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.

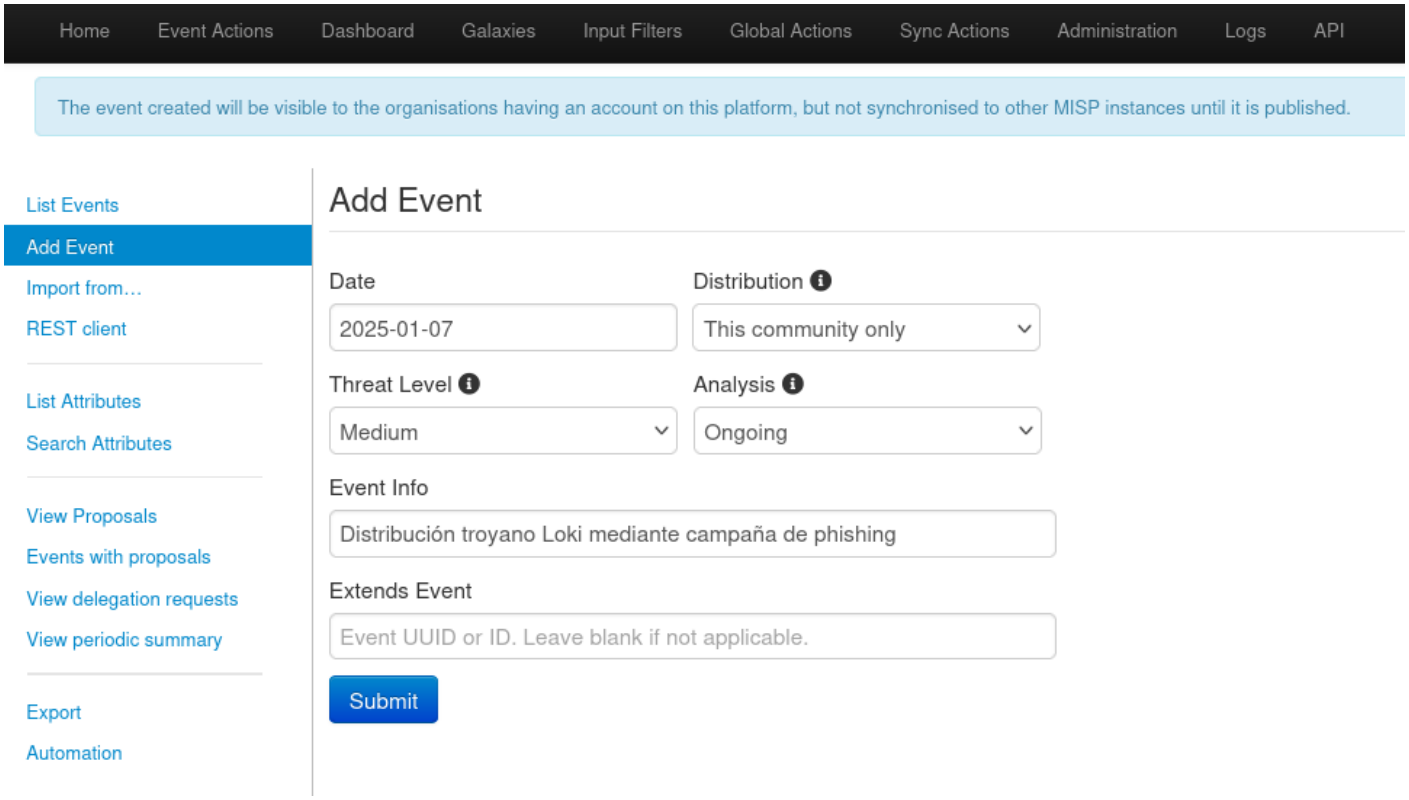
Contexto

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.

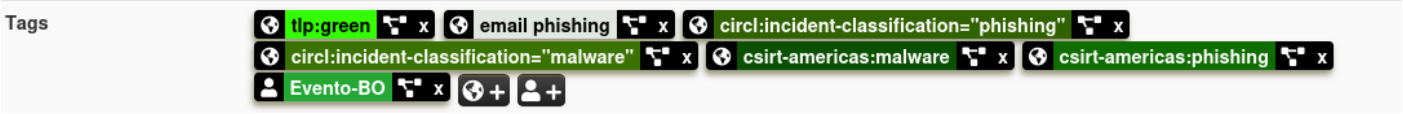
ASIGNACIÓN DE TAGS

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.



