

# 10 Mandamientos de MISP

Recomendaciones y buenas prácticas para codificar información



# Recursos

- Buenas prácticas en Inteligencia de Amenazas
  - <https://www.misp-project.org/best-practices-in-threat-intelligence.html>
- Desde evidencia a información accionable
  - <https://github.com/MISP/misp-training-lea/blob/main/output/e.206-from-evidences-to-actionable-information.pdf>

# Elegir bien el título del Evento

- Usar inglés si piensas que la información será compartida con otros
  - Event.info (título) está dedicado a ser leído por humanos
  - Elige un título **conciso y claro**

Intento fallido de phishing dirigido a compañía de TELCO en LU

VS

Phishing

# Dedicar tiempo a codificar la información

- Es lo que otros usuarios verán, piensa desde su perspectiva
- Facilita el trabajo de filtrado, exportación, agregación
  - Piensa como otros **sistemas** pueden procesar esta información
  - Piensa como otros **humanos** interpretan esta información
- Una vez acostumbrado con la entrada manual de datos, automatizarlo

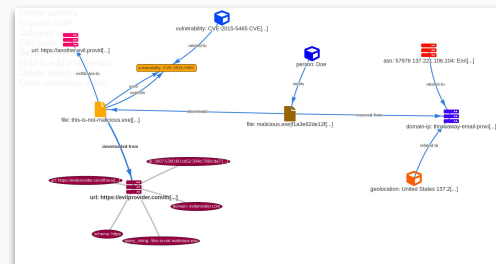
# Priorizar el uso de Objetos frente a Atributos

- Agrupan atributos para **facilitar la lectura**

Category	Type	Value
Payload delivery	email-src	john.doe@luxembourg.edu
Network activity	domain	throwaway-email-provider.com
Network activity	ip-dst	137.221.106.104
Network activity	url	https://evilprovider.com/this-is-not-malicious.exe
Network activity	ip-dst	2607:5300:60:cd52:304b:760d:da7:d5
External analysis	vulnerability	CVE-2015-5465
Network activity	url	https://another.evil.provider.com
Network activity	ip-dst	118.217.182.36

2022-12-06		Object name: url	References: 0	Referenced by: 1
<input type="checkbox"/>	2022-12-06	Network activity	url: url	https://evilprovider.com/this-is-not-malicious.exe
<input type="checkbox"/>	2022-12-06	Network activity	domain: domain	evilprovider.com
<input type="checkbox"/>	2022-12-06	Network activity	ip: ip-dst	2607:5300:60:cd52:304b:760d:da7:d5
<input type="checkbox"/>	2022-12-06	Other	query_string: text	/this-is-not-malicious.exe
<input type="checkbox"/>	2022-12-06	Other	scheme: text	https

- Convierte la información en un **grafo conectado** que cuenta una historia
  - Usar los verbos existentes para las relaciones



- Proveen mayor libertad para **expresar indicadores técnicos no convencionales** gracias a un sistema flexible de plantillas

# Revisar las propiedades to\_ids y correlation

- to\_ids: Es necesario que sea propagado a herramientas de protección?
- correlation: Debería ser correlacionado?

