Mapping investigations and cases in MISP

E.205

CIRCL Computer Incident Response Center Luxembourg

MISP Project
https://www.misp-project.org/

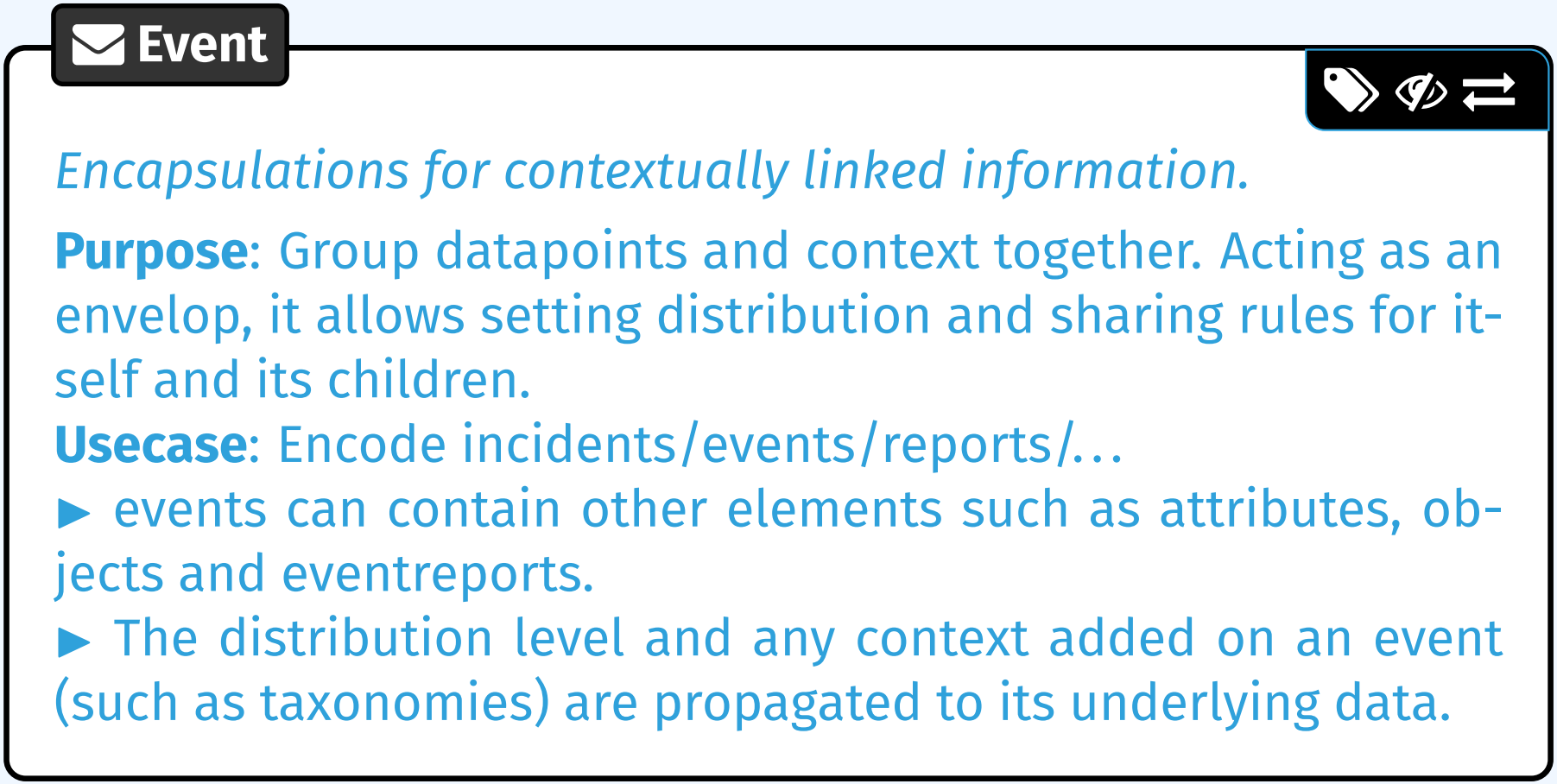
March 25, 2022 - v0.7

Objectives of this module

- Recap on MISP data model and distribution levels
- Data from cases to be structured and encoded:
  - **Network indicators**: `ip`, `domain`, `url`, ...
  - **Files and binaries**: non-malicious / malicious `payload`
  - **Emails**: `content`, `header`, `attachment`, ...
  - **Web**: URL, `cookies`, `x509`
  - **Cryptographic materials**: public / private `key`, `certificate`
  - **Infrastructure and devices**
  - **Financial fraud**: `bank-account`, `phone-number`, `btc`
  - **Person**: `name`, `online accounts`, `passport`, `visa`
  - **Support tools**: `yara`, detection/remediation scripts
  - **Vulnerabilities**: `cve`
  - **External analysis**: Reports, blogpost, ransome notes
- Relationships and timeliness
- Enrichments via module and correlation
- Preparing data for sharing with other LE partners, CSIRT, SOC

MISP Data model and distribution levels

MISP Event



Encapsulations for contextually linked information.

Purpose: Group datapoints and context together. Acting as an envelop, it allows setting distribution and sharing rules for itself and its children.

Usecase: Encode incidents/events/reports/...

- events can contain other elements such as attributes, objects and eventreports.
- The distribution level and any context added on an event (such as taxonomies) are propagated to its underlying data.

MISP Attribute

Attribute

Basic building block to share information.

Purpose: Individual data point. Can be an indicator or supporting data.
Usecase: Domain, IP, link, sha1, attachment, ...

- attributes cannot be duplicated inside the same event and can have sightings.
- The difference between an indicator or supporting data is usualy indicated by the state of the attribute's `to_ids` flag.

