

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**.

The event created will be visible to the organisations having an account on this platform, but not synchronised to other MISP instances until it is published.

List Events

Add Event

Import from...

REST client

List Attributes

Search Attributes

View Proposals

Events with proposals

View delegation requests

View periodic summary

Export

Automation

Add Event

Date	Distribution i
<input type="text" value="2025-01-07"/>	<input style="border: none;" type="text" value="This community only"/>
Threat Level i	Analysis i
<input style="border: none;" type="text" value="Medium"/>	<input style="border: none;" type="text" value="Ongoing"/>
Event Info	
<input type="text" value="Distribución troyano Loki mediante campaña de phishing"/>	
Extends Event	
<input type="text" value="Event UUID or ID. Leave blank if not applicable."/>	
<input type="button" value="Submit"/>	

- **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**.

- Edit Event
- Delete Event
- Add Attribute
- Add Object**
- Add Attachment
- Add Event Report
- Populate from...
- Enrich Event
- Merge attributes from...

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:

<input checked="" type="checkbox"/>	Email-body email-body	Body of the email	Payload delivery	Estimado señor	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Inherit event
<input checked="" type="checkbox"/>	Email-body-attachment attachment	Body of the email as an attachment	External analysis	8Y10916.r19	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Inherit event
<input checked="" type="checkbox"/>	Eml attachment	Full EML	External analysis	Browse... Pago.eml	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Inherit event
<input checked="" type="checkbox"/>	From email-src	Sender email address	Payload delivery	dimotikiastinomia@voio.gr	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Inherit event
<input type="checkbox"/>	From-display-name email-src-display-name	Display name of the sender	Payload delivery		<input type="checkbox"/>	<input type="checkbox"/>	Inherit event
<input checked="" type="checkbox"/>	From-domain domain	Sender domain address (when only the source domain is known)	Payload delivery	voio.gr	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Inherit event
<input checked="" type="checkbox"/>	Subject email-subject	Subject	Payload delivery	Confirmación de pago	<input type="checkbox"/>	<input type="checkbox"/>	Inherit event

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.

<input checked="" type="checkbox"/>	Filename filename	Filename on disk	Payload delivery	8Y10916	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Inherit event
<input checked="" type="checkbox"/>	Malware-sample malware-sample	The file itself (binary)	Payload delivery	8Y10916.scrjaf62a7cef3db5f166802e40e9de03953	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Inherit event
<input checked="" type="checkbox"/>	Md5 md5	[Insecure] MD5 hash (128 bits)	Payload delivery	af62a7cef3db5f166802e40e9de03953	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Inherit event
<input type="checkbox"/>	Pattern-in-file pattern-in-file	Pattern that can be found in the file	Payload installation		<input checked="" type="checkbox"/>	<input type="checkbox"/>	Inherit event
<input checked="" type="checkbox"/>	Sha1 sha1	[Insecure] Secure Hash Algorithm 1 (160 bits)	Payload delivery	204a8055e76a27adfd98421e64e54bad2d38ab4	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Inherit event
<input checked="" type="checkbox"/>	Sha256 sha256	Secure Hash Algorithm 2 (256 bits)	Payload delivery	dc4878195313c420686d10517c8e1d908b23aeea8c0cbae69d0	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Inherit event

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

The screenshot shows the MISP interface with two event objects. The first object, dated 2025-01-07, has an object name of 'email-body' and a value of 'Archivo de correo recibido'. The email body text is: 'Estimado señor', 'Se adjunta una copia del pago según las instrucciones de su cliente.', and 'Saludos cordiales!'. The second object, also dated 2025-01-07, has an object name of 'filename' and a value of '8Y10916', with a comment 'Ransom.loki categoria troyano'.

EVENT REPORT.

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

Event Reports

[+ Add Event Report](#) [Generate report from Event](#) [All](#) [Default](#) [Deleted](#)

Name: Distribution:

Content:

El árbol de procesos en el JSON proporcionado muestra una serie de ejecuciones de un archivo llamado "8Y10916.scr.exe" ubicado en la carpeta temporal del usuario. El archivo es ejecutado por un proceso principal con el mismo nombre y ruta. Los programas legítimos pueden utilizar la carpeta temporal para almacenar y ejecutar archivos, por lo que este comportamiento puede considerarse legítimo. Sin embargo, el

[Submit](#) [Cancel](#)

- 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

Publish Event	Threat Level — Medium
Publish (no email)	Analysis Ongoing
Run Ad-Hoc Workflow	Distribution This community only  
Contact Reporter	Published No (last published at 2025-01-07 15:47:48)
Download as...	#Attributes 12 (2 Objects)

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**'

Published	Yes	2025-01-07 18:44:10
------------------	---	---------------------

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