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.

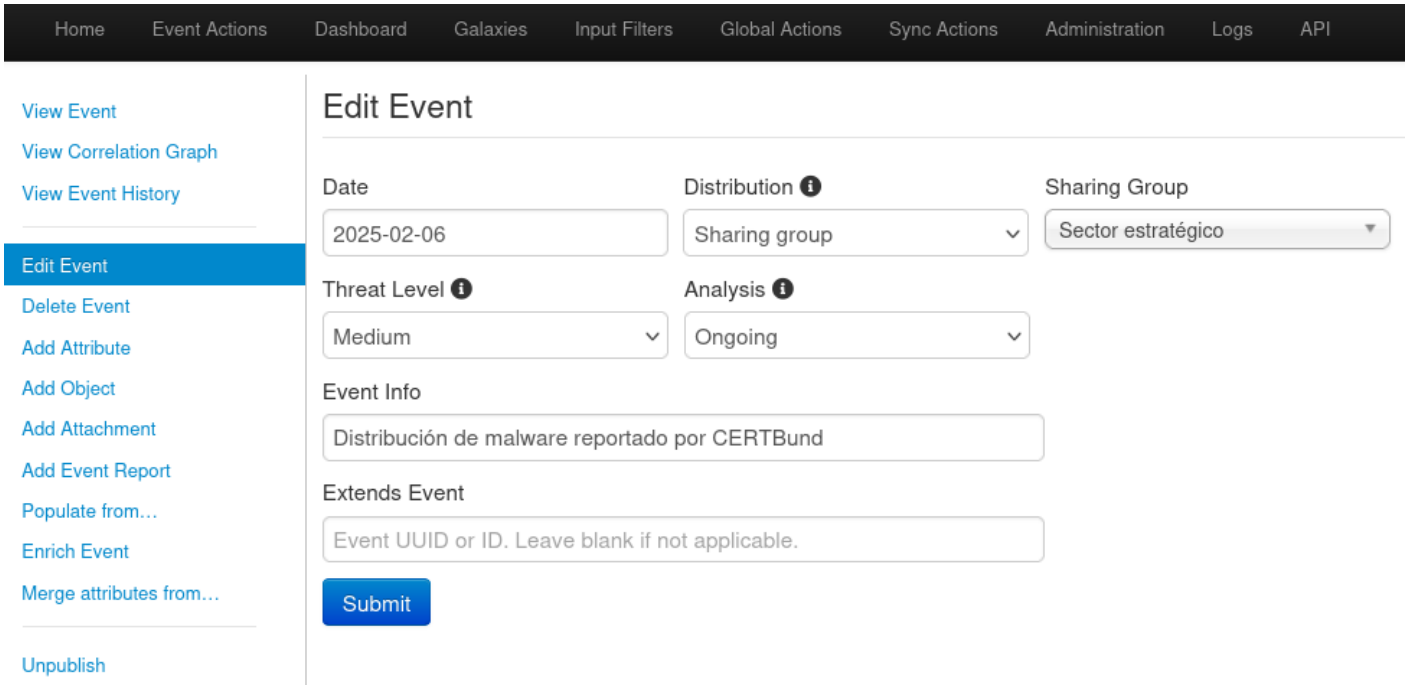
Contexto

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.

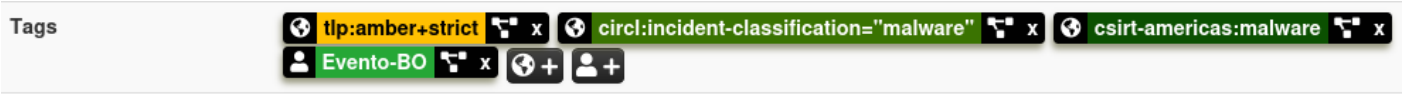
ASIGNACIÓN DE TAGS

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

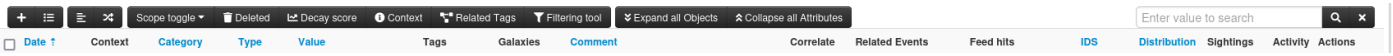
Los atributos para este caso son de actividad de red, esto nos sirve para organizar la información.

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.