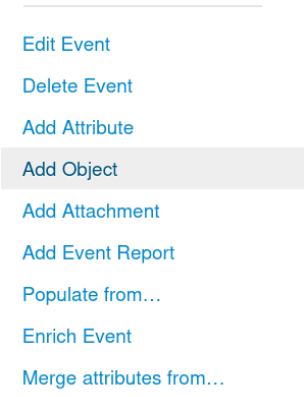
- **TAG local.** Al añadirlo se utilizará esta etiqueta personalizada para filtrar eventos específicos de Bolivia.

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,

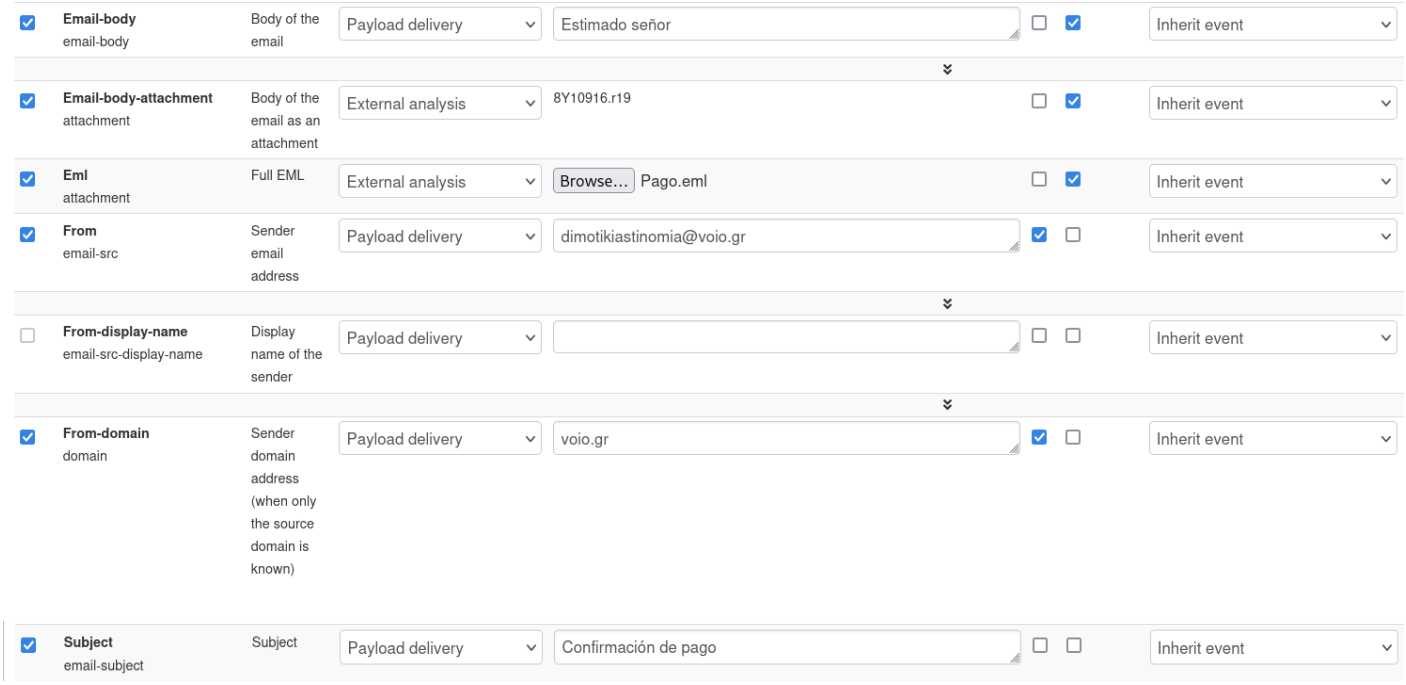
por favor confirme y contáctenos de inmediato, es urgente,
gracias

