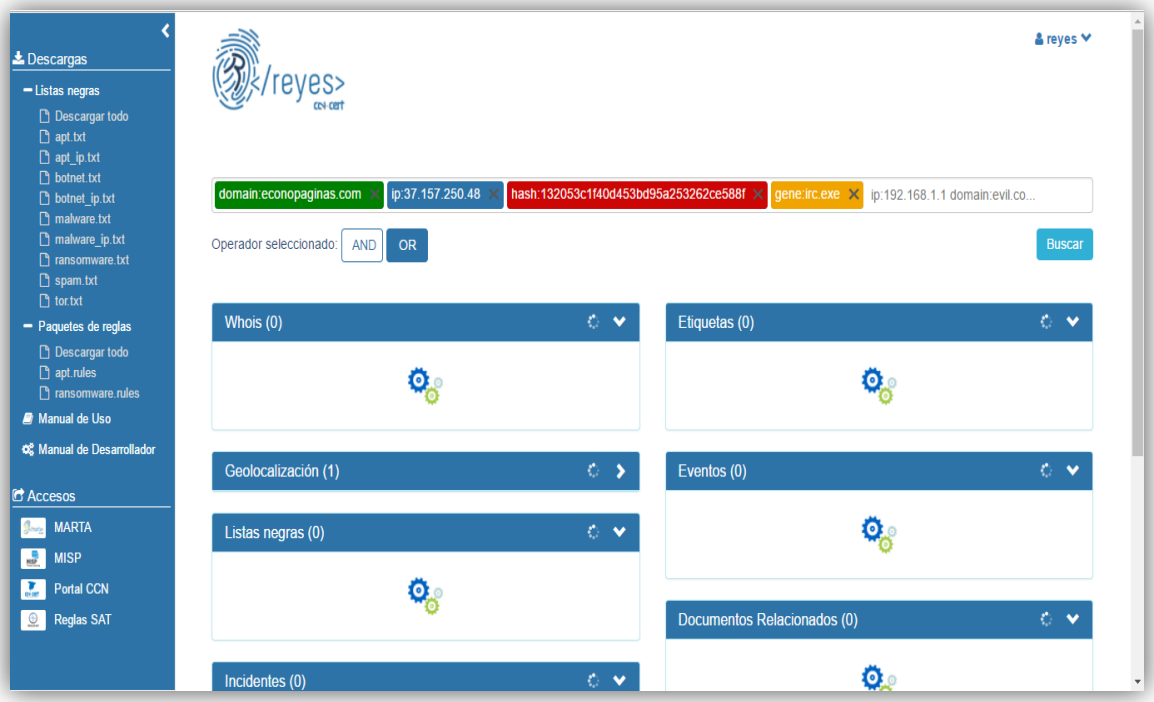


Figura 33. Ejemplo Búsqueda

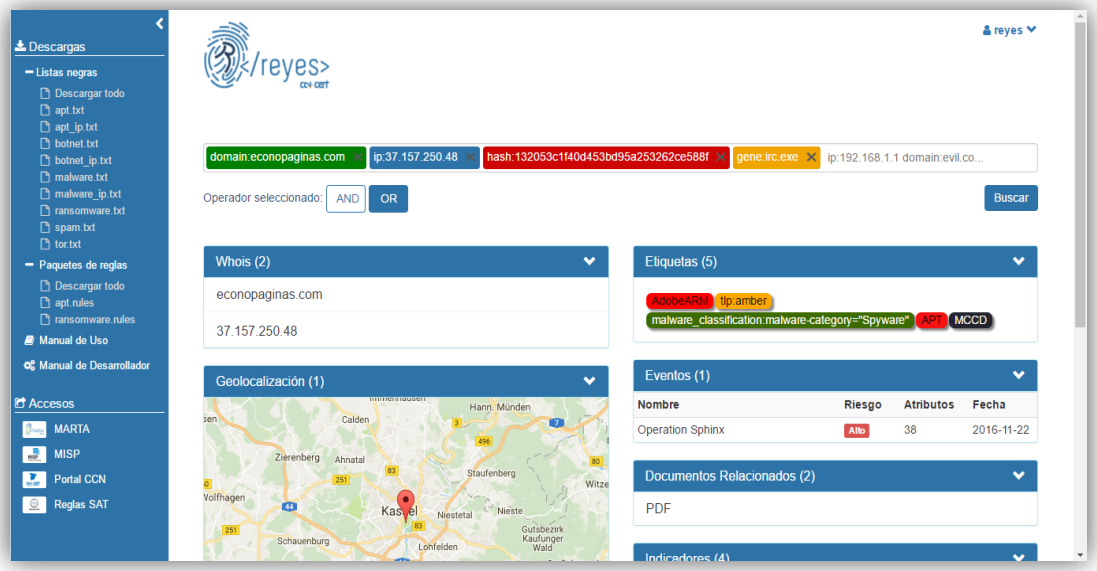


Figura 34. Ejemplo Búsqueda II

1.5 ACCESOS

1.5.1 MARTA

38. Motor de Análisis de Troyanos Avanzados (MARTA) es una aplicación dedicada al análisis automatizado de ficheros que podrían tener un comportamiento dañino.

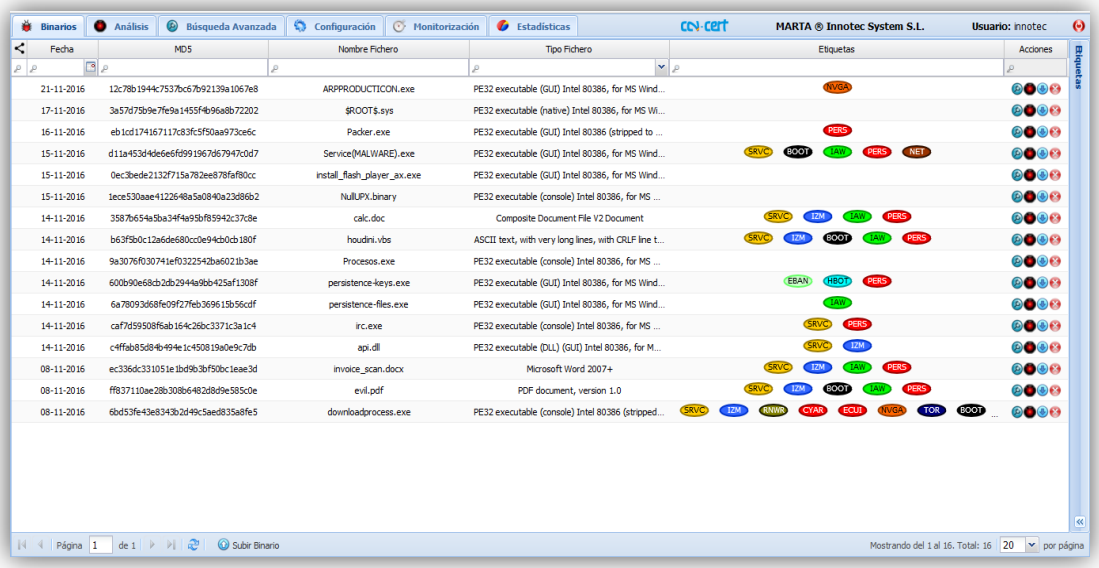


Figura 35. Pantalla de Inicio de Marta

1.5.2 MISP

39. Malware Information Sharing Platform (MISP) es una plataforma diseñada para automatizar el intercambio de información y conocimiento sobre ciberamenazas.

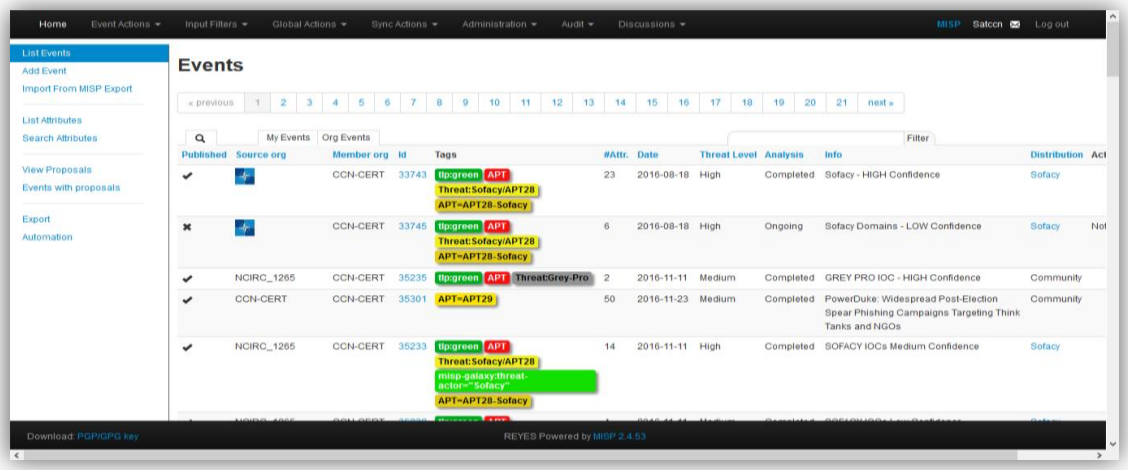


Figura 36. Pantalla de Inicio MISP

1.5.3 PORTAL DEL CCN-CERT

40. Portal web del CCN-CERT es la Capacidad de Respuesta a incidentes de Seguridad de la Información del Centro Criptológico Nacional.

Figura 37. Pantalla de Inicio del Portal del CCN-CERT

1.5.4 GESTOR DE REGLAS SAT

41. El gestor de reglas SAT permite la gestión ágil de reglas de SNORT e indicadores IDS.

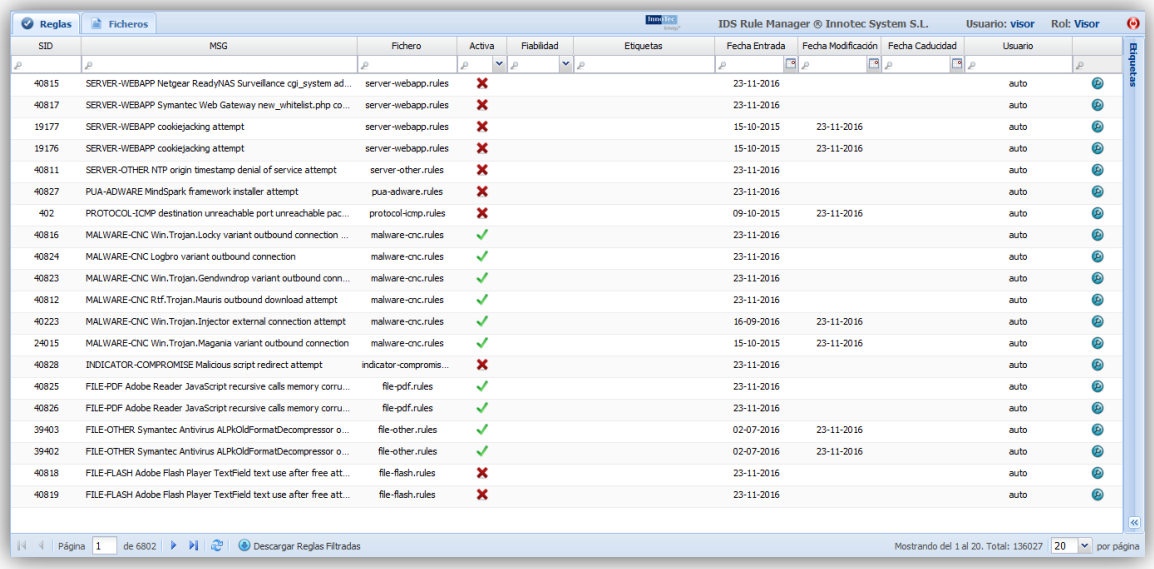


Figura 38. Pantalla de Inicio del Gestos de Reglas

1.6 Contenidos

42. Los resultados de una búsqueda se muestran en cajas de contenido.

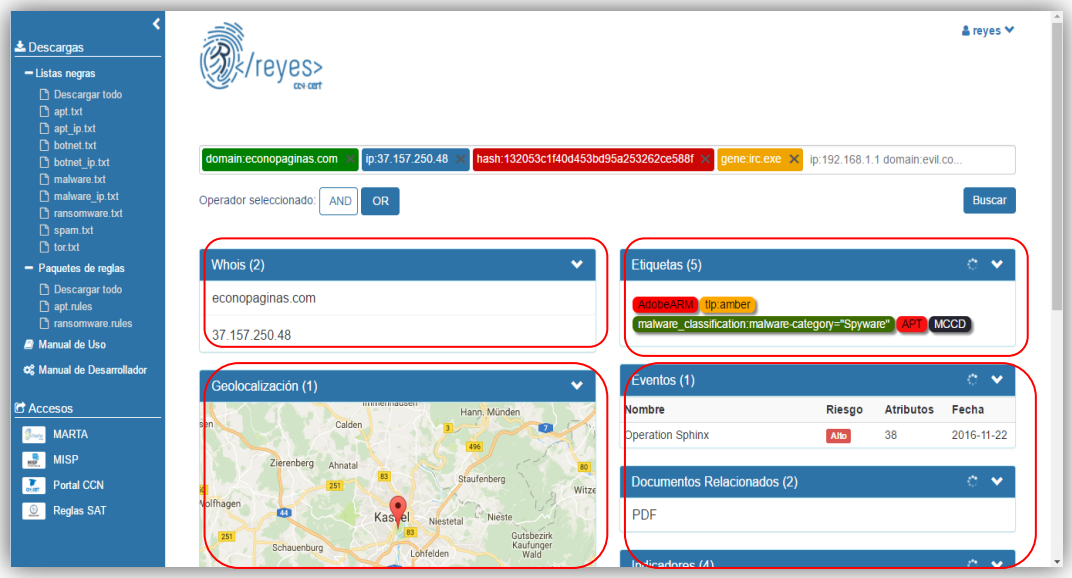


Figura 39. Pantalla de Cajas de REYES

43. Los contenidos pueden variar en función de los términos de búsqueda. Por ejemplo, la información de WhoIs y Geolocalización sólo está disponible para dominios y direcciones IP.

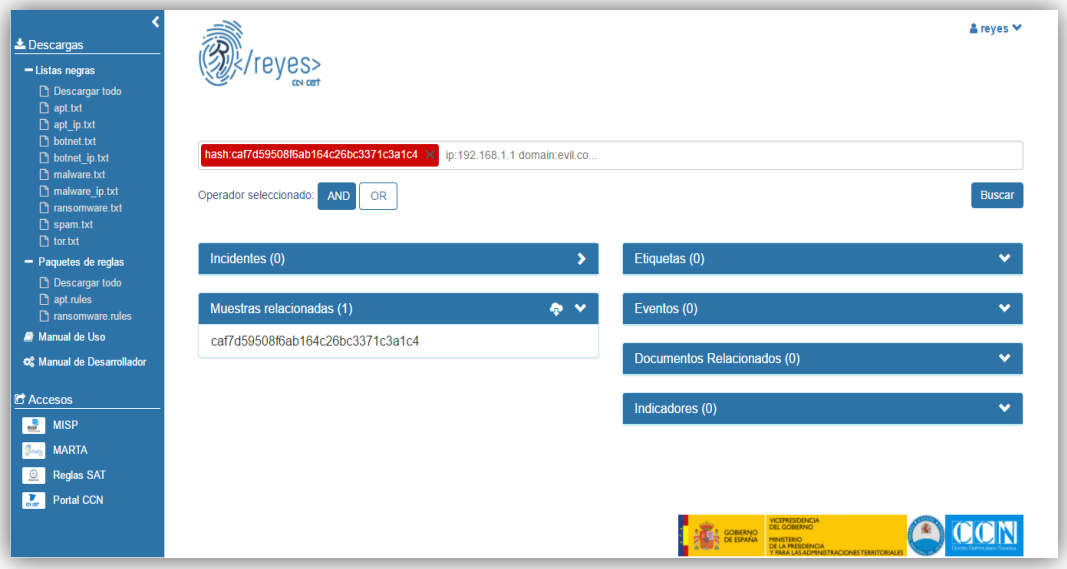


Figura 40. Contenido de una búsqueda

44. Actualmente existen 9 tipos de contenido: **WhoIs, Geolocalización, Listas Negras, Incidentes, Muestras, Etiquetas, Eventos, Documentos e Indicadores.**

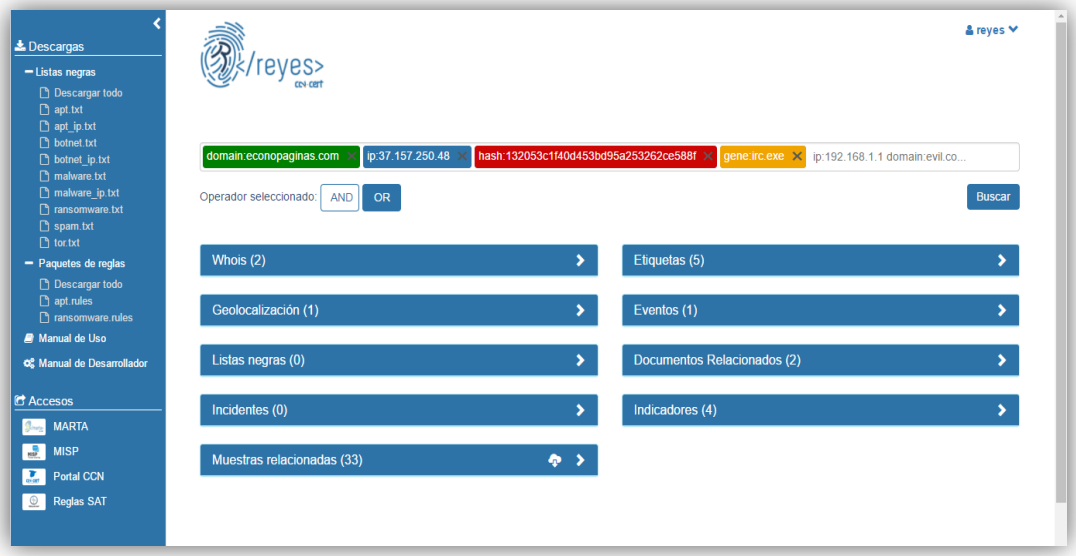


Figura 41. Contenidos de búsqueda de REYES

1.6.1 WHOIS

45. Los contenidos de WhoIs aparecen a partir de búsquedas de dominios y direcciones IP, y la información se obtiene de servidores de WhoIs, a través de la aplicación GWhois. Estos contenidos proporcionan información interesante acerca del dominio o la IP, como la fecha de alta, la persona responsable, emails asociados, etc.

46. Cada dominio y cada dirección IP tiene su propio contenido de Whols.

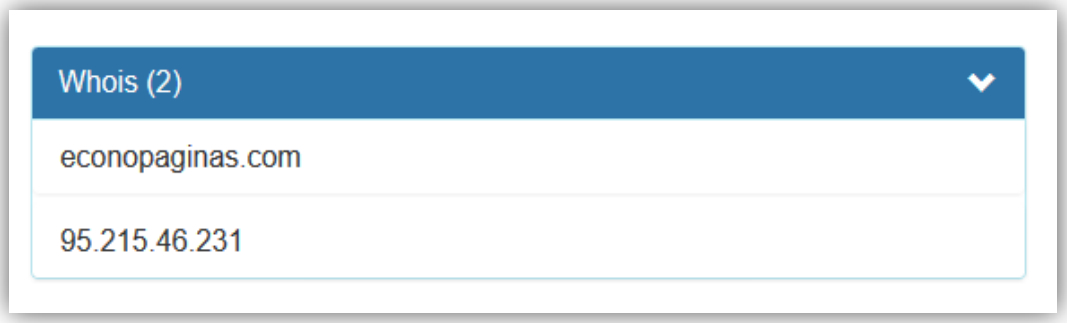
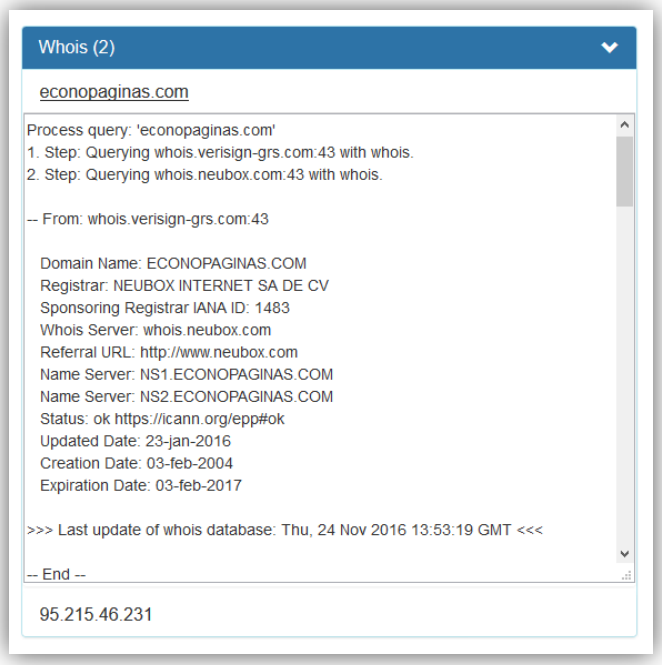


Figura 42. Caja de contenido de Whols

47. Se puede ver el contenido clicando en el dominio o la dirección IP concreta que se desee consultar.



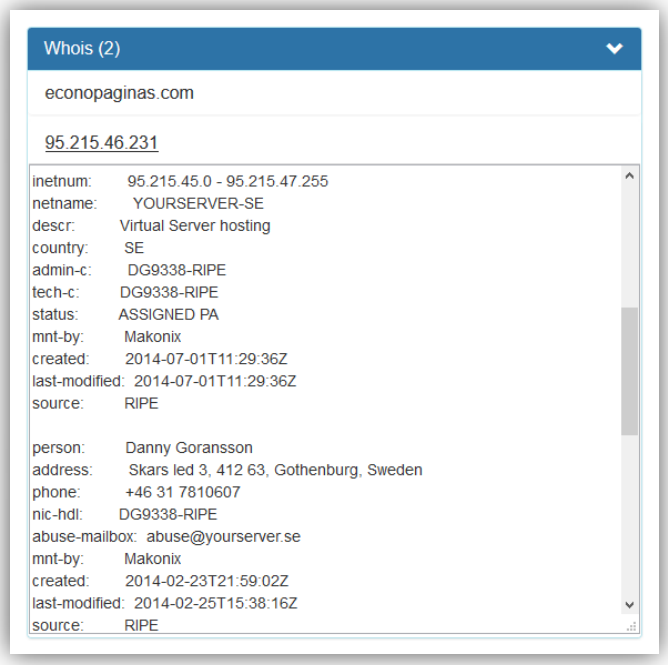


Figura 43. Resultado de la Caja de contenido de Whols

1.6.2 GEOLOCALIZACIÓN

48. Los contenidos de Geolocalización aparecen a partir de búsquedas de dominios y direcciones IP, y la información se obtiene de la aplicación Maxmind, y se muestra haciendo uso de Google Maps. Estos contenidos proporcionan información acerca de la posición actual del dominio o la IP.