MISP Object

Advanced building block providing attribute compositions via templates.

Purpose: Groups attributes that are intrinsically linked together.
Usecase: File, person, credit-card, x509, device, ...
▶ objects have their attribute compositions described in their respective template. They are instanciated with attributes and can reference other attributes or objects.
▶ MISP is not required to know the template to save and display the object. However, *edits* will not be possible as the template to validate against is unknown.

MISP Relationships (aka object reference)

↗ Object Reference

Relationships between individual building blocks.

Purpose: Allows to create relationships between entities, thus creating a graph where they are the edges and entities are the nodes.

Usecase: Represent behaviours, similarities, affiliation, …

▶ references can have a textual relationship which can come from MISP or be set freely.

MISP Event report

Event Report

Advanced building block containing formated text.

Purpose: Supporting data point to describe events or processes.

Usecase: Encode reports, provide more information about the event, ...

▶ Event reports are markdown-aware and include a special syntax to reference data points or context.

General rule of thumb

Which structure should be used when encoding data?

- **Attribute** vs **Object**
  - If the value is contextually linked to another element or is a subpart of a higher concept, an **object** should be used
  - If the value is part of a large list of atomic data, an **attribute** should be used
- **`Annotation` Object** vs **Event Report**
  - If it is possible to encode the text (raw text or markdown), an **event report** is prefered
  - If the text is written in a specific format (e.g pdf, docx), an **`annotation` object** should be used

Case study 1: Scam call

Case study 1: Scam call

Case: A victim was asked to transfer money to a novice scammer

Chronology - 2022-03-24

11:42:43 UTC+0: Scammer called the victim pretending to be a microsoft employee

11:47:27 UTC+0: Scammer convinced the victim to be helped via remote desktop assistance

12:06:32 UTC+0: Scammer downloaded the binary on the victim's computer

12:08:18 UTC+0: Scammer installed the binary on the victim's computer

12:17:51 UTC+0: Scammer asked the victim to transfer money on a bank account for the help he provided

12:25:04 UTC+0: Victim executed the money transfer

2022-03-25 08:39:21 UTC+0: Victim contacted police

Case study 1: Scam call

Collected evidences

- RDP Log file
- installed binary
- victim's browser history
- bank account statement
- victim's phone call log

Data extracted from evidences

- Scammer's **ip address**
- Potentially **malicious binary**
- **URL** (and **domain**) from which the binary was downloaded
- Scammer's **bank account** and **phone number**
- Scammer's full name and nationality

Case study 1: Scam call

Extracted values

- `194.78.89.250`
  - ip-address from log file
- `bin.exe`
  - downloaded binary
- `https://zdgyot.ugicok.ru/assets/bin.exe`
  - download URL
- `GB 29 NWBK 601613 31926819`
  - IBAN number
  - Swift: `NWBK`, Account number: `31926819`, Currency: GBP
- `+12243359185`
  - phone number
- `Wallace Breen` is from `GB`
  - name and nationality