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

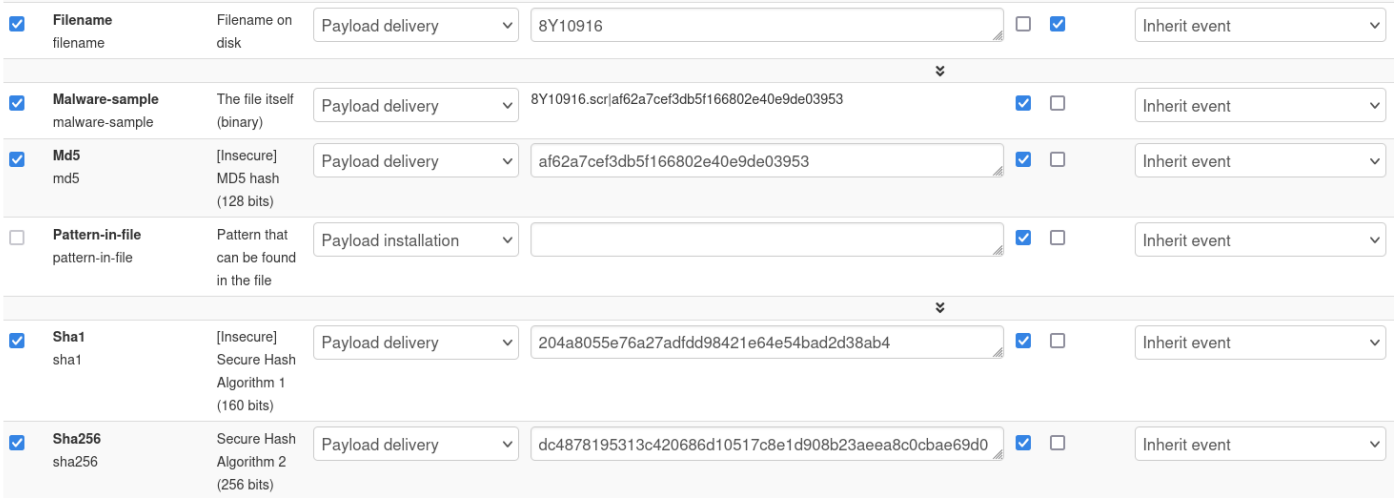
- Los atributos correspondientes se añaden al objeto **Correo** de la siguiente manera:



Objeto 2. Archivo adjunto (malware).

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

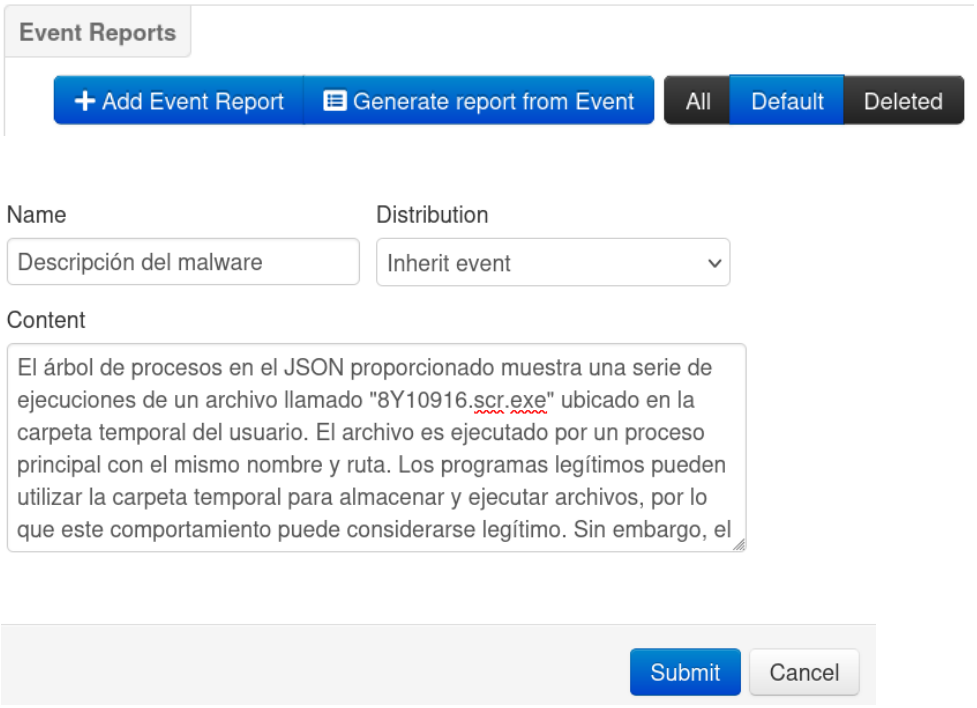
- En este caso la información que puede ser extraída para el análisis contiene hashes (MD5, SHA-1, SHA-256), nombre del archivo y metadatos como podemos ver a continuación.



