Eventos MISP

Manual de creación de eventos en la plataforma MISP

00- Doble factor de autenticación para cuenta MISP

Para fortalecer la seguridad de su cuenta en la plataforma, se debe habilitar la autenticación de dos factores debido a la información que se encuentra en la plataforma.

A continuación, se detallan los pasos para activar esta función en su perfil de usuario:

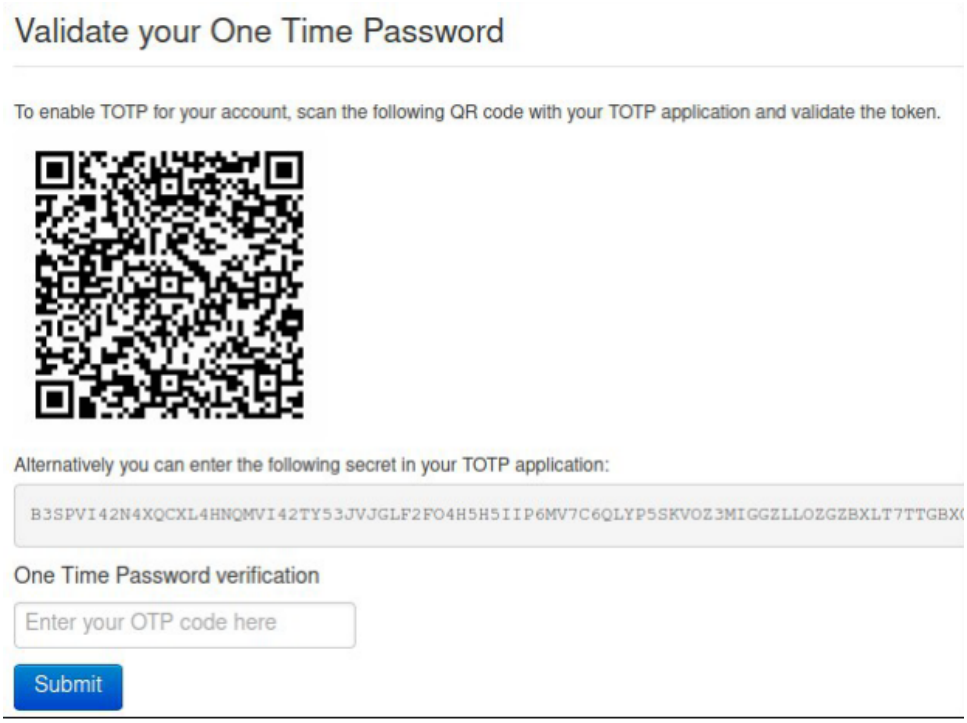
Acceda a su perfil de usuario:

- Inicie sesión en su instancia de MISP.
- Haga clic en “Admin” ubicado en la esquina superior derecha.

Habilite TOTP.

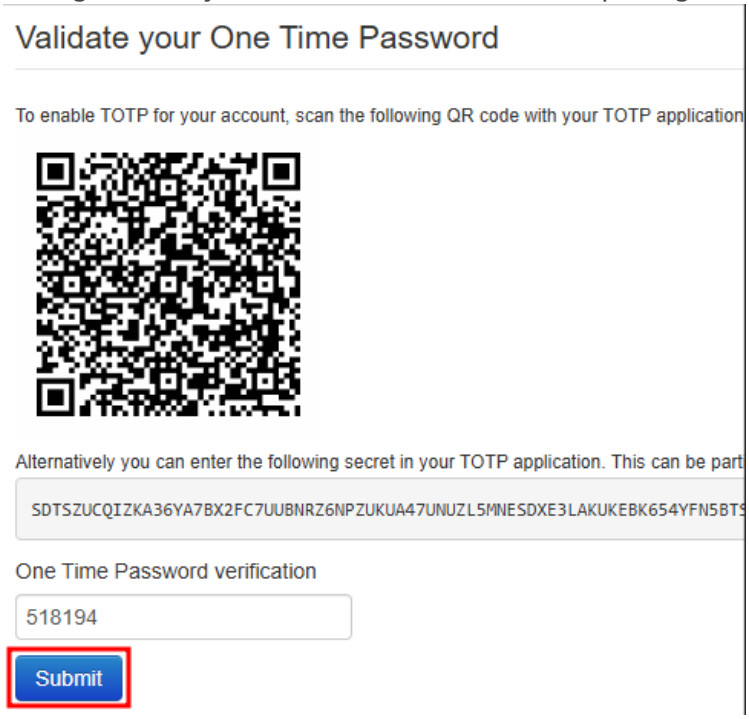
- En la sección de su perfil, busque la opción para habilitar TOTP.

- En la sección de su perfil, busque la opción para habilitar TOTP.



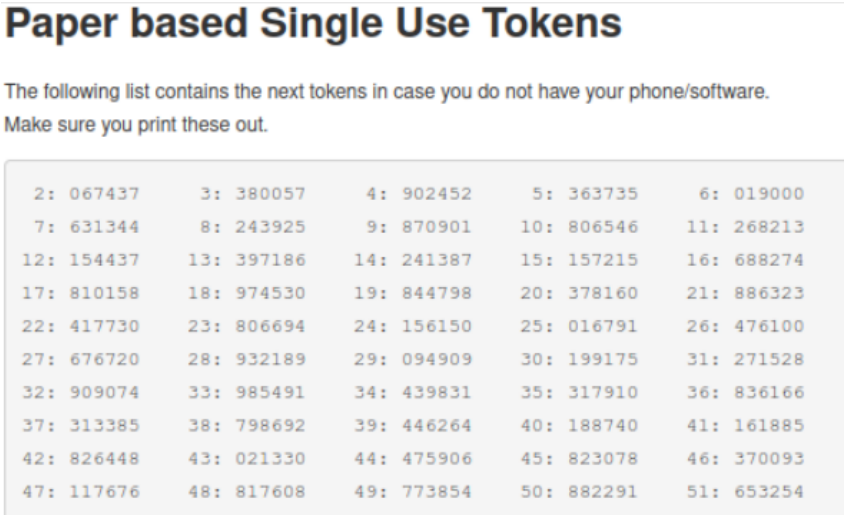
Configure la aplicación de autenticación:

- Utilice una aplicación de autenticación compatible con TOTP, como Google Authenticator, Microsoft Authenticator o Authy.
- Abra la aplicación en su dispositivo móvil.
- Seleccione la opción para agregar una nueva cuenta y escanee el código QR proporcionado por MISP.
- Después de escanear el código QR, la aplicación generará códigos temporales de seis dígitos.
- Ingrese uno de estos códigos en el campo de verificación en MISP para confirmar la configuración y de click al botón "Submit" para guardar.



Guarde sus códigos de recuperación (HOTP):

- Una vez verificado el TOTP, MISP le proporcionará una lista de códigos de un solo uso (HOTP) que puede utilizar en caso de no tener acceso a su dispositivo móvil.
- Guarde los códigos en un lugar seguro, ya que serán esenciales para acceder a su cuenta si pierde el acceso a la aplicación de autenticación.
- A partir de ahora, al iniciar sesión, después de ingresar su nombre de usuario y contraseña, se le solicitará un código TOTP generado por su aplicación de autenticación.



Paper based Single Use Tokens

The following list contains the next tokens in case you do not have your phone/software.
Make sure you print these out.

2: 067437	3: 380057	4: 902452	5: 363735	6: 019000
7: 631344	8: 243925	9: 870901	10: 806546	11: 268213
12: 154437	13: 397186	14: 241387	15: 157215	16: 688274
17: 810158	18: 974530	19: 844798	20: 378160	21: 886323
22: 417730	23: 806694	24: 156150	25: 016791	26: 476100
27: 676720	28: 932189	29: 094909	30: 199175	31: 271528
32: 909074	33: 985491	34: 439831	35: 317910	36: 836166
37: 313385	38: 798692	39: 446264	40: 188740	41: 161885
42: 826448	43: 021330	44: 475906	45: 823078	46: 370093
47: 117676	48: 817608	49: 773854	50: 882291	51: 653254

01- Distribución de phishing evento MISP

Introducción

MISP es una herramienta de código abierto diseñada para facilitar el intercambio de información sobre amenazas cibernéticas, permitiendo a los usuarios compartir indicadores de compromiso (IOC's), análisis de malware y otros datos relevantes de seguridad.

Esta guía te ayudará a utilizar la plataforma MISP (Malware Information Sharing Platform & Threat Sharing) para crear y distribuir eventos de manera eficiente y completa. Tenemos como finalidad proporcionar un paso a paso detallado para crear, configurar y publicar eventos en MISP, tomando distintos ejemplos. Su objetivo es estandarizar el proceso de documentación y compartir inteligencia sobre amenazas de manera eficiente, asegurando que los usuarios de la plataforma puedan aprovechar la información para fortalecer sus defensas y prevenir incidentes similares.

