

MISP Ten Commandments

Recommendations and Best Practices when encoding data



Resources

- Best practices in threat intelligence document
 - <https://www.misp-project.org/best-practices-in-threat-intelligence.html>
- From evidences to actionable information
 - <https://github.com/MISP/misp-training-lea/blob/main/output/e.206-from-evidences-to-actionable-information.pdf>

Choose the Event title wisely

- Use English if you ever think the data will be shared with others
 - Event.info is meant for human
 - **Concise & self-explanatory** title

Failed spear phishing attempt targeting telco company in LU

VS

Phishing

Take your time to properly encode data

- This is what everyone see and get notified about
- Make things easier to filter, export, aggregate and compute trends
 - **Think machine** processing the data
 - **Think human** consuming the data
- Once you are at ease with the manual work, automate it!

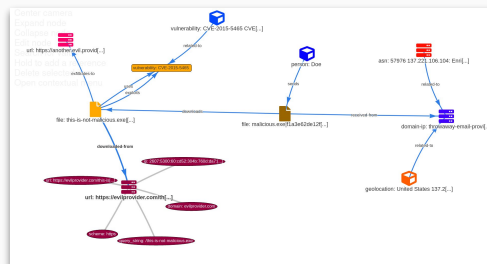
Prefer to use object rather than attributes

- You can group attribute and make things **more readable**

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

- You can turn flat data into a **connected graph** that tells a story
 - Try to use existing verbs if possible



- You have more freedom to **express non-standard** technical indicators thanks to the flexible templating system

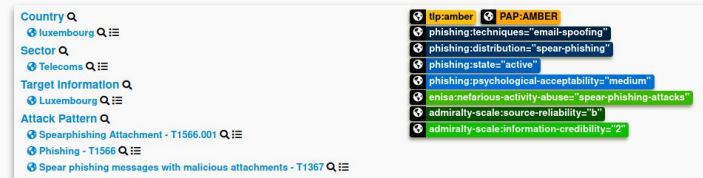
Review the to_ids & correlation flags

- to_ids: Should it be marked to be used for automation and fed to protective tools
- correlation: Should it (not?) correlate

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:	1e417a9ba4139dda529da11be4140fe492ae77652c3cab35a3201e3cf36f56e3dca517b1b891f4148f3c42fb1a836998726500efa7d1ddce9ff974f6bc648f				<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:wcxBGTIC4kh9RL0kvRoRzY+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

Contextualize your data

- Start with the Event
 - Attributes and Objects **inherit** the parent's context
- If possible, **add context to attributes** as well
 - E.g. c2 server, exfiltration URL, techniques



VS



Priority when contextualizing:

1. *Releasability and Permissible Actions*
2. *Adversarial Tactics, Techniques and Common Knowledge (ATT&CK)*
3. Event class (misp:event-type, event-classification)
4. If malware involved → *malware-type / malware-family*
5. If incident → *Incident Type*

Agree on which vocabulary to use, and keep using it

- Use normalized vocabularies such as **Taxonomy & Galaxy**
- It makes life easier for you to **understand** and **automate**
- It simplifies the lives of the **recipients** as well

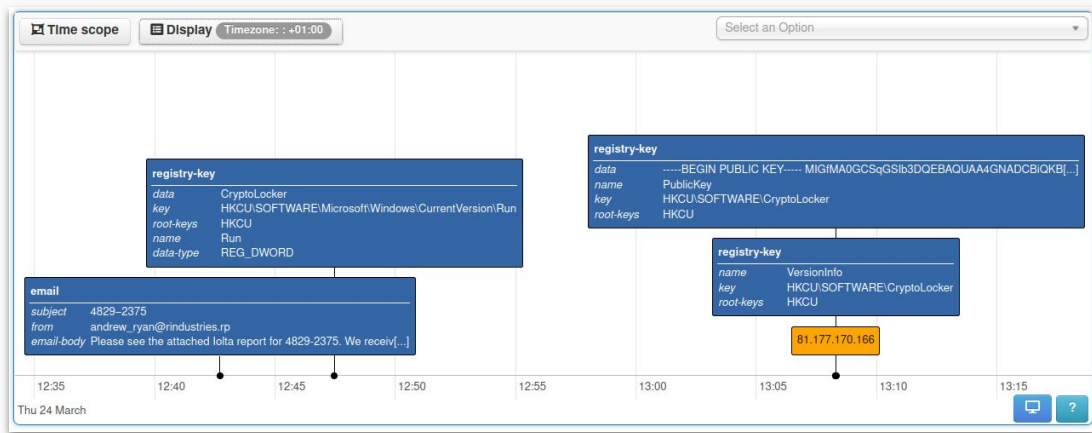
TLP AMBER
TLP:AMBER
Threat tlp:Amber
tlp-amber
tlp::amber
tlp:amber