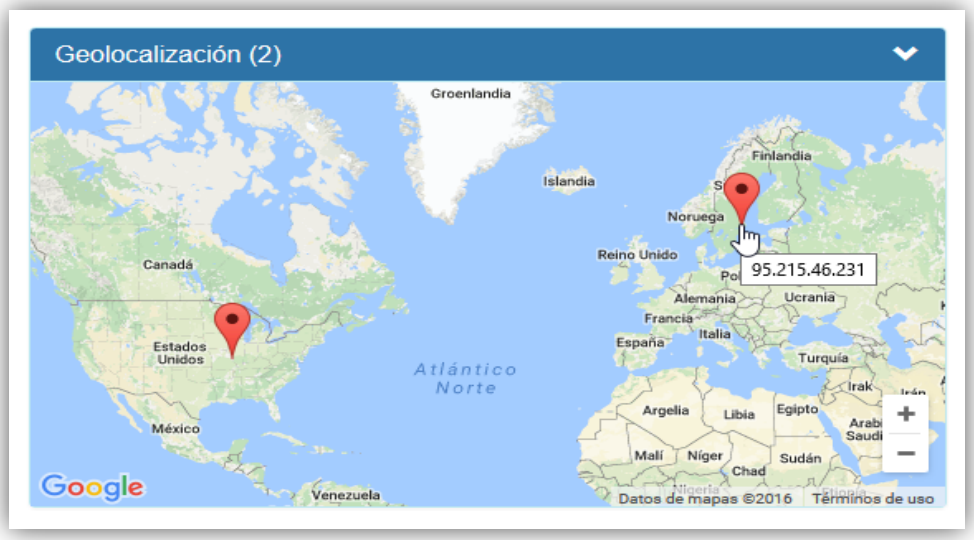


Figura 44. Caja de contenido de Geolocalización

1.6.3 LISTAS NEGRAS

49. Los contenidos de Listas Negras aparecen a partir de búsquedas de dominios y direcciones IP, y la información se obtiene de la aplicación CIF (Collective Framework Intelligence). Estos contenidos proporcionan información acerca de la aparición del dominio o la IP en listas negras.

50. Cada dominio y cada dirección IP tiene sus propios contenidos de Listas Negras, indicando, para cada uno, el nombre de la lista negra, y cuándo fue incluido por última vez en ella.

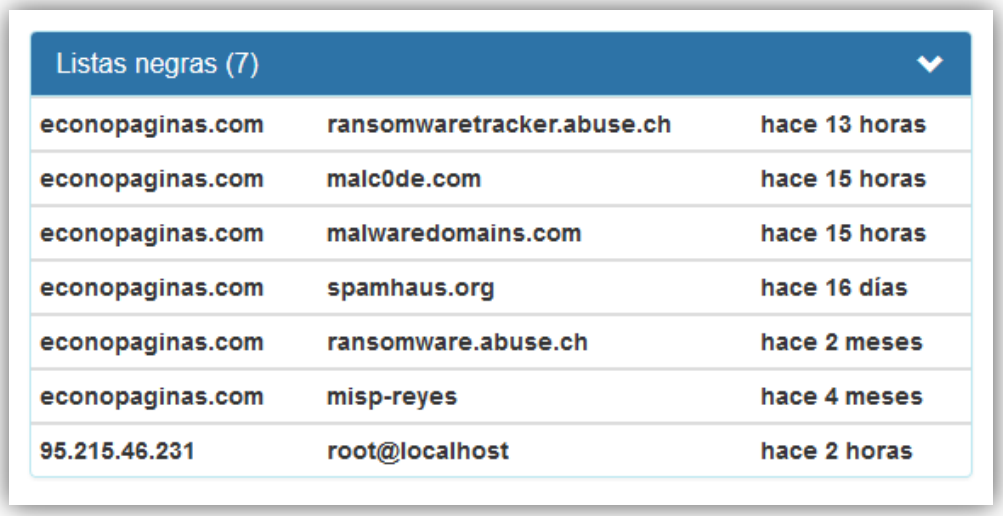


Figura 45. Caja de contenido de Listas Negras

1.6.4 INCIDENTES

51. Los contenidos de Incidentes aparecen a partir de búsquedas de cualquier término y la información se obtiene de la aplicación **LUCIA**. Estos contenidos proporcionan información acerca de incidentes que están relacionados con los términos buscados. Solo se mostraran los incidentes de los que tenga visibilidad la organización del usuario. Cada incidente se identifica por su número de ticket o título de incidente.

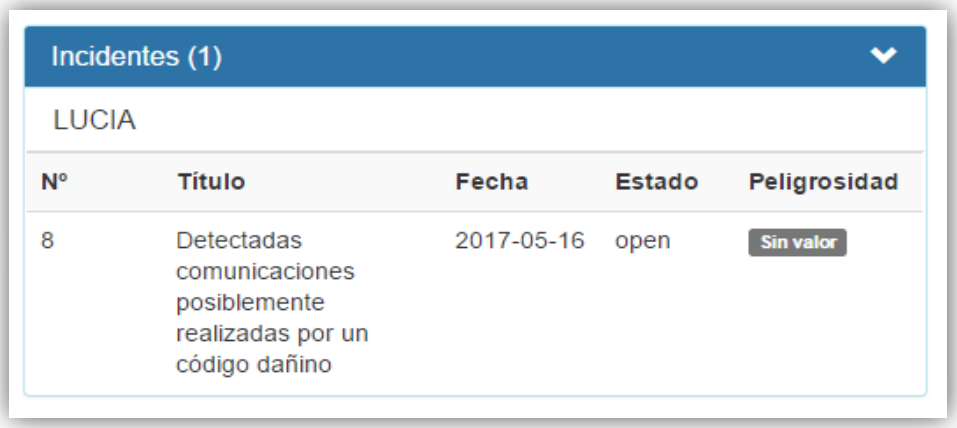


Figura 46. Caja de contenido de Incidentes

52. Colocando el cursor sobre cualquiera de ellos se puede obtener información acerca de donde proviene.

Figura 47. Información de procedencia del incidente

53. Para obtener más información sobre el incidente se debe entrar en la aplicación de LUCIA, clicando en cualquier número ticket se abrirá una nueva pestaña de navegador con la aplicación.

1.6.5 MUESTRAS

54. Los contenidos de Muestras aparecen a partir de búsquedas de cualquier término, y la información se obtiene de las aplicaciones MISP y MARTA. Estos contenidos proporcionan información acerca de ficheros (normalmente código dañino) que están relacionados con los términos buscados. Cada fichero se identifica por su MD5, SHA1 o SHA256.

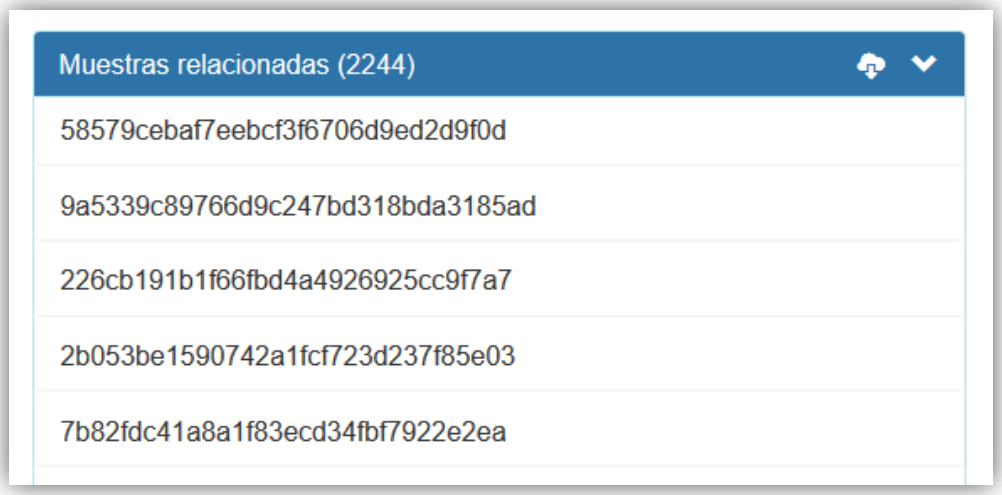


Figura 48. Caja de contenido de muestras

55. Haciendo clic en cualquiera de ellos, se puede obtener información acerca de donde proviene.

56. Si proviene de MISP, aparece el tipo de atributo y el nombre del evento.

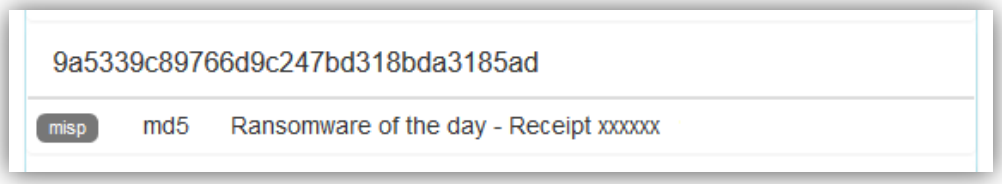


Figura 49. Información del evento de MISP

57. Si proviene de MARTA, aparece el tipo de hash y el hash de la muestra.

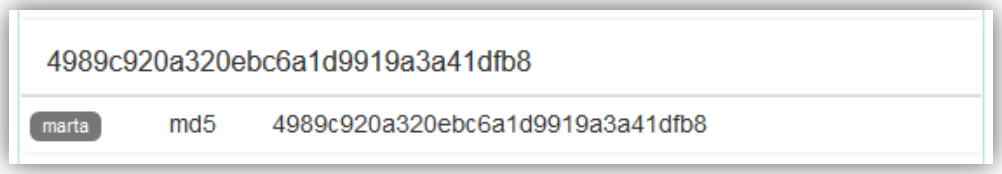


Figura 50. Información del evento de MARTA

58. En el caso de MISP, clicando en el nombre del evento, se accede directamente al evento en MISP.

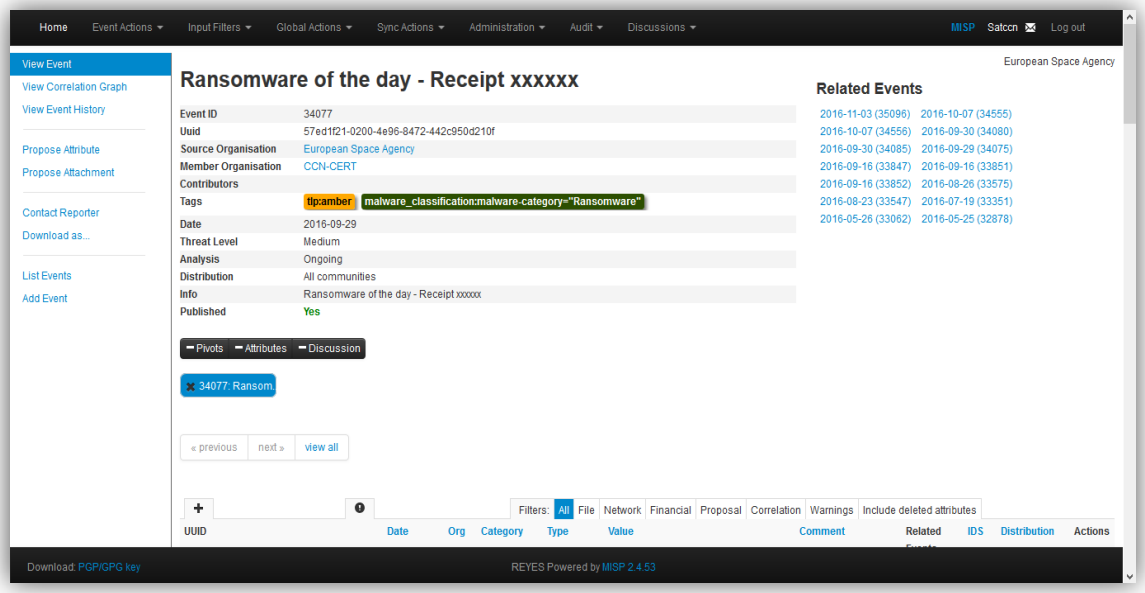


Figura 51. Información del evento en MISP

59. En el caso de MARTA, clicando en el tipo de hash, se accede directamente a la muestra en MARTA.

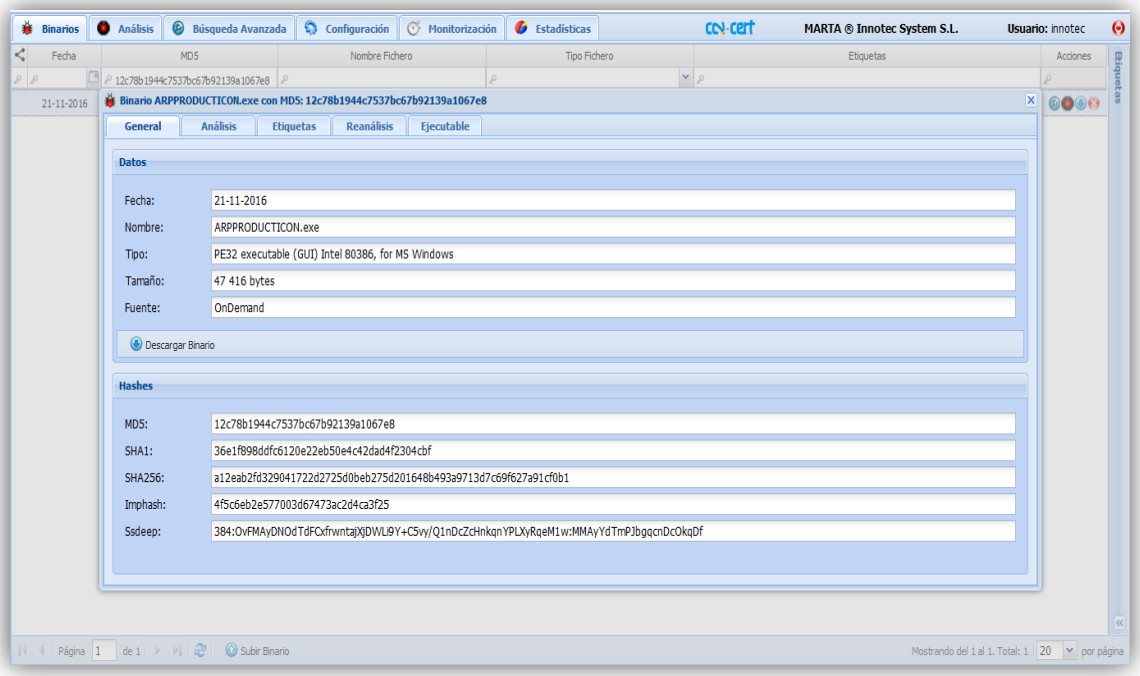


Figura 52. Información del evento en MARTA

60. Adicionalmente, es posible descargar los hashes de todas las muestras en un fichero de texto clicando en el botón de descarga de la cabecera de la caja.

Figura 53. Descargas de Hash de muestras

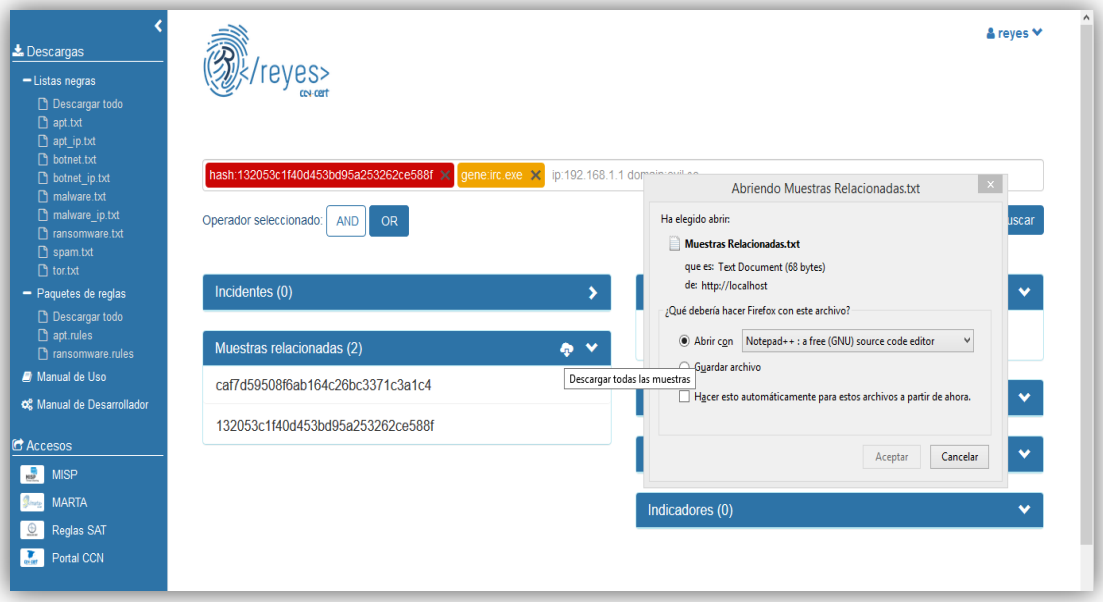


Figura 54. Descarga de la lista de HASHES

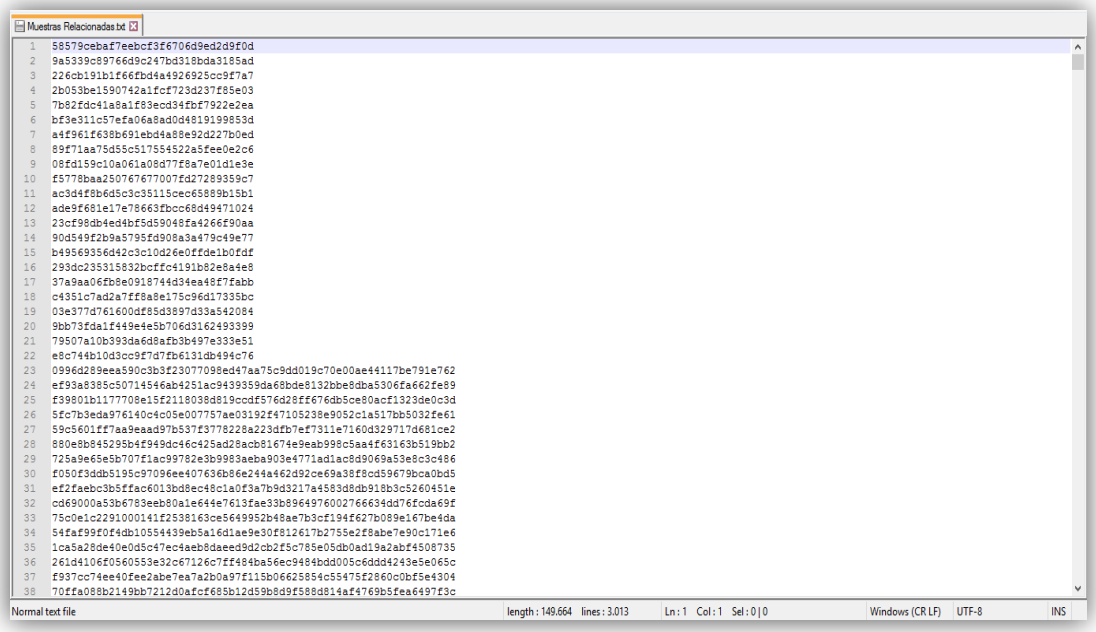


Figura 55. Lista de HASHES en formato texto

1.6.6 ETIQUETAS

61. Los contenidos de Etiquetas aparecen a partir de búsquedas de **cualquier término**, y la información se obtiene de las aplicaciones **MISP** y **MARTA**. Estos contenidos proporcionan información acerca de etiquetas que están relacionadas con los términos buscados. Cada etiqueta tiene un texto y un color, y aparece de mayor o menor tamaño en función del número de elementos (eventos de MISP y muestras de MARTA) a los que está asignada.

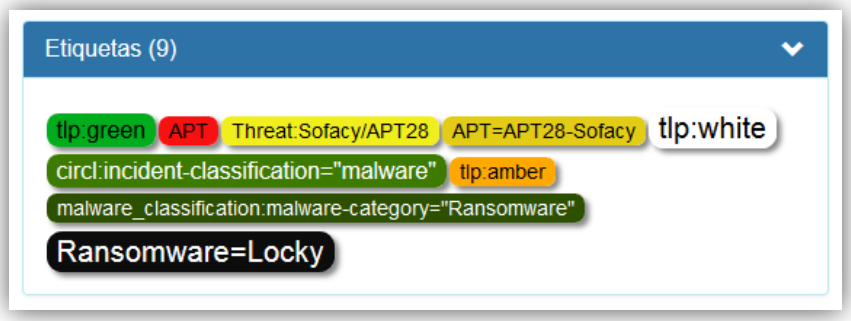


Figura 56. Caja de Etiquetas

62. Manteniendo el ratón sobre cualquiera de las etiquetas, se puede obtener información acerca de donde proviene.

63. Si proviene de MISP, aparece el nombre del evento.

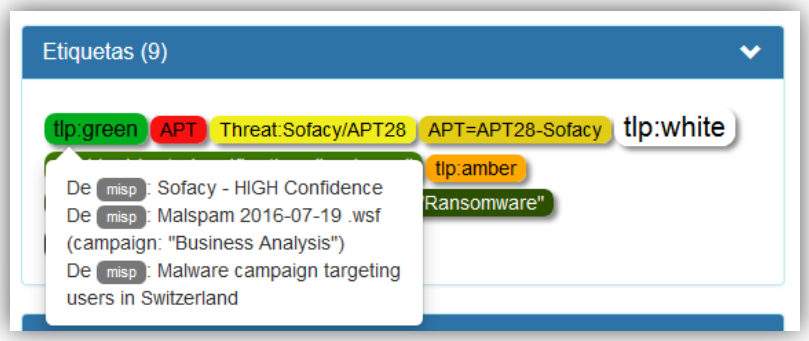


Figura 57. Información del evento en REYES

64. Si proviene de MARTA, aparece el hash de la muestra.

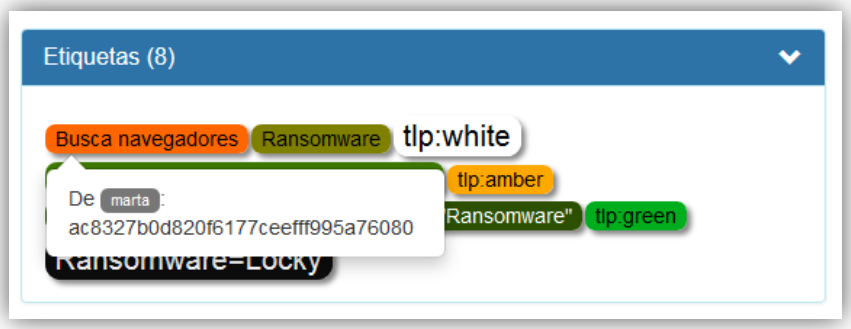


Figura 58. Información del evento en MARTA

1.6.7 EVENTOS

65. Los contenidos de Eventos aparecen a partir de búsquedas de **cualquier término**, y la información se obtiene de la aplicación **MISP**. Estos contenidos proporcionan información acerca de eventos que están relacionadas con los términos buscados. De cada evento, se muestra su nombre, nivel de riesgo, cantidad de atributos y fecha.