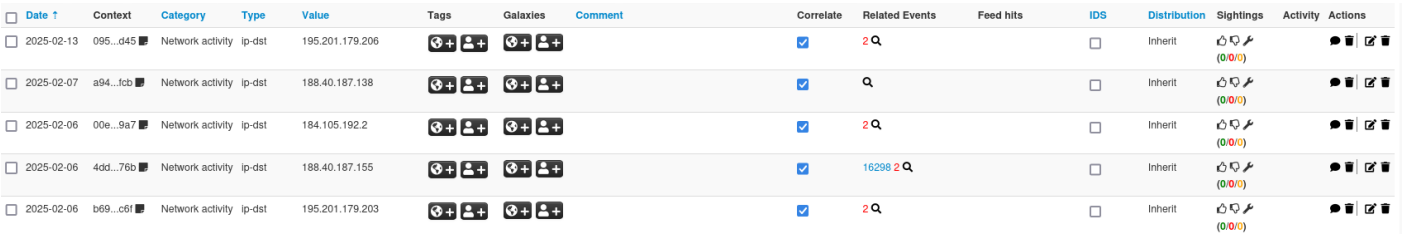


Estos atributos se clasifican en la categoría de actividad de red e IP destino por que son las direcciones IP a las que se comunican los equipos infectados.

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.

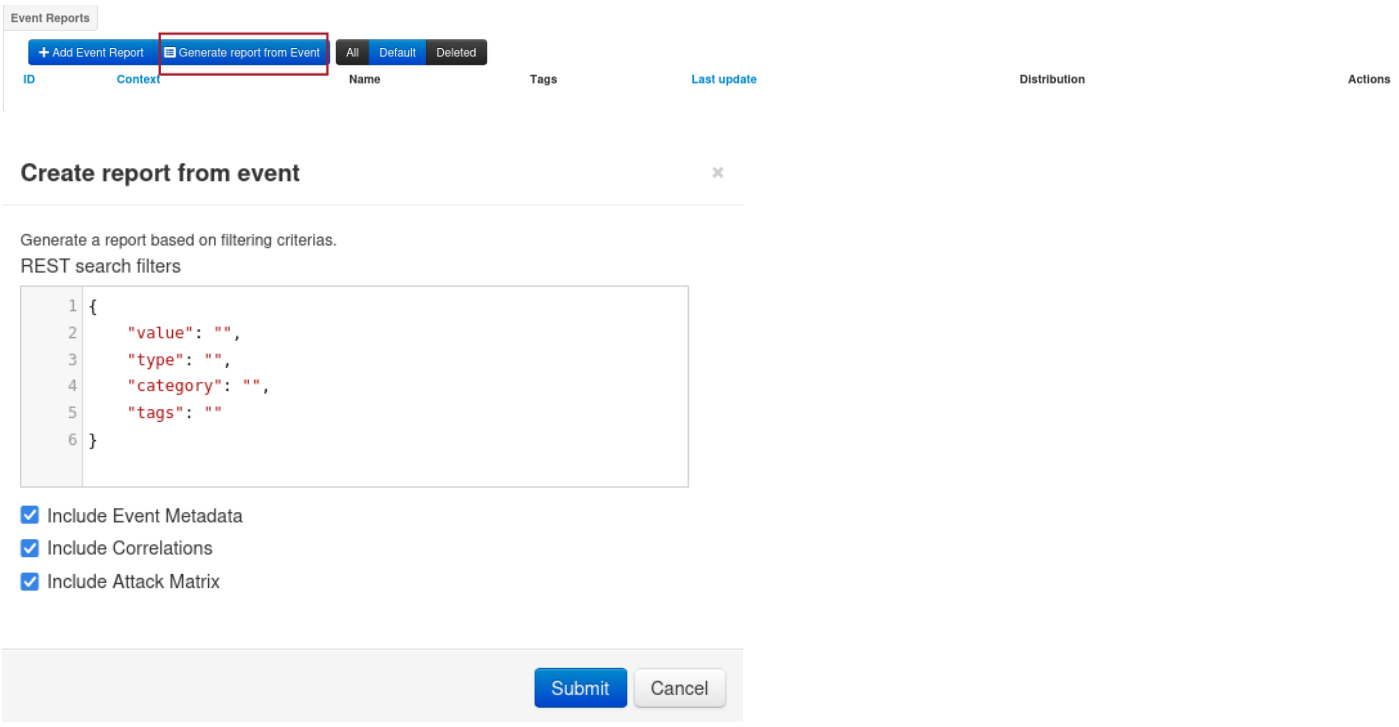


- La forma recomendada para visualizar la correlación se encuentra en la esquina superior derecha donde podemos encontrar eventos que fueron relacionados con las direcciones IP