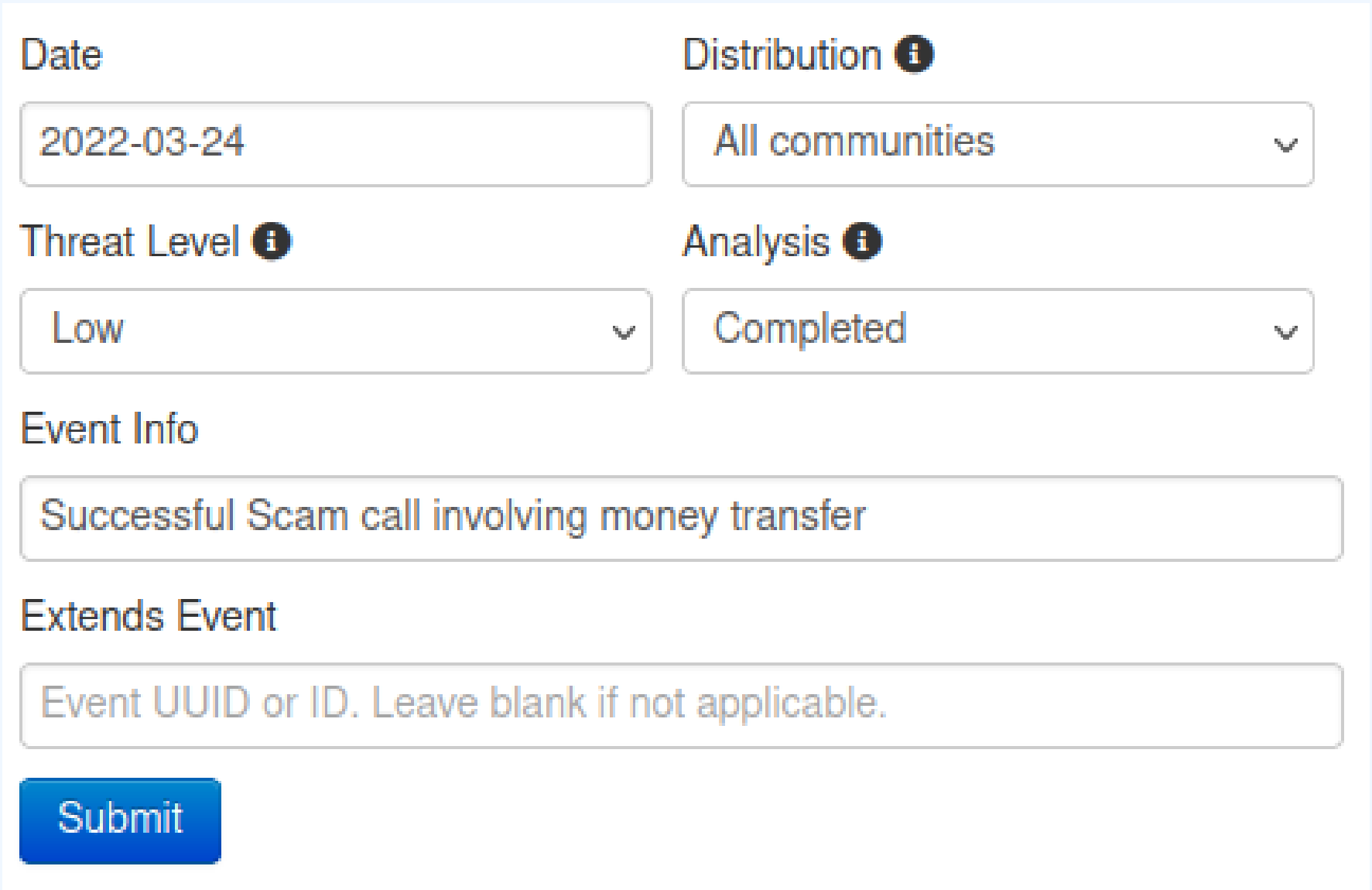
Case study 1: Scam call

Tasks

- Create an new *event* to be shared with **all**
- Encode `binary` to be shared with **CSIRT**
- Encode `ip address` to be shared with both **ISP** and **CSIRT**
- Encode `domain` and `url` to be shared with both **ISP** and **CSIRT**
- Encode `bank account` to be shared with **Financial sector**
- Encode `phone number` to be shared with **Telecomunication sector**
- Encode `full name` and `nationality` to be shared with **LEA only**
- Add relationships to recreate the events
- Add time component to recreate the chronology
- Perform enrichments on the binary, and domain
- Add contextualization
- Create a small write-up as an *event report*
- Review the distribution level and publish