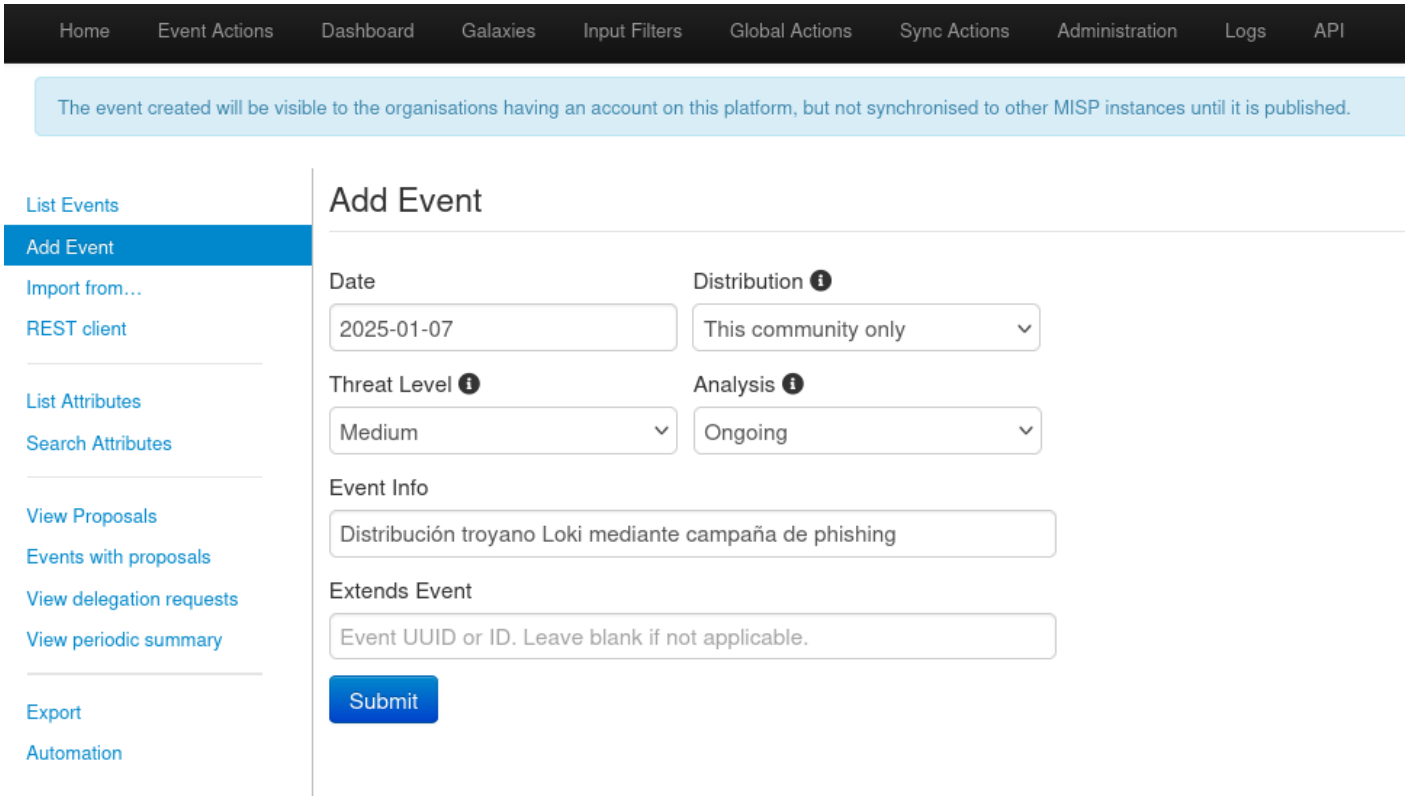
Contexto

El Centro de Gestión de Incidentes Informáticos ha identificado una campaña de phishing masiva que distribuye malware a través de adjuntos en correos electrónicos.

Los pasos para publicar el evento en MISP pueden variar según la información disponible, pero en este ejemplo se detallarán los indicadores de compromiso (IOCs) más comunes asociados a correos de phishing. En casos específicos, es posible que no se encuentren todos los datos mencionados, por lo que solo se debe incluir información verificada.

CREACIÓN DEL EVENTO.

- Ingresar a la sección de **Events** posteriormente **Event Actions** y por último seleccionar **Add event**.



- **Distribution.**
  Define el alcance de visibilidad del evento.
- **Threat level.**
  Define el nivel de amenaza del evento.
- **Analysis.**
  Define el evento en Inicial,Ongoing (en curso) o finalizado.
- **Event info.**
  Incluir el resumen de una descripción del evento.
- **Extends Event.**
  Si el evento está relacionado con uno previo, agregar el UUID correspondiente para vincularlos.

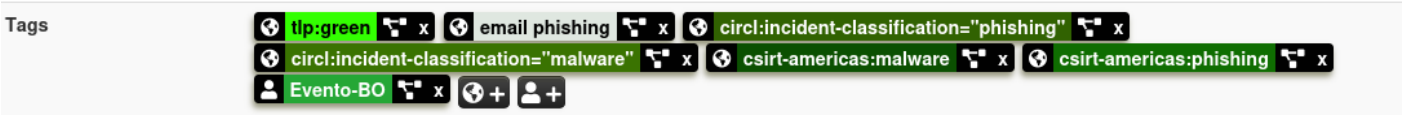
ASIGNACIÓN DE TAGS

El uso de tags nos ayuda en gran medida a contextualizar y enriquecer la información compartida. Estas etiquetas no solo facilitan la categorización y búsqueda eficiente de eventos también permiten establecer relaciones claras entre incidentes, amenazas y campañas maliciosas.

Al incorporar tags descriptivos, los usuarios de la plataforma pueden priorizar, filtrar y correlacionar datos con mayor precisión, mejorando así la respuesta ante ciberamenazas entre la comunidad de seguridad.

- **TLP "GREEN".** La información no está restringida y puede compartirse para prevenir ataques.
- **"email phishing".** indica el método de distribución del malware.

- **Taxonomías estandarizadas de CIRCL y CSIRT Américas.** Estas etiquetas facilitan la contextualización del evento, especialmente para organizaciones y países que filtran amenazas basándose en dichas taxonomías.



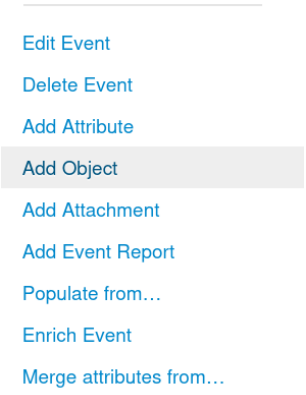
- **TAG local.** Al añadirlo se utilizará esta etiqueta personalizada para filtrar eventos específicos de Bolivia.

Asignación de Atributos y Objetos

Los atributos se agruparán en objetos para este caso, esto nos sirve para organizar la información (cuerpo del correo, archivo adjunto, etc.).

OBJETOS.

Para crear los objetos nos dirigimos al menú lateral de la derecha y seleccionamos la opción **Add Object**.



Objeto 1. Correo electrónico. Extraemos los datos relevantes del correo malicioso.

- En al correo electrónico recibido, podemos extraer (remitente, asunto, adjuntos, etc.).

De Verónica Gárate Correa <dimotikiastinomia@voio.gr>

A undisclosed-recipients:;

Asunto **Pago**

Hola

Adjunto la confirmación SWIFT del pago realizado hoy en su cuenta bancaria,

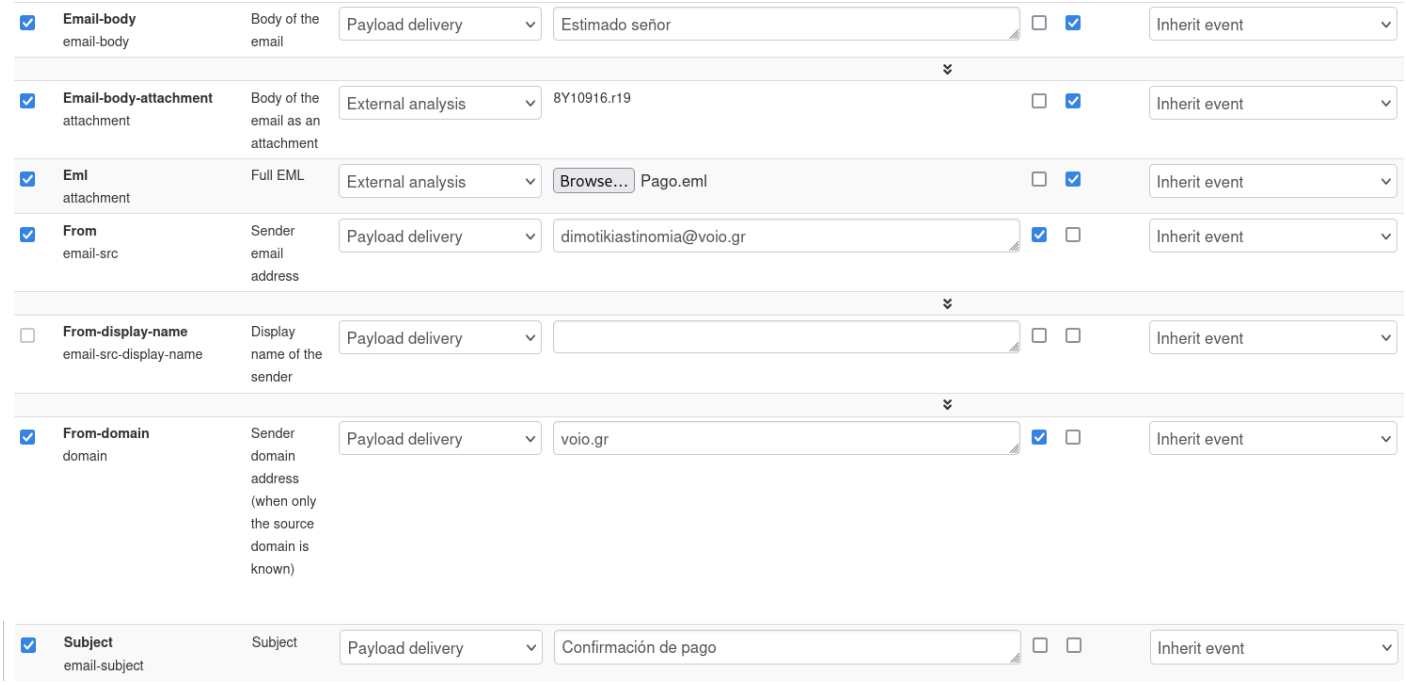
por favor confirme y contáctenos de inmediato, es urgente,
gracias

Saludos cordiales!