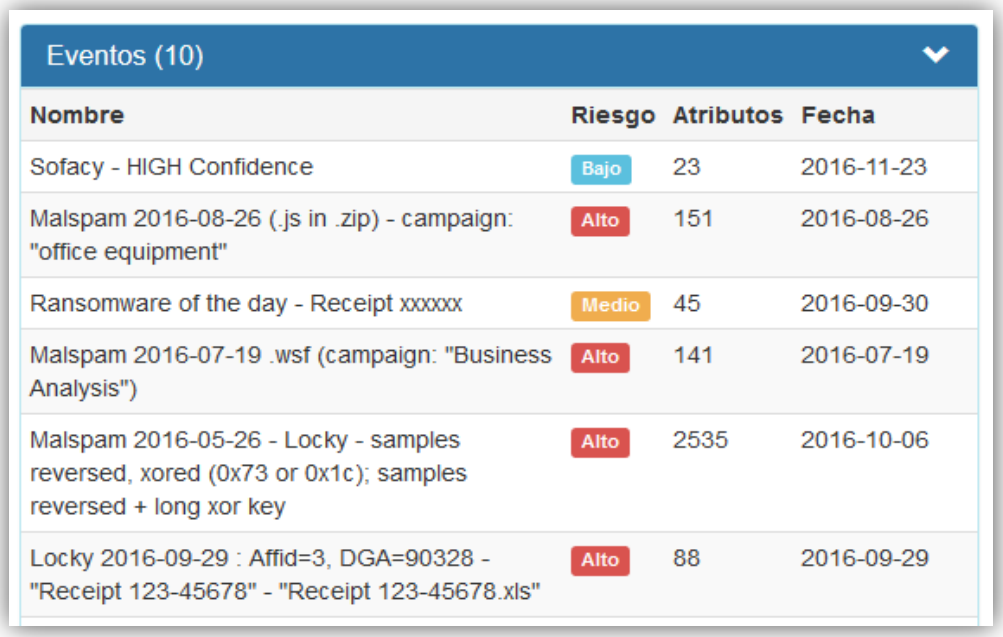


Figura 59. Caja de Contenidos de Eventos

66. El nivel de riesgo se indica tal y como aparece en MISP. Riesgo bajo indica que el evento está relacionado con código dañino de masas, riesgo medio indica código dañino de una APT (Amenaza Persistente Avanzada), y riesgo alto indica código dañino de una APT sofisticada con ataque de día cero (0-day).

67. Manteniendo el ratón sobre el nombre de un evento, se puede obtener el término a partir del que se ha encontrado.

Figura 60. Información del evento en MISP

68. Clicando en el nombre del evento, se accede directamente al evento en MISP.

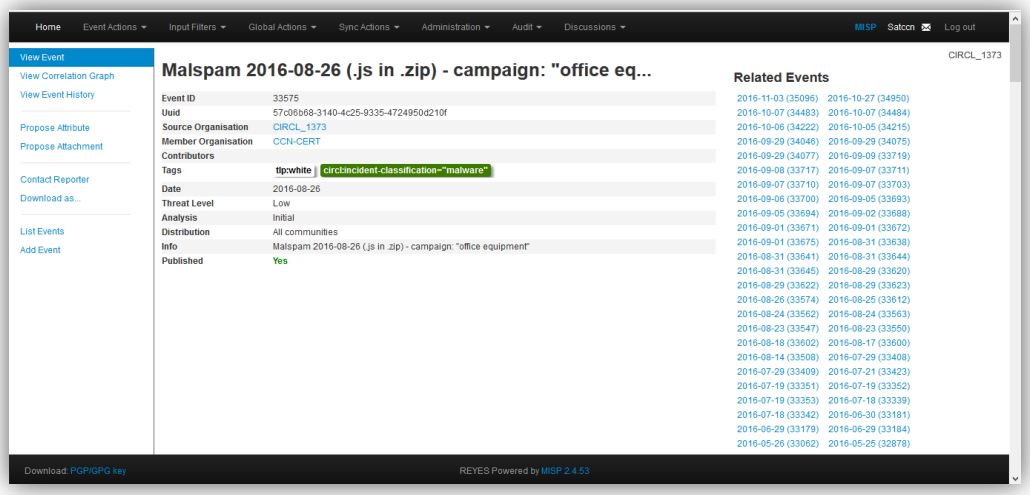


Figura 61. Información del evento en MISP

1.6.8 DOCUMENTOS

69. El contenido de Documentos aparecen a partir de búsquedas de **cualquier término**, y la información se obtiene de la aplicación **MISP** y del **portal web del CCN-CERT**. Estos contenidos proporcionan documentos y enlaces que están relacionados con los términos buscados agrupados por extensión de fichero.

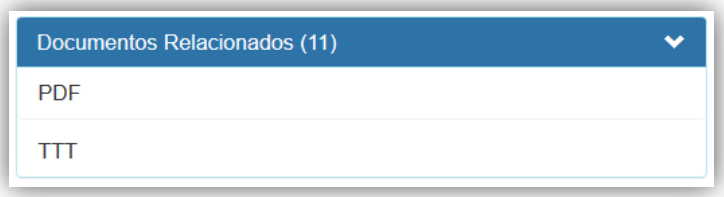


Figura 62. Caja de Contenido de Documentos

70. Manteniendo el ratón sobre un documento, se puede obtener la aplicación de la que proviene y el término a partir del que se ha encontrado.

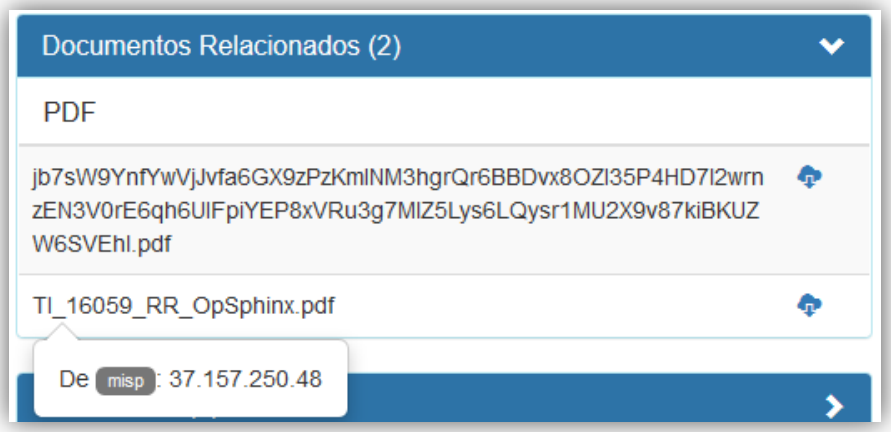


Figura 63. Información del evento en MISP

71. Clicando en el icono de descarga, se descarga el documento, o se accede al enlace.

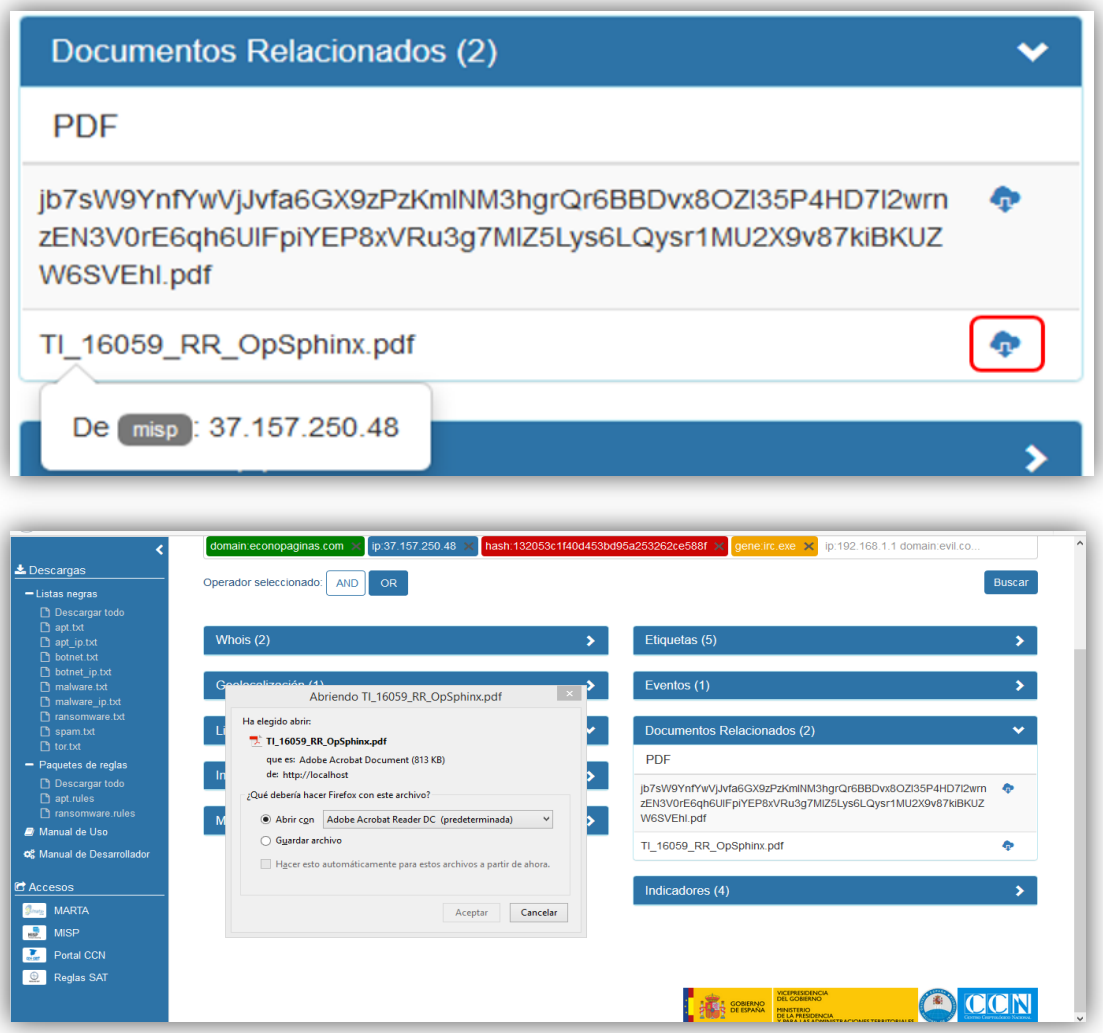
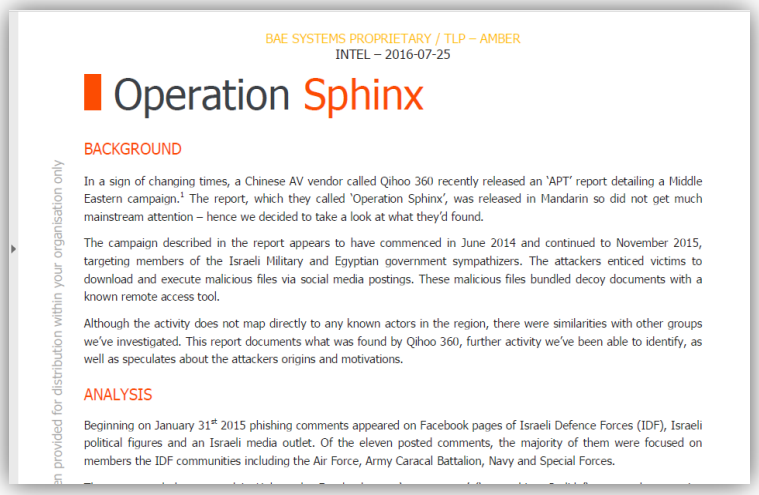


Figura 64. Descarga de Documentos


BAE SYSTEMS PROPRIETARY / TLP – AMBER
INTEL – 2016-07-25

Operation Sphinx

BACKGROUND

In a sign of changing times, a Chinese AV vendor called Qihoo 360 recently released an 'APT' report detailing a Middle Eastern campaign.[1] The report, which they called 'Operation Sphinx', was released in Mandarin so did not get much mainstream attention – hence we decided to take a look at what they'd found.

The campaign described in the report appears to have commenced in June 2014 and continued to November 2015, targeting members of the Israeli Military and Egyptian government sympathizers. The attackers enticed victims to download and execute malicious files via social media postings. These malicious files bundled decoy documents with a known remote access tool.

Although the activity does not map directly to any known actors in the region, there were similarities with other groups we've investigated. This report documents what was found by Qihoo 360, further activity we've been able to identify, as well as speculates about the attackers origins and motivations.

ANALYSIS

Beginning on January 31st 2015 phishing comments appeared on Facebook pages of Israeli Defence Forces (IDF), Israeli political figures and an Israeli media outlet. Of the eleven posted comments, the majority of them were focused on members the IDF communities including the Air Force, Army Caracal Battalion, Navy and Special Forces.

Figura 65. Ejemplo de Documento

1.6.9 INDICADORES

72. Los contenidos de Indicadores aparecen a partir de búsquedas de **cualquier término**, y la información se obtiene de las aplicaciones **MISP** y **Gestor de Reglas SAT**. Estos contenidos proporcionan reglas e indicadores de detección de diferentes tipos, que están relacionados con los términos buscados.

    Actualmente se buscan indicadores de 4 tipos:

    - **IDS:** Indicadores de red en formato reglas de Snort y Suricata.
    - **IOC:** Indicadores de actividad potencialmente maliciosa en formato OpenIOC.
    - **RPZ:** Indicadores de red para desplegar en servidores DNS con la funcionalidad de Response Policy Zones.
    - **YARA:** Reglas de identificación y clasificación de software malicioso basadas en strings.

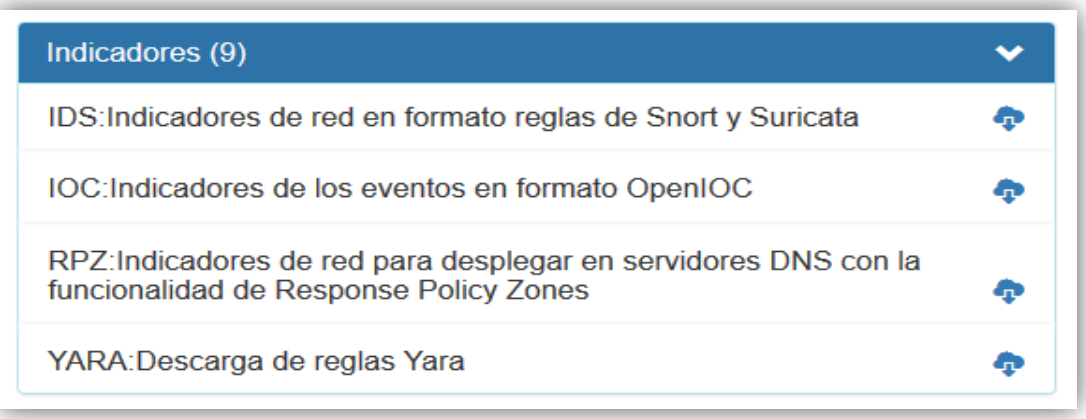
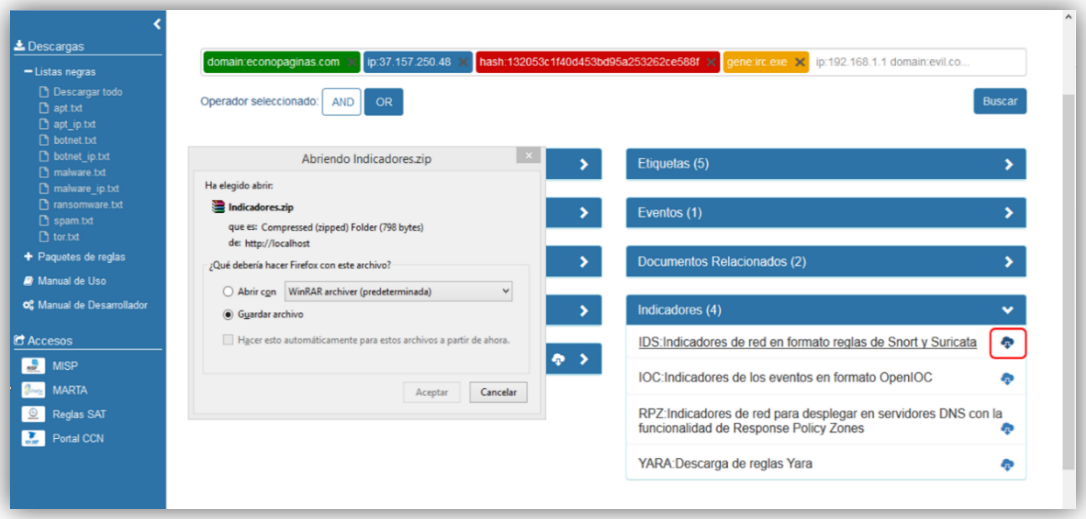


Figura 66. Caja de Contenido de Indicadores

73. Haciendo click en los iconos de descarga, se pueden obtener todos los indicadores del tipo seleccionado en un fichero zip.



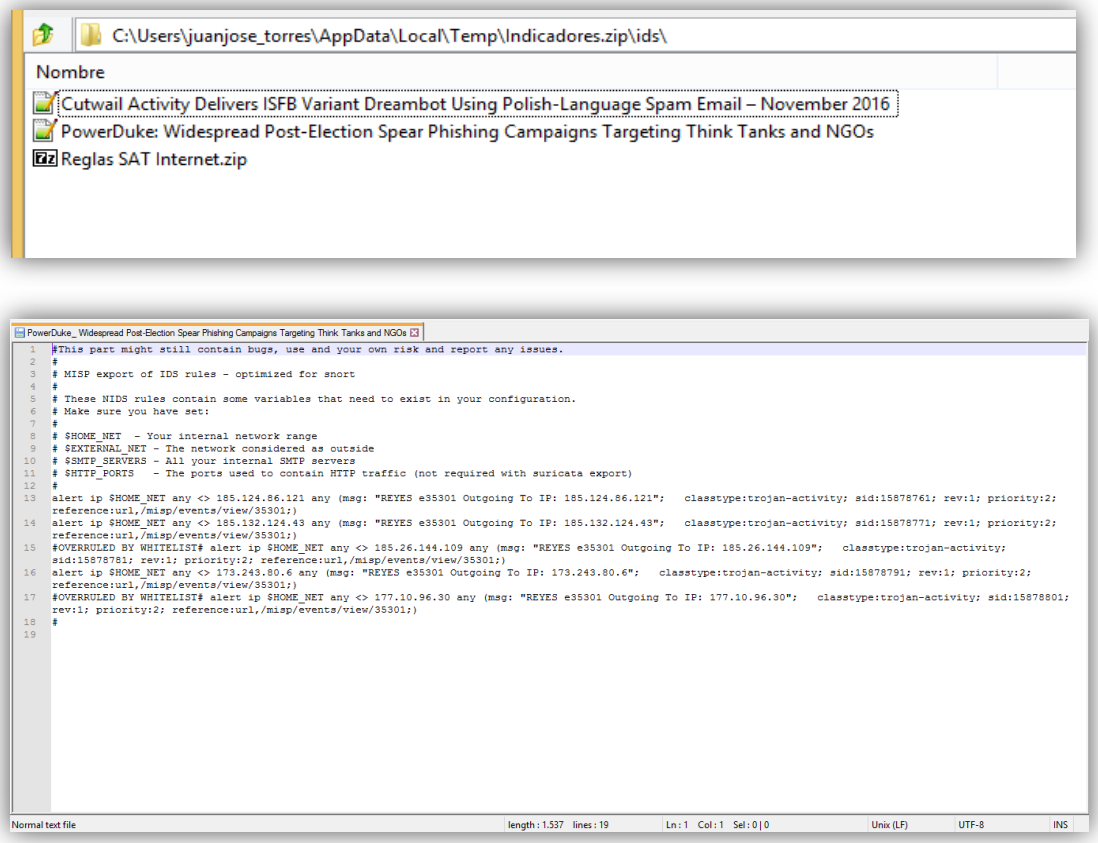
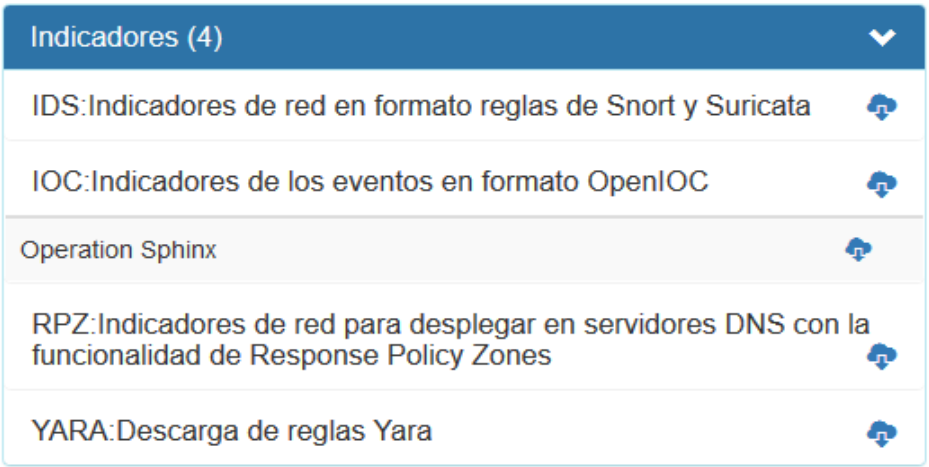


Figura 67. Descarga de Indicadores I

74. También es posible desplegar los indicadores de un tipo concreto y descargarlos individualmente.



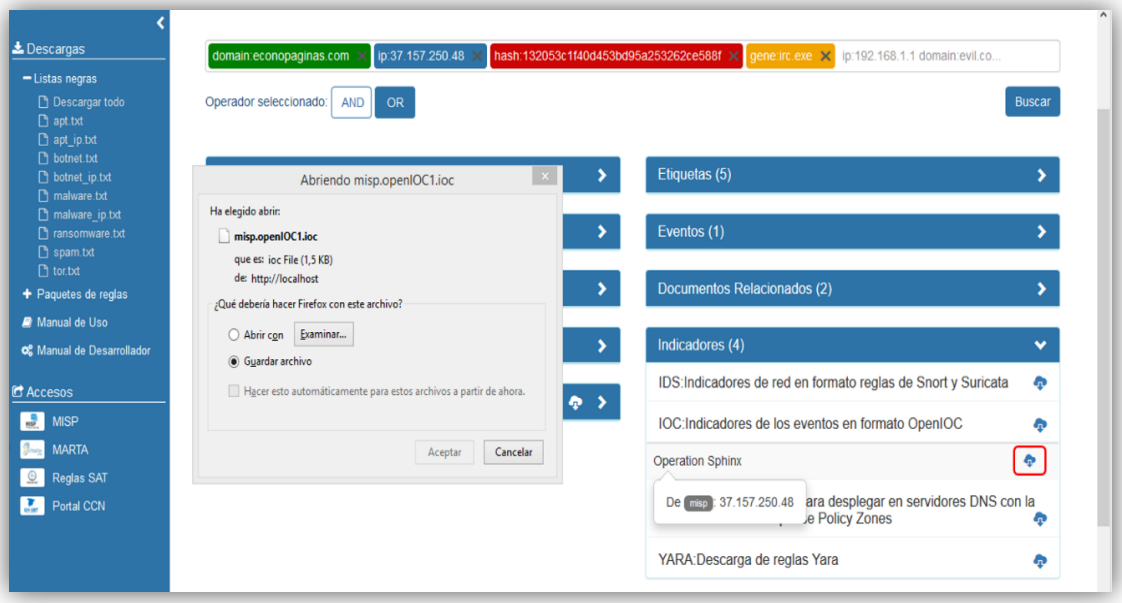


Figura 68. Descarga de Indicadores II

75. Manteniendo el ratón sobre un indicador, se puede obtener la aplicación de la que proviene y el término a partir del que se ha encontrado.