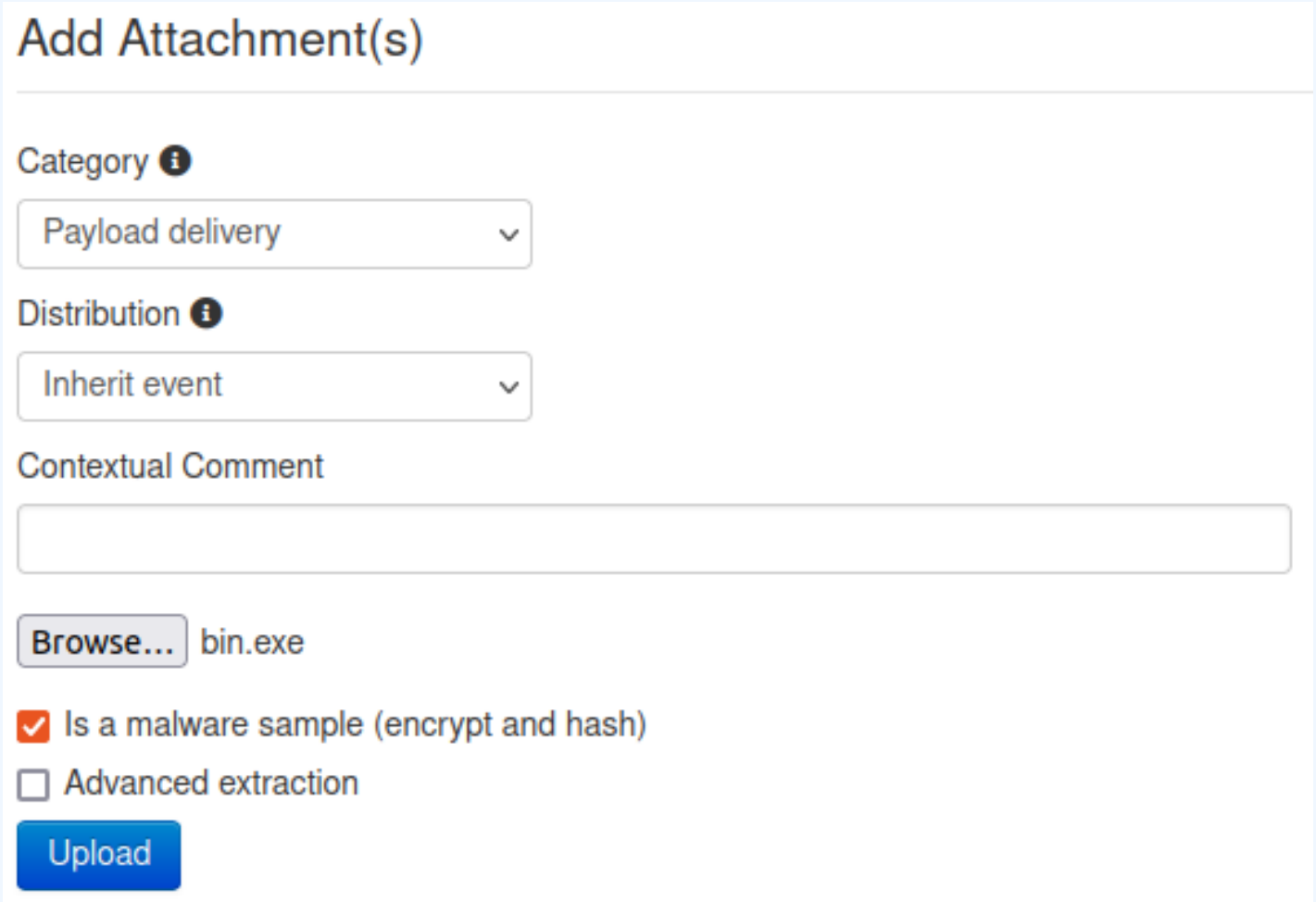
Case study 1: Scam call

- Creating the *event* in MISP



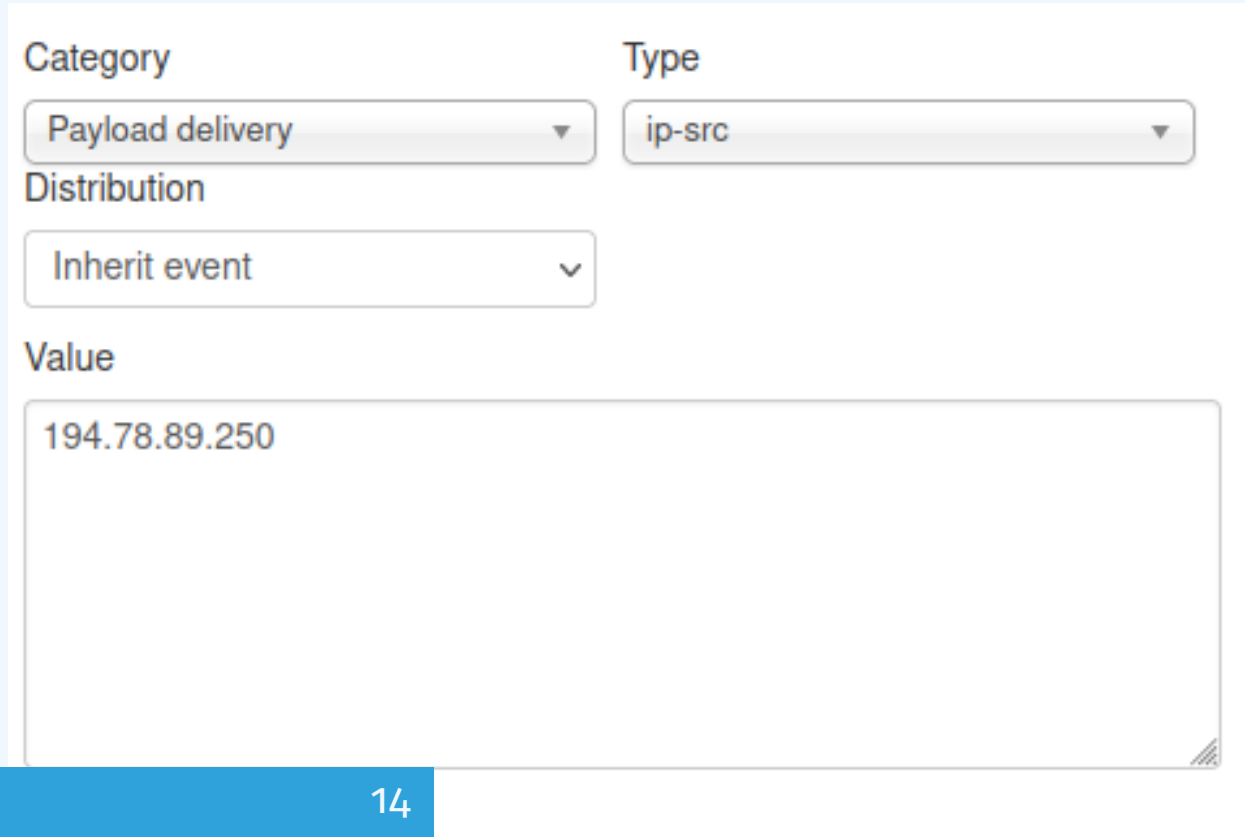
Case study 1: Scam call

- Adding the binary as attachment
- Pick the `Payload Delivery` category
- Check *Is a malware sample*



Case study 1: Scam call

- Encode the IP address of the scammer with an *attribute*
- Pick the `Payload Installation` category and `ip-src` `type`
- Check the `For Intrusion Detection System`
- Add a contextual comment such as: `IP address of the scammer collected from the RDP log file`



Case study 1: Scam call

- Encode the domain and the URL from which the binary was downloaded
- As these two attributes are contextually linked between each others, we should use an URL *object*
- Add a contextual comment such as: `URL used by the scammer to download the binary`
- Include at least: `url`, `domain` and `ressource_path`

Case study 1: Scam call

Object pre-save review

Make sure that the below Object reflects your expectation before submitting it.

Name	url
Template version	9
Meta-category	network
Distribution	Inherit event
Comment	URL used by the scammer to download the binary
First seen	2022-03-24T12:06:32.000000+00:00
Last seen	

Attribute	Category	Type	Value	To IDS
url	Network activity	url	https://zdgyot.ugic0k.ru/assets/bin.exe	Yes
domain	Network activity	domain	zdgyot.ugic0k.ru	Yes
domain_without_tld	Other	text	zdgyot.ugic0k	No
resource_path	Other	text	/assets/bin.exe	No
scheme	Other	text	https	No
tld	Other	text	ru	No

Update object | Back to review | Cancel

Case study 1: Scam call

- Encode the bank account
- As these 4 attributes are contextually linked between each others, we should use an `bank-account` *object*
- Add a contextual comment such as: `Bank account that received the money. Supposed to belong to the scammer`
- Include at least: `iban`, `swift`, `account` and `currency_code`

Case study 1: Scam call

Object pre-save review

Make sure that the below Object reflects your expectation before submitting it.