Verónica Gárate Correa
Asistente de Gerencia
Bolivian Movers SRL.
Av. Saavedra. N° 2086, Miraflores. La Paz - Bolivia
Ph. +591- 2 - 2226434 / 2221509 / 2222433
Fax : 591 - 2 - 2228143
Po BOX: 7467
e-mail: removals@bolivianmovers.com
Web: www.bolivianmovers.com

1 adjunto: 8Y10916.r19 723 KB

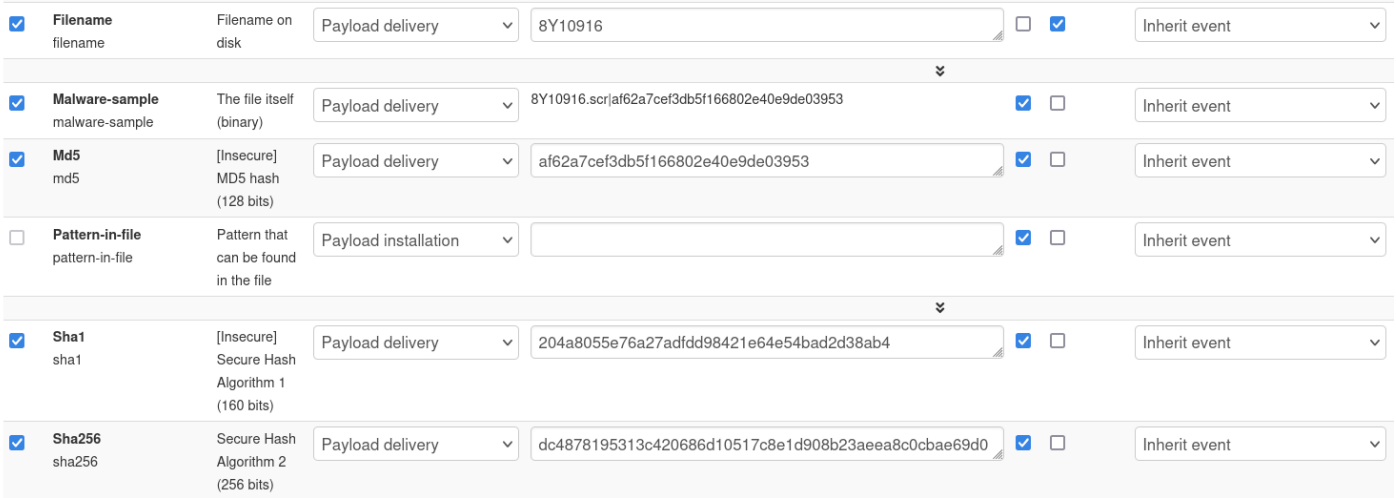
- Los atributos correspondientes se añaden al objeto **Correo** de la siguiente manera:



Objeto 2. Archivo adjunto (malware).

Es posible analizar el archivo en herramientas como VirusTotal, Any.Run o Hybrid Analysis.

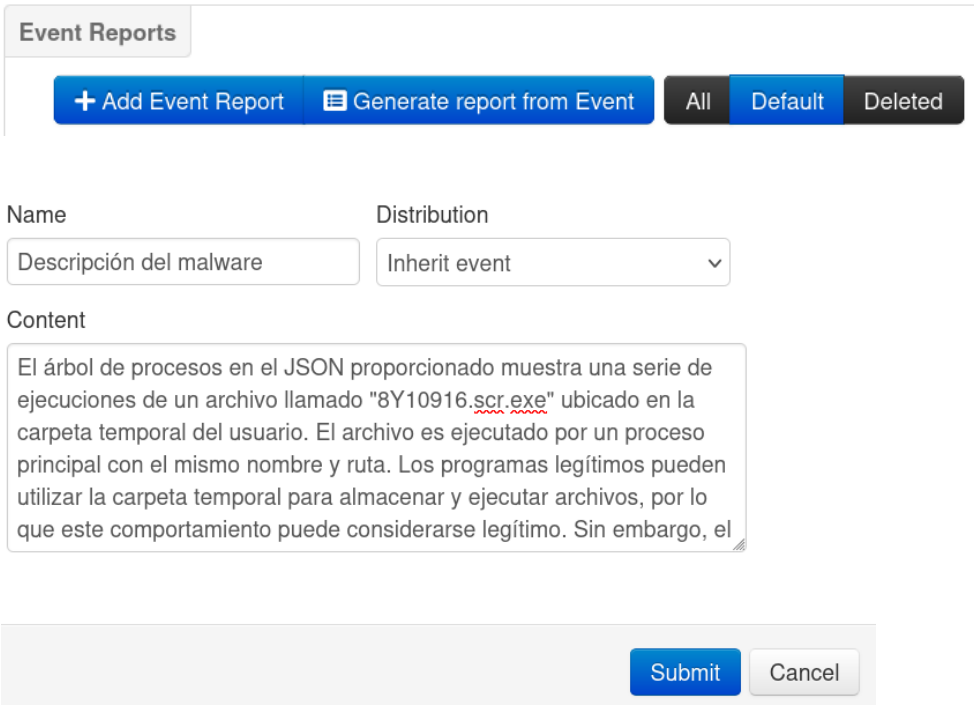
- En este caso la información que puede ser extraída para el análisis contiene hashes (MD5, SHA-1, SHA-256), nombre del archivo y metadatos como podemos ver a continuación.



- Los objetos y sus atributos se listarán en la sección correspondiente.

EVENT REPORT.

- Para contextualizar el impacto del malware complementando la información del evento creamos un Event Report de forma manual en primera instancia.



- Opcionalmente, generamos un informe automático con **Generate Report From Event**, este reporte agrupará los indicadores de compromiso e información de los tags existentes de manera que puede ser enviado como alerta al personal que no tiene la cuenta de MISP habilitada facilitando la comprensión del evento.

Distribución troyano Loki mediante campaña de phishing

- *Date*: 2025-01-07
- *Last update*: 2025-01-07 18:22:06
- *Threat level*: Medium
- *Attribute count*: 12

Tags

- tlp:green
- infoleak:analyst-detection="mail"
- circl:incident-classification="malware"
- circl:incident-classification="phishing"

Galaxies

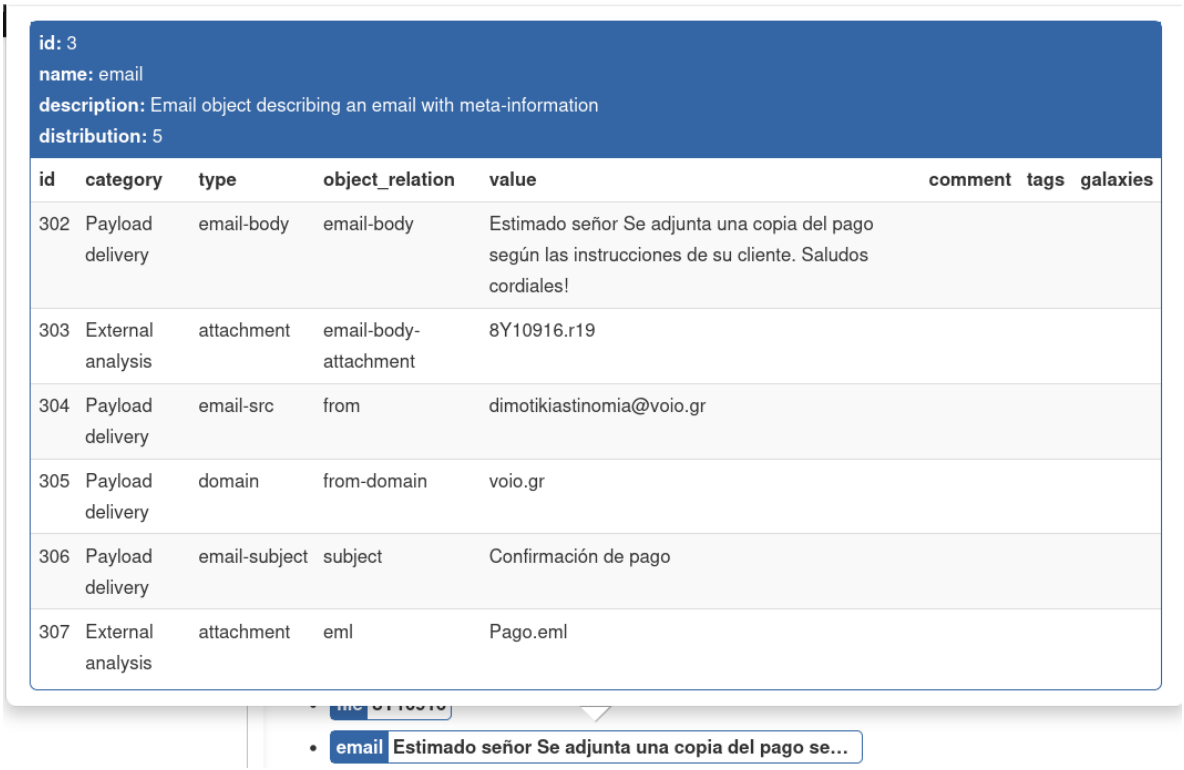
Correlations

Objects

- file 8Y10916
- email Estimado señor Se adjunta una copia del pago se…

Attributes

- Al realizar click en cualquiera de los objetos se tendrá como resultado los atributos que lo componen.