- 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

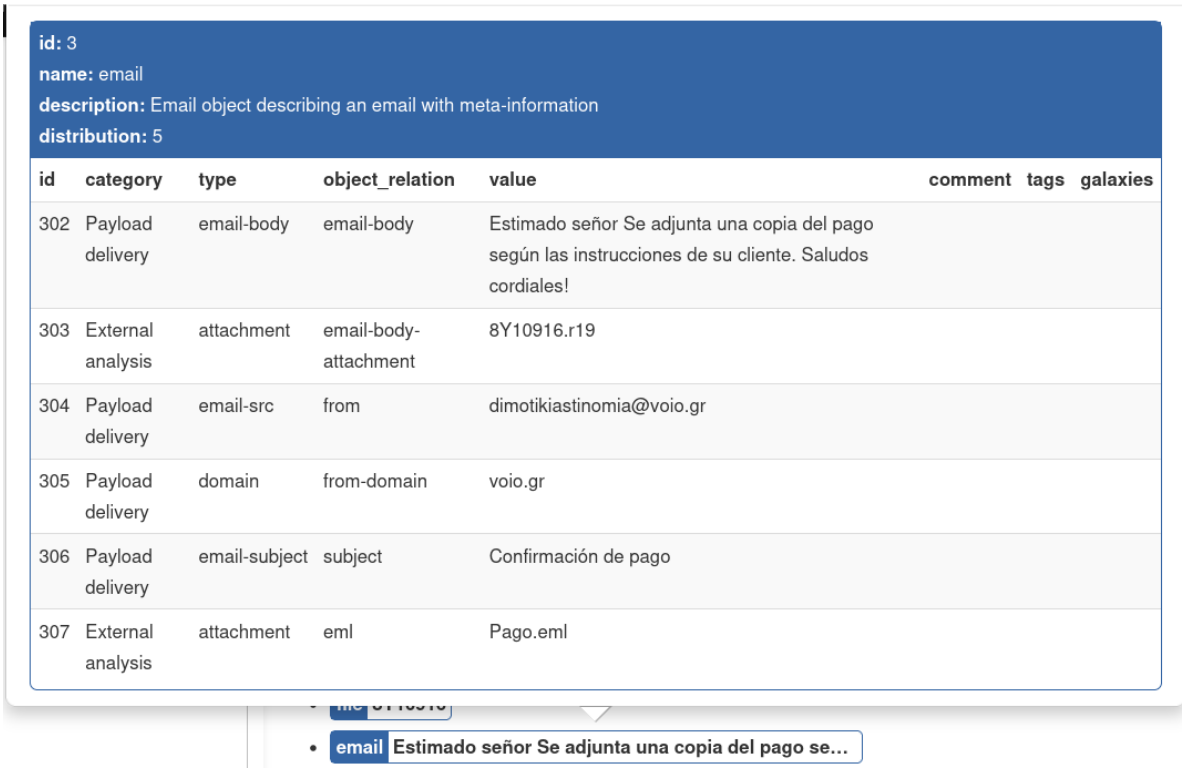
Correlations

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.



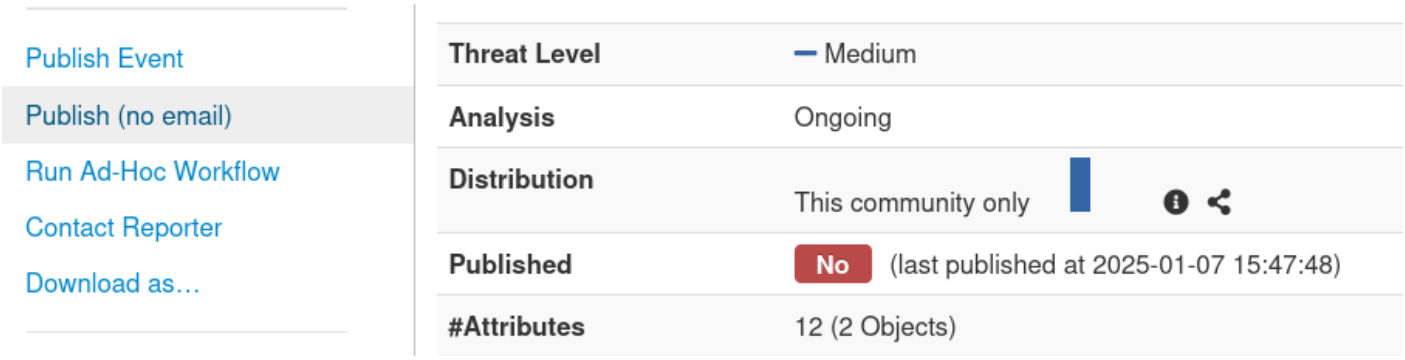
id: 3
name: email
description: Email object describing an email with meta-information
distribution: 5

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…

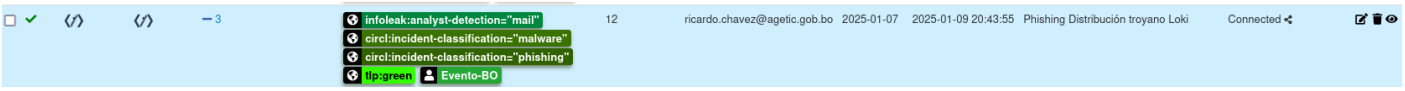
Publicación del evento.

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.



Revision #16
Created 26 marzo 2025 11:08:41 by Ricardo Alberto
Updated 31 marzo 2025 09:57:00 by Ricardo Alberto