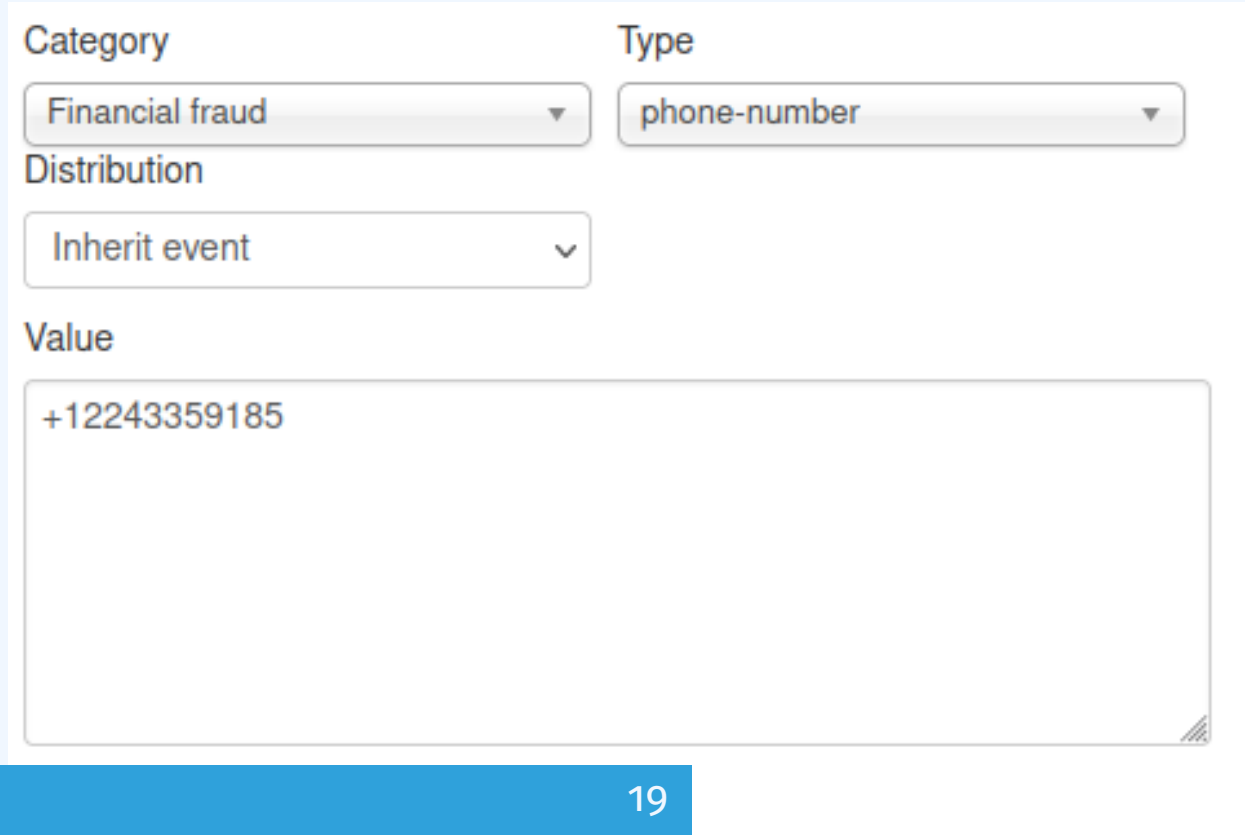
Name	bank-account
Template version	3
Meta-category	financial
Distribution	Inherit event
Comment	Bank account that received the money. Supposed to belong to the scammer
First seen	
Last seen	

Attribute	Category	Type	Value	To IDS
iban	Financial fraud	iban	GB29NWBK60161331926819	Yes
swift	Financial fraud	bic	NWBK	Yes
account	Financial fraud	bank-account-nr	31926819	Yes
currency-code	Other	text	GBP	No

Update object | Back to review | Cancel

Case study 1: Scam call

- Encode the phone number
- Pick the `Financial Fraud` category and `phone-number` `type`
- Add a contextual comment such as: `Phone number used by the scammer to call the victim`
- Check *For Intrusion Detection System*



Case study 1: Scam call

- Encode the full name and nationality
- As these attributes are contextually linked between each others, we should use a `person` *object*
- Add a contextual comment such as: `Name of the scammer given to the victim`
- Include at least: `full-name`, `nationality` and `role`

Case study 1: Scam call

Object pre-save review

Make sure that the below Object reflects your expectation before submitting it.