Date	Category	Type	Value	Type	Details	Comment	Correlate	Related Events	Feed Info	IDS	Distribution
2023-02-08	Object name: file										Inspect
	References: 1										
2023-02-08	Payload delivery	filename:	11b1b2375d9d840912cfd1f0d0d04d93ed0cddb0ae4ddb550a5b62cd044d6				<input type="checkbox"/>	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	Inspect
		filename	b66				<input type="checkbox"/>	<input checked="" type="checkbox"/>		<input type="checkbox"/>	Inspect
2023-02-08	Other	size-in-bytes:	48694				<input type="checkbox"/>	<input checked="" type="checkbox"/>		<input type="checkbox"/>	Inspect
		size-in-bytes	47.55 kB				<input type="checkbox"/>	<input checked="" type="checkbox"/>		<input type="checkbox"/>	Inspect
2023-02-08	Other	entropy:	5.686847556779				<input type="checkbox"/>	<input checked="" type="checkbox"/>		<input type="checkbox"/>	Inspect
		float					<input type="checkbox"/>	<input checked="" type="checkbox"/>		<input type="checkbox"/>	Inspect
2023-02-08	Payload delivery	md5:	87b010bc90cd7dd776fb42ea5b3f85d3				<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	Inspect
		md5					<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	Inspect
2023-02-08	Payload delivery	sha1:	f25846f8cda8b0460e1db02ba6d3836ad3721f62				<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	Inspect
		sha1					<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	Inspect
2023-02-08	Payload delivery	sha256:	11b1b2375d9d840912cfd1f0d0d04d93ed0cddb0ae4ddb550a5b62cd044d6				<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	Inspect
		sha256	b66				<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	Inspect
2023-02-08	Payload delivery	sha512:	1e417a9ba4139dda529da11be4140fe492ae7f7652c3cab35a3201e3cf36f56e3dca517b1b891f4148f3c42fb1a836998726500efa7d1ddce9ffd974f6bc648f				<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	Inspect
		sha512					<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	Inspect
2023-02-08	Payload delivery	malware-sample:	11b1b2375d9d840912cfd1f0d0d04d93ed0cddb0ae4ddb550a5b62cd044d6				<input type="checkbox"/>	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	Inspect
		malware-sample	b66 87b010bc90cd7dd776fb42ea5b3f85d3				<input type="checkbox"/>	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	Inspect
2023-02-08	Artifact dropped	mimetype:	application/x-executable				<input type="checkbox"/>	<input checked="" type="checkbox"/>		<input type="checkbox"/>	Inspect
		mime-type					<input type="checkbox"/>	<input checked="" type="checkbox"/>		<input type="checkbox"/>	Inspect
2023-02-08	Payload delivery	ssdeep:	768:wx:BGBTIC4kh9RL0kvRoRzY+0kwKIG8HP6eQPK2:bBUTK+0kwKIG1eQPd				<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	Inspect
		ssdeep					<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	Inspect

# Contextualizar la información

- Comenzar a nivel Evento
  - Los atributos y Objetos **heredan** el contexto
- Añadir contexto a los **Atributos**
  - E.x. servidor c2, URL de exfiltración, técnicas

Country Q  
luxembourg Q

Sector Q  
Telecoms Q

Target Information Q  
Luxembourg Q

Attack Pattern Q  
Spearphishing Attachment - T1566.001 Q  
Phishing - T1566 Q  
Spear phishing messages with malicious attachments - T1367 Q

ttp:amber PAP:AMBER  
phishing:techniques="email-spoofing"  
phishing:distribution="spear-phishing"  
phishing:state="active"  
phishing:psychological-acceptability="medium"  
enisa:nefarious-activity-abuse="spear-phishing-attacks"  
admiralty-scale:source-reliability="b"  
admiralty-scale:information-credibility="2"

VS

ttp:white osint:lifetime="perpetual" osint:certainty="50"  
workflow:state="draft" smo:sync

Prioridades cuando contextualizando:

1. *Reglas de intercambio (audiencia y permisibilidad)*
2. *Tácticas del adversario (MITRE ATT&CK)*
3. Tipo de evento (misp:event-type, event-classification)
4. Si involucra malware → *malware-type / malware-family*
5. Si es un incidente → *Incident Type*

# Acordar qué vocabulario usar, y seguir usándolo

- Utilizar vocabularios normalizados como Taxonomías y Galaxias
- Facilita la interpretación y automatización
- Simplifica la interpretación para otros que reciben la información