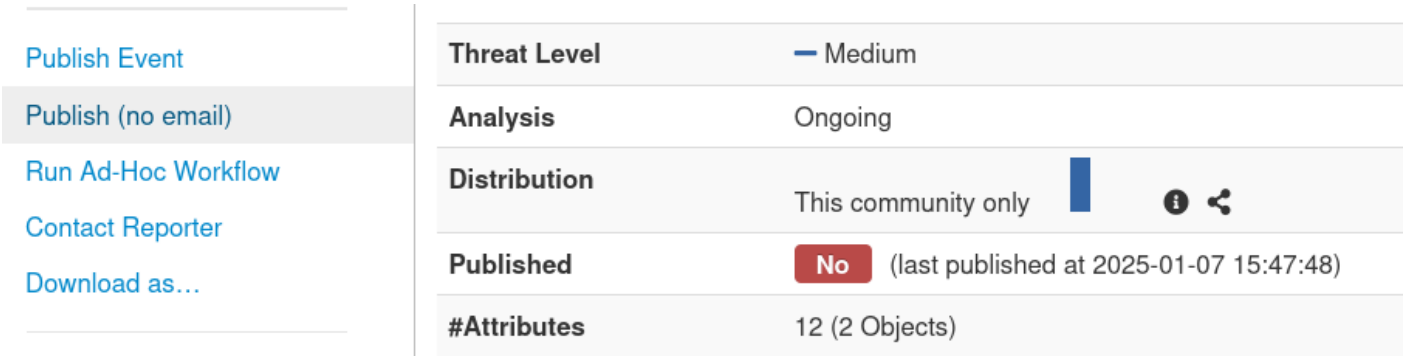
id: 3
name: email
description: Email object describing an email with meta-information
distribution: 5

id	category	type	object_relation	value	comment	tags	galaxies
302	Payload delivery	email-body	email-body	Estimado señor Se adjunta una copia del pago según las instrucciones de su cliente. Saludos cordiales!			
303	External analysis	attachment	email-body-attachment	8Y10916.r19			
304	Payload delivery	email-src	from	dimotikiastinomia@voio.gr			
305	Payload delivery	domain	from-domain	voio.gr			
306	Payload delivery	email-subject	subject	Confirmación de pago			
307	External analysis	attachment	eml	Pago.eml			

email Estimado señor Se adjunta una copia del pago se…

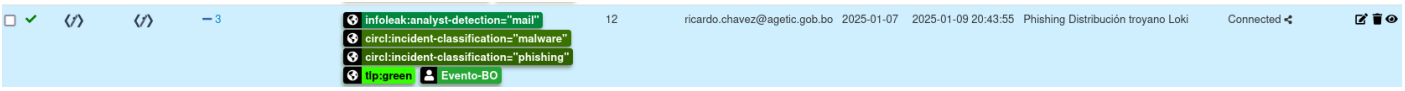
Publicación del evento.

Para modificar el estado inicial del evento y permitir que los demás usuarios de la plataforma accedan a él, según su nivel de distribución, observamos inicialmente que el evento aparece con el estado '**Published=No**', como se muestra en la siguiente captura de pantalla



Con la opción 'Publish (No Email)', se realiza la publicación en la plataforma sin enviar un correo electrónico a los usuarios. Si se requiere el envío de correos, debe seleccionarse la opción 'Publish Event'. Después de elegir cualquiera de las dos opciones, el estado del evento cambia a '**Published=Yes**'

Cuando el evento es publicado se asigna un ID al evento en este caso "**3**" y el primer valor del evento en la lista es un check que indica que los usuarios que están dentro del criterio de distribución pueden ver la información del evento como se muestra a continuación.



02- Direcciones IP con actividad de malware evento MISP

Introducción

MISP es una herramienta de código abierto diseñada para facilitar el intercambio de información sobre amenazas cibernéticas, permitiendo a los usuarios compartir indicadores de compromiso (IOC's), análisis de malware y otros datos relevantes de seguridad.

Esta guía te ayudará a utilizar la plataforma MISP (Malware Information Sharing Platform & Threat Sharing) para crear y distribuir eventos de manera eficiente y completa. Tenemos como finalidad proporcionar un paso a paso detallado para crear, configurar y publicar eventos en MISP, tomando distintos ejemplos. Su objetivo es estandarizar el proceso de documentación y compartir inteligencia sobre amenazas de manera eficiente, asegurando que los usuarios de la plataforma puedan aprovechar la información para fortalecer sus defensas y prevenir incidentes similares.

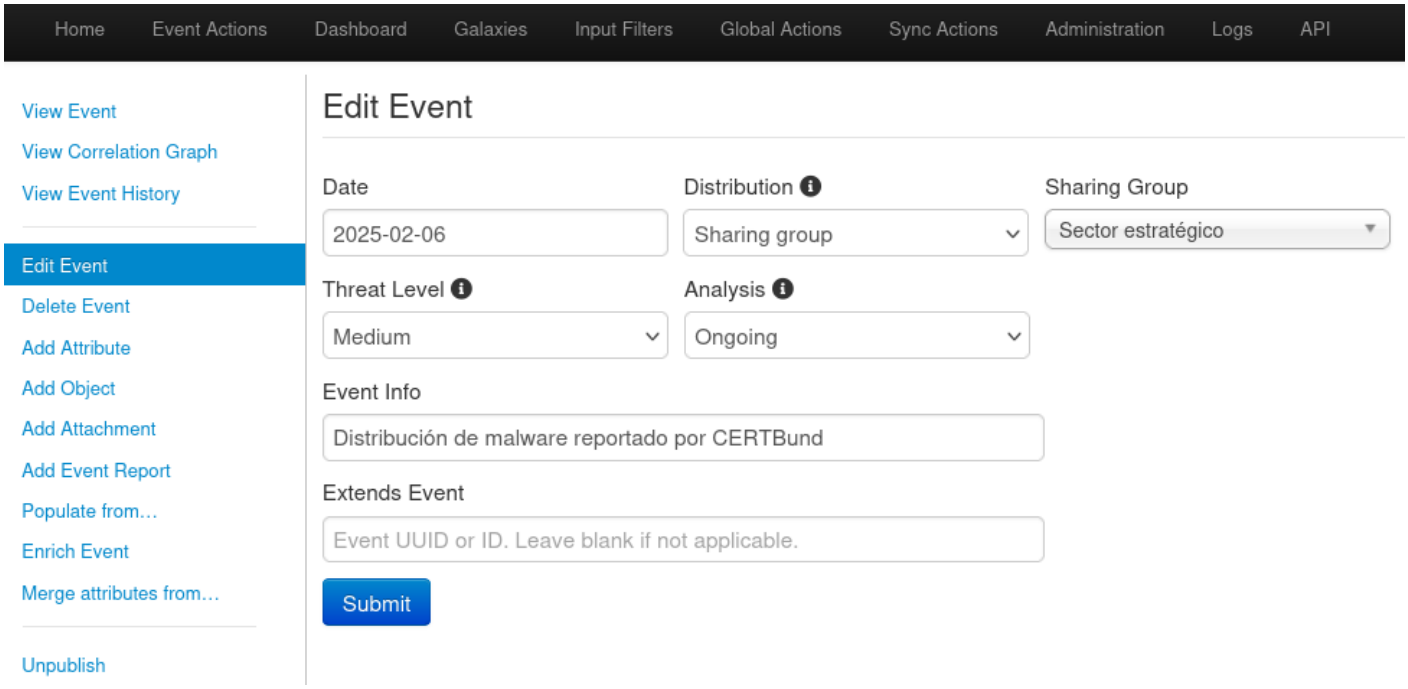
Contexto

El Centro de Gestión de Incidentes Informáticos recibió una alerta de seguridad que contiene información delicada (Lista de direcciones IP) de una red de distribución de malware activa dentro del país.

Los pasos para publicar el evento en MISP pueden variar según la información disponible, pero en este ejemplo se detallarán los indicadores de compromiso (IOCs) más comunes asociados a distribución de malware. En casos específicos, es posible que no se encuentren todos los datos mencionados, por lo que solo se debe incluir información verificada.

CREACIÓN DEL EVENTO.

- Ingresar a la sección de **Events** posteriormente **Event Actions** y por último seleccionar **Add event**.