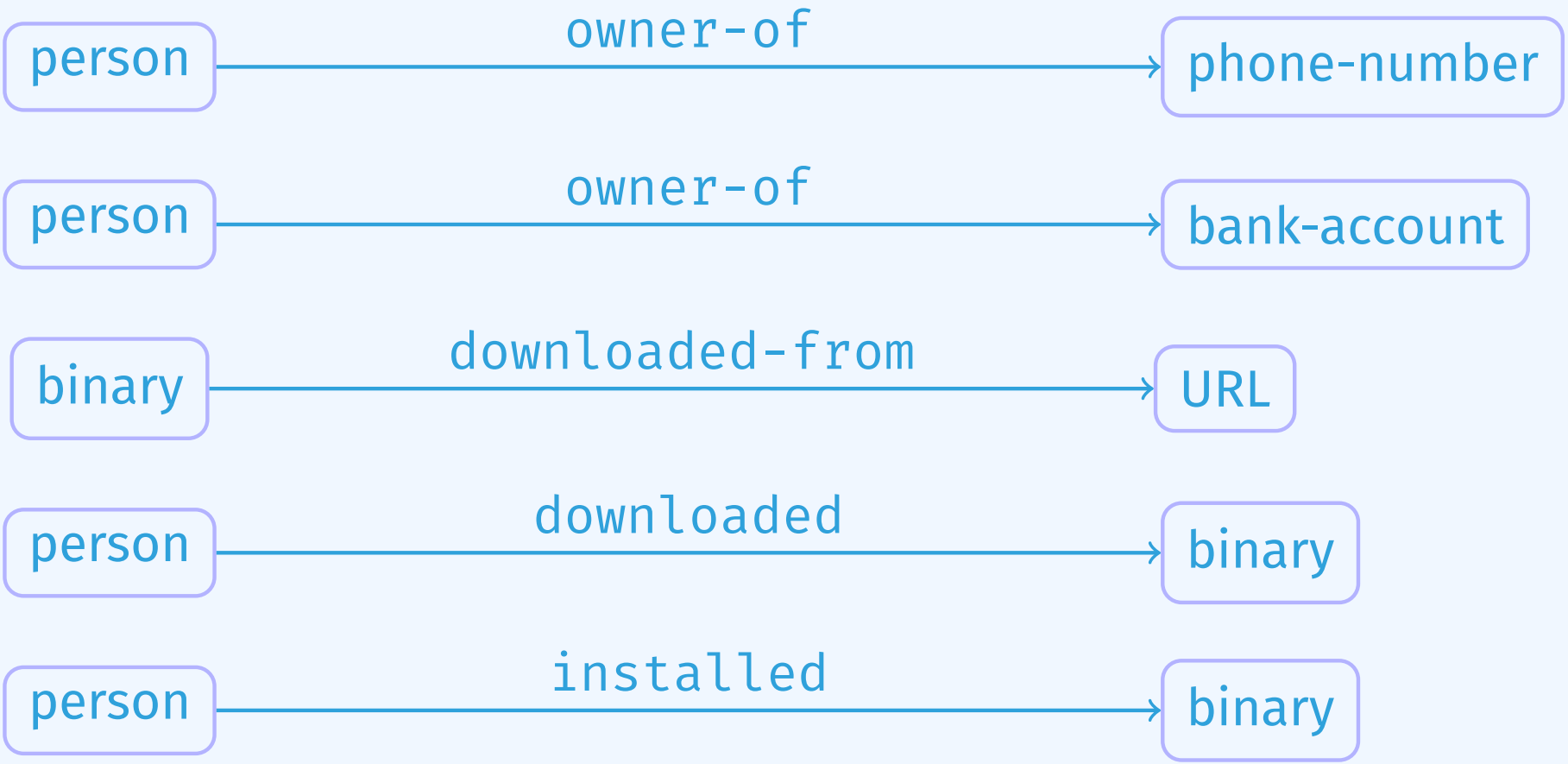
Name	person
Template version	16
Meta-category	misc
Distribution	Inherit event
Comment	Name of the scammer given to the victim. Name confirmed to be the owner of the bank account and phone number
First seen	
Last seen	

Attribute	Category	Type	Value	To IDS
last-name	Person	last-name	Breen	No
full-name	Person	full-name	Wallace Breen	No
first-name	Person	first-name	Wallace	No
role	Other	text	Accused	No
gender	Person	gender	Male	No
nationality	Person	nationality	British	No