TLP AMBER
TLP:AMBER
Threat tlp:Amber
tlp-amber
tlp::amber
tlp:amber

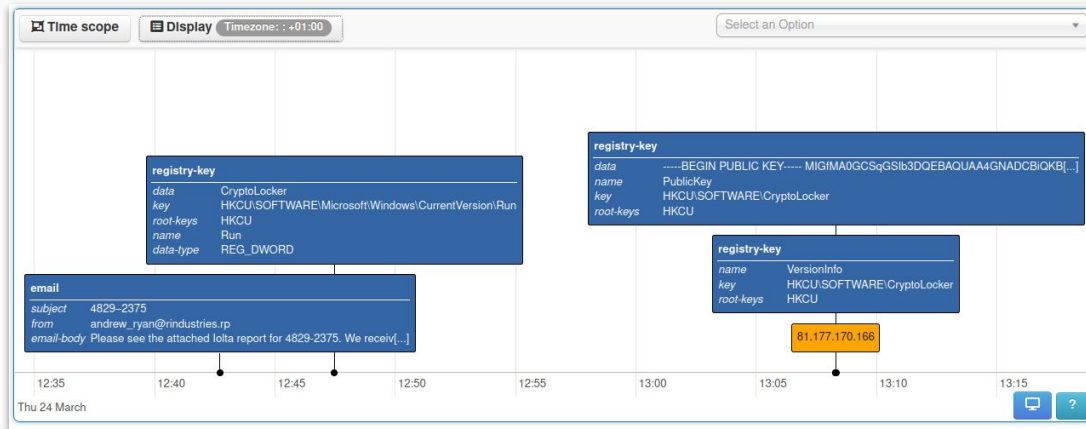
VS

Expanded	Numerical Value	# Events	# Attributes	Tag
(TLP:AMBER) Limited disclosure, recipients can only spread this on a need-to-know basis within their organization and its clients.	337	31		tlp:amber
Limited disclosure, recipients can only spread this on a need-to-know basis within their organization.	0	0		tlp:amber+strict
(TLP:CLEAR) Recipients can spread this to the world, there is no limit on disclosure.	9	1		tlp:clear
(TLP:EX:CHR) Information extended with a specific tag called Chatham House Rule (CHR). When this specific CHR tag is mentioned, the attribution (the source of information) must not be disclosed. This additional rule is at the discretion of the initial sender who can decide to apply or not the CHR tag.	0	0		tlp:ex:chr
(TLP:GREEN) Limited disclosure, recipients can spread this within their community.	148	29		tlp:green
(TLP:RED) For the eyes and ears of individual recipients only, no further disclosure.	13	8		tlp:red
(TLP:WHITE) Information can be shared publicly in accordance with the law.	2535	896		tlp:white



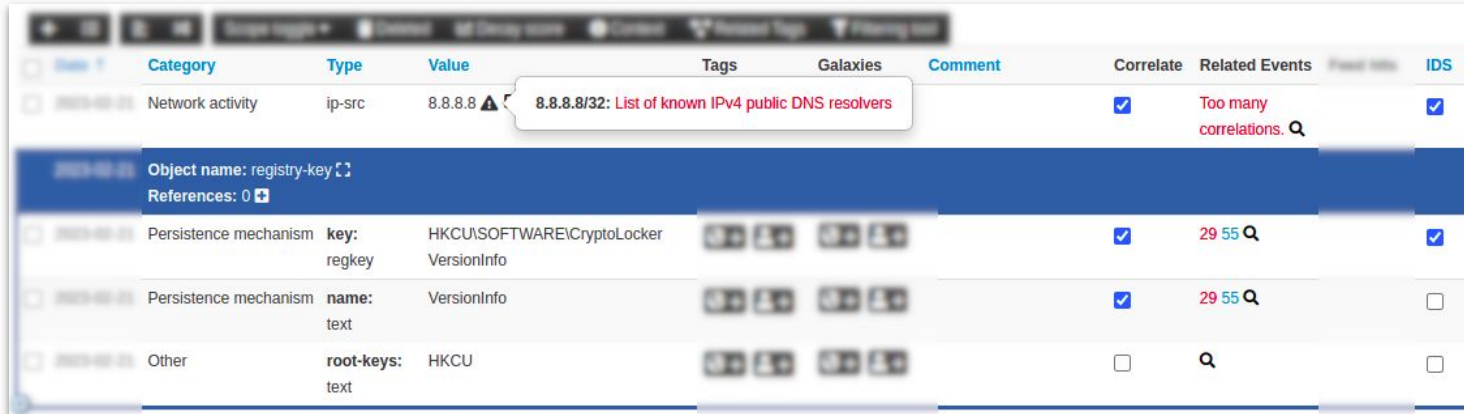
# Añadir el componente de tiempo a las entidades