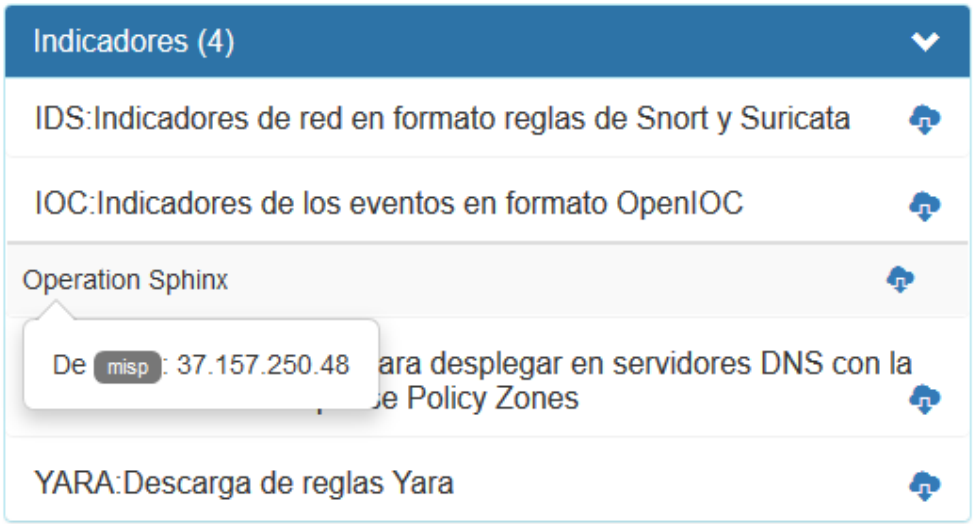


Figura 69. Información del indicador encontrado

1.7 ACCESO A LUCIA

76. Este acceso permite mostrar información en el contenido de Incidentes que tengan relación con los términos buscados. Se puede establecer el acceso a LUCIA clicando en el menú de la esquina superior derecha de la vista principal.

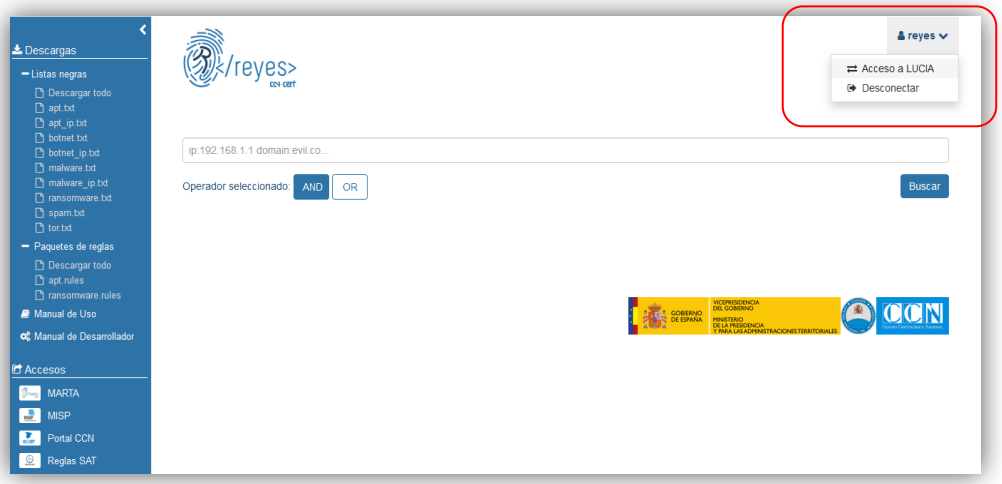


Figura 70. Acceso a LUCIA

77. A continuación se muestra la siguiente ventana en la que el usuario debe introducir sus credenciales.

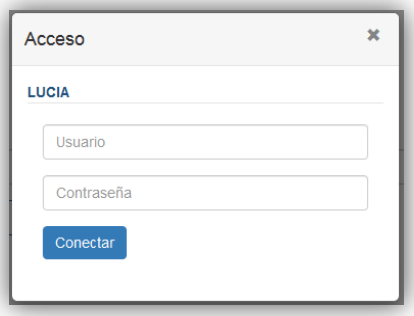


Figura 71. Introducción de credenciales en LUCIA

78. Una vez introducidos, si son correctos, se muestra el acceso a LUCIA.

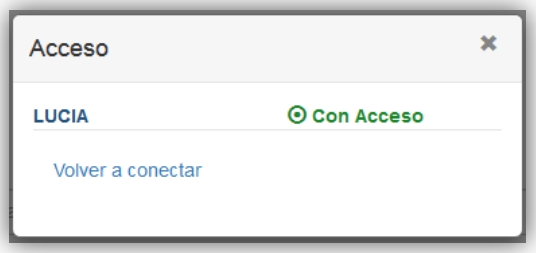


Figura 72. Acceso correcto a LUCIA

79. Mientras las credenciales sean válidas, no será necesario volver a introducirlas, incluso si se recarga la página. Sin embargo, se puede finalizar el acceso o cambiar las credenciales actuales clicando en Volver a conectar.

2 INTRODUCCIÓN A MISP

80. MISP (Malware Information Sharing Platform) es un sistema funcional y utilizable por las organizaciones para implementar una plataforma para intercambio de ciberinteligencia. Puesto que su principal caso de uso es el de intercambio de información, la herramienta está especialmente ideada para ofrecer un modo de intercambio para distintas organizaciones que internamente generan ciberinteligencia. Los usuarios del sistema tienen por tanto la oportunidad de facilitar y consumir elementos de ciberinteligencia.

81. Inicialmente fue desarrollada en el marco de las fuerzas armadas belgas (www.mil.be) pero desde 2012 se ha facilitado abiertamente a la comunidad con una licencia de código abierto y participan diversos equipos de respuesta a incidentes como NATO NCIRC[1], CIRCL[2], y CERT-EU[3].

82. Este sistema está adquiriendo bastante popularidad entre distintos equipos de respuesta a incidentes que tienen relación con el NATO NCIRC y actualmente el CIRCL (CSIRT nacional de Luxemburgo) ha implementado una plataforma de intercambio de ciberinteligencia[4] con MISP en la que participan varios CSIRT[5] nacionales europeos y algunos privados.

83. El sistema ofrece una base de datos centralizada de eventos de ciberseguridad en un formato estructurado compatible con iniciativas como OpenIOC[6] o STIX, y con funcionalidades como correlación de eventos en base a sus atributos, importación y exportación de estos eventos en distintos formatos (XML, texto plano, OpenIOC, YARA[7], STIX[8], CSV[9], etc.).

84. Como plataforma de intercambio, el sistema está diseñado focalizando en ofrecer distintas capacidades de interrelación entre las distintas entidades que colaborarían en una instancia de MISP y también entre distintas instancias de MISP.

    - En una instancia de MISP, una organización colaboradora puede disponer de múltiples usuarios con distintos niveles de privilegios de visibilidad de la información y con registro de sus actividades. Igualmente a nivel de organizaciones también se pueden implementar distintos niveles de visibilidad.

[1] Nato Computer Incident Response Capability
[2] Computer Incident Response Center Luxemburg
[3] Computer Emergency Response Team. European Union
[4] http://www.circl.lu/services/misp-malware-information-sharing-platform/
[5] Computer Security Incident Response Team
[6] Open Indicator of Compromise. Indicadores de Compromiso de código abierto
[7] YARA. Reglas muy precisas que permiten la detección de firmas y patrones en el código
[8] Structured threat information expression. Estructuración de la información de la amenaza
[9] Comma- Separated Value

- Entre distintas instancias de MISP (distintas comunidades) es posible establecer relaciones en las que se establezcan limitaciones como distintos niveles de visibilidad de información, dirección en que se puede realizar la transferencia de información.
- A fecha de realización de esta guía, la última versión disponible de MISP permite la integración con otros sistemas (otras instancias de MISP u otros) pero no empleando TAXII[10] como medio de transporte.

85. El acceso a la plataforma desplegada por el CCN-CERT se realiza a través del portal ubicado en la siguiente dirección: https://reyes.ccn-cert.cni.es. Para poder acceder es necesario disponer tanto de un certificado válido como de credenciales de acceso -usuario y contraseña-.

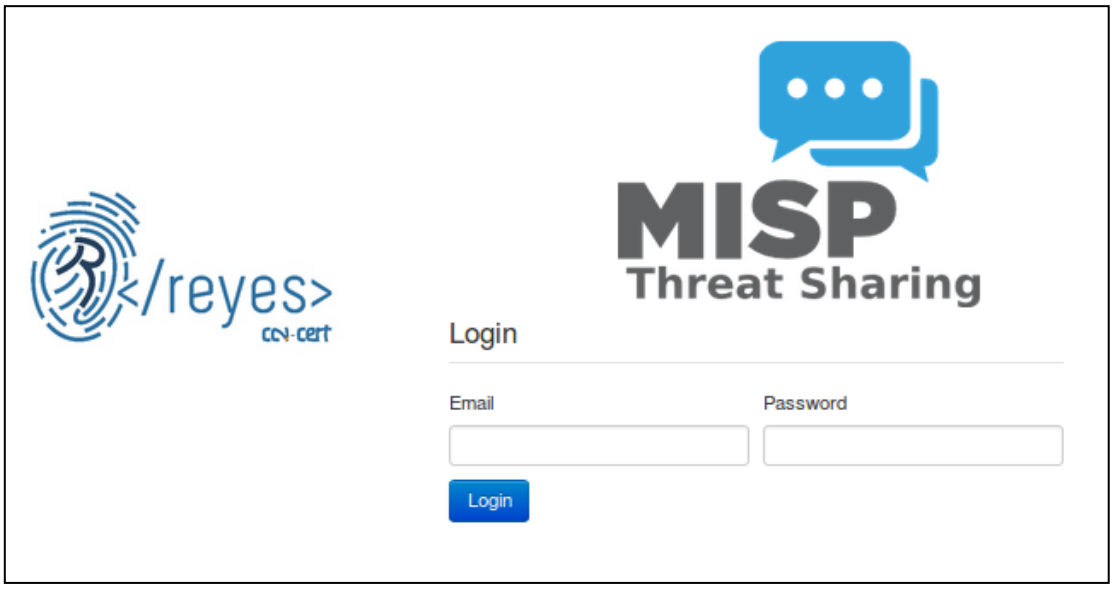


Figura 73. Pantalla de inicio de MISP

2.1 DESCRIPCIÓN GENERAL

86. La estructura de los datos almacenados en una instancia de MISP está organizada de una manera compatible con STIX. El elemento principal de MISP es el evento, que engloba una serie de atributos o indicadores. Todos los atributos de cada evento deben guardar alguna relación entre sí, ya sea porque corresponden a un incidente de seguridad o forman parte de una misma familia de código dañino (malware).

87. Por ejemplo, un incidente de seguridad es un evento que podrá contener atributos como direcciones de internet (IP) de equipos afectados, dominios de mando y control (C&C) utilizados y funciones resumen (hashes) de las muestras encontradas durante la investigación del incidente.

[10] TAXII. Trusted Automated eXchange of Indicator Information

88. Los eventos pueden estar etiquetados. Las etiquetas permiten realizar una clasificación de los eventos y agruparlos por una característica que pueda indicar que varios eventos tienen algo en común. Un ejemplo sería clasificar todos los eventos relacionados con Ransomware[11] mediante una etiqueta o pertenezcan a una misma campaña de ataque.

2.2 MODELO DE INTERCAMBIO DE INFORMACIÓN

89. En MISP el nivel de intercambio y visibilidad de la información se define mediante el parámetro de distribución (*distribution*) del evento y de cada uno de sus atributos. Además de la visibilidad que tendrán los usuarios sobre los eventos dentro de MISP, este parámetro también controla si el evento será sincronizado con otras instancias. En la visibilidad del evento juega un papel fundamental la organización (*organization*) a la que pertenece el usuario que crea el evento. La organización a la que pertenece el usuario se define en la creación del propio usuario.

90. MISP establece 5 niveles de intercambio de información:

- *Yourorganizationonly*: Este nivel sólo permite que los usuarios pertenecientes a la misma organización puedan ver el evento. Cuando se crea un usuario, éste debe pertenecer a una organización concreta, por lo que solo esos usuarios podrán ver el evento. Si se desea compartir el evento con instancias remotas, el usuario de sincronización deberá pertenecer a dicha organización.
- *Thiscommunnityonly*: Este nivel permite que los usuarios que pertenecen a la misma comunidad puedan ver el evento, es decir, los usuarios pertenecientes a la propia organización del usuario, a todas las organizaciones existentes en la propia instancia de MISP, y a las organizaciones que sincronizan con la instancia de MISP.
- *Connectedcommunities*: Este nivel permite que los usuarios que formen parte de la comunidad puedan ver los eventos de su comunidad de origen y de comunidades vecinas, es decir, todas las organizaciones definidas en la propia instancia de MISP, todas las organizaciones en instancias remotas de MISP que se sincronicen directamente y el de las instancias que se conectan a estas últimas (dos saltos desde la instancia inicial).
- *Allcommunities*: Se compartirá el evento con todas las comunidades permitiéndose que se propague de un servidor a otro.

1. [11]Consiste en el secuestro del ordenador (imposibilidad de usarlo) o el cifrado de sus archivos (Cryptoware) y la promesa de liberarlo tras el pago de una cantidad de dinero por el rescate.

- *Sharinggroup*: Es una visibilidad personalizada en la que se incluyen determinadas organizaciones para que puedan visualizar el evento.

2.3 PROPUESTA DE ATRIBUTOS

91. Aunque un usuario no puede modificar un evento del que no es dueño, existe la posibilidad de añadir información a eventos que son propiedad de otro mediante una propuesta (*proposal*) de nuevos atributos. A través de esta propuesta, el propietario del evento podrá decidir si incluir dichos atributos en el evento. En el apartado 4.3.3 Propuesta de atributos y adjuntos se detalla cómo se realiza este proceso.

2.4 MENÚ DE USUARIO

2.4.1 MENÚ PRINCIPAL

92. La barra superior contiene todas las funciones principales de la herramienta en forma de menús.

Figura 74. Menú principal de MISP.

93. Las funciones disponibles son:

- *Home*: Pantalla de inicio de la herramienta. Muestra los últimos eventos añadidos.
- *Eventsactions*: Toda la información introducida en MISP se realiza mediante objetos llamados eventos, '*events*', que contienen atributos. Este menú da acceso a toda la funcionalidad de creación, modificación, borrado, publicación, búsqueda y listado de eventos y sus atributos.
- *Galaxies*: Lista los galaxies disponibles en la herramienta MISP.
- *Input filters*: Con este menú se acceden a los filtros de entrada que modifican la información que se introduce en la instancia. Además de la validación de atributos por tipo, es posible definir expresiones regulares y listas negras para ciertos valores así como bloquearlos de ser exportables.
- *Global actions*: Este menú ofrece acceso a información de la instancia de MISP como ver el perfil, manual de usuario de MISP, etc.
- *SyncActions*: Este menú muestra la lista de instancias conectadas y permite la configuración de la sincronización con ellas además de añadir nuevas.

2.4.2 MENÚ EVENTS ACTIONS

94. Desde el menú *Events actions* se gestiona la creación de los eventos.

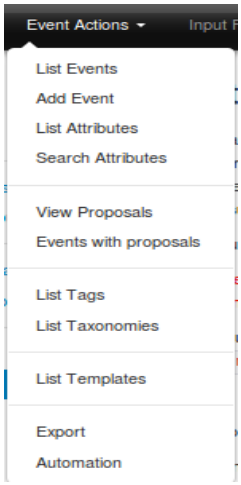


Figura 75. Menú Event Actions.

95. Las acciones disponibles son:

- *List Events*: Lista todos los eventos del sistema, se pueden ver, añadir, modificar y borrar (si se tiene permisos) desde la columna Actions, a la derecha de la pantalla.
- *Add Event*: Permite la creación de un evento y añadir atributos a dicho evento.
- *List Attributes*: Muestra todos los atributos visibles por el usuario. Se pueden modificar, añadir o ver cada uno de estos atributos desde esta pantalla.
- *Search Attributes*: Opción para encontrar atributos gracias a varios filtros de búsqueda.
- *View Proposals*: Muestra una lista de propuestas de atributos a un evento ya existente creadas por su organización y que se encuentran pendientes de aprobación por parte del propietario del evento.
- *Events with proposals*: Se muestran eventos que contienen propuesta de atributos.
- *List tags*: Muestra las etiquetas creadas.
- *List Taxonomies*: Muestra las taxonomías disponibles. Cada taxonomía contiene una serie de etiquetas que pueden ser compartidas entre distintas instancias de MISP.
- *List Templates*: Muestra las plantillas creadas por los usuarios.
- *Export*: Exporta los datos deseados en distintos formatos.
- *Automation*: Información y clave de acceso (API[12] KEY) con la que se puede usar el API REST[13] para la automatización y el volcado automático de datos.

[12] Application Programming Interface

2.4.3 MENÚ GALAXIES

96. Desde el menú *List Galaxies* se muestran las agrupaciones de galaxies disponibles:

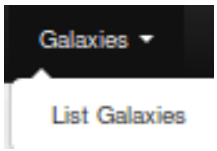


Figura 4. Menú Galaxies.

97. Galaxies es un método estructurado que permite clasificar un evento en función del atacante, métodos y herramientas utilizadas. Este método permite que la gran cantidad de información que hay almacenada en MISP esté correctamente clasificada y estructurada.

98. Actualmente MISP dispone de los siguientes galaxies.

99. *Galaxy Threat Actor*: Grupos APT. (Agrupa en una única clasificación todos los nombres y campañas por los que es conocido un único actor)

100. *Galaxy Tool*: Herramientas utilizadas por actor.

101. *Galaxy Microsoft Activity Group Actor*: Grupos APT. (Agrupa en una única clasificación todos los nombres y campañas por los que es conocido un único actor según Microsoft).

2.4.4 MENÚ INPUT FILTERS

102. Las acciones disponibles son:

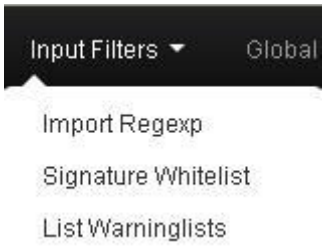


Figura 5. Menú Input Filters.

103. *ImportRegexp*: Se pueden visualizar expresiones regulares que permiten modificar la información que se introduce en el sistema. Puede ser útil cuando se desea, por ejemplo, filtrar información personal de importaciones automáticas.

104. *Signature Whitelist*: Quedarán excluidos en la exportación de datos los atributos que coincidan con la lista blanca.

[13] Representational State Transfer

105. *ListWarninglists*: Se muestran las diferentes listas sobre indicadores conocidos como legítimos, entre las que se incluye la lista de Alexa con el top 5000 de direcciones URL[14] legítimas.

106. Dentro de un evento, muestra una casilla de información/advertencia

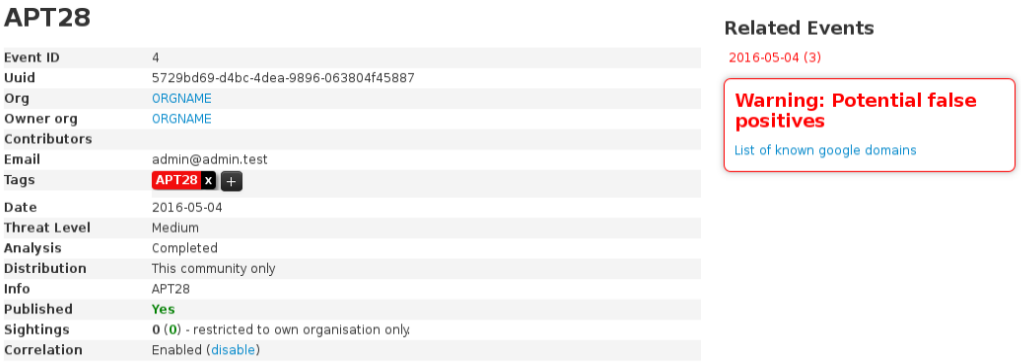


Figura 6. Menú WarningLists.

2.4.5 MENÚ GLOBAL ACTIONS

107. Las acciones disponibles son:

Figura 7. Menú Global Actions.

[14] URL.Uniform Resource Locator, Localización uniforme de recurso. Es la forma en la que se identifica un sitio en Internet. Ej: https:\\www.ccn.cni.es

- ***News:*** Visualiza las últimas noticias sobre el sistema MISP.
- ***MyProfile*:** Gestiona la cuenta del usuario conectado.
- ***Dashboard:*** Visualiza las notificaciones y los cambios en los eventos desde la última visita.
- ***Organisations:*** Permite editar las organizaciones locales y remotas que están definidas en la instancia.
- ***Role Permissions:*** Visualiza los permisos del usuario.
- ***ListSharingGroups:*** Visualiza los grupos de compartición.
- ***Add SharingGroup:*** Permite crear un grupo de compartición.
- ***UserGuide:*** Enlace a una guía de usuario de MISP.
- ***Terms&Conditions:*** Visualiza los términos y condiciones.
- ***Statistics:*** Muestra una serie de estadísticas sobre los usuarios y la información de la instancia de MISP.
- ***List Discussions:*** Visualiza los debates abiertos en la herramienta.
- ***StartDiscussions:*** Permite iniciar un debate.

2.5 PANTALLA DE INICIO

108. En la pantalla de inicio se muestra una lista de los últimos 60 eventos. La información que se muestra en esta pantalla es la siguiente:

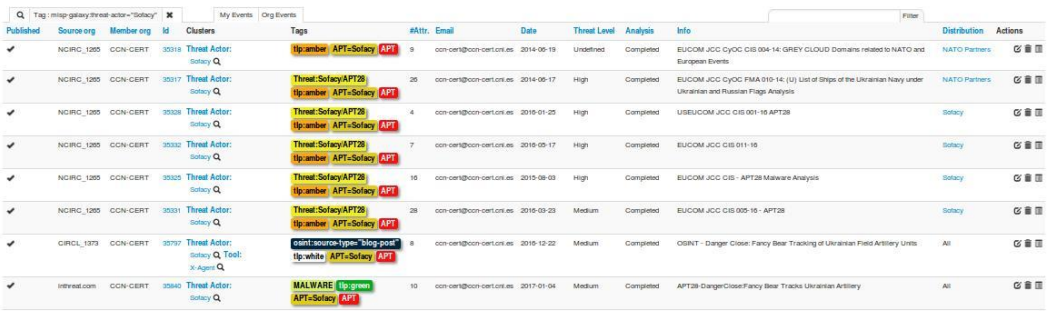


Figura 8. Listado de eventos.