Update object | Back to review | Cancel

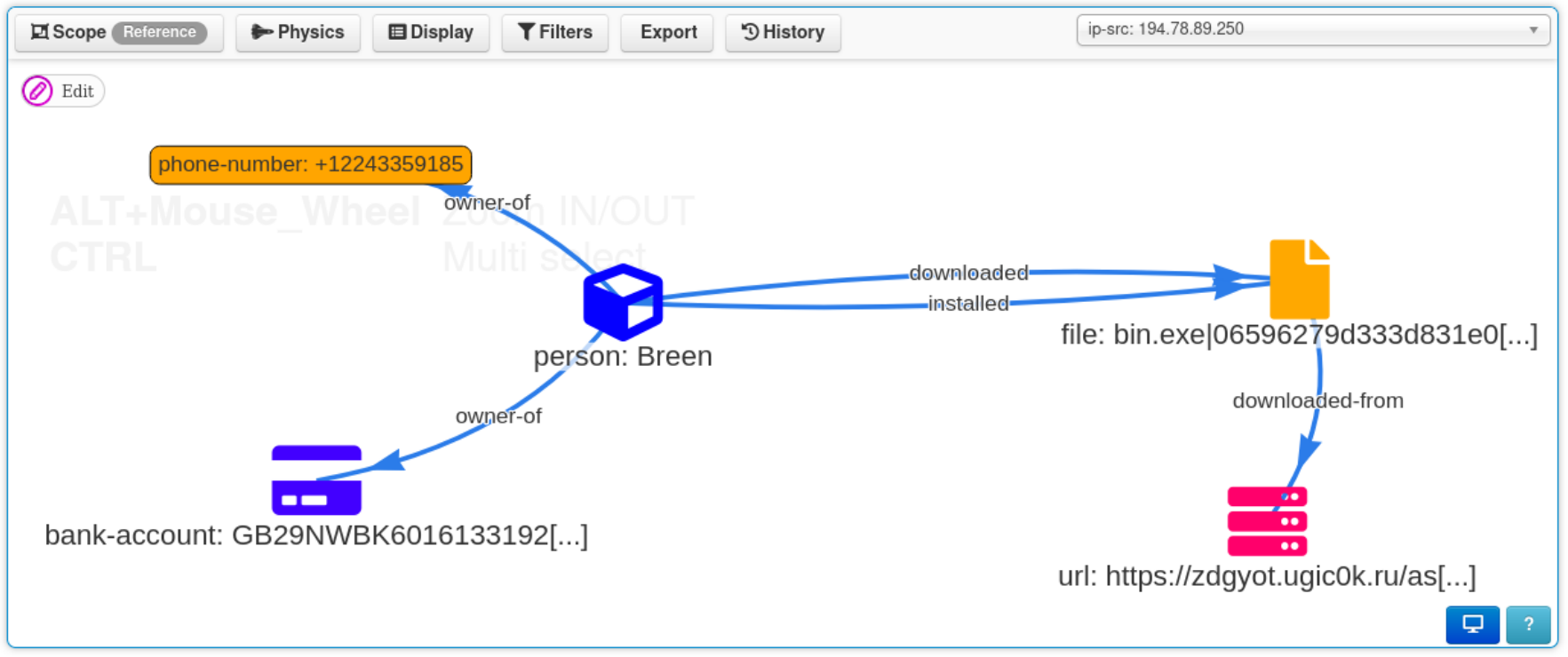
Case study 1: Scam call

Add relationships to recreate the story



Case study 1: Scam call

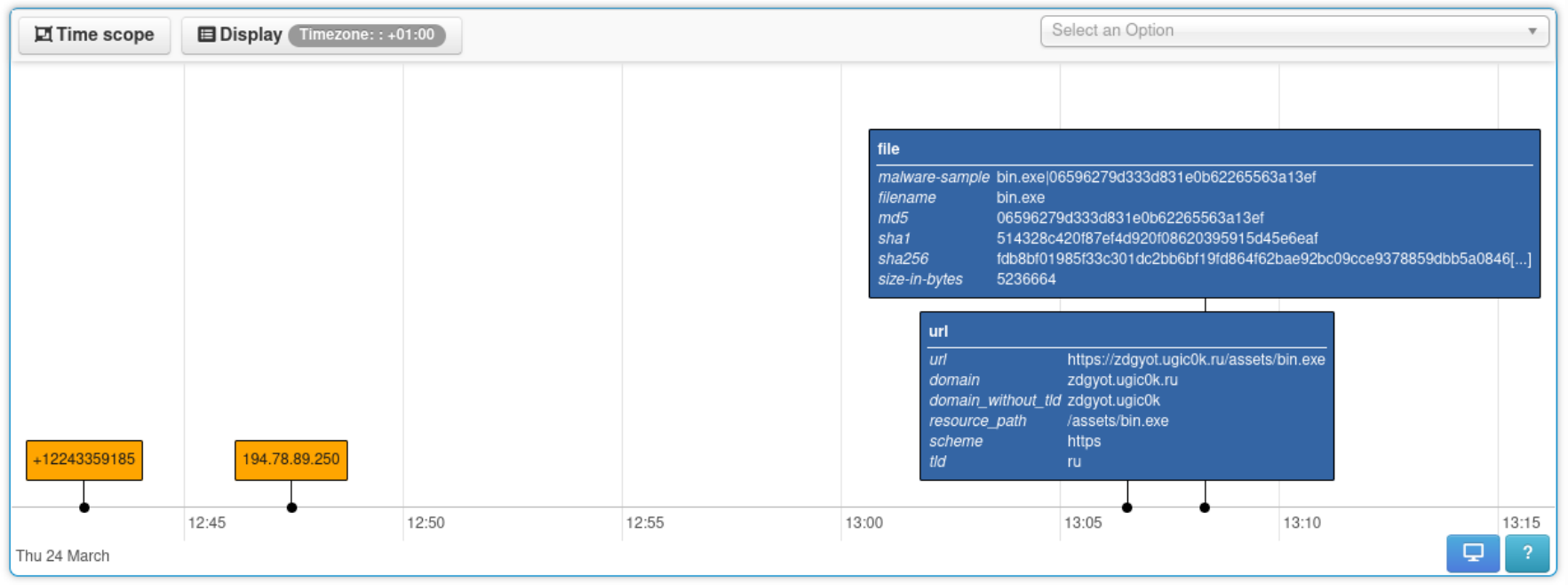
Add relationships to recreate the story



Case study 1: Scam call

Add time component to recreate the chronology

- Main focus is the Cyber Threat Intelligence (CTI) aspect



Case study 1: Scam call

Perform enrichments

- Scammer IP address to get its location
- Binary to check if it's an existing (and malicious) application

Mmdb Lookup:

Object: geolocation

country	Belgium
countrycode	BE
latitude	50.8333
longitude	4
text	db_source: GeoOpen-Country. build_db: 2022-02-05 10:37:33. Latitude and longitude are country average.

Object: geolocation

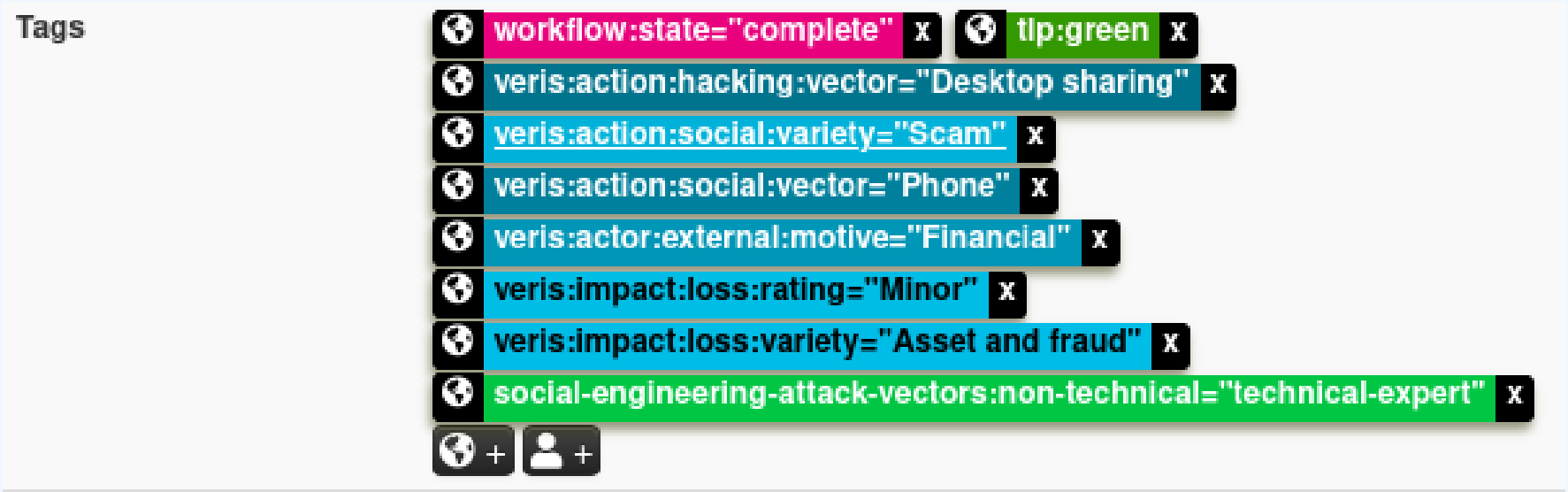
country	Belgium
countrycode	BE
latitude	50.8333
longitude	4
text	db_source: GeoOpen-Country-ASN. build_db: 2022-02-06 09:30:25. Latitude and longitude are country average.