- Los componentes de tiempo son `first_seen`, `last_seen` y `sightings`
- Beneficio inmediato: líneas de tiempo del incidente/evento
- Útil para ilustrar una serie de acciones o cuándo algo estuvo activo
- El motor de gestión del ciclo de vida de loC utiliza esta información



# Verificar las warninglists y correlation hits

- Coincidencias de warninglists (listas de alertas)
  - Permiten evitar compartir falsos positivos
  - No hacer enojar al SOC
- Correlaciones
  - Pueden dar indicios sobre el contexto
  - También pueden ayudar a detectar falsos positivos (valores sobre-correlacionados)

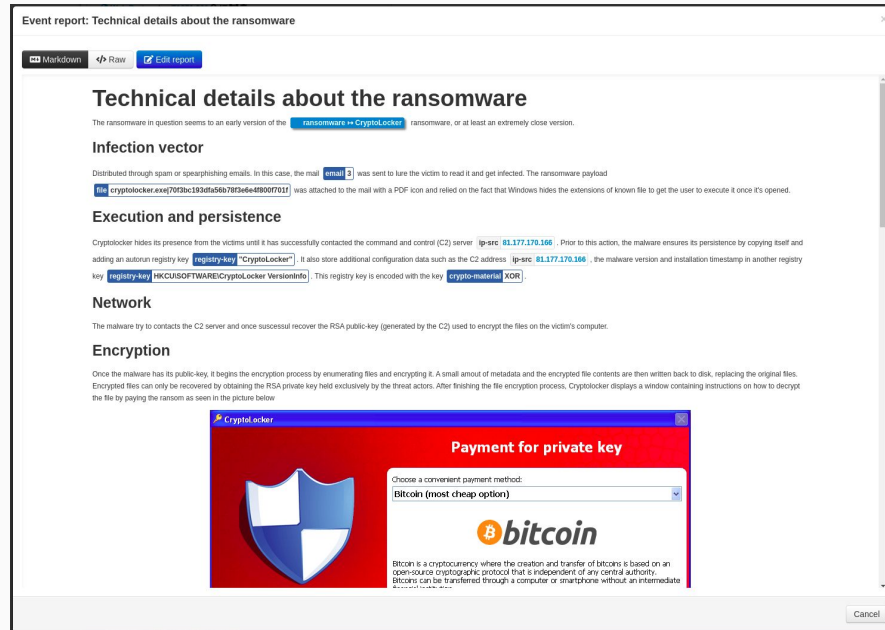


The screenshot shows a security dashboard interface with a table of events. A tooltip is displayed over the 'Value' column of the first row, showing a warning list entry for the IP address 8.8.8.8.

Category	Type	Value	Tags	Galaxies	Comment	Correlate	Related Events	Final Hits	IDS
Network activity	ip-src	8.8.8.8	8.8.8.8/32: List of known IPv4 public DNS resolvers			<input checked="" type="checkbox"/>	Too many correlations.		<input checked="" type="checkbox"/>
Object name: registry-key References: 0									
Persistence mechanism	key: regkey	HKCU\SOFTWARE\CryptoLocker VersionInfo				<input checked="" type="checkbox"/>	29 55		<input checked="" type="checkbox"/>
Persistence mechanism	name: text	VersionInfo				<input checked="" type="checkbox"/>	29 55		<input type="checkbox"/>
Other	root-keys: text	HKCU				<input type="checkbox"/>			<input type="checkbox"/>

# Crear una descripción del evento en el Reporte de Evento

- Los reportes tienen como objetivo ser leídos por humanos, no sistemas
- Son utilizados por operadores o analistas para comprender en profundidad un evento



**Event report: Technical details about the ransomware**

Markdown Raw Edit report

## Technical details about the ransomware

The ransomware in question seems to be an early version of the `ransomware` `Cryptolocker` ransomware, or at least an extremely close version.