- **Distribution.**
  Define el alcance de visibilidad del evento.
- **Threat level.**
  Define el nivel de amenaza del evento.
- **Analysis.**
  Define el evento en Inicial,Ongoing (en curso) o finalizado.
- **Event info.**
  Incluir el resumen de una descripción del evento.
- **Extends Event.**
  Si el evento está relacionado con uno previo, agregar el UUID correspondiente para vincularlos.

ASIGNACIÓN DE TAGS

El uso de tags nos ayuda en gran medida a contextualizar y enriquecer la información compartida. Estas etiquetas no solo facilitan la categorización y búsqueda eficiente de eventos también permiten establecer relaciones claras entre incidentes, amenazas y campañas maliciosas.

Al incorporar tags descriptivos, los usuarios de la plataforma pueden priorizar, filtrar y correlacionar datos con mayor precisión, mejorando así la respuesta ante ciberamenazas entre la comunidad de seguridad.

- **TLP "AMBER+STRICT".** La información está restringida y es compartida solamente con individuos autorizados (usuarios MISP del nodo nacional).
- **Taxonomías estandarizadas de CIRCL y CSIRT Américas.** Estas etiquetas facilitan la contextualización del evento, especialmente para organizaciones y países que filtran amenazas basándose en dichas taxonomías.

- **TAG local.** Al añadirlo se utilizará esta etiqueta personalizada para filtrar eventos específicos de Bolivia.

Asignación de Atributos

Los atributos para este caso son de actividad de red, esto nos sirve para organizar la información.

OBJETOS.

En este caso específico no se tienen objetos, como muestras de malware o distribución por phishing o spam debido a que el origen de la información nos detalla direcciones IP que distribuyen malware.

ATRIBUTOS.

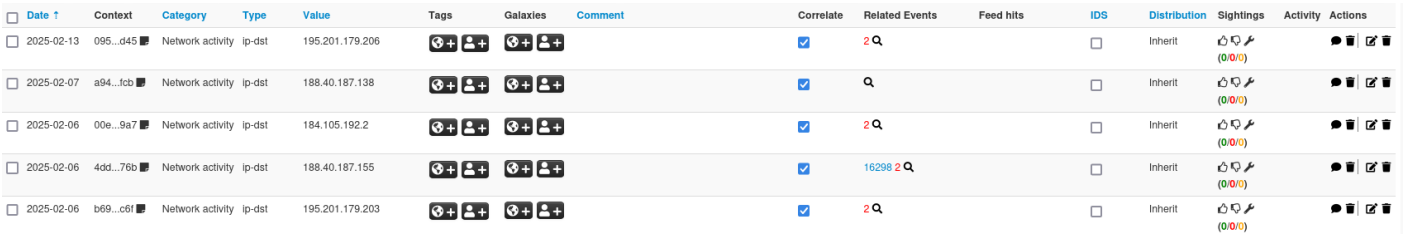
Para agregar la lista de IP's procedemos a seleccionar el boton de "+" para añadir los atributos.

Estos atributos se clasifican en la categoría de actividad de red e IP destino por que son las direcciones IP a las que se comunican los equipos infectados.

Una vez seleccionada la opción **Submit** podemos observar que los atributos han sido agregados correctamente observando si existe una correlación con otros eventos

CORRELACIÓN DE EVENTOS.

- El evento creado automáticamente se correlaciona con el evento 2 y 16298 como podemos ver a en la columna Related Events a continuación.

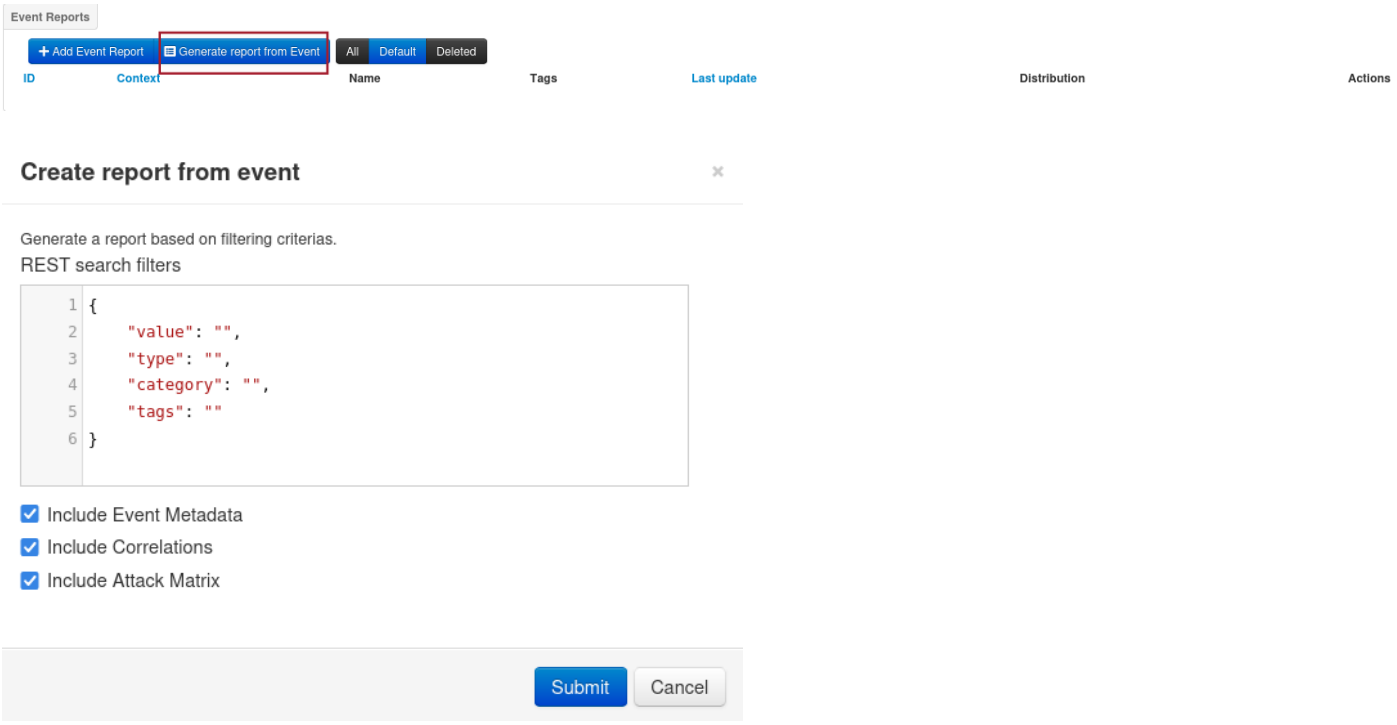


- La forma recomendada para visualizar la correlación se encuentra en la esquina superior derecha donde podemos encontrar eventos que fueron relacionados con las direcciones IP reportadas como maliciosas por el proveedor de información, con esta nueva información

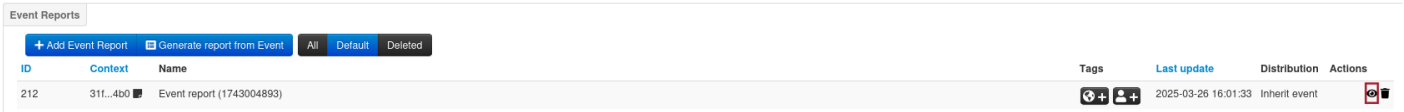
comprobamos que las direcciones IP están relacionadas con malware *Agent tesla* y se vio involucrada en realización de solicitudes maliciosas a dominios del país.

EVENT REPORT.

- Generamos un event report automático con Generate Report From Event, este reporte agrupará los indicadores de compromiso e información de los tags existentes de manera que puede ser enviado como alerta al personal que no tiene la cuenta de MISP habilitada facilitando la comprensión del evento.



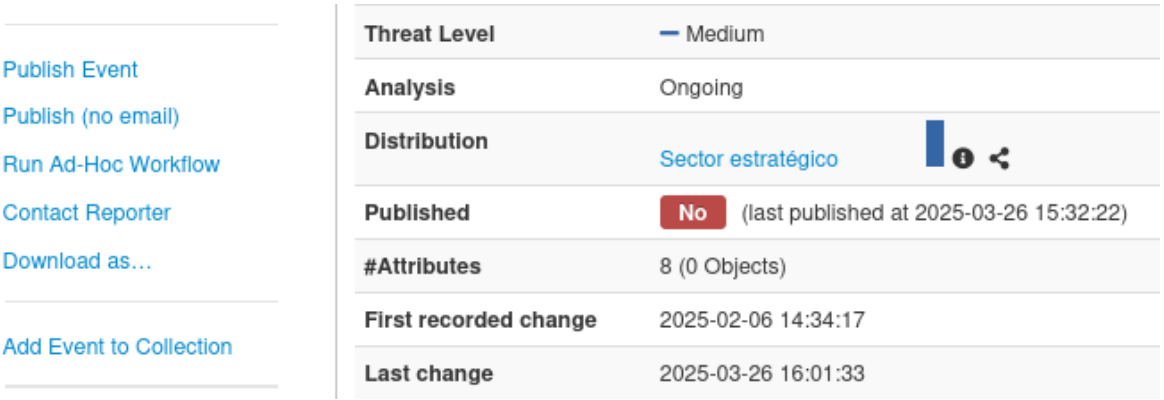
- Una vez generado el reporte se observa en el apartado de Event Reports el resumen de los datos relevantes del reporte.