- ***Published*:** Si el evento se encuentra publicado o no. Un evento no publicado solo es visible por su autor, de forma que ni se sincroniza ni es visto por nadie más que por él mismo. Esto permite crear eventos y trabajar con ellos como si fuera un borrador antes de publicarlos y que formen parte de la información común que se comparte en MISP.
- ***SourceOrg y MemberOrg*:** La organización y el miembro que creó el evento.
- ***ID*:** El identificador del evento asignado automáticamente por el sistema.
- ***Clusters*:** Muestra el nombre de los actores que realizan la amenaza y los nombres de las herramientas utilizadas.

- ***Tags*:** Etiquetas asignadas al evento.
- ***Attr*:** El número de atributos que tiene el evento.
- ***Date*:** Fecha de creación del evento.
- ***Threatlevel*:** Nivel de amenaza del evento:
  - *Low*: Código dañino común.
  - *Medium*: APT[15].
  - *High:* APT sofisticado y exploit 0 day[16].
- ***Analysis:*** Estado del análisis de la amenaza.
- ***Info:*** Una breve descripción del evento.
- ***Distribution:*** El nivel de compartición del evento.
- ***Actions:*** Listado de acciones disponibles sobre el evento:
  - Publicar.
  - Editar.
  - Borrar.
  - Ver.
  - Enriquecer con *passivetotal.*

2.6 USO DE MISP

2.6.1 CREACIÓN DE EVENTOS

109. El proceso de creación de un evento se divide en 4 fases:

- Creación del evento en sí.
- Inclusión de atributos.
- Adjuntar binarios.
- Publicar el evento.

110. En la fase de inclusión de atributos se tiene la opción de importar la información de fuentes externas con formatos (*freetext import, populateusing a template, OpenIOC import y threatConnect Import CSV*).

[15] Advanced Persistent Threat. Amenaza persistente avanzada

[16] Un exploit es un programa que explota o aprovecha una vulnerabilidad de un sistema informático en beneficio propio. Por su parte, los llamados exploits de día-cero (zero-day) son aquellos que todavía no se han publicado y, por tanto, no disponen de soluciones de seguridad que eviten la vulnerabilidad

2.6.1.1 ADD EVENT

111. En la creación del evento, en la opción *AddEvent*, se pide rellenar la siguiente información:

112. ***Date*:** Indica la fecha en la que ha sucedido el incidente.

113. ***Distribution*:** Este parámetro define quién podrá visualizar el evento una vez que se publique. En el apartado 2.1 se detalla la visibilidad de cada valor.

114. ***Threatlevel*:** Contempla 4 niveles: sin definir, bajo, medio y alto.

115. ***Analysis*:** Indica el estado de análisis del evento: inicial, en progreso o completado.

116. ***Event Info*:** Una breve y concisa descripción del evento.

117. ***GFI Sandro*:** Es posible subir resultados exportados de la *sandios GFI* en formato Zip.

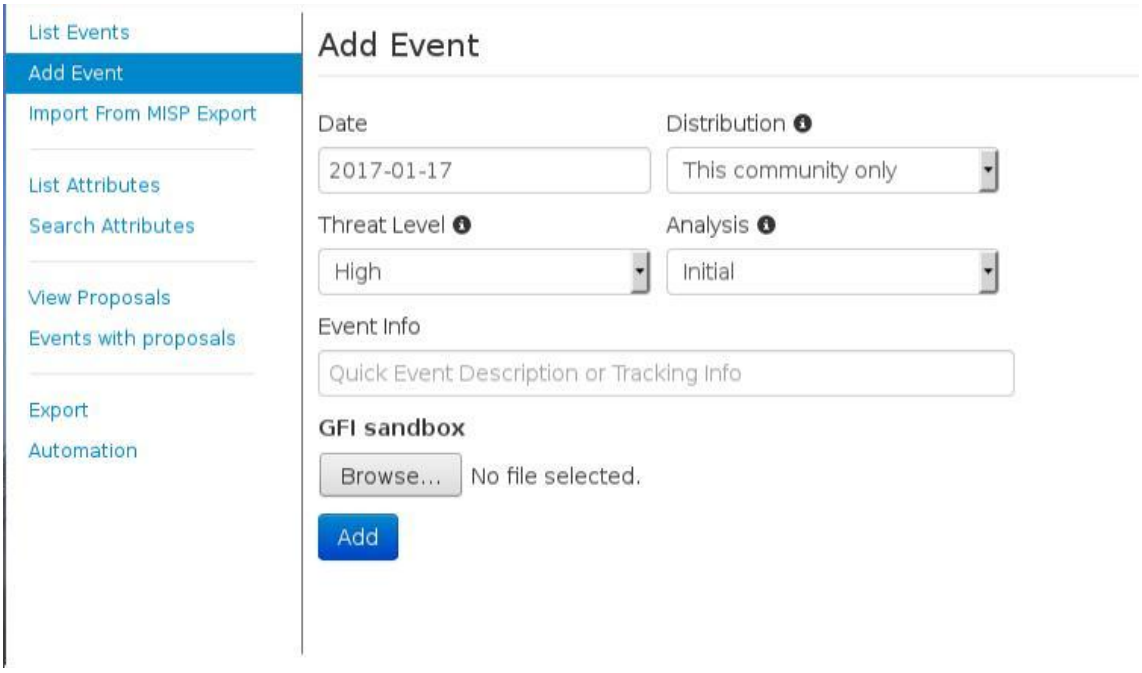


Figura 9. Creación de un evento.

118. Una vez creado el evento se accede a la vista del mismo, igual que si se visualizara cualquier otro evento del sistema. A través del panel de la izquierda se podrán realizar acciones sobre el evento:

Figura 10. Acciones disponibles sobre un evento.

2.6.1.2 VIEW CORRELATION GRAPH

119. Muestra un gráfico de correlación de eventos, en el cual muestra la relación de atributos entre distintos eventos.

Figura 11. Gráfico de correlación de eventos.

2.6.2 VIEW EVENT HISTORY

120. Muestra un histórico de las acciones realizadas sobre un evento, como por ejemplo: creación de atributos, etiquetado o publicación.

Org	Action	Model	Title	Created
InnotecSystem	publish	Event	Event (32333): Campaña TorrentLocker	2016-04-15 21:34:55
InnotecSystem	tag	Event	Attached tag (63) to event (32333)	2016-04-15 21:34:50
InnotecSystem	add	Attribute	Attribute (1301610) from Event (32333): Network activity/domain barrout.org	2016-04-15 21:34:33
InnotecSystem	add	Attribute	Attribute (1301609) from Event (32333): Network activity/domain zrepudax.barrout.org	2016-04-15 21:34:33

Figura 12. Histórico de acciones sobre un evento.

2.6.2.1 ADD ATTRIBUTE

121. El siguiente paso tras la creación de un evento es la inclusión de atributos. Se puede realizar de forma manual o a través de formatos conocidos como: (*freetext import, populateusing a template, OpenIOC import y threatConnect Import CSV*)

122. Mediante el botón Add Atribute se pueden añadir atributos al evento.

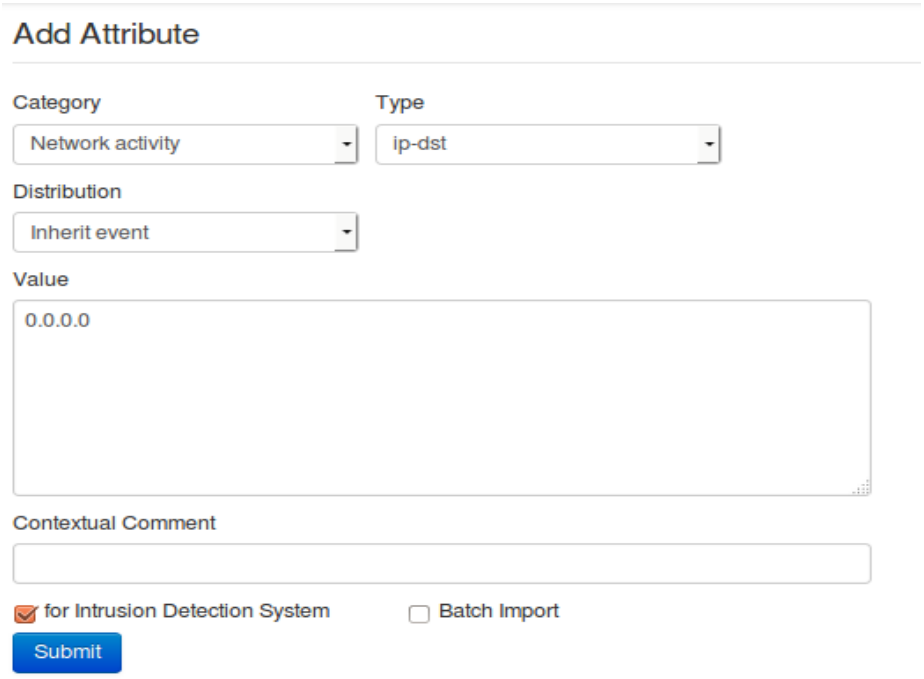


Figura 13. Inclusión de un nuevo atributo.

123. Los campos a rellenar son:

- ***Category***: Este desplegable define la categoría del atributo indicando qué aspecto del evento se está describiendo. Puede ver en detalle el significado de cada categoría en el Anexo I.
- ***Type***: Mientras que las categorías determinan qué aspecto de un evento se está describiendo, el type explica concretamente qué se está describiendo. Como ejemplo, una dirección IP origen de un ataque, una dirección de email o un fichero enviado a través de un adjunto pueden pertenecer a la

categoría payloaddelivery si son métodos utilizados para la distribución de un código dañino.

- **Distribution:** Visibilidad que se le asigna al atributo. Siempre prevalecerá la distribución asignada al evento si ésta es más restrictiva. La *visibilidadInheritEvent*, permite heredar al atributo la visibilidad asignada al evento.
- ***Value*:** El valor asignado al atributo.
- ***Contextual Comment*:** Permite añadir un comentario al atributo
- ***ForIntrusionDetectionSystem*:** Esta opción permite al atributo ser usado en una regla de IDS[17] cuando se exporta como reglas NIDS[18] (Snort, Suricata y Bro).
- ***BatchImport*:** Si hay varios atributos del mismo tipo, se pueden incluir todos de una vez separados por filas para que el sistema genere un atributo por cada valor insertado.

2.6.2.2 ADD ATTACHMENT

124. Se pueden añadir adjuntos a un evento como, por ejemplo, evidencias del incidente, documentos con análisis externos relacionados, artefactos generados por un código dañino o, incluso, el propio código dañino.

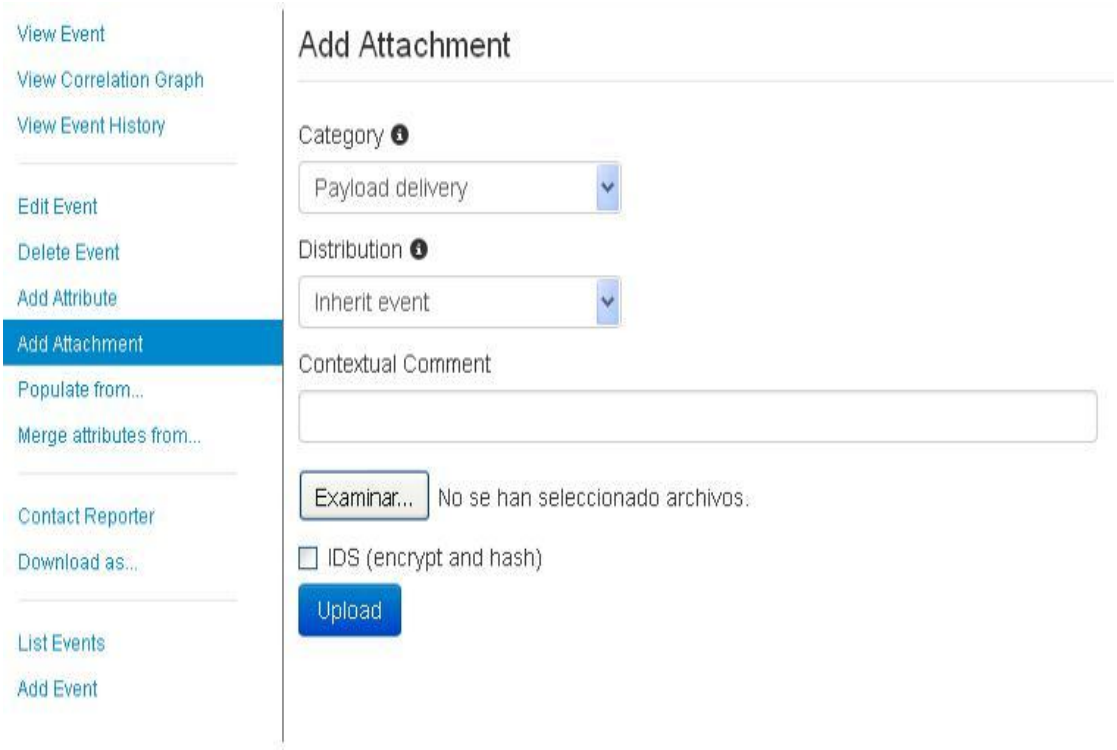


Figura 14. Inclusión de un adjunto.

[17] Intrusion Detection System
[18] Network Intrusion Detection System

125. Los campos que se tienen que rellenar son:

- ***Category*:** Este desplegable define la categoría del atributo indicando qué aspecto del evento se está describiendo. Puede ver en detalle el significado de cada categoría en el Anexo I.
- ***Distribution*:** Visibilidad que se le da al atributo. Siempre prevalecerá la distribución asignada al evento si ésta es más restrictiva.
- ***Contextual Comment*:** Permite añadir un comentario al atributo.
- ***Examine*:** Abre un cuadro de diálogo para subir el fichero.
- ***IDS (encrypt and hash)*:** Esta casilla indica si el fichero debe marcarse como código dañino o no. Si se trata de código dañino comprime el fichero y le asigna una contraseña para evitar que accidentalmente un usuario pueda ejecutar el fichero e infectarse. Además extraerá los hashes MD5[19] SHA1[20] y SHA256

2.6.2.3 POPULATE FROM…

126. Su función es importar un atributo al evento, ya sea importándolo en texto plano, usando una plantilla, utilizando un fichero con formato *OpenIOC o CSV.*

127. Para ello basta con pulsar el botón populate from y elegir una de las cuatro opciones disponibles (*freetext import, populateusing a template, OpenIOC import y threatConnect Import*) según corresponda el tipo de formato del fichero a importar. MISP se encargará de analizar sintácticamente (*parsear*) y añadir su información en forma de atributos del evento.

128. Si se dispone de un fichero OpenIOC o de tipo CSV de ThreatConnectse pueden importar al evento los atributos definidos en el fichero IOC. Para ello basta con pulsar el botón *OpenOIC Import o ThreatConnect Import*, según el formato del fichero a importar.

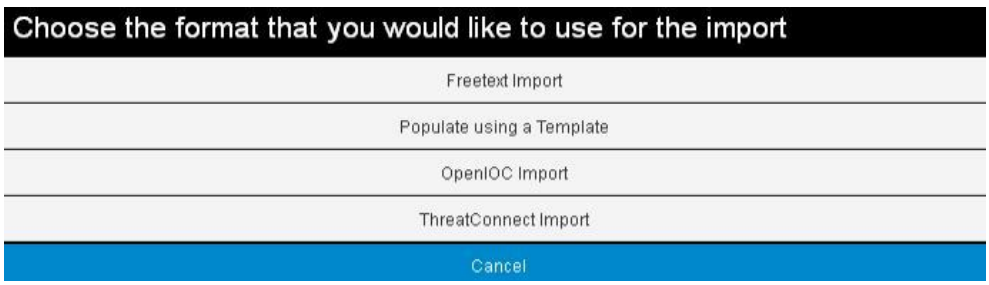


Figura 15. Selección de formato de fichero a importar.

- ***Freetext Import*:** Permite añadir una lista de atributos en texto plano.

[19] Algoritmo de cifrado Message Digest 5

[20] Secure Hash Algorithm

- ***Populate using a Template*:** Se importa la información para crear el atributo usando una plantilla ya existente con campos predefinidos.
- ***OpenIOC Import***: Importar un fichero con formato OpenIOC.
- ***ThreatConnect Import*:** Importar un fichero con formato CSV.

2.6.2.4 MERGE ATTRIBUTES FROM…

129. Su función es fusionar dos eventos que tengan atributos en común. Basta con pulsar en dicha opción y la herramienta pedirá el evento con el que se quiere fusionar.

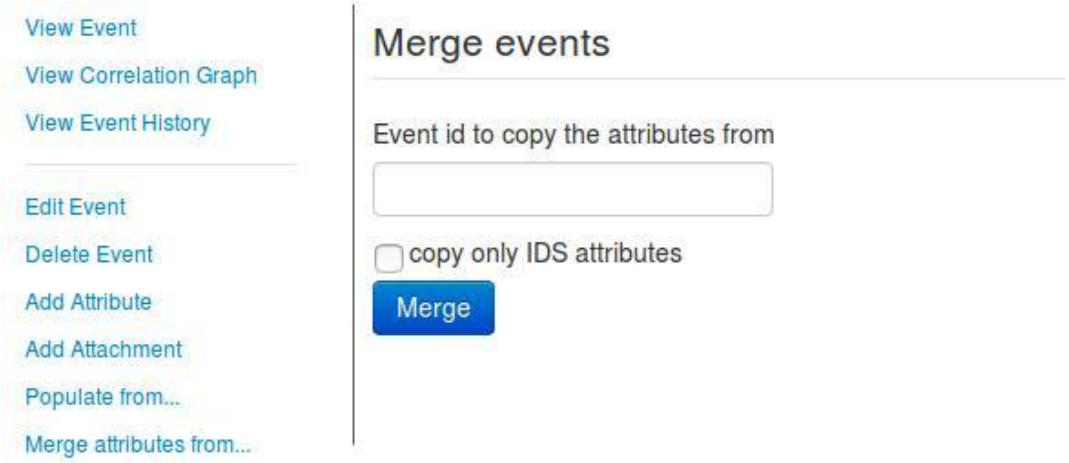


Figura 16.Merge events.

130. A continuación se mostrarán los atributos que van a ser creados, hay que garantizar que los tipos de atributos son correctos, ya que se ofrecerán varias opciones de forma automática.

2.6.2.5 PUBLISH EVENT

131. El último paso es la publicación de eventos. Una vez que todos los atributos y adjuntos están subidos, se puede publicar el evento pulsando el botón *Publish.* Esta acción alertará a los usuarios y propagará el evento a instancias conectadas.

132. Existe la posibilidad de publicar eventos sin alertar a otros usuarios mediante el botón *Publish (no email)*. Esta opción sólo se debería usar para correcciones menores.

2.7 USO DE GALAXIES

133. MISP *Galaxy* es un método simple y estructurado que permite clasificar un evento agrupando todos los nombres por los que es conocido el actor de una amenaza.

134. Para clasificar eventos con *Galaxies*, pulsamos en *add new clúster*.

Figura 17. Clasificación con galaxies.

135. Se selecciona el actor de la amenaza.

Figura 18. Selección de actor.

136. Como se muestra en la imagen, en el cluster se agrupan todos los nombres con los que está relacionada la amenaza, de forma que utilizando cualquiera de los alias, MISP lo clasifica automáticamente con el galaxy al que pertenece.

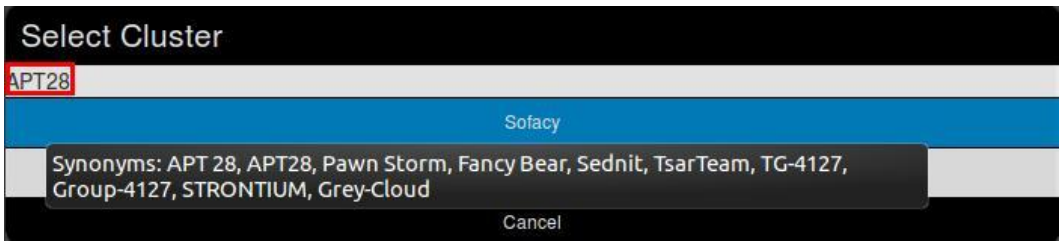


Figura 19. Selección de cluster.

137. Permite incluir las herramientas utilizadas en la amenaza, pulsando en ***Galaxy:tool***

Figura 20. Selección de herramientas.

138. Una vez dentro se incluyen las herramientas utilizadas.

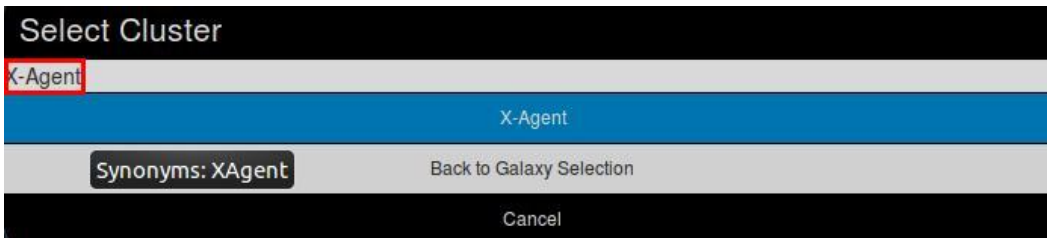


Figura 21. Inclusión de herramientas.

139. En la pantalla principal, se observan los eventos clasificados con Galaxies.

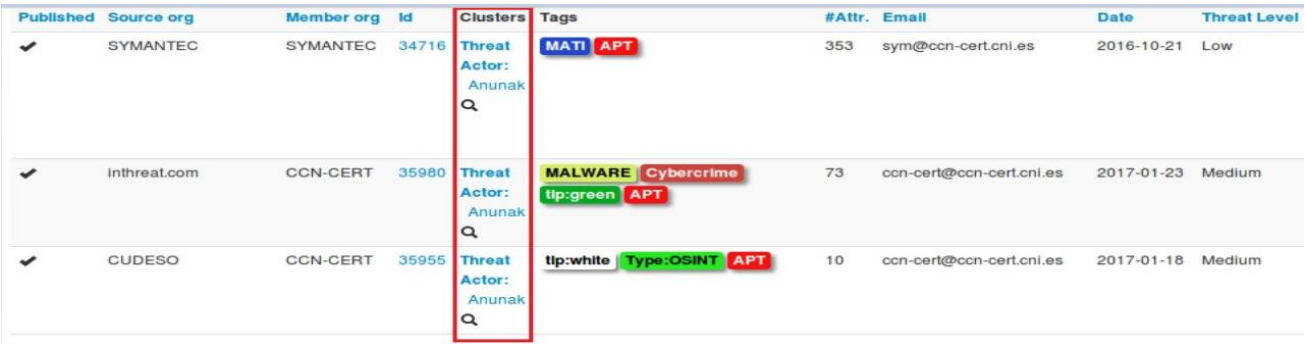


Figura 22. Eventos clasificados con Galaxies.

2.8 VISUALIZACIÓN DE EVENTOS

140. En la pantalla del listado de eventos (*ListEvents*) se puede acceder a cada evento pulsando en su identificador único, *Id*, que mostrará la información del evento.

