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.

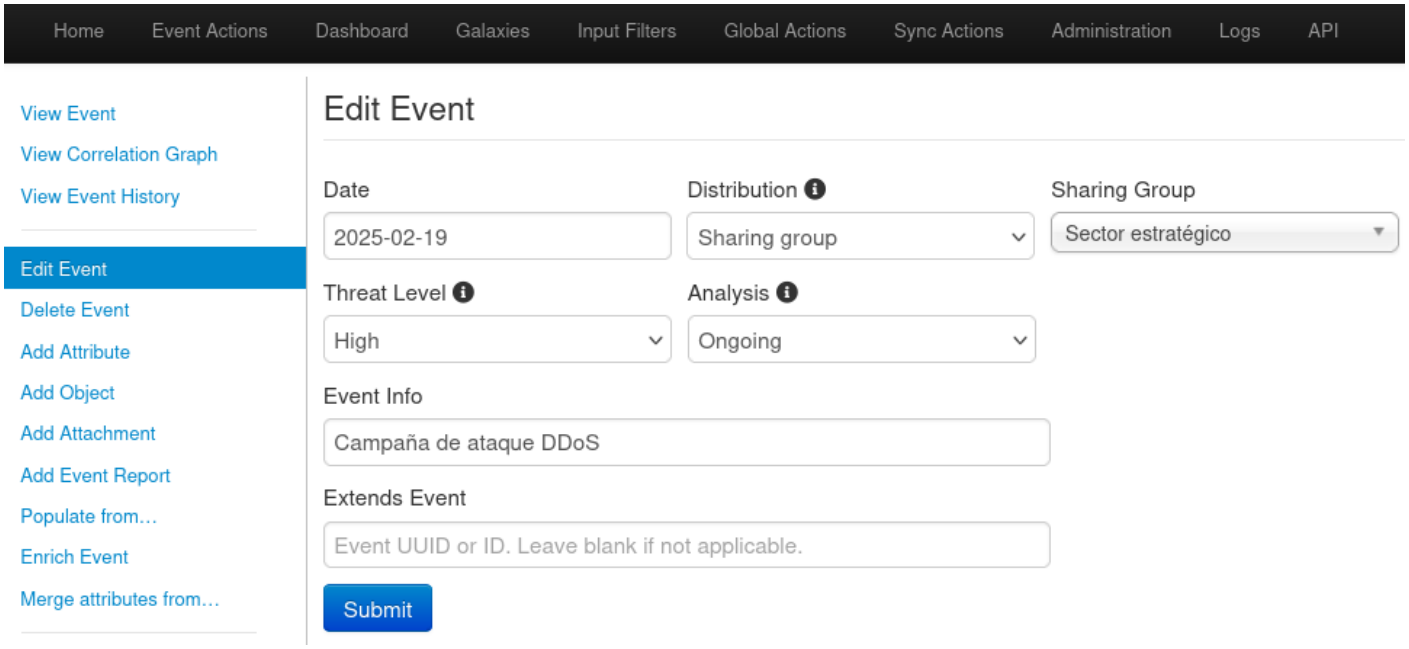
Contexto

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.

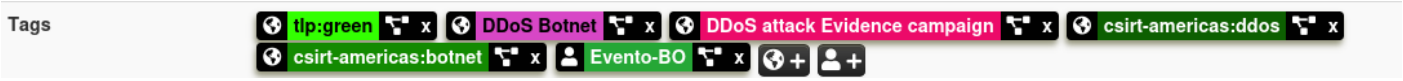
ASIGNACIÓN DE TAGS

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.