- El reporte generado resume la información del evento en la siguiente plantilla:

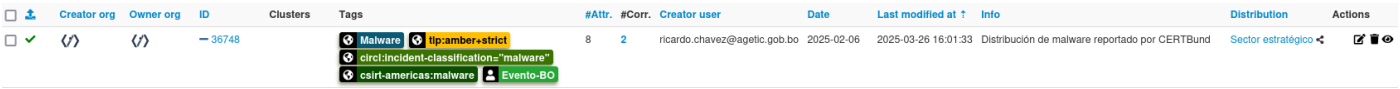
Publicación del evento.

Para modificar el estado inicial del evento y permitir que los demás usuarios de la plataforma accedan a él, según su nivel de distribución, observamos inicialmente que el evento aparece con el estado '**Published=No**', como se muestra en la siguiente captura de pantalla



Con la opción 'Publish (No Email)', se realiza la publicación en la plataforma sin enviar un correo electrónico a los usuarios. Si se requiere el envío de correos, debe seleccionarse la opción 'Publish Event'. Después de elegir cualquiera de las dos opciones, el estado del evento cambia a '**Published=Yes**'

Cuando el evento es publicado se asigna un ID al evento en este caso "**36748**" y el primer valor del evento en la lista es un check que indica que los usuarios que están dentro del criterio de distribución pueden ver la información del evento como se muestra a continuación.



03- Campaña DDoS evento MISP

Introducción

MISP es una herramienta de código abierto diseñada para facilitar el intercambio de información sobre amenazas cibernéticas, permitiendo a los usuarios compartir indicadores de compromiso (IOC's), análisis de malware y otros datos relevantes de seguridad.

Esta guía te ayudará a utilizar la plataforma MISP (Malware Information Sharing Platform & Threat Sharing) para crear y distribuir eventos de manera eficiente y completa. Tenemos como finalidad proporcionar un paso a paso detallado para crear, configurar y publicar eventos en MISP, tomando distintos ejemplos. Su objetivo es estandarizar el proceso de documentación y compartir inteligencia sobre amenazas de manera eficiente, asegurando que los usuarios de la plataforma puedan aprovechar la información para fortalecer sus defensas y prevenir incidentes similares.

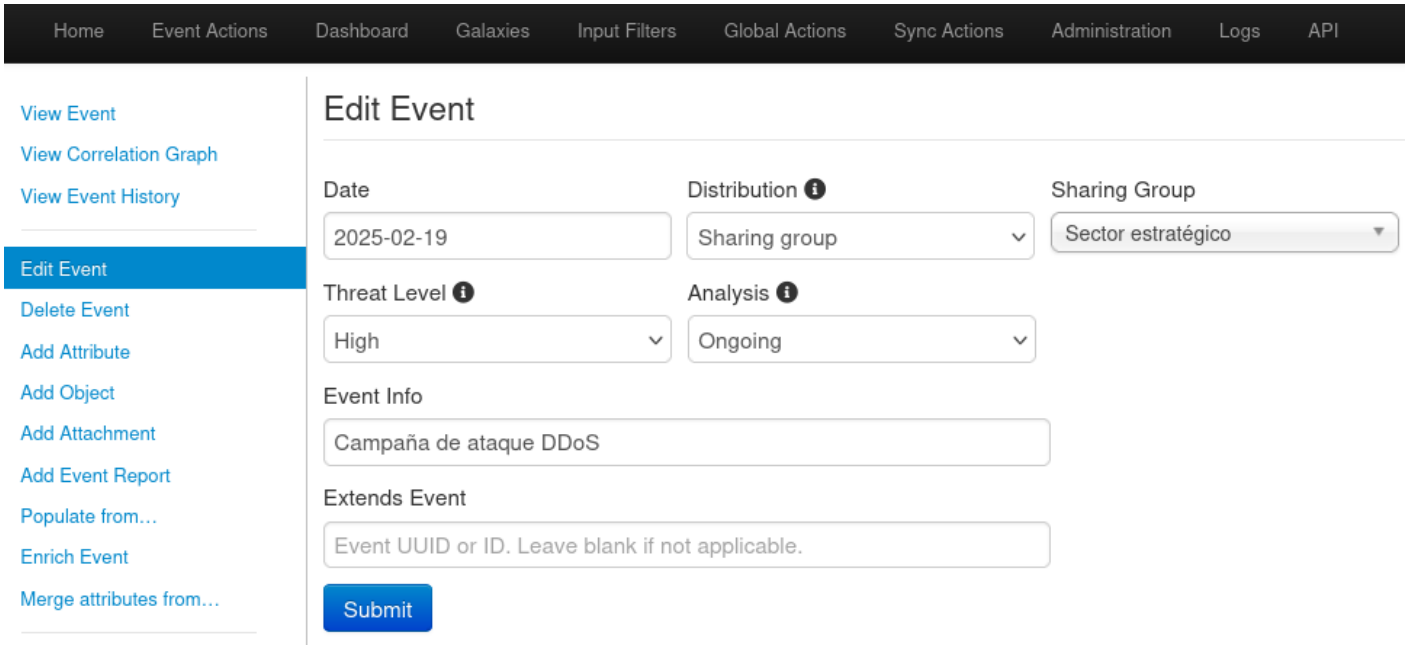
Contexto

El Centro de Gestión de Incidentes Informáticos realiza la investigación de un intento de ataque de denegación de servicio (DDoS) hacia servidores gubernamentales en Bolivia, durante esta investigación se pudo recopilar una gran cantidad de direcciones IP que pertenecen a la botnet para realizar ataques, se utilizaron criterios de numero de solicitudes realizadas y tipo de solicitudes para identificar estas solicitudes.

Los pasos para publicar el evento pueden variar ligeramente según el contenido y la información proporcionada a la plataforma. En este ejemplo de creación de un evento en MISP, se detallan conjuntos de direcciones IP que luego fueron reportadas a los respectivos países para tomar acciones de mitigación desde sus jurisdicciones. En casos específicos de DDoS, los datos más importantes son las *direcciones IP de origen*, los *rangos de IP* y la *geolocalización*, ya que son atributos clave para correlacionar. Como contexto adicional, los *tiempos entre solicitudes* son muy útiles para identificar *patrones en solicitudes automatizadas*.

CREACIÓN DEL EVENTO.

- Ingresar a la sección de **Events** posteriormente **Event Actions** y por último seleccionar **Add event**.



- **Distribution.**
  Define el alcance de visibilidad del evento.
- **Threat level.**
  Define el nivel de amenaza del evento.
- **Analysis.**
  Define el evento en Inicial,Ongoing (en curso) o finalizado.
- **Event info.**
  Incluir el resumen de una descripción del evento.
- **Extends Event.**
  Si el evento está relacionado con uno previo, agregar el UUID correspondiente para vincularlos.

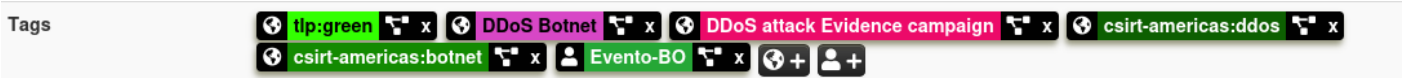
ASIGNACIÓN DE TAGS

El uso de tags nos ayuda en gran medida a contextualizar y enriquecer la información compartida. Estas etiquetas no solo facilitan la categorización y búsqueda eficiente de eventos también permiten establecer relaciones claras entre incidentes, amenazas y campañas maliciosas.

Al incorporar tags descriptivos, los usuarios de la plataforma pueden priorizar, filtrar y correlacionar datos con mayor precisión, mejorando así la respuesta ante ciberamenazas entre la comunidad de seguridad.

- **TLP "GREEN".** La información no está restringida y puede compartirse para prevenir ataques.
- **"DDoS Botnet" y "DDoS attack Evidence campaign".** Debido al comportamiento malicioso observado en la mayoría de las direcciones IP y la investigación realizada donde se anuncia el ataque de denegación de servicio.

- **Taxonomías estandarizadas de CSIRT Américas.** Estas etiquetas facilitan la contextualización del evento, especialmente para organizaciones y países que filtran amenazas basándose en dichas taxonomías.



- **TAG local.** Al añadirlo se utilizará esta etiqueta personalizada para filtrar eventos específicos de Bolivia.

Asignación de información al evento.

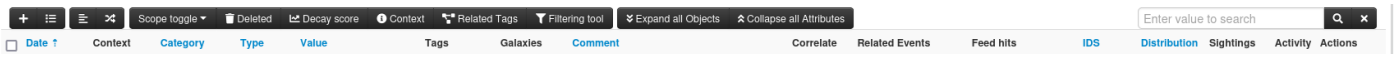
Los atributos para este caso pertenecen a la categoría de actividad de red, esto nos sirve para organizar la información.

OBJETOS.