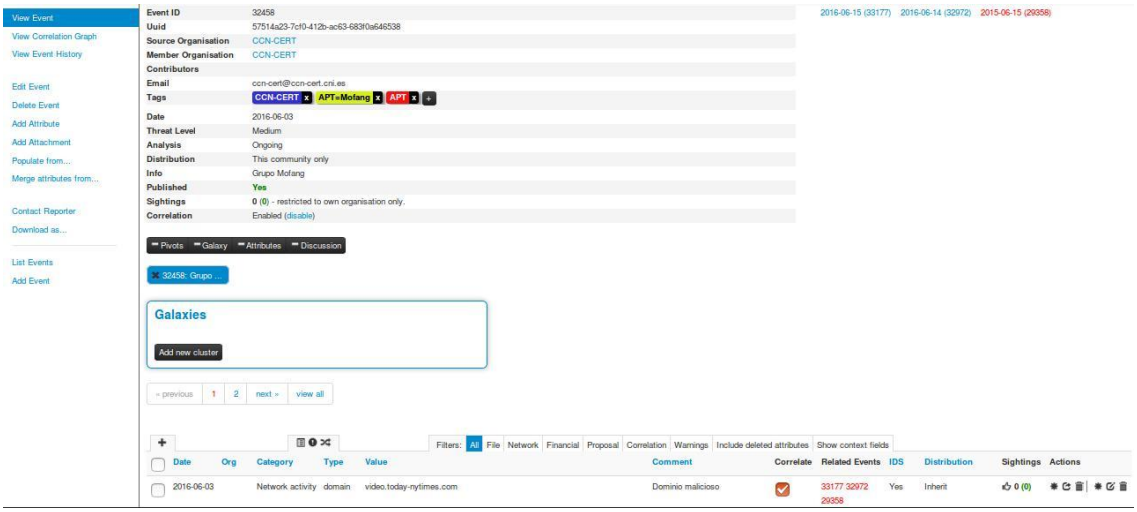


Figura 23. Detalles de un evento.

141. En la parte superior se muestra la información relacionada con el propio evento:

- ***ID*:** El identificador del evento.
- ***Uuid*:** Valor utilizado para evitar colisiones entre eventos y atributos.
- ***SourceOrganisation*:** La organización fuente del evento.
- ***MemberOrganisation*:** La organización miembro de la instancia de MISP dueña del evento.
- ***Contributors*:** Lista de organizaciones que han contribuido al evento mediante propuestas (proposals).
- ***Tags:*** Lista de etiquetas asociadas al evento.
- ***Date*:** Fecha de creación del evento.
- ***ThreatLevel*:** Nivel de amenaza asignado al evento.
- ***Analysis*:** El estado del análisis del evento.
- ***Distribution*:** Nivel de distribución del evento.
- ***Description*:** Breve descripción del evento.
- ***Published*:** Indica si el evento está publicado o no. Publicar el evento permite que todos sus atributos puedan ser incluidos en las exportaciones de eventos.

142. Más abajo aparece una tabla que contiene todos los atributos con la siguiente información:

- ***Date*:** Fecha de inclusión del atributo.
- ***Category*:** Categoría del atributo.
- ***Type*:** Tipo de atributo.
- ***Value*:** Valor asignado al atributo.
- ***Comment*:** Comentarios añadidos al atributo.
- ***Relatedevents*:** Eventos que tienen un atributo con el mismo valor.
- ***IDS*:** Indicador de si el atributo se encuentra marcado para exportar como regla IDS.
- ***Distribution*:** Nivel de compartición del atributo.
- ***Sightings*:** Permite validar la fiabilidad de un atributo. Esta opción es independiente para cada organización y solo los usuarios de la organización podrán visualizar dicha información.
- ***Actions*:** Diferentes acciones a realizar sobre el atributo, como publicarlo, editarlo, borrarlo y enriquecerlo con información de *PassiveTotal.*
- Desde el menú de la izquierda se pueden realizar modificaciones sobre el evento. En función de si somos o no el propietario del evento, se tendrán disponibles más o menos acciones. Este es el listado de acciones para eventos de los cuales no somos propietarios
- ***Propose Attribute/Attachment*:** Proponer un nuevo atributo o fichero adjunto al evento. El propietario del evento deberá validar la propuesta.
- ***Download as*:** Permite la descarga del evento en diversos formatos como CSV, STIX, XML[21] o JSON[22].

[21] eXtended Markup Language

[22] JavaScript Object Notation. Formato de texto para intercambio de datos

2.8.1 INCLUSIÓN DE ETIQUETAS

143. En la vista general de un evento se pueden añadir etiquetas al evento. Para añadir una etiqueta se hace clic en el botón '+' del campo *Tags*. Aparecerá un desplegable con un listado de todas las etiquetas:

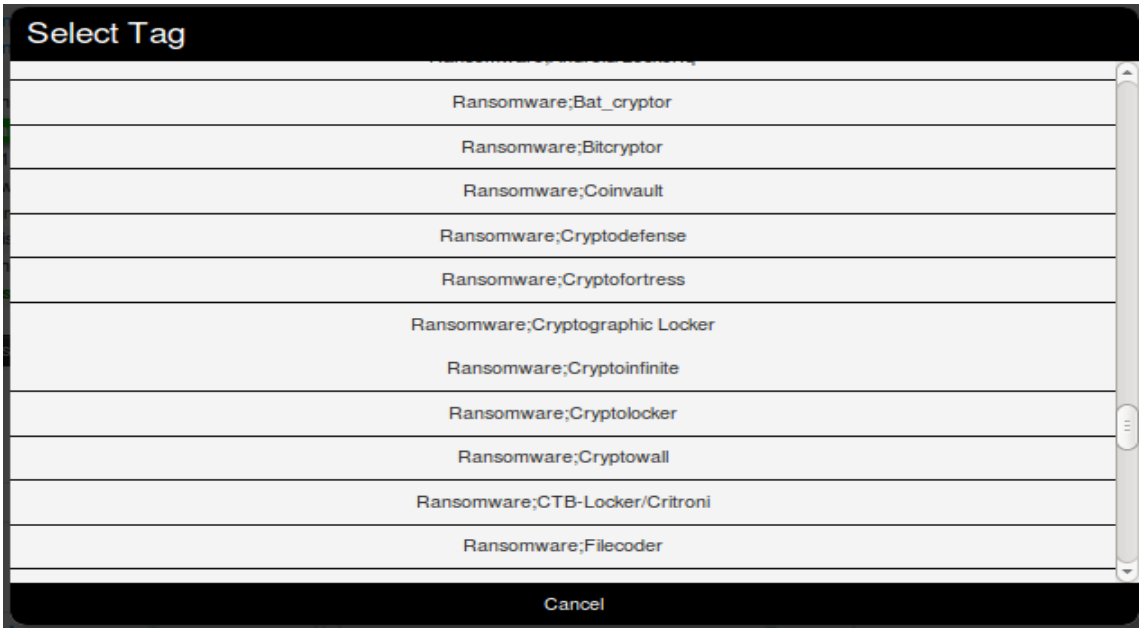


Figura 24. Listado de etiquetas.

144. Se pueden asignar tantas etiquetas como se desee a cada evento.

2.8.2 BÚSQUEDA DE ATRIBUTOS

145. Se pueden buscar únicamente atributos de unos determinados eventos a través del botón *Search Attributes*, dentro de la lista de eventos (*List Events*).

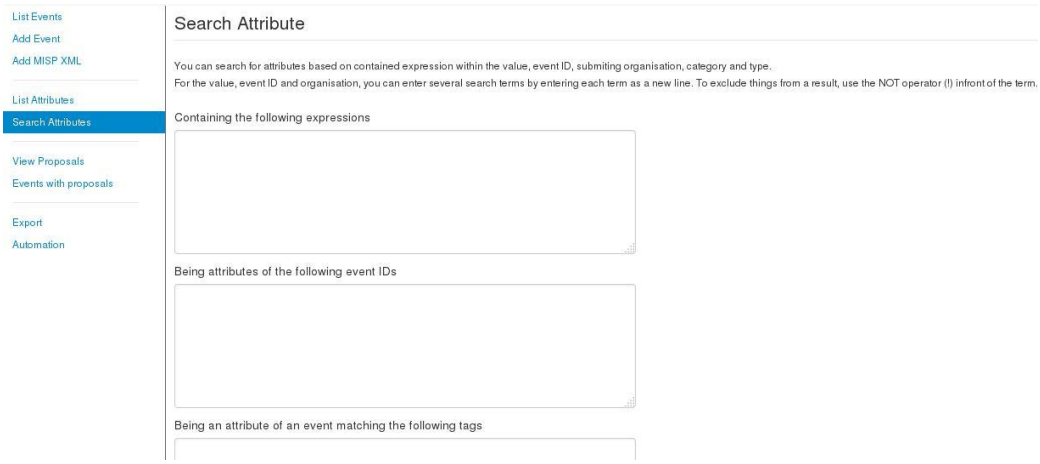


Figura 25. Búsqueda de atributos.

146. En la pantalla se podrán buscar atributos que:

- Contengan una expresión o expresiones que se indiquen.

- Vengan de unos eventos concretos indicando el ID del evento.
- Cumplan una o varias etiquetas asignadas.
- Pertenezcan a una organización concreta.

Figura 26. Búsqueda de atributos por tipo y/o categoría.

147. Por último, se puede seleccionar el tipo de atributo que se quiera visualizar, así como la categoría. Una vez finalizado se pulsa el botón "Search", que mostrará la información solicitada. A la izquierda del resultado de la búsqueda aparecerá la opción de descargar el listado de atributos en formato XML, JSON y CSV.

2.8.3 PROPUESTA DE ATRIBUTOS Y ADJUNTOS

148. Si se desean añadir atributos o adjuntos a un evento del que no se es propietario, se puede proponer el atributo o adjunto para que el propietario lo añada si lo estima conveniente. En el evento donde se desea añadir el atributo se hace clic en *ProposeAttribute.*

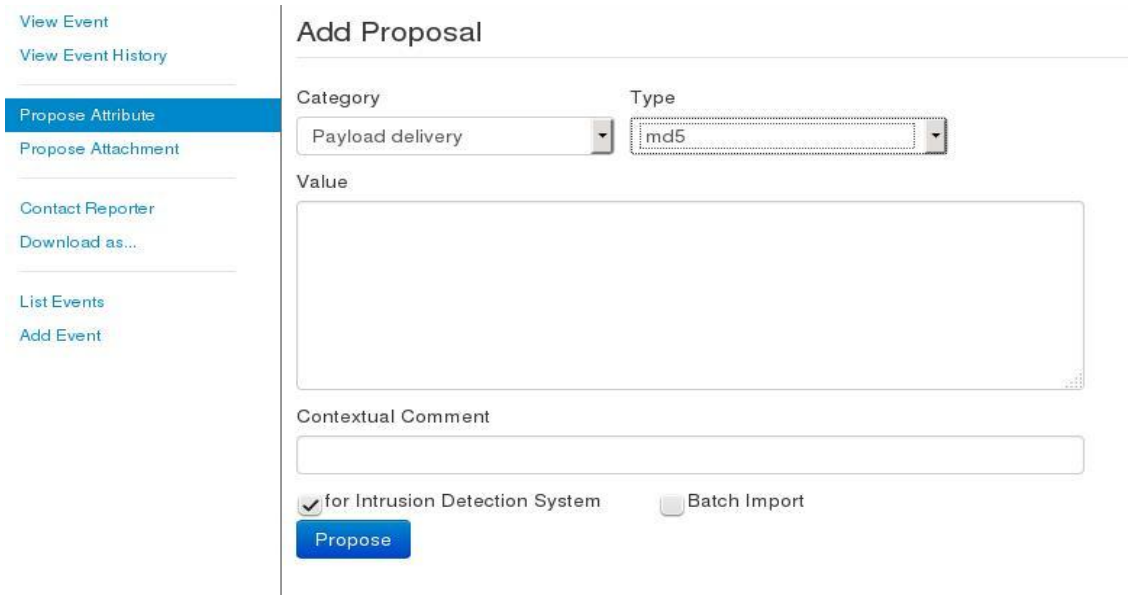


Figura 27. Propuesta de atributos.

149. La finalidad de cada campo se encuentra explicada en el apartado Inclusión de atributos.

2.8.4 SHARING GROUPS

150. Esta característica permite crear grupos de compartición personalizados de modo que un evento o un atributo solo serán vistos por los organismos o comunidades que pertenecen a dicho grupo o *Sharing group*.

151. Para crear un nuevo *Sharing group* se hace clic en el menú superior en *global actions* y posteriormente en *addsharinggroups.*

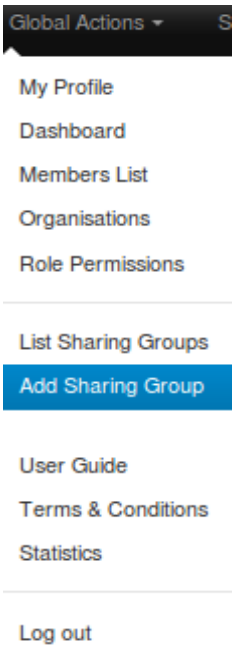


Figura 28. Menú global actions.

152. En la pestaña General se indica el nombre del grupo, las organizaciones y/o comunidades a las que será aplicable y un campo de descripción. La casilla *Make the sharing group selectable* habilita o deshabilita que el grupo.

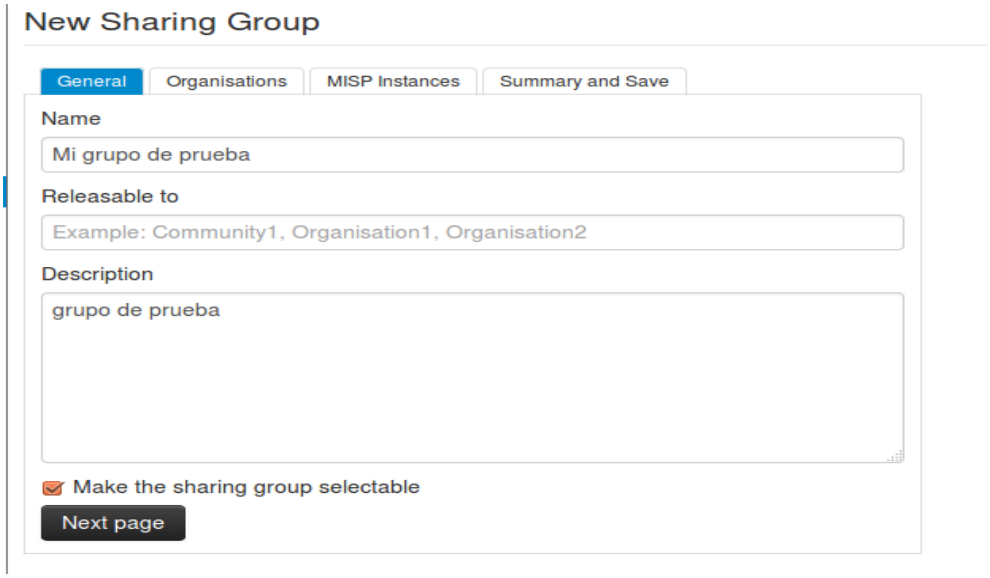


Figura 29. Ventana crear nuevo grupo de compartición.

153. En la pestaña "*organisations*" se añaden las organizaciones que se desea que pertenezcan al grupo creado. Se pueden agregar tanto organizaciones locales como organizaciones remotas de la instancia de MISP. También ofrece la posibilidad de marcar "*extend*" que permite ampliar el grupo de compartición a otras organizaciones.

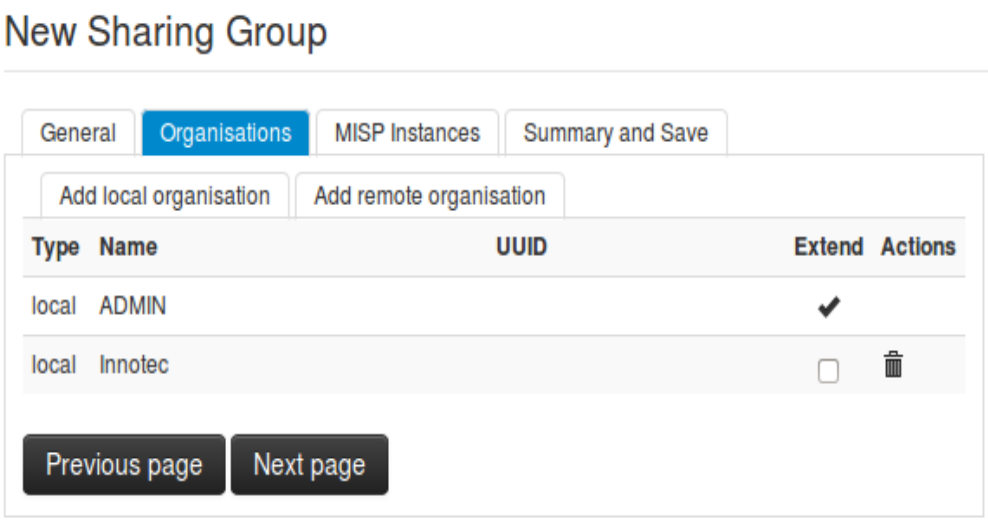


Figura 30. Pestaña organisations.

154. En la pestaña MISP instances se pueden añadir instancias de MISP al grupo en cuestión, también ofrece la opción de marcar "*Allorgs*", el cual añadirá todas las organizaciones de la instancia al grupo en cuestión. En la pestaña *MISP Instancesse* pueden añadir comunidades al grupo que pertenezcan a la instancia propia de MISP o a instancias remotas. La casilla *Allorgs* hace el grupo visible a todas las comunidades de la instancia de MISP correspondiente.

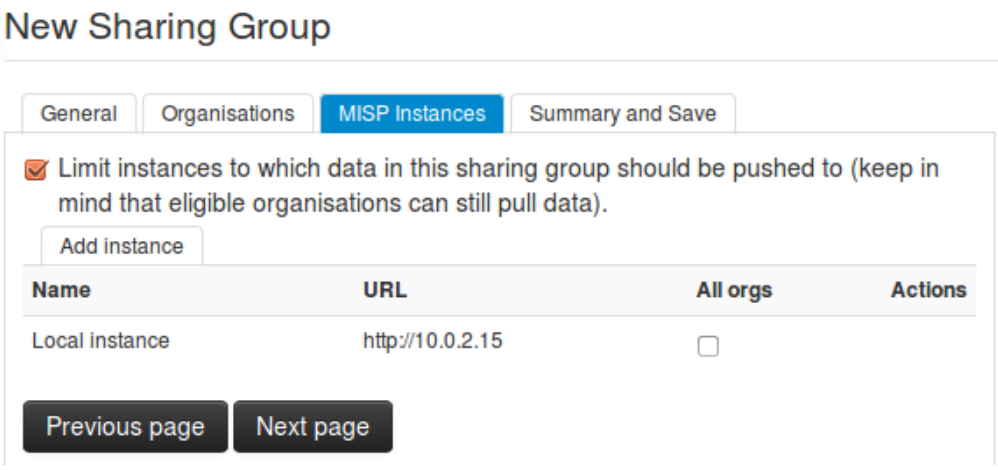


Figura 31. Pestaña de instancias de MISP.

155. Por último, en la pestaña *summary and save*, se muestra un resumen de las organizaciones y las comunidades que pertenecen al grupo.

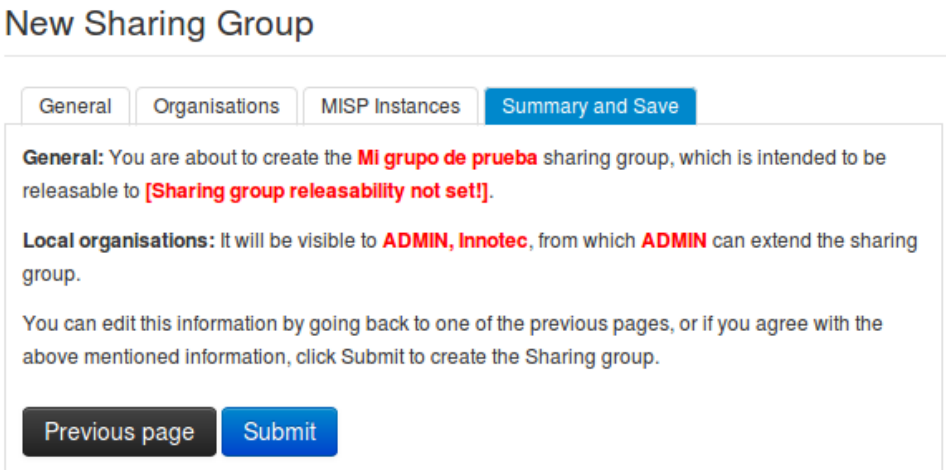


Figura 32. Pestaña summary and save.

2.9 EXPORTACIÓN DE EVENTOS

2.9.1 EXPORTACIÓN AUTOMÁTICA

156. MISP permite la exportación automática de eventos en distintos formatos para lo cual hace falta comunicarse con MISP a través de una conexión HTTPS[23] que presente el certificado digital del usuario y una clave de autenticación, *AUTH KEY,* que tiene definido cada usuario.

157. Este *AUTH KEY* se puede encontrar en el menú *EventsActions ->Automation.* La *AUTH KEY* se añade como una cabecera más en el protocolo HTTPS de forma similar a la siguiente:

```
Authorization: <AUTH KEY>
```

158. Utilizando esta cabecera se pueden descargar los eventos en función de la URI[24] que se utilice.

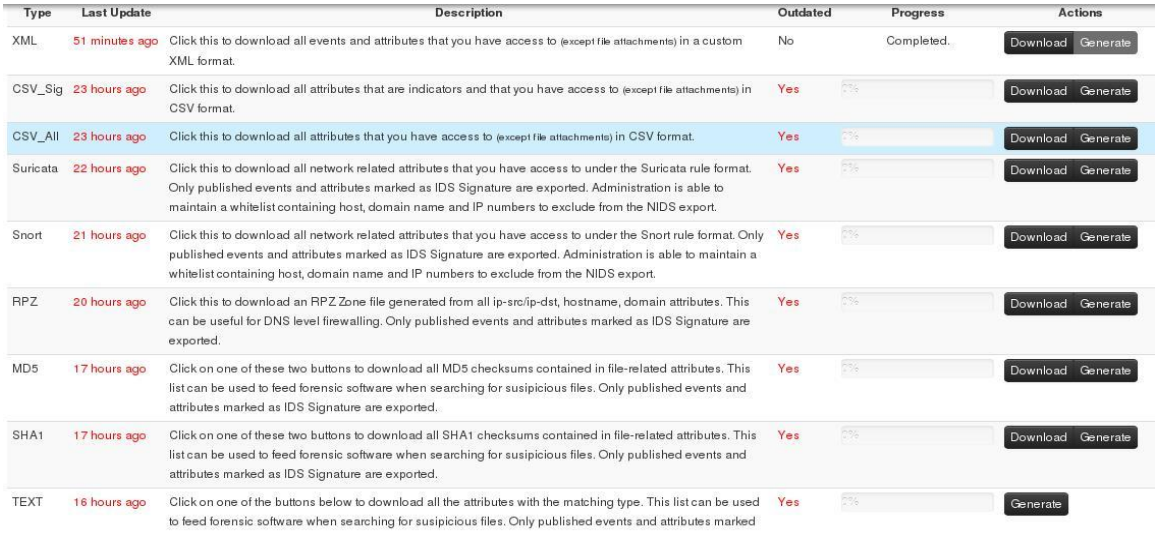
159. MISP ofrece un API REST para la descarga de la información de forma automática. Mediante peticiones HTTPS se puede realizar la descarga de información para su inclusión en fuentes de seguridad. En el Anexo II se detalla el uso de este API.