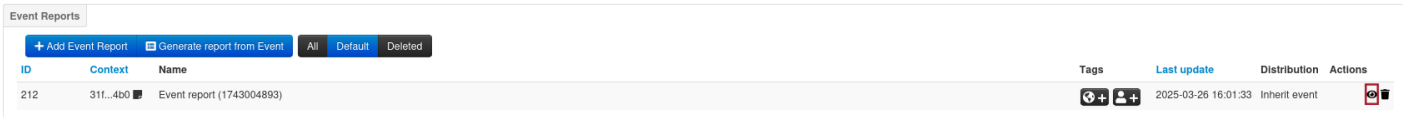
reportadas como maliciosas por el proveedor de información, con esta nueva información comprobamos que las direcciones IP están relacionadas con malware *Agent tesla* y se vio involucrada en realización de solicitudes maliciosas a dominios del país.

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:

Distribución de malware reportado por CERTBund

- *Date*: 2025-02-06
- *Last update*: 2025-03-26 15:58:35
- *Threat level*: Medium
- *Attribute count*: 8

Tags

- Malware
- tlp:amber+strict
- circl:incident-classification="malware"
- csirt-americas:malware

Galaxies

Correlations

- Direcciones IP maliciosas realizando solicitudes a servidores gubernamentales
- Agent tesla - Malware IOC

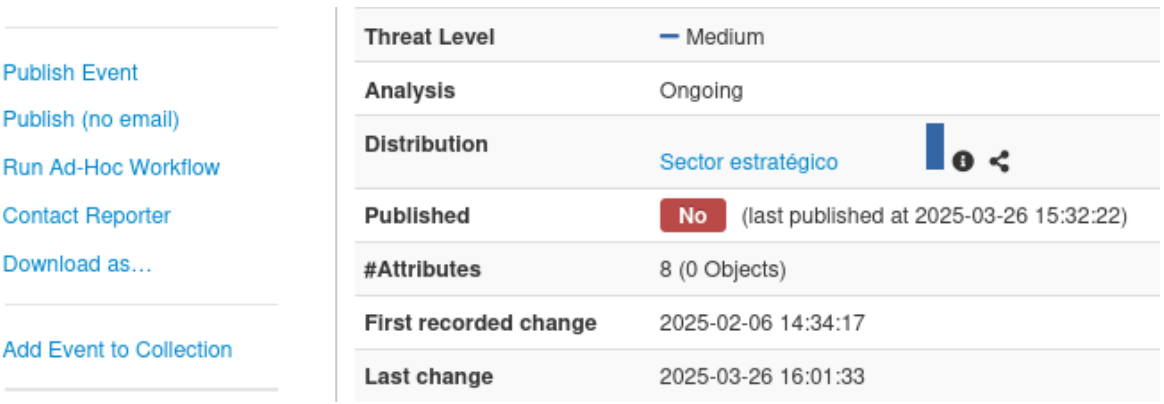
Objects

Attributes

- ip-dst 184.105.192.2
- ip-dst 188.40.187.155
- ip-dst 195.201.179.203
- ip-dst 188.40.187.138
- ip-dst 195.201.179.206
- ip-dst 195.201.179.204
- ip-dst 216.218.185.162
- ip-dst 85.214.228.140

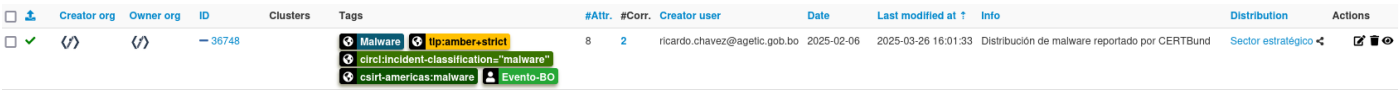
Publicación del evento.

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.



Revision #14
Created 26 marzo 2025 11:31:28 by Ricardo Chavez
Updated 31 marzo 2025 09:57:22 by Ricardo Chavez