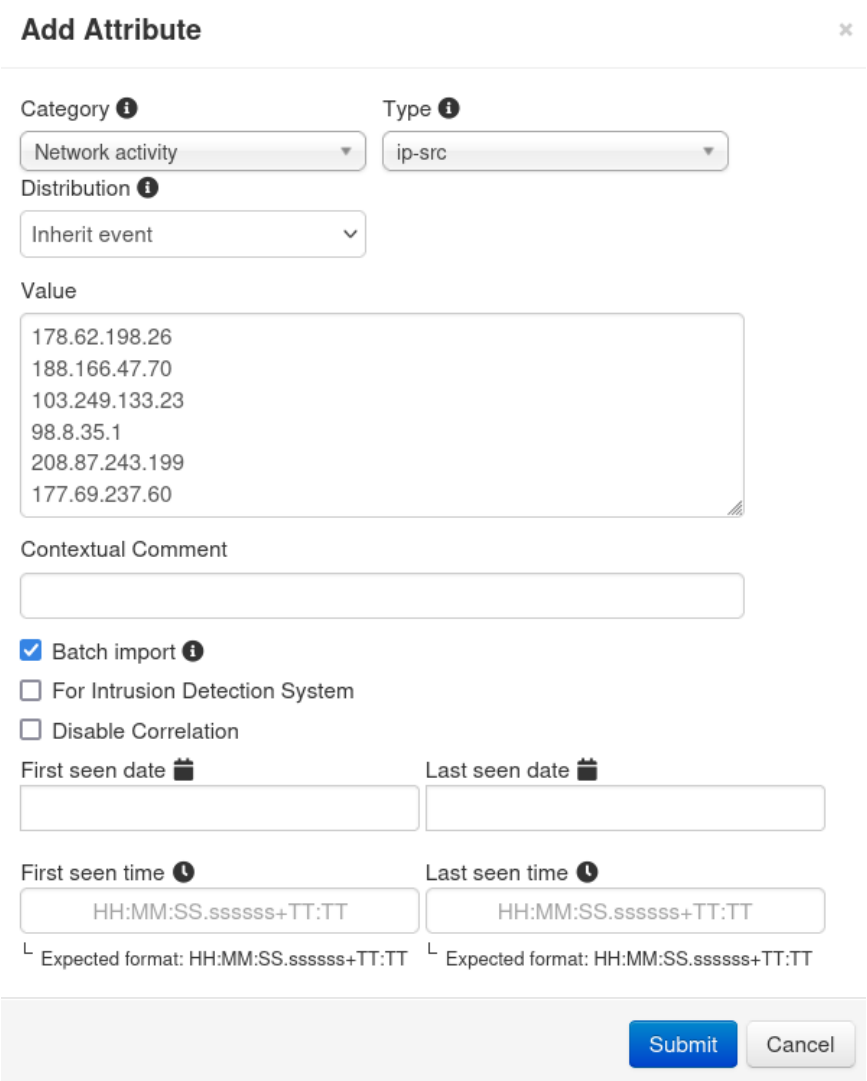
En este caso específico no se incluyen objetos, como muestras de malware o archivos maliciosos, ya que el origen de la información se limita a direcciones IP que forman parte de la botnet responsable del ataque DDoS. Por este motivo, no se añadirán objetos al análisis.

ATRIBUTOS.

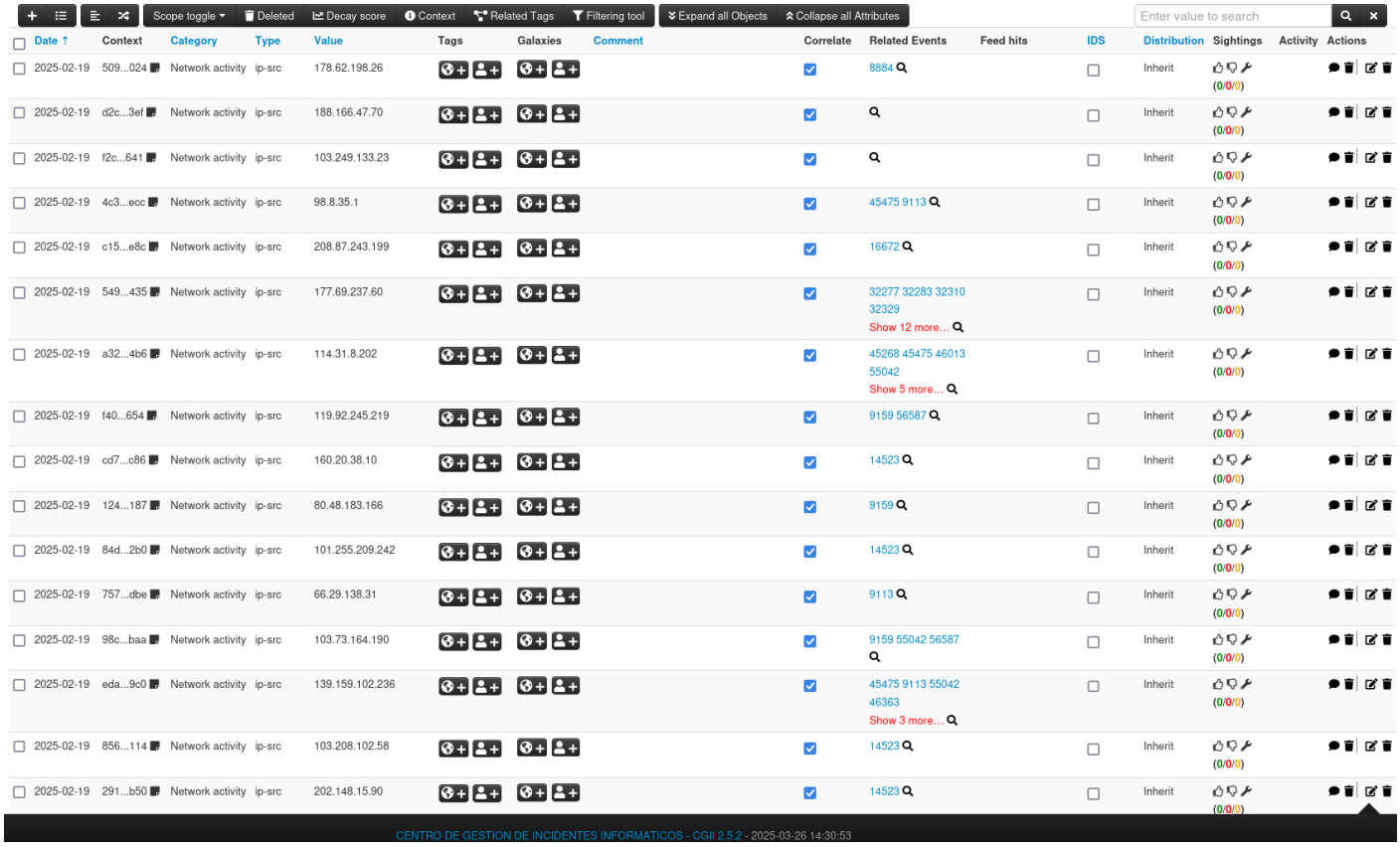
Para agregar la lista de direcciones IP procedemos a seleccionar el botón "**+**" para añadir los atributos.



Estos atributos se clasifican en la categoría de actividad de red e IP fuente por que son las direcciones IP desde las que se realizó el intento de denegación de servicio.



Una vez seleccionada la opción '**Submit**', podemos verificar que los atributos se han agregado correctamente y comprobar si existe correlación con otros eventos. En este caso particular, dado el volumen elevado de direcciones IP, se recomienda revisar las correlaciones en la esquina superior derecha de la interfaz. En la columna adyacente pueden observarse los atributos que han sido añadidos al evento

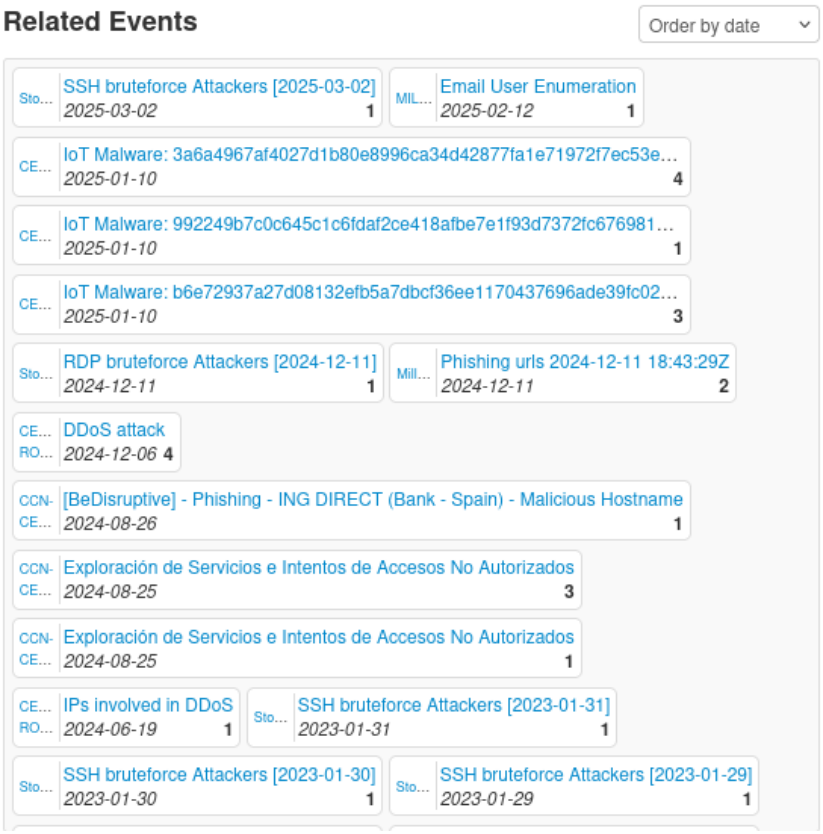


CORRELACIÓN DE EVENTOS.