2.9.2 EXPORTACIÓN MANUAL

160. Se pueden exportar los atributos de MISP en ficheros, a través de la opción *EventsActions ->Export* se muestran las opciones de exportado que se encuentran disponibles. Las opciones que se muestran para exportar son las que aparecen. Si se desea realizar alguna exportación concreta basada en una búsqueda se deberá implementar a través del API como una exportación automática.

[23] Secure HyperText Transfer Protocol

[24] Uniform Resource Identifier



Type	Last Update	Description	Outdated	Progress	Actions
XML	51 minutes ago	Click this to download all events and attributes that you have access to (except file attachments) in a custom XML format.	No	Completed.	Download Generate
CSV_Sig	23 hours ago	Click this to download all attributes that are indicators and that you have access to (except file attachments) in CSV format.	Yes	0%	Download Generate
CSV_All	23 hours ago	Click this to download all attributes that you have access to (except file attachments) in CSV format.	Yes	0%	Download Generate
Suricata	22 hours ago	Click this to download all network related attributes that you have access to under the Suricata rule format. Only published events and attributes marked as IDS Signature are exported. Administration is able to maintain a whitelist containing host, domain name and IP numbers to exclude from the NIDS export.	Yes	0%	Download Generate
Snort	21 hours ago	Click this to download all network related attributes that you have access to under the Snort rule format. Only published events and attributes marked as IDS Signature are exported. Administration is able to maintain a whitelist containing host, domain name and IP numbers to exclude from the NIDS export.	Yes	0%	Download Generate
RPZ	20 hours ago	Click this to download an RPZ Zone file generated from all ip-src/ip-dst, hostname, domain attributes. This can be useful for DNS level firewalling. Only published events and attributes marked as IDS Signature are exported.	Yes	0%	Download Generate
MD5	17 hours ago	Click on one of these two buttons to download all MD5 checksums contained in file-related attributes. This list can be used to feed forensic software when searching for susipicious files. Only published events and attributes marked as IDS Signature are exported.	Yes	0%	Download Generate
SHA1	17 hours ago	Click on one of these two buttons to download all SHA1 checksums contained in file-related attributes. This list can be used to feed forensic software when searching for susipicious files. Only published events and attributes marked as IDS Signature are exported.	Yes	0%	Download Generate
TEXT	16 hours ago	Click on one of the buttons below to download all the attributes with the matching type. This list can be used to feed forensic software when searching for susipicious files. Only published events and attributes marked	Yes	0%	Generate

Figura 33. Vista de exportación de atributos.

161. A continuación se describe cada columna de la tabla:

- ***Type*:** El tipo de datos exportado, como XML, Suricata[25], Snort, MD5, etc.
- ***LastUpdate*:** La fecha de generación del fichero de volcado.
- ***Description*:** Una descripción del volcado.
- ***Outdated*:** Indica si hay eventos nuevos desde la fecha de generación del fichero de volcado. En caso afirmativo se puede hacer clic en Generate para generar un nuevo fichero de volcado.
- ***Progress*:** Indica el progreso de la generación del fichero de volcado.

162. En los botones de abajo se encuentran disponibles distintos tipos de atributos:

Figura 34. Tipos de atributos exportables.

163. Al hacer clic sobre un botón, se exportarán en formato texto todos los valores del atributo indicado. Por ejemplo, si se hace clic sobre el botón *ip-src* se podrán descargar en formato texto todas las direcciones IP origen de todos los eventos. El formato es un atributo por fila. Ver Anexo III Exportación manual.

[25] Las reglas suricata, al igual que las reglas Snort son utilizadas por un motor de detección para comparar los paquetes de datos recibidos y generar las alertas en caso de existir coincidencia.

ANEXO I: CATEGORÍAS DISPONIBLES

164. La siguiente tabla muestra las categorías a las pueden pertenecer los atributos:

Categoría	Descripción
Internal Reference	Identificador de referencia interno utilizado por la organización que aporta la información (por ejemplo, número de identificación de incidente)
Targeting data	Información sobre los objetivos: correo electrónico del destinatario, las máquinas infectadas, departamento, y/o ubicación.
Antivirus detection	Lista de proveedores de antivirus que detectan el malware o información sobre el rendimiento de detección (por ejemplo, 13/43 o 67%). Adjunto con la lista de detección o enlace URL podría ser colocado aquí también.
Payload delivery	Información sobre la forma en que la "carga útil" del código dañino es entregada inicialmente, por ejemplo, información sobre el correo electrónico o página web, la vulnerabilidad utilizada, las direcciones IP origen, etcétera. La muestra del código dañino debería adjuntarse aquí.
Artifacts dropped	Cualquier artefacto (archivos, claves de registro, registros de actividad, herramientas, etcétera) generado por la actividad del código dañino u otras modificaciones al sistema.
Payload installation	Ubicación y mecanismos empleados por el código dañino para colocar la "carga útil" en el sistema comprometido. Por ejemplo, se podría añadir un atributo de tipo filename|md5 como "c:\\windows\\system32\\malicious.exe"|42d8cd98f00b204e9800998ecf8423a
Persistence mechanism	Mecanismos utilizados por el código dañino para iniciarse en el arranque del sistema comprometido. Esto podría ser una clave de registro, modificación llegítima de un driver, archivo de tipo LNK en el arranque del sistema, etcétera.
Network Activity	Información sobre el tráfico de red generado por el código dañino.
Payload activity	Información sobre la "carga útil" final empleada por el código dañino. Puede contener una funcionalidad de ésta, por ejemplo, keylogger, RAT, o un nombre más identificativo de alguna carga útil como las APT's ya conocidas como PoisonIvy o Darkomet, etcétera.
Attribution	Identificación del grupo, organización o país detrás del ataque.
External analysis	Cualquier otro resultado de un análisis adicional del código malicioso, como por ejemplo las salidas de herramientas (salida de analizador de documentos PDF, de entornos de análisis dinámico de código dañino, informes de ingeniería inversa del código dañino, etcétera.)
Financial Fraud	Información relativa a fraude financiero, como cuentas de BitCoin, identificadores bancarios IBAN, BIC o BIN.
Other	Atributos que no son parte de cualquier otra categoría

ANEXO II: EXPORTACIÓN AUTOMÁTICA DE EVENTOS

165. La descarga automática de eventos se realiza mediante peticiones HTTPS, en las que se presenta el certificado del usuario, y que incluyan una cabecera de autenticación del siguiente modo:

Authorization: <AUTH_KEY>

166. La AUTH KEY es única para cada usuario y se puede conocer accediendo a Event Actions -> Automation.

167. A continuación se muestran algunos volcados que se pueden automatizar:

```
https://reyes.ccn-cert.cni.es/attributes/text/download/sha1
https://reyes.ccn-cert.cni.es/attributes/text/download/sha256
https://reyes.ccn-cert.cni.es/attributes/text/download/filename
https://reyes.ccn-cert.cni.es/attributes/text/download/filename|md5
https://reyes.ccn-cert.cni.es/attributes/text/download/filename|sha1
https://reyes.ccn-cert.cni.es/attributes/text/download/filename|sha256
https://reyes.ccn-cert.cni.es/attributes/text/download/ip-src
https://reyes.ccn-cert.cni.es/attributes/text/download/ip-dst
https://reyes.ccn-cert.cni.es/attributes/text/download/hostname
https://reyes.ccn-cert.cni.es/attributes/text/download/domain
https://reyes.ccn-cert.cni.es/attributes/text/download/email-src
https://reyes.ccn-cert.cni.es/attributes/text/download/email-dst
https://reyes.ccn-cert.cni.es/attributes/text/download/email-subject
https://reyes.ccn-cert.cni.es/attributes/text/download/email-attachment
https://reyes.ccn-cert.cni.es/attributes/text/download/url
https://reyes.ccn-cert.cni.es/attributes/text/download/http-method
https://reyes.ccn-cert.cni.es/attributes/text/download/user-agent
https://reyes.ccn-cert.cni.es/attributes/text/download/regkey
https://reyes.ccn-cert.cni.es/attributes/text/download/regkey|value
https://reyes.ccn-cert.cni.es/attributes/text/download/AS
https://reyes.ccn-cert.cni.es/attributes/text/download/snort
https://reyes.ccn-cert.cni.es/attributes/text/download/pattern-in-file
https://reyes.ccn-cert.cni.es/attributes/text/download/pattern-in-traffic
https://reyes.ccn-cert.cni.es/attributes/text/download/pattern-in-memory
https://reyes.ccn-cert.cni.es/attributes/text/download/yara
https://reyes.ccn-cert.cni.es/attributes/text/download/vulnerability
https://reyes.ccn-cert.cni.es/attributes/text/download/attachment
```

Figura 35. Listado de algunos atributos exportables.

1 VOLCADO DE STIX

168. Se puede descargar toda la información de los eventos en formato STIX mediante la siguiente URL:

https://reyes.ccn-cert.cni.es/events/stix/download

169. Es posible descargar algunos eventos únicamente para lo cual se puede utilizar la siguiente URL con los parámetros:

https://reyes.ccn-cert.cni.es/events/stix/download/[id]/[withAttachments]/[tags]/[from]/[to]/[last]

- ***Id*:** El identificador del evento.
- ***WithAttachments*:** Se incluye adjuntos.
- ***Tags*:** Eventos que cumplan con las etiquetas indicadas. Se pueden concatenar varias etiquetas con los operadores '&&' o negar etiquetas con '!'.
- ***From*:** Eventos de una fecha posterior a la indicada.
- ***To*:** Eventos con una fecha anterior a la indicada.
- ***Last*:** Eventos publicados en las últimas horas (12h), minutos (30m) o (5d) días.

2 VOLCADO PARA NIDS

170. Existe la posibilidad de exportar reglas para el IDS que se encuentren etiquetadas con los atributos relacionados con tráfico de red en formato regla de IDS (snort o suricata). Para descargar reglas de IDS se puede acceder a través de Automation y la URL de descarga de reglas de IDS es:

https://reyes.ccn-cert.cni.es/events/nids/suricata/download https://reyes.ccn-cert.cni.es/events/nids/snort/download

171. Debido a que la descarga de todos los eventos va a generar numerosas reglas, se pueden realizar filtros en la URL:

https://reyes.ccn-cert.cni.es/events/nids/[format]/download/[eventid]/[frame]/[tags]/[from]/[to]/[last]

- ***Format*:** Formato de volcado que puede ser 'snort' o 'suricata'.
- ***Eventid*:** Restringe la descarga de un único evento con ese identificador.
- ***Frame*:** Información de contexto de las reglas. Puede ser '*true*' o '*false*'.
- ***Tags*:** Eventos que se encuentren etiquetados con ese nombre de etiqueta. Se puede invertir el resultado con el operador '!' o encadenar varias etiquetas con el operador '&&'.
- ***From*:** Fecha desde la cual buscar eventos.

- ***To*:** Fecha hasta la cual buscar eventos.
- ***Last*:** Últimos X eventos publicados

172. En parámetros opcionales se debe usar '*false*' o '*null*' en la URL. Un ejemplo de URL de descarga de reglas Snort para eventos etiquetados como 'APT28' es el siguiente:

```
https://reyes.ccn-cert.cni.es/events/nids/snort/download/null/true/apt28
```

3 VOLCADO PARA CSV

173. Existe la posibilidad de descargar los atributos de los eventos en formato CSV. Para descargar los atributos en formato CSV se puede acceder a través de Automation y la URL.

```
https://reyes.ccn-cert.cni.es/events/csv/download/[eventid]/[ignore]/[tags]/
[category]/[type]/[includeContext]/[from]/[to]/[last]
```

- ***Eventid*:** Restringe la descarga de un único evento con ese identificador.
- ***Ignore*:** Incluye los atributos que no sean exportables a IDS.
- ***Tags*:** Eventos que se encuentren etiquetados con ese nombre de etiqueta. Se puede invertir el resultado con el operador '!' o encadenar varias etiquetas con el operador '&&'.
- ***Category*:** Categoria del atributo, permite cualquier categoría de atributo valido en MISP.
- ***Type*:** Tipo de atributo, permite cualquier tipo de atributo valido en MISP.
- ***IncludeContext*:** Incluye los datos del evento con cada atributo.
- ***From*:** Fecha desde la cual buscar eventos.
- ***To*:** Fecha hasta la cual buscar eventos.
- ***Last*:** Últimos X eventos publicados

174. A continuación se exponen algunos de los ejemplos más comunes de exportación de atributos a un fichero CSV:

175. Para descargar todos los atributos de eventos con un '*tag*' determinado:

```
https://reyes.ccn-cert.cni.es/events/csv/download/false/[ignore]/Panda
https://reyes.ccn-cert.cni.es/events/csv/download/false/[ignore]/APT=APT29
```

176. Descargar los atributos exportables a IDS de un '*tag*' determinado:

```
https://reyes.ccn-cert.cnicert.cni.es/events/csv/download/false/false/Panda
https://reyes.ccn-cert.cnicert.cni.es/events/csv/download/false/false/APT=APT29
```

177. Descargar los atributos de Hash MD5:

https://reyes.ccn-cert.cni.es/events/hids/md5/download

178. Descargar los atributos de Hash SHA1:

https://reyes.ccn-cert.cni.es/events/hids/sha1/download

179. Descargar los atributos de Hash de un '*Galaxy o un tag*' determinado:

https://reyes.ccn-cert.cni.es/events/hids/md5/download/misp-galaxy:threat-actor="Sofacy"

https://reyes.ccn-cert.cni.es/events/hids/sha1/download/MATI

180. Descargar los atributos de Hash MD5 o SHA1 de 2 '*tags*' determinados:

https://reyes.ccn-cert.cni.es/events/hids/md5/download/MATI&&Panda

181. Descargar reglas de Snort de un '*tag*' determinado:

https://reyes.ccn-cert.cni.es/events/nids/snort/download/false/false/APT=APT29

182. Descargar reglas de Snort de 2 '*tags*' determinados:

https://reyes.ccncert.cni.es/events/nids/snort/download/false/false/APT=APT29 &&CCN-CERT

183. Descargar los atributos de dominio:

https://reyes.ccn-cert.cni.es/events/csv/download/false/false/false/false/domain

184. Descargar los atributos de dominio de un "*tag*" determinado:

https://reyes.ccn-cert.cni.es/events/csv/download/false/false/MATI/Network%20activity/domain

185. Descargar atributos de dominio de 2 "*tags*" determinados:

https://reyes.ccn-cert.cni.es/events/csv/download/false/false/MATI&&Panda/ Network%20activity/domain

186. Descargar atributos con categoría '*Network activity*' de un '*tag*' determinado:

https://reyes.ccn-cert.cni.es/events/csv/download/false/false/APT=APT29/ Network %20activity

187. Descargar atributos con categoría '*Network activity*' de 2 '*tags*' determinados:

https://reyes.ccn-cert.cni.es/events/csv/download/false/false/APT=APT29&& Panda/Network%20activity

ANEXO III: CASOS DE USO: EXPORTACIÓN MANUAL DE EVENTOS

188. Las exportaciones manuales se realizan accediendo a Event actions -> Export.

1 EXPORTACIÓN DE EVENTOS PARA DNS

189. Una lista de dominios RPZ (*Response Policy Zone*) se puede incluir en la configuración de un DNS[26].

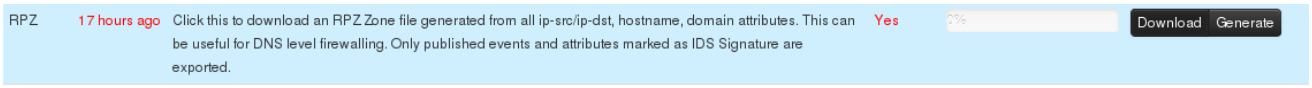


Figura 36. Descarga de una lista de dominios RPZ.

190. Si el fichero indica que está obsoleto (*outdated*) se puede hacer clic en *Generate* para que actualice la lista antes de descargarla.

2 EXPORTACIÓN DE EVENTOS PARA EL CORTAFUEGOS (FIREWALL)

191. Se puede incluir en el cortafuego (*firewall*) una lista de direcciones IP para que sean bloqueadas a partir de todos los eventos publicados en MISP. Para ello se pulsará el botón *ip-src*.

Figura 37. Descarga de una lista de direcciones IP origen.

3 EXPORTACIÓN DE EVENTOS PARA PROXY27

192. Si se desea bloquear tráfico a los dominios que se encuentren en eventos de MISP se puede descargar la lista mediante el botón *domain*.

Figura 38. Descarga de una lista de dominios.

[26] Domain Name System

[27] Es un ordenador que sirve de intermediario entre un navegador web y Internet contribuyendo a la seguridad de la red al filtrar cierto contenido web y programas dañinos.

ANEXO IV: EJEMPLOS DE PETICIONES AUTOMÁTICAS

1 EJEMPLO DE PETICIÓN AUTOMÁTICA REALIZADA EN PYTHON

```
import urllib2, httplib


classHTTPSClientAuthHandler(urllib2.HTTPSHandler):
def __init__(self, key, cert):
urllib2.HTTPSHandler.__init__(self)
self.key = key
self.cert = cert
defhttps_open(self, req):
returnself.do_open(self.getConnection, req)
defgetConnection(self, host, timeout=300):
returnhttplib.HTTPSConnection(host, key_file=self.key, cert_file=self.cert)


opener = urllib2.build_opener(HTTPSClientAuthHandler('<certificado.key>',
'<certificado.crt>') )
opener.addheaders = [('Authorization','<API_KEY>')]
response = opener.open("https://reyes.ccn-
cert.cni.es/events/nids/snort/download/false/false/Ransomware ")
printresponse.read()
```

2 EJEMPLO DE PETICIÓN AUTOMÁTICA REALIZADA EN JAVA

```
import java.io.*;
import java.net.*;
importjavax.net.ssl.*;
importjava.security.SecureRandom;
import java.security.cert.X509Certificate;


public class ReyesLoader {


public static String getHTML(String urlToRead) throws Exception {
StringBuilder result = new StringBuilder();
    URL url = new URL(urlToRead);
```

```
HttpsURLConnection conn = (HttpsURLConnection) url.openConnection();
conn.setRequestMethod("GET");

SSLSocketFactorysslsocketfactory = (SSLSocketFactory) SSLSocketFactory.getDefault();
conn.setSSLSocketFactory(sslsocketfactory);
conn.setRequestProperty ("Authorization", "<api-key>");

BufferedReaderrd = new BufferedReader(new
InputStreamReader(conn.getInputStream()));
    String line;
while ((line = rd.readLine()) != null) {
result.append(line);
    }
rd.close();
returnresult.toString();
  }

public static void main(String[] args) throws Exception
  {
System.out.println(getHTML("https://reyes.ccn-
cert.cni.es/events/nids/snort/download/false/false/Ransomware"));
}
}
```

3 EJEMPLO DE PETICIÓN AUTOMÁTICA REALIZADA MEDIANTE CURL

```
curl -H " Authorization: <api-key>" -H \"Accept: application/xml\" -H \"Content-Type:
text/xml\" https://reyes.ccn-
cert.cni.es/events/nids/snort/download/false/false/Ransomware”
```

ANEXO V: INTEGRACIÓN DE MISP CON DNS BIND

193. En este anexo se explica cómo integrar la información de seguridad de MISP con un servidor DNS, en concreto BIND. La información útil que se puede extraer de MISP para cualquier servidor DNS es una lista de dominios y direcciones IP en un fichero de configuración de zona RPZ (response policy zone). Mediante RPZ se define una resolución personalizada de la lista de dominios insertada, como por ejemplo que el dominio no existe (*NXDOMAIN*) o que se modifique la dirección IP a la que resuelve mediante *CNAME*, y también se definen direcciones IP que serán bloqueadas si llegan como respuesta de alguna petición DNS.

194. MISP ofrece un volcado de un fichero de configuración de zona RPZ. Este fichero se puede obtener mediante la siguiente URL utilizando uno de los ejemplos de automatización del Anexo IV. La URL a utilizar es la siguiente:

```
https://reyes.ccn-cert.cni.es/events/downloadExport/rpz
```

195. El fichero de zona RPZ empieza del siguiente modo:

```
$TTL 1w;
@ SOA localhost. root.localhost (2015121500 2h 30m 30d 1h) NS localhost.
; The following list of IP addresses will timeout.
32.0.0.0.0.rpz-ip CNAME rpz-drop.
32.4.5.1.1.rpz-ip CNAME rpz-drop.
```

196. Una vez descargado el fichero de zona RPZ hay que añadirlo a la configuración de BIND. Se deberá añadir un fichero (por ejemplo rpz.zone) con el siguiente contenido:

```
zone "rpz.zone" {
  type master;
file "/etc/bind/db.rpz.zone";
allow-query {none;};
};
```

197. Con esta configuración hay que renombrar el fichero descargado desde MISP a ‘db.rpz.zone’ e incluirlo en la ruta indicada en el parámetro file.

198. Dentro del bloque de ‘options’ añadir la siguiente línea:

```
response-policy { zone "rpz.zone"; };
```

199. Y añadir la siguiente línea dentro del fichero de configuración:

```
include "/etc/bind/rpz.zone";
```

200. Y por último reiniciar BIND para aplicar los cambios.

ANEXO VI: GUIDELINES

1 DIRECTRICES

201. El propósito de estas secciones es proporcionar unas directrices sobre el intercambio de información dentro de la comunidad MISP, una visión general sobre la mejor forma de contribuir a la herramienta, qué información debe agregarse, cómo deben estructurarse los datos, cómo manejar y compartir información propia o la recibida a través de MISP.

202. Aunque estas directrices pueden variar, intente seguirlas a la hora de agregar información en MISP.

2 PARTICIPACIÓN ACTIVA

203. Uno de los principios básicos de MISP es el intercambio de información, es por eso que se pide a todos los participantes que contribuyan tanto como sea posible.

204. Todas las acciones, como crear un evento, agregar atributos o proponer cambios, son contribuciones muy valiosas y nos ayudan a detectar y entender mejor las campañas de ataques y malware.

2.1 PRIORIZAR LA CALIDAD A LA CANTIDAD

205. Cuanto mayor sea la calidad de la información, mayor será el beneficio para toda la comunidad, es por eso que recomendamos filtrar y revisar la información antes de compartirla en MISP.