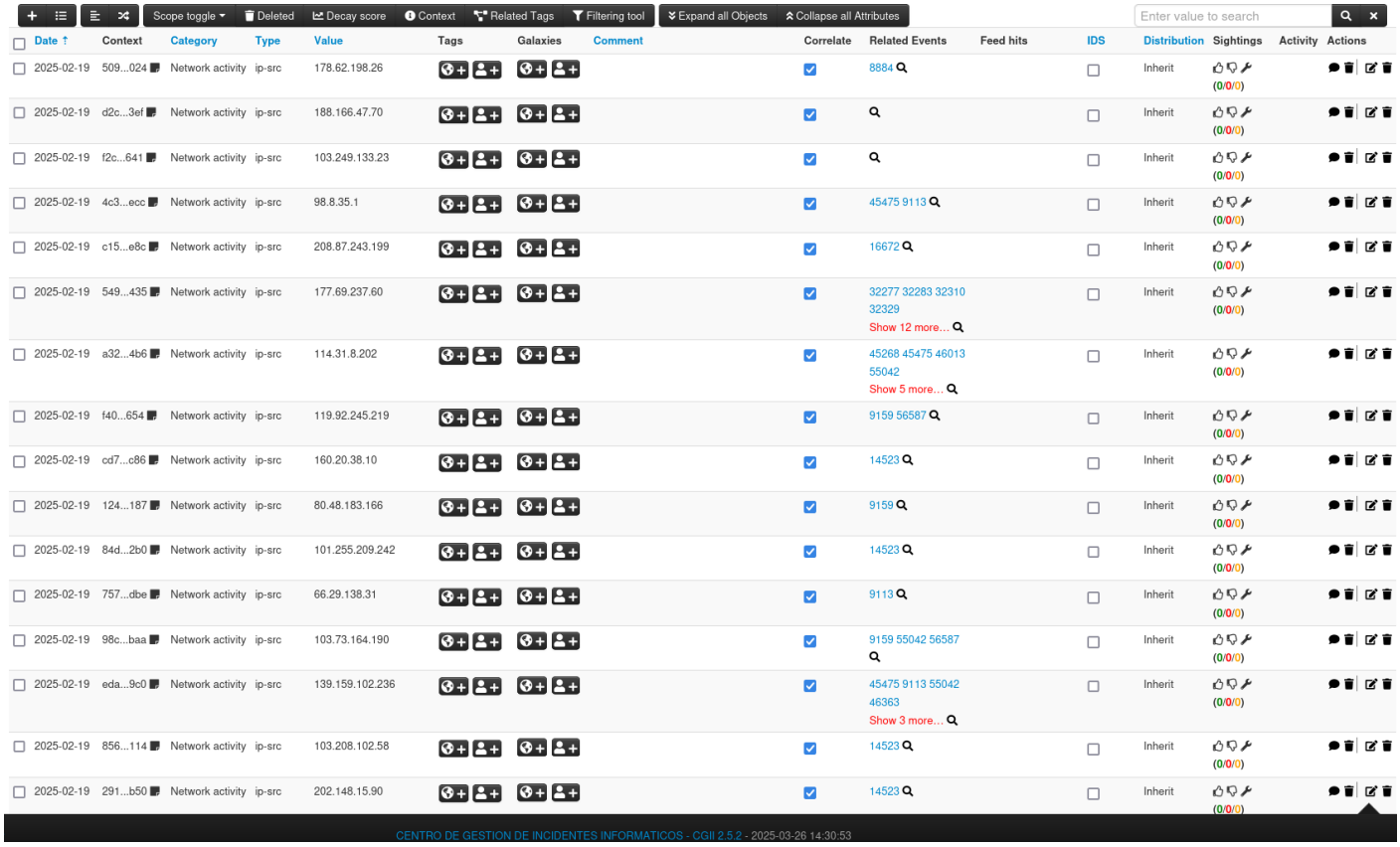
En este caso específico no se incluyen objetos, como muestras de malware o archivos maliciosos, ya que el origen de la información se limita a direcciones IP que forman parte de la botnet responsable del ataque DDoS. Por este motivo, no se añadirán objetos al análisis.

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

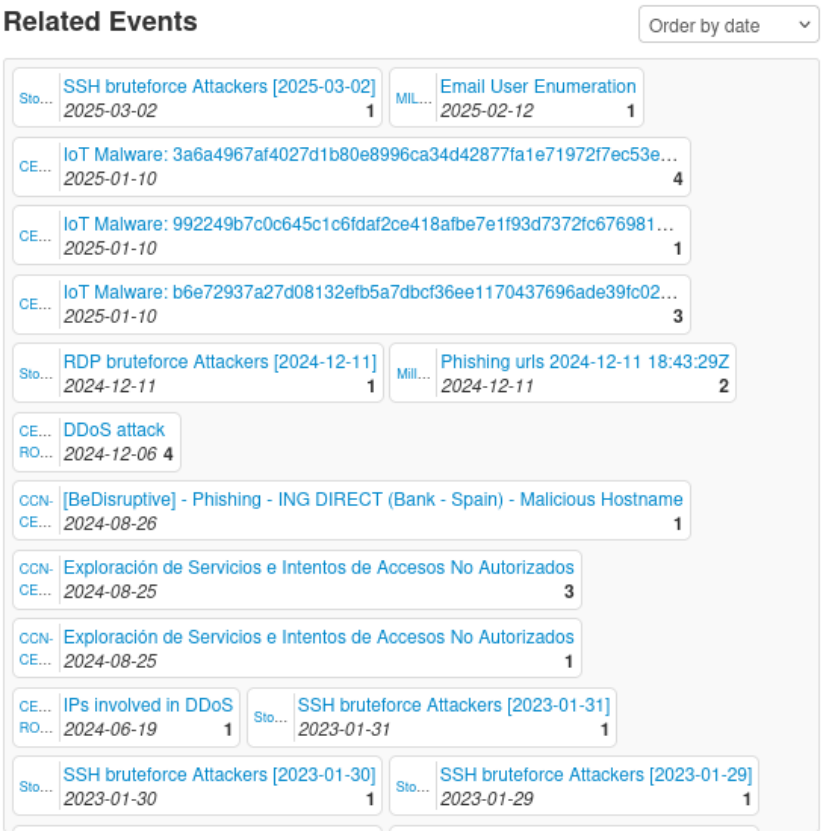


CORRELACIÓN DE EVENTOS.