### Infection vector

Distributed through spam or spearfishing emails. In this case, the mail `email` was sent to lure the victim to read it and get infected. The ransomware payload `cryptolocker.exe{702bc192d56b7892e6449807011}` was attached to the mail with a PDF icon and relied on the fact that Windows hides the extensions of known file to get the user to execute it once it's opened.

### Execution and persistence


Cryptolocker hides its presence from the victims until it has successfully contacted the command and control (C2) server `ip-arc: 81.177.170.106`. Prior to this action, the malware ensures its persistence by copying itself and adding an autorun registry key `registry-key "Cryptolocker"`. It also store additional configuration data such as the C2 address `ip-arc: 81.177.170.106`, the malware version and installation timestamp in another registry key `registry-key HKCUSOFTWARE\Cryptolocker\VersionInfo`. This registry key is encoded with the key `crypto-material XOR`.

### Network

The malware by contacts the C2 server and once successful recover the RSA public-key (generated by the C2) used to encrypt the files on the victim's computer.

### Encryption

Once the malware has its public-key, it begins the encryption process by enumerating files and encrypting it. A small amount of metadata and the encrypted file contents are then written back to disk, replacing the original files. Encrypted files can only be recovered by obtaining the RSA private key held exclusively by the threat actors. After finishing the file encryption process, Cryptolocker displays a window containing instructions on how to decrypt the file by paying the ransom as seen in the picture below.



**Cryptolocker**

**Payment for private key**

Choose a convenient payment method:  
Bitcoin (most cheap option)

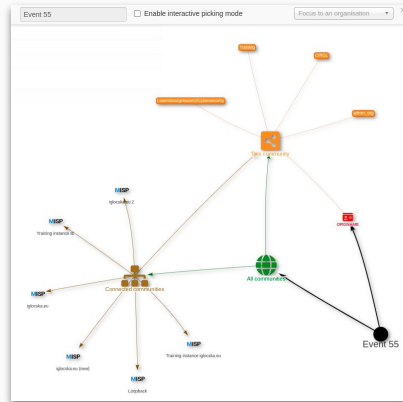
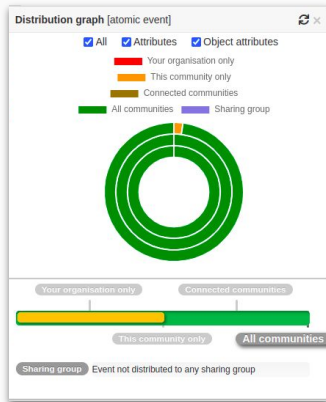
**bitcoin**

Bitcoin is a cryptocurrency where the creation and transfer of bitcoins is based on an open-source cryptographic protocol that is independent of any central authority. Bitcoins can be transferred through a computer or smartphone without an intermediate

Cancel

# Revisar el nivel de distribución y publicar

- Evitar filtración de datos y asegurar que la información será compartida debidamente
  - Proteger potenciales víctimas, ocultar referencias internas
  - Consejo: Comenzar con un nivel restrictivo y ampliarlo luego



- Publicar el evento es necesario para:
  - Sincronizar con otras instancias de MISP
  - Notificar a la comunidad
  - Exponer la información para poder ser utilizada por sistemas externos

### Publish Event

Are you sure this event is complete and everyone should be informed?

▼ Servers

- Loopback: **Event will be pushed**
- iglowska.eu: The server rules blocks it from being pushed.
- iglowska.eu (new): **Event will be pushed**
- Training instance iglowska.eu: **Event will be pushed**

# 10 Mandamientos de MISP

## Deberás:

1. Elegir bien el título del evento
2. Dedicar tiempo a codificar la información
3. Priorizar Objetos frente a Atributos
4. Revisar las propiedades **to\_ids** y **correlation**
5. Contextualizar la información
6. Acordar qué vocabulario usar, y seguir usándolo
7. Añadir el componente de tiempo a las entidades
8. Verificar las warninglists y correlation hits
9. Crear un descripción del evento en el Reporte de Evento
10. Revisar el nivel de distribución y publicar