3 PUBLICAR INFORMACIÓN

206. Esto no es una lista exhaustiva, pero dará a los contribuyentes algunas orientaciones sobre qué datos deben ser publicados en MISP:

- Malware y grupos APT (infraestructura C&C, dropzone, dispositivos afectados, etc...)
- Indicadores de compromiso relacionados con investigaciones e incidentes de seguridad
- Indicadores de compromiso relacionados con malware y código dañino
- Vulnerabilidades día cero (0-day) en software de terceros
- Información sobre redes bots, servidores de mando y control y direcciones IP
- Malware y patrones de ataques sobre sistemas SCADA[28]/ICS[29]
- Vulnerabilidades de aplicaciones web, exploits 0-day, etc…

[28] Supervisory Control and Data Acquisition
[29] Industrial Control System. Sistema de control industrial

- Los informes OSINT también se pueden agregar a MISP después de una cuidadosa selección.

207. Los siguientes datos no deben ser compartidos a través de MISP:

- Información relacionada con fraude bancario.
- Información relacionada con fraude a compañías aéreas o de alquiler de vehículos.
- Nombres o información sobre las víctimas.

4 ESTRUCTURA DE LA INFORMACIÓN

4.1 EVENTOS

208. La entidad que añada los datos debe establecer una distribución correcta.

4.2 FECHA

209. Define la fecha de detección, no la fecha en que se agregó a MISP.

4.3 EL NIVEL DE AMENAZA DEBE ESTABLECERSE DE LA SIGUIENTE MANERA:

- **Alta**: APTs sofisticados o Zero-days
- **Medio**: Amenazas avanzadas persistentes (APT).
- **Bajo**: Códigos dañinos (Malware) común.
- **Undefined**: Familia de malware desconocida o no definida.

4.4 TAXONOMÍAS O ETIQUETAS ESTRUCTURADAS

210. Se recomienda utilizar taxonomías o etiquetas estructuradas en vez de etiquetas simples de texto. Las taxonomías sólo deben ser usadas para describir datos y no como una marca de nivel de clasificación de información.

211. Para etiquetar eventos dentro de MISP, NCIRC utiliza las siguientes taxonomías:

Dominio		Taxonomía
Actor	name	misp-galaxy:threat-actor:*
	type	customtags: APT APT=Sofacy veris:actor:motive veris:actor:motive="Espionage" veris:actor:motive="Financial"

Malware	name	misp-galaxy:tool:*
	type	veris:action: veris;action;malware;variety="Ransomware" veris:action:malware:variety="Spyware/Keylogger" veris:action:social:variety="Phishing" veris:action:social:variety="Spam"
Releasability		tlp:* tlp:green TLP:AMBER NATO
Source		custom tags: CERT-EU, CIMBL, ThreatConnect, CERT-EU osint:* osint:source-type="blog-post" osint:source-type="expansion" osint:source-type="mailing-list" osint:source-type="technical-report"
Confidencelevel		admiralty-scale:information-credibility 1 = veryhigh 2, 3, 4 = high/medium/low = improbable = cannot be judged admiralty-scale;information-credibility="1" admiralty-scale;information-credibility="3" admiralty-scale;information-credibility="5" admiralty-scale;information-credibility="6"

4.5 ATRIBUTOS:

212. La mayoría de los atributos son fáciles de usar, pero los siguientes requieren un uso más estricto para asegurar un enfoque estandarizado y común:

Tipo	Formato
hostname	(prefix)+.domain – prefix, one or more times dot domain
domain	name.tld
url	scheme://prefix.domain:port/path/filename
link	

5 DISTRIBUCIÓN DE LA INFORMACIÓN:

5.1 NIVEL DE CLASIFICACIÓN PREDETERMINADA:

213. A menos que se indique lo contrario, toda la información debe considerarse como TLP: Amber.[30]

5.2 COMPARTIR INFORMACIÓN PROPIA:

214. Cada contribuyente debe compartir su propia información como mejor le parezca, teniendo en cuenta las políticas de seguridad. Hay que tener en cuenta que no compartir información permite al atacante continuar con su actividad.

5.3 COMPARTIR LA INFORMACIÓN RECIBIDA DE LA OTAN A TRAVÉS DE MISP:

Distribución	Compartir
NATO Alliance	OTAN más los organismos gubernamentales de los países miembros de la OTAN (nivel compartido por defecto de los datos del NCIRC)
NATO Partners	Todos los anteriores más los socios de la OTAN
NATO IPA	Todos los grupos anteriores y los miembros del Acuerdo de Asociación Industrial de la OTAN
Industry	Todas las organizaciones arriba mencionadas y las organizaciones que participan en el NATO Industry Cyber Partnership (NICP)
Community	Todas las organizaciones que pertenezcan a la comunidad
Organization	Todos los usuarios que pertenezcan a la organización
All	Todas las entidades de miembros de la OTAN o no pertenecientes a la OTAN

5.4 OTRAS MARCAS:

215. Cada entidad que tenga acceso a la OTAN y agregue datos al MISP debe hacerlo basándose en su fiabilidad (etiqueta TLP).

216. También deben tomarse medidas apropiadas para su custodia.

[30] Traffic Ligth Protocol. Protocolo de luces de semáforo que fue creado para fomentar el intercambio de información sensible (no clasificada) en el ámbito de la ciberseguridad

ANEXO VII: BINARIO

217. El cliente de escritorio (Binario) permite interactuar de una forma cómoda y sencilla con la API de Reyes.

218. Una vez enviado el correo para obtener el cliente de escritorio a la cuenta de reyes, hay que obtener el token.

219. Con el cliente personalizado de reyes (reyes.jar) y el token se puede acceder a la ayuda desde la línea de comandos, la cual mostrará una lista con todas las acciones que se pueden realizar.

```
java1.8 -jar reyes.jar -t "TOKEN" -h
usage: reyes [-and | -or] [-application <arg>] [-b] [-d <arg>] [-domain
       <arg>] [-gene <arg>] [-h] [-hash <arg>] [-ip <arg>] [-o <PATH>]
       [-r] -t <arg> [-v]
Interface por linea de comandos para Reyes

 -and                  Operacion AND
 -application <arg>    Aplicacion donde buscar
 -b,--blacklist        Descargar listas negras
 -d,--download <arg>   Descargar recurso ej:
                       /reyes/content/download-content?id-search=1&content
                       -type=downloadableIndicator&type=rpz&value=misp.rpz
                       .event-1.txt
 -domain <arg>         Busqueda por Dominio
 -gene <arg>           Busqueda por generico
 -h,--help             Mensaje de ayuda
 -hash <arg>           Busqueda por Hash
 -ip <arg>             Busqueda por IP
 -o,--output <PATH>    Ruta de destino para guardar el resultado de la
                       peticion
 -or                   Operacion OR
 -r,--rule             Descargar reglas
 -t,--token <arg>      Token del usuario
 -v,--version          Version de la aplicacion
```

220. Las peticiones que se realicen a partir del binario devolverán los resultados en formato Json, a excepción de las listas negras y reglas Snort que las devuelve en formato de texto.

221. En la siguiente imagen se muestra la petición al binario y una muestra de las reglas snort descargadas:

```
java1.8 -jar reyes.jar -t "TOKEN" -r

alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"cerber HTTP rawentyrinity.top"; flow:to_server,established;
content:"rawentyrinity.top"; nocase; http_header; pcre:"/(Host\:)(\s[a-zA-Z0-9.-]+\.|\s)(rawentyrinity.top)\r\n/iH"; classtype:trojan-
activity; sid:1702003232; rev:1;)
alert udp $HOME_NET any -> $EXTERNAL_NET 53 (msg:"cerber DNS rawentyrinity.top"; byte_test:1,!&,64,2; byte_test:1,!&,32,2; byte_test:1,!
&,16,2; byte_test:1,!&,8,2; content:"|0D|rawentyrinity|03|top|00|"; classtype:trojan-activity; sid:1702003233; rev:1;)
alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"cerber HTTP rawentyrinity.top/search.php"; flow:to_server,established; uricontent:"/
search.php"; nocase; content:"rawentyrinity.top"; nocase; http_header; classtype:trojan-activity; sid:1702003234; rev:1;)
alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"satan HTTP dxrhy6anghkdt6th.onion.lu"; flow:to_server,established;
content:"dxrhy6anghkdt6th.onion.lu"; nocase; http_header; pcre:"/(Host\:)(\s[a-zA-Z0-9.-]+\.|\s)(dxrhy6anghkdt6th.onion.lu)\r\n/iH";
classtype:trojan-activity; sid:1702003235; rev:1;)
alert udp $HOME_NET any -> $EXTERNAL_NET 53 (msg:"satan DNS dxrhy6anghkdt6th.onion.lu"; byte_test:1,!&,64,2; byte_test:1,!&,32,2;
byte_test:1,!&,16,2; byte_test:1,!&,8,2; content:"|10|dxrhy6anghkdt6th|05|onion|02|lu|00|"; classtype:trojan-activity; sid:1702003236;
rev:1;)
alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"satan HTTP ejmv6pxsuwqrofa3.onion.to"; flow:to_server,established;
content:"ejmv6pxsuwqrofa3.onion.to"; nocase; http_header; pcre:"/(Host\:)(\s[a-zA-Z0-9.-]+\.|\s)(ejmv6pxsuwqrofa3.onion.to)\r\n/iH";
classtype:trojan-activity; sid:1702003237; rev:1;)
alert udp $HOME_NET any -> $EXTERNAL_NET 53 (msg:"satan DNS ejmv6pxsuwqrofa3.onion.to"; byte_test:1,!&,64,2; byte_test:1,!&,32,2;
byte_test:1,!&,16,2; byte_test:1,!&,8,2; content:"|10|ejmv6pxsuwqrofa3|05|onion|02|to|00|"; classtype:trojan-activity; sid:1702003238;
rev:1;)
alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"satan HTTP ij63zawstx4mpyfq.onion.link"; flow:to_server,established;
content:"ij63zawstx4mpyfq.onion.link"; nocase; http_header; pcre:"/(Host\:)(\s[a-zA-Z0-9.-]+\.|\s)(ij63zawstx4mpyfq.onion.link)\r\n/iH";
classtype:trojan-activity; sid:1702003239; rev:1;)
alert udp $HOME_NET any -> $EXTERNAL_NET 53 (msg:"satan DNS ij63zawstx4mpyfq.onion.link"; byte_test:1,!&,64,2; byte_test:1,!&,32,2;
byte_test:1,!&,16,2; byte_test:1,!&,8,2; content:"|10|ij63zawstx4mpyfq|05|onion|04|link|00|"; classtype:trojan-activity; sid:1702003240;
rev:1;)
```

222. En la siguiente imagen se muestra la petición y los ficheros de listas negras descargados:

```
java1.8 -jar reyes.jar -t "TOKEN" -b
```

apt.txt apt_ip.txt apt_rpz_bind.txt botnet.txt botnet_ip.txt malware.txt malware_ip.txt

ransomware.txt spam.txt tor.txt

223. La siguiente imagen muestra la petición de búsqueda de una dirección IP.

```
java1.8 -jar reyes.jar -t "TOKEN" -ip  176.56.62.143
Start
..
FINALIZADO
```

224. Entre las peticiones que se pueden hacer al binario se encuentra la opción recursos (-d), la cual permite descargar las reglas RPZ, IOC y SNORT a partir del Json que devuelve la búsqueda de direcciones ip y dominios.

225.

226. Una vez descargado el Json con la dirección IP, se cogen las siguientes direcciones para descargar los archivos con las reglas.


```
type=downloadableIndicator&type=rpz&value=misp.rpz.event-39273.txt\"}","date":null,"type":"rpz","name":"M2M -  Locky 2017-09-11/11 :
Affid=3, \".lukitus\" : \"Bankwest - You have a new eStatement\" - /statement.html links","value":"misp.rpz.event-39273.txt","url":"/reyes/
content/download-content?id-search=26987&content-type=downloadableIndicator&type=rpz&value=misp.rpz.event-39273.txt"},{"searchOperand":
{"term":"176.56.62.143"},"appInfo":"{\"eventId\":\"39273\",\"eventName\":\"M2M -  Locky 2017-09-11/11 : Affid=3, \\\".lukitus\\\" : \\
\"Bankwest - You have a new eStatement\\\" - /statement.html links\",\"eventUrl\":\"/misp/events/view/39273\",\"url\":\"/reyes/content/
download-content?id-search=26987&content-type=downloadableIndicator&type=ioc&value=misp.openIOC39273.ioc
\"}","date":null,"type":"ioc","name":"M2M -  Locky 2017-09-11/11 : Affid=3, \".lukitus\" : \"Bankwest - You have a new eStatement\" - /
statement.html links","value":"misp.openIOC39273.ioc","url":"/reyes/content/download-content?id-search=26987&content-
type=downloadableIndicator&type=ioc&value=misp.openIOC39273.ioc"},{"searchOperand":{"term":"176.56.62.143"},"appInfo":"{\"eventId\":\"39273
\",\"eventName\":\"M2M -  Locky 2017-09-11/11 : Affid=3, \\\".lukitus\\\" : \\\"Bankwest - You have a new eStatement\\\" - /statement.html
links\",\"eventUrl\":\"/misp/events/view/39273\",\"url\":\"/reyes/content/download-content?id-search=26987&content-
type=downloadableIndicator&type=ids&value=misp.snort.event39273.rules\"}","date":null,"type":"ids","name":"M2M -  Locky 2017-09-11/11 :
Affid=3, \".lukitus\" : \"Bankwest - You have a new eStatement\" - /statement.html links","value":"misp.snort.event39273.rules","url":"/
reyes/content/download-content?id-search=26987&content-type=downloadableIndicator&type=ids&value=misp.snort.event39273.rules"}],"blacklists"
```



```
type=downloadableIndicator&type=rpz&value=misp.rpz.event-39273.txt\"}","date":null,"type":"rpz","name":"M2M -  Locky 2017-09-11/11 :
Affid=3, \".lukitus\" : \"Bankwest - You have a new eStatement\" - /statement.html links","value":"misp.rpz.event-39273.txt","url":"/reyes/
content/download-content?id-search=26987&content-type=downloadableIndicator&type=rpz&value=misp.rpz.event-39273.txt"},{"searchOperand":
{"term":"176.56.62.143"},"appInfo":"{\"eventId\":\"39273\",\"eventName\":\"M2M -  Locky 2017-09-11/11 : Affid=3, \\\".lukitus\\\" : \\
\"Bankwest - You have a new eStatement\\\" - /statement.html links\",\"eventUrl\":\"/misp/events/view/39273\",\"url\":\"/reyes/content/
download-content?id-search=26987&content-type=downloadableIndicator&type=ioc&value=misp.openIOC39273.ioc
\"}","date":null,"type":"ioc","name":"M2M -  Locky 2017-09-11/11 : Affid=3, \".lukitus\" : \"Bankwest - You have a new eStatement\" - /
statement.html links","value":"misp.openIOC39273.ioc","url":"/reyes/content/download-content?id-search=26987&content-
type=downloadableIndicator&type=ioc&value=misp.openIOC39273.ioc"},{"searchOperand":{"term":"176.56.62.143"},"appInfo":"{\"eventId\":\"39273
\",\"eventName\":\"M2M -  Locky 2017-09-11/11 : Affid=3, \\\".lukitus\\\" : \\\"Bankwest - You have a new eStatement\\\" - /statement.html
links\",\"eventUrl\":\"/misp/events/view/39273\",\"url\":\"/reyes/content/download-content?id-search=26987&content-
type=downloadableIndicator&type=ids&value=misp.snort.event39273.rules\"}","date":null,"type":"ids","name":"M2M -  Locky 2017-09-11/11 :
Affid=3, \".lukitus\" : \"Bankwest - You have a new eStatement\" - /statement.html links","value":"misp.snort.event39273.rules","url":"/
reyes/content/download-content?id-search=26987&content-type=downloadableIndicator&type=ids&value=misp.snort.event39273.rules"}],"blacklists"
```


227. Dado el ejemplo anterior, las consultas para la descarga de los archivos con las reglas serían las siguientes:

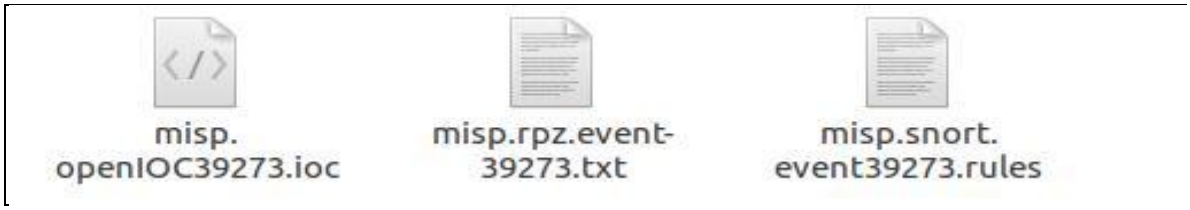
```
java1.8 -jar reyes.jar -t "TOKEN" -d "/reyes/content/download-content?id-search=26987&content-
type=downloadableIndicator&type=rpz&value=misp.rpz.event-39273.txt"


java1.8 -jar reyes.jar -t "TOKEN" -d "/reyes/content/download-content?id-search=26987&content-
type=downloadableIndicator&type=ioc&value=misp.openIOC39273.ioc"


java1.8 -jar reyes.jar -t "TOKEN" -d "/reyes/content/download-content?id-search=26987&content-
type=downloadableIndicator&type=ids&value=misp.snort.event39273.rules"
```

228. **Importante:** Es necesario entrecomillar la petición como se muestra en el ejemplo.

229. A continuación, se muestran los 3 archivos obtenidos tras las consultas:



230. El contenido del archivo para las reglas RPZ:

```
$TTL 1w;
@               SOA localhost. root.localhost (2017092100 2h 30m 30d 1h)
                NS localhost.

; The following hostnames will timeout.
420ent.com CNAME rpz-drop.
afilhadaemmocambique.com CNAME rpz-drop.
beepop.info CNAME rpz-drop.
bellevuecommunityband.org CNAME rpz-drop.
bingleybuilder.co.uk CNAME rpz-drop.
cedricanimation.com CNAME rpz-drop.
chimachinenow.com CNAME rpz-drop.
comtechadsl.com CNAME rpz-drop.
conectivaconsultores.com CNAME rpz-drop.
crystalballcruise.com CNAME rpz-drop.
cutwell.ca CNAME rpz-drop.
dbatee.gr CNAME rpz-drop.
duaneandirisblue.com CNAME rpz-drop.
e-chards.com CNAME rpz-drop.
envi-herzog.de CNAME rpz-drop.
ericweb.co.za CNAME rpz-drop.
eternallyclassicjewelry.com CNAME rpz-drop.
excel-conduite.com CNAME rpz-drop.
expresspermis.com CNAME rpz-drop.
fexx.co.uk CNAME rpz-drop.
fiore-web.it CNAME rpz-drop.
hostprodirect.com CNAME rpz-drop.
irmak.web.tr CNAME rpz-drop.
jenyeong.com CNAME rpz-drop.
lakeroadlavender.com CNAME rpz-drop.
linksoft.co.nz CNAME rpz-drop.
matern-eger.de CNAME rpz-drop.
```

231. El contenido del archivo para las reglas IOC:

```
-<ioc id="59b7cd9e-57e4-42c6-b1ce-440d950d210f" last-modified="2017-09-12T00:00:00">
   <short_description>Event #39273</short_description>
  -<description>
     M2M - Locky 2017-09-11/11 : Affid=3, ".lukitus" : "Bankwest - You have a new eStatement" - /statement.html links (59b7cd9e-57e4-42c6-
     b1ce-440d950d210f)
   </description>
   <keywords/>
   <authored_by>CIRCL_1373</authored_by>
   <authored_date>2017-09-12T00:00:00</authored_date>
   <links/>
  -<definition>
   -<Indicator operator="OR" id="59c37c52-31b8-43d9-ba55-38a40a646538">
    -<IndicatorItem id="59b7cd9f-981c-4c2c-8b53-46fb950d210f" condition="is">
       <Context document="FileItem" search="FileItem/Md5sum" type="mir"/>
       <Content type="md5">2518037ef7d7524a631c4bf9086428f8</Content>
     </IndicatorItem>
    -<IndicatorItem id="59b7cd9f-56d4-428f-b365-4303950d210f" condition="is">
       <Context document="FileItem" search="FileItem/Md5sum" type="mir"/>
       <Content type="md5">230606dd8b0d62e2a8a04ef61b2d8707</Content>
     </IndicatorItem>
    -<IndicatorItem id="59b7cda0-8008-44f0-8882-02fa950d210f" condition="is">
       <Context document="RouteEntryItem" search="RouteEntryItem/Destination" type="mir"/>
       <Content type="string">420ent.com</Content>
```

232. El contenido del archivo para las reglas SNORT:

```
#This part might still contain bugs, use and your own risk and report any issues.
#
# MISP export of IDS rules - optimized for snort
#
# These NIDS rules contain some variables that need to exist in your configuration.
# Make sure you have set:
#
# $HOME_NET      - Your internal network range
# $EXTERNAL_NET - The network considered as outside
# $SMTP_SERVERS - All your internal SMTP servers
# $HTTP_PORTS   - The ports used to contain HTTP traffic (not required with suricata export)
#
alert udp any any -> any 53 (msg: "REYES e39273 Hostname: 420ent.com"; content:"|01 00 00 01 00 00 00 00 00 00|"; depth:10; offset:2;
content:"|00||06|420ent|03|com|00|"; fast_pattern; nocase;  classtype:trojan-activity; sid:18482541; rev:1; priority:3;
reference:url,https://misp.ccn-cert.cni.es/events/view/39273;)
alert tcp any any -> any 53 (msg: "REYES e39273 Hostname: 420ent.com"; content:"|01 00 00 01 00 00 00 00 00 00|"; depth:10; offset:2;
content:"|00||06|420ent|03|com|00|"; fast_pattern; nocase; flow:established;  classtype:trojan-activity; sid:18482542; rev:1; priority:3;
reference:url,https://misp.ccn-cert.cni.es/events/view/39273;)
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg: "REYES e39273 Outgoing HTTP Hostname: 420ent.com"; flow:to_server,established;
content: "Host|3a| 420ent.com"; nocase; http_header; pcre: "/(^|[^A-Za-z0-9-\.])420ent\.com[^A-Za-z0-9-\.]/H"; tag:session,600,seconds;
classtype:trojan-activity; sid:18482543; rev:1; priority:3; reference:url,https://misp.ccn-cert.cni.es/events/view/39273;)
alert udp any any -> any 53 (msg: "REYES e39273 Hostname: afilhadaemmocambique.com"; content:"|01 00 00 01 00 00 00 00 00 00|"; depth:10;
offset:2; content:"|00||14|afilhadaemmocambique|03|com|00|"; fast_pattern; nocase;  classtype:trojan-activity; sid:18482551; rev:1;
priority:3; reference:url,https://misp.ccn-cert.cni.es/events/view/39273;)
alert tcp any any -> any 53 (msg: "REYES e39273 Hostname: afilhadaemmocambique.com"; content:"|01 00 00 01 00 00 00 00 00 00|"; depth:10;
offset:2; content:"|00||14|afilhadaemmocambique|03|com|00|"; fast_pattern; nocase; flow:established;  classtype:trojan-activity;
sid:18482552; rev:1; priority:3; reference:url,https://misp.ccn-cert.cni.es/events/view/39273;)
```