Object: asn

Case study 1: Scam call

- Contextualizing the data
- Different country / sectors might use different nomemclature
- Suggestions for tagging:
  - `circl:incident-classification="scam"`
  - `social-engineering-attack-vectors:non-technical="technical-expert"`
  - `veris:action:hacking:vector="Desktop sharing"`
  - `veris:action:malware:vector="Direct install"`
  - `veris:action:social:variety="Scam"`
  - `veris:action:social:vector="Phone"`
  - `veris:actor:external:motive="Financial"`
  - `veris:impact:loss:rating="Minor"`
  - `veris:impact:loss:variety="Asset and fraud"`
  - `workflow:state="complete"`
  - `tlp:green`

Case study 1: Scam call



Case study 1: Scam call

Create a small write-up as an *event report*

- Create the *event report* with a concise name
- Example: Executive summary of the case
  - Leave its content empty as it can be edited with more ease in the editor afterward
- Write a summary with
  - Quick chronology
  - Written explanation of the steps tooks by the scammer
  - Reference to existing *attributes* or *objects* whenever possible
    - The special syntax is: `@[scope]{uuid}`

Case study 1: Scam call

Create a small write-up as an *event report*

Executive summary of the case

A victim was called by the suspected scammer person Wallace Breen using the following number: phone-number +12243359185 . The scammer prentended to be a a microsoft employee, managed to convince the victim that he could help by using remote desktop assistance.

Once he had access, the scammer downloaded a binary file bin.exe from the following url url https://zdgyot.ugic0k.ru/assets/bin.exe . He then proceed to install the binary, probably to use it a backdoor for future access.

After the installation, he asked the victim to transfer money to the scammer bank account: bank-account ↦ iban GB29NWBK60161331926819

The day after, the victim suspecting a scam contacted the police.

Technique used

Social vector	veris:action:social:vector="Phone"
Potential hacking vector	veris:action:hacking:vector="Desktop sharing"
Actor motive	veris:actor:external:motive="Financial"
Impacted loss	veris:impact:loss:variety="Asset and fraud"
Loss rating	veris:impact:loss:rating="Minor"

Information collected after analysis

- According to the phone number, IP address and bank account, the scammer person Wallace Breen is very likely based in geolocation ↦ country Belgium .

Timeline

- **2022-03-25 11:42:43 UTC+0**: Scammer called the victim pretending to be a microsoft employee
- **2022-03-25 11:47:27 UTC+0**: Scammer convinced the victim to be helped via remote desktop assistance
- **2022-03-25 12:06:32 UTC+0**: Scammer downladed the binary on the victim's computer
- **2022-03-25 12:08:18 UTC+0**: Scammer installed the binary on the victim's computer
- **2022-03-25 12:17:51 UTC+0**: Scammer asked the victim to transfer money on a bank account for the help he provided
- **2022-03-25 12:25:04 UTC+0**: Victim executed the money transfer

Case study 1: Scam call

Review the distribution level and publish

- In our case, we consider the following MISP network topology
- The current instance is owned and managed by a LEA
- The current instance is connected to a central MISP instance acting as a "hub"
- The "hub" is connected to various other MISP instances such as other LEAs, CSIRTs, Financial and telecom institutions

Case study 1: Scam call

Review the distribution level and publish

- `binary file`: **All communities**
- `person`: **LEA Sharing group**
- `geolocation`: **LEA Sharing group**
- `ip`: **LEA Sharing group**
  - The IP might be reassigned
- `phone`
  - If part of a telco sharing group **Telco Sharing group**
  - **Connected communities** otherwise
- `bank account`
  - If part of a financial sharing group **Financial Sharing group**
  - **Connected communities** otherwise

$\rightarrow$ **Publish the event!**

Case study 2: Ransomware

Case study 2: Ransomware

Case: xxxx

Chronology - 2022-03-24

- **11:42:43 UTC+0:**
- **11:47:27 UTC+0:**
- **12:06:32 UTC+0:**
- **12:08:18 UTC+0:**
- **12:17:51 UTC+0:**
- **12:25:04 UTC+0:**
- **2022-03-25 08:39:21 UTC+0:**

Case study 2: Ransomware

Collected evidences

- x

Data extracted from evidences

- x

Case study 1: Scam call

Extracted values

- x
  - x

Case study 2: Ransomware

Tasks

- Create an new *event* to be shared with **all**
- Encode data to be shared
- Add relationships to recreate the events
- Add time component to recreate the chronology
- Perform enrichments on the binary, and domain
- Add contextualization
- Create a small write-up as an *event report*
- Review the distribution level and publish