La forma recomendada para visualizar la correlación se encuentra en la esquina superior derecha donde podemos encontrar eventos que fueron relacionados con nuestro evento.

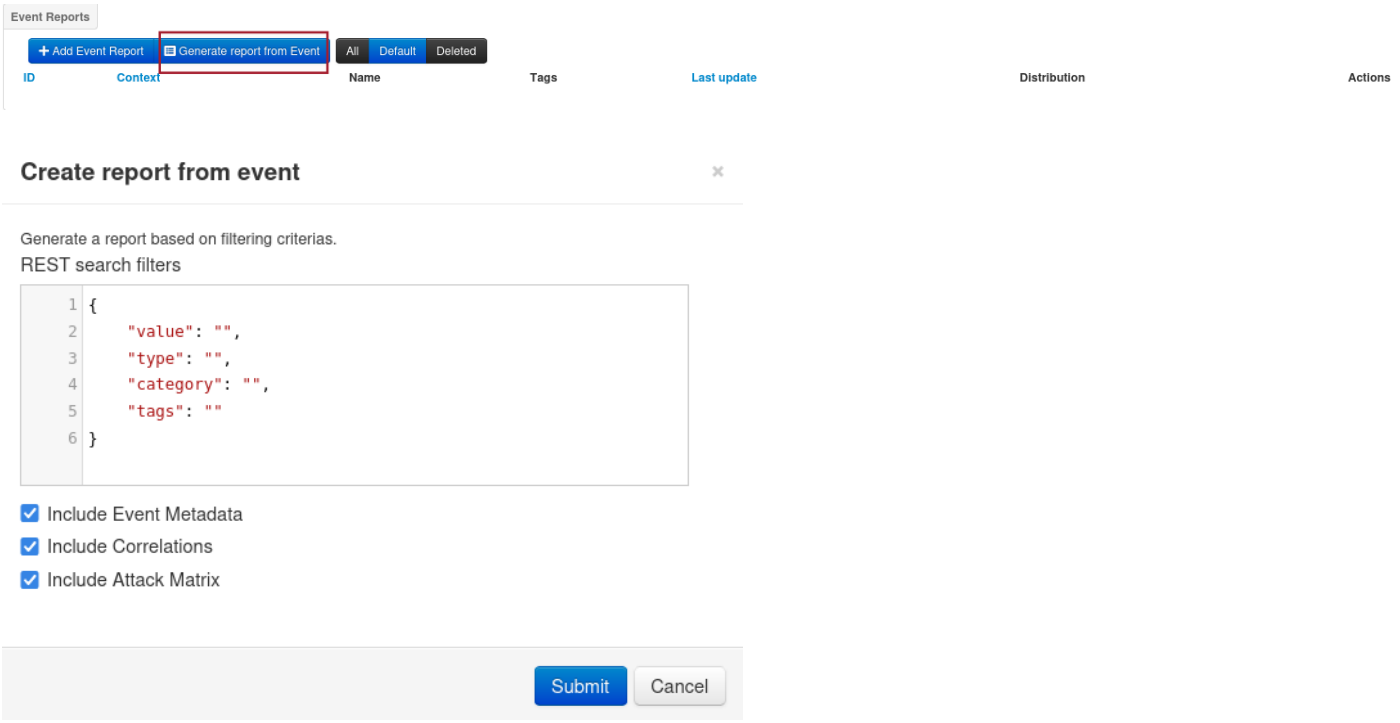
En la esquina superior derecha de la interfaz se visualizan los eventos relacionados con las direcciones IP identificadas como parte de la red involucrada en el ataque DDoS, extraídas durante la investigación. Este contexto nos permite establecer que:

- Direcciones IP asociadas a actividad maliciosa.
- Dispositivos IoT comprometidos.
- Direcciones dedicadas a enumeración de usuarios.
- Intentos de exploración no autorizados.

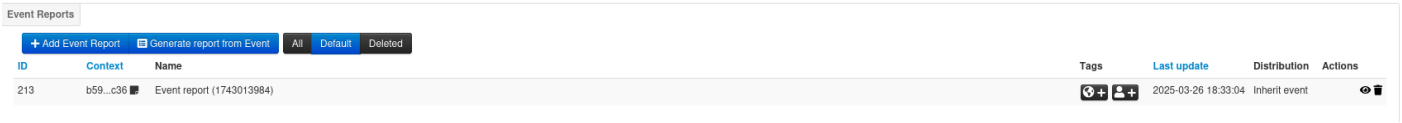


EVENT REPORT.

- Generamos un event report automático con Generate Report From Event, este reporte agrupará los indicadores de compromiso e información de los tags existentes de manera que puede ser enviado como alerta al personal que no tiene la cuenta de MISP habilitada facilitando la comprensión del evento.



- Una vez generado el reporte se observa en el apartado de Event Reports el resumen de los datos relevantes del reporte.



- El reporte generado resume la información del evento en la siguiente plantilla:

Campaña de ataque DDoS

- *Date*: 2025-02-19
- *Last update*: 2025-03-27 14:35:17
- *Threat level*: Medium
- *Attribute count*: 16

Tags

- tlp:green
- DDoS Botnet
- DDoS attack Evidence campaign
- csirt-americas:ddos
- csirt-americas:botnet

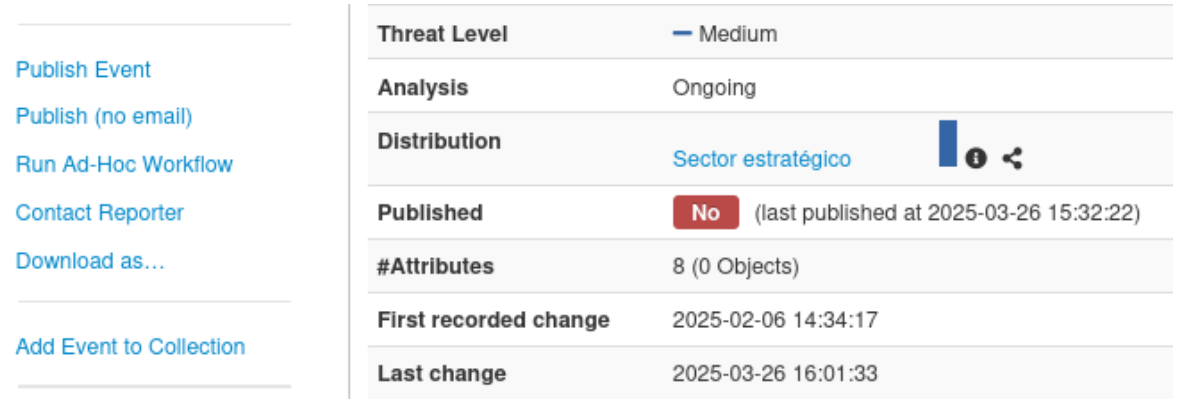
Galaxies

Correlations

- SSH bruteforce Attackers [2025-03-02]
- Email User Enumeration
- IoT Malware: 3a6a4967af4027d1b80e8996ca34d42877fa1e71972f7ec53eeba34c2c2e905d
- IoT Malware: 992249b7c0c645c1c6fdaf2ce418afbe7e1f93d7372fc6769817126a24e09177
- IoT Malware: b6e72937a27d08132efb5a7dbcf36ee1170437696ade39fc0217ef6a43347c27
- RDP bruteforce Attackers [2024-12-11]
- Phishing urls 2024-12-11 18:43:29Z
- DDoS attack
- [BeDisruptive] - Phishing - ING DIRECT (Bank - Spain) - Malicious Hostname
- Exploración de Servicios e Intentos de Accesos No Autorizados
- Exploración de Servicios e Intentos de Accesos No Autorizados
- IPs involved in DDoS
- SSH bruteforce Attackers [2023-01-31]
- SSH bruteforce Attackers [2023-01-30]
- SSH bruteforce Attackers [2023-01-29]
- SSH bruteforce Attackers [2023-01-28]
- SSH bruteforce Attackers [2023-01-27]
- SSH bruteforce Attackers [2023-01-26]
- SSH bruteforce Attackers [2023-01-24]
- SSH bruteforce Attackers [2023-01-23]
- SSH bruteforce Attackers [2023-01-22]
- SSH bruteforce Attackers [2023-01-20]

Publicación del evento.

Para modificar el estado inicial del evento y permitir que los demás usuarios de la plataforma accedan a él, según su nivel de distribución, observamos inicialmente que el evento aparece con el estado '**Published=No**', como se muestra en la siguiente captura de pantalla.



Con la opción 'Publish (No Email)', se realiza la publicación en la plataforma sin enviar un correo electrónico a los usuarios. Si se requiere el envío de correos, debe seleccionarse la opción 'Publish Event'. Después de elegir cualquiera de las dos opciones, el estado del evento cambia a '**Published=Yes**'

Cuando el evento es publicado se asigna un ID al evento en este caso "**53289**" y el primer valor del evento en la lista es un check que indica que los usuarios que están dentro del criterio de distribución pueden ver la información del evento como se muestra a continuación.