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

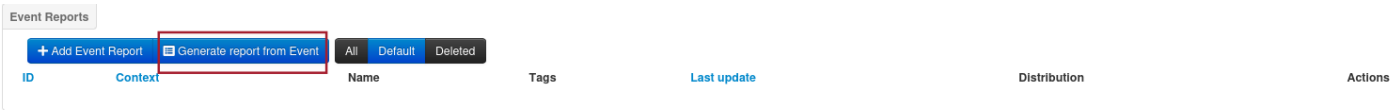
En la esquina superior derecha de la interfaz se visualizan los eventos relacionados con las direcciones IP identificadas como parte de la red involucrada en el ataque DDoS, extraídas durante la investigación. Este contexto nos permite establecer que:

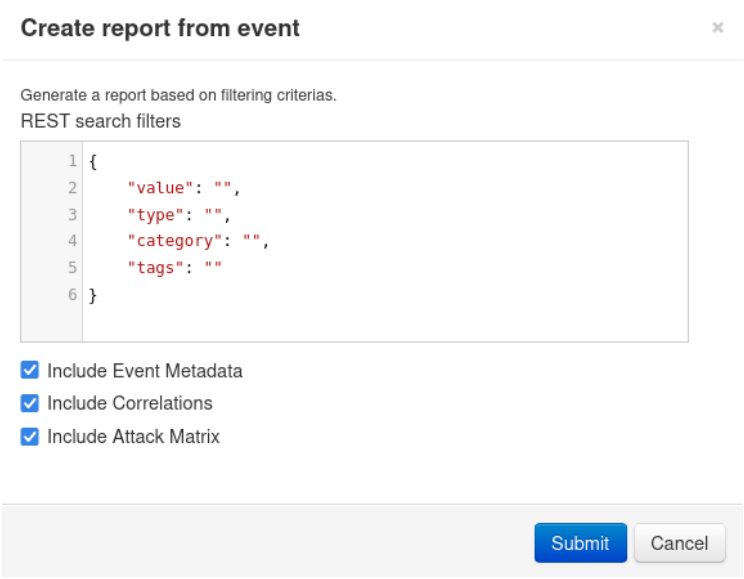
- Direcciones IP asociadas a actividad maliciosa.
- Dispositivos IoT comprometidos.
- Direcciones dedicadas a enumeración de usuarios.
- Intentos de exploración no autorizados.



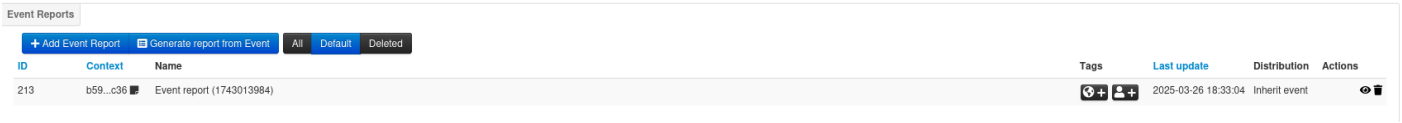
EVENT REPORT.

- 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

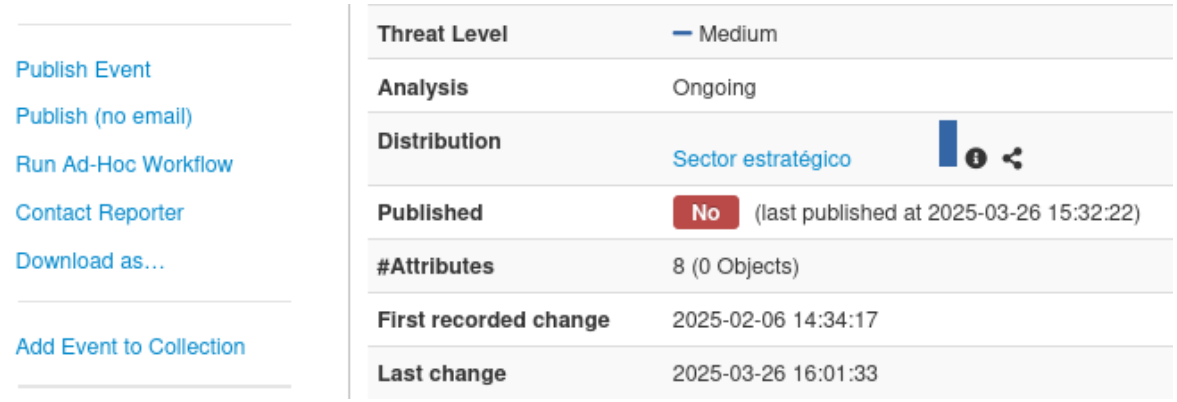
Galaxies

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.

Revision #10
Created 26 marzo 2025 14:32:23 by Ricardo Alberto
Updated 31 marzo 2025 09:57:23 by Ricardo Alberto