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

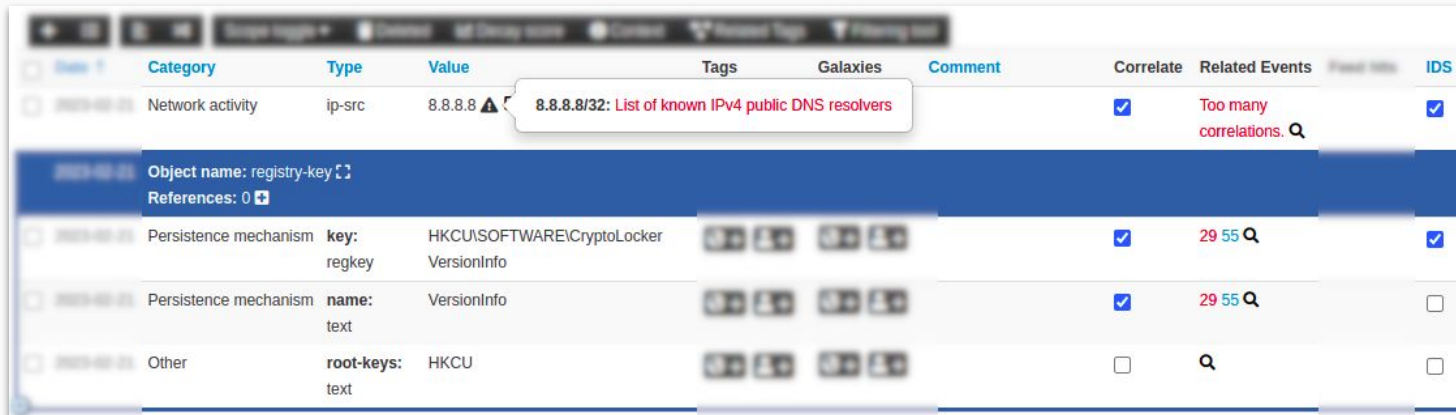
Add a time component to entities




















- Time components can be `first_seen`, `last_seen` and `sightings`
- You get **automatic timelines** for free
- Handy to illustrate a series of actions or when something was active
- The IoC **life-cycle** management system can leverage these data points



Check the warninglist and correlation hits

- Warninglist hits
 - Allow to avoid common false positives
 - Do not make SOC and partners angry
- Correlation hits
 - Might give more hint about the context
 - Can also detect other false positives



Category	Type	Value	Tags	Galaxies	Comment	Correlate	Related Events	Feed 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"/>

Create a small write-up with an event report

- Event reports cannot be consumed by automation system
- But, they can be used by operators or analysts to obtain a **comprehensive understanding** of the event

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 `file cryptolocker.exe[7073bc193af5467873de4ff007931]` 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-addr: 81.177.178.166`. Prior to this action, the malware ensures its persistence by copying itself and adding an autorun registry key `registry-key "CryptLocker"`. It also store additional configuration data such as the C2 address `ip-addr: 81.177.178.166`, the malware version and installation timestamp in another registry key `registry-key HKCU\SOFTWARE\CryptLocker\VersionInfo`. This registry key is encoded with the key `crypto-material XOR`.

Network

The malware try to 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

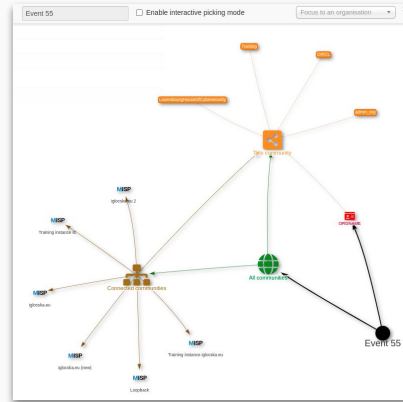
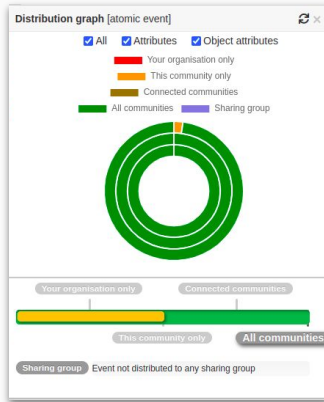
Once the malware has its public-key, it begins the encryption process by enumerating files and encrypting it. A small amount of metadata and the encrypted file contents are then written back to disk, replacing the original files. Encrypted files can only be recovered by obtaining the RSA private key 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



Cancel

Review distribution and publish

- Avoid data leak & make sure everything will be **shared as intended**
 - Protect potential victims, hide internal references, ...
 - Hint: Start with strict distribution level and make it more permissive later on



- Publishing is needed for
 - Synchronization to other MISP instances
 - Notifying the community
 - Exposing the data to be consumed by automation system

Publish Event

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

▼ Servers

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

MISP Ten Commandments

Thou shalt:

1. Choose the Event title wisely
2. Take your time to properly encode data
3. Prefer to use object rather than attributes
4. Review the `to_ids` & correlation flags
5. Contextualize your data
6. Agree on which vocabulary to use, and keep using it
7. Add a time component to entities
8. Check the warninglist and correlation hits
9. Create a small write-up with an event report
10. Review distribution and publish

