

Disinformation during a pandemic

lesson's learnt from the MISP COVID-19 community

CIRCL / Team MISP Project

MISP Project

<https://www.misp-project.org/>

ISED 2021



MISP
Threat Sharing

- COVID-19 MISP is a MISP instance retrofitted for COVID-19 info sharing
- We are focusing on two areas of sharing:
 - ▶ **Medical** information
 - ▶ **Cyber threats** related to / abusing COVID-19
- Low barrier of entry, aiming for wide spread
- Already a **massive community** - 1560 users

- We are obviously interested on a personal level, as is everyone
- **Information sharing is what we do anyway**
- The tools that we are building are expanding our capabilities for the future
- Bridging different domains affected in different ways can reveal correlations

WHO IS THIS MEANT FOR?

- Anyone wanting to gain **situational awareness** for the current situation
- Security practitioners trying to fend off covid related attacks
- Those wanting to share, collaborate, visualise, automate data
- All data is contextualised as **either medical or security** related information for easy filtering

WHAT IS MISP?

- MISP¹ is a threat information sharing free & open source software.
- MISP has **a host of functionalities** that assist users in creating, collaborating & sharing threat information - e.g. flexible sharing groups, **automatic correlation**, free-text import helper, event distribution & proposals.
- Many export formats which support IDses / IPses (e.g. Suricata, Bro, Snort), SIEMs (eg CEF), Host scanners (e.g. OpenIOC, STIX, CSV, yara), analysis tools (e.g. Maltego), DNS policies (e.g. RPZ).
- A rich set of MISP modules² to add expansion, import and export functionalities.

¹<https://github.com/MISP/MISP>

²<https://www.github.com/MISP/misp-modules>

GETTING SOME NAMING CONVENTIONS OUT OF THE WAY...

■ Data layer

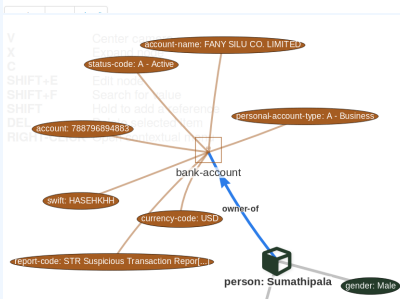
- ▶ **Events** are encapsulations for contextually linked information
- ▶ **Attributes** are individual data points, which can be indicators or supporting data.
- ▶ **Objects** are custom templated Attribute compositions
- ▶ **Object references** are the relationships between other building blocks

■ Context layer

- ▶ **Tags** are labels attached to events/attributes and can come from **Taxonomies**
- ▶ **Galaxy-clusters** are knowledge base items used to label events/attributes and come from **Galaxies**.

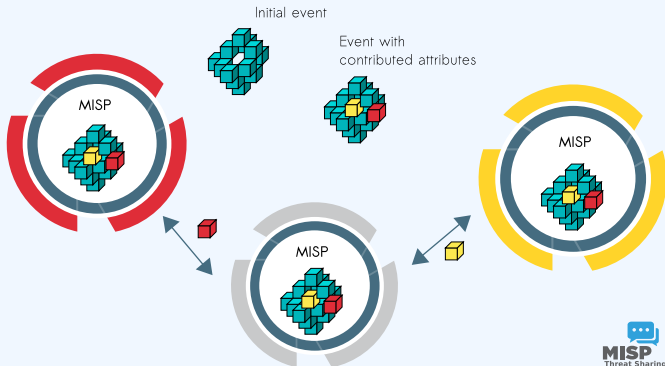
A RICH DATA-MODEL: TELLING STORIES VIA RELATIONSHIPS

Date	Org	Category	Type	Value	Tags	Galaxies	Comment	Correlate	Related Events
2018-09-28		Other	status-code:	A - Active		Add		<input type="checkbox"/>	
2018-09-28		Other	report-code:	STR Suspicious Transaction Report		Add		<input type="checkbox"/>	
2018-09-28		Other	personal-account-type:	A - Business		Add		<input type="checkbox"/>	
2018-09-28		Financial fraud	swift:	HASEH09H		Add		<input checked="" type="checkbox"/>	3849 11320 11584
2018-09-28		Financial fraud	account:	788796894883		Add		<input checked="" type="checkbox"/>	
2018-09-28		Other	account-name:	FANY SILU CO. LIMITED		Add		<input checked="" type="checkbox"/>	
2018-09-28		Other	currency-code:	USD		Add		<input type="checkbox"/>	



MISP CORE DISTRIBUTED SHARING FUNCTIONALITY

- MISP is a **peer to peer** sharing software
- As such, everyone can be a **consumer** and/or a **producer** of information.
- Immediate benefit without the obligation to contribute.
- Low barrier of entry to get acquainted with the system.



- Correlating data
- Feedback loop from detections via **Sightings**
- **False positive management** via the warninglist system
- **Enrichment system** via MISP-modules
- **Integrations** with a plethora of tools and formats
- Flexible **API** and support **libraries** such as PyMISP to ease integration
- **Timelines** and giving information a temporal context
- Full chain for **indicator life-cycle management**

MODELLING NEW DATA STRUCTURES FOR COVID-19

2020-03-20		Name: covid19-csse-daily-report		References: 0
2020-03-20	Other	country-region: text	Belgium	+ +
2020-03-20	Other	update: datetime	2020-03-19T11:13:17.000000+0000	+ +
2020-03-20	Other	confirmed: counter	1795	+ +
2020-03-20	Other	death: counter	21	+ +
2020-03-20	Other	recovered: counter	31	+ +

We are rapidly building new models for the different COVID-19 related information sources

- From health and cyber security, the community started to gather and share more information about **disinformation**
- Contextualisation improved (e.g. dedicated "pandemic" taxonomy)
- Specific data models such as **misinformation patterns** started to be used
- Particular features used in digital forensic were used to create timeline of the disinformation events
- Take control of the open source tools to extend the system for their own needs

DISINFORMATION #WEWONTSTAYHOME

Disinfo: #wewontstayhome

Event ID: 670
URL: [https://www.facebook.com/RealNewsStudio/](#)

Created by: Crigen-Cohen
Created on: Crigen-Cohen
Created with: facebook7x

Tags: [#wewontstayhome](#) [#wontstayhome](#) [#wearewithyou](#) [#wecantstayhome](#) [#wearenotstayinghome](#)

Date: 2020-04-13
Event Level: 7 Undefined
Analysis: Initial
Event Status: All components

Info: Details: #wewontstayhome

Attachments:

Attachments: 2 (1-2) Details

First recorded change: 2020-04-13 04:00:44
Last change: 2020-04-17 07:30:19

Multi-User Map:

Extended by: Event 2553: Covid Check, Tether Photo
 Continuity in article view

Highlights: 8 (8): [highlighted to view aggregation only](#)

Articles:

Related Events

Covid Check, Tether Photo
 2020-04-20

Warning: Potential 1
 Top 1000 article view rank

Dedupes:

- Multi-Information Platform
- Create Tracking
- Monitor
- Complexity resources
- Site Tracking
- Engage resource pages and assets



Filter:

Date	Tag	Category	Type	Value	Tags	Status	Comments	Continue	Related Events	Feed Info
2020-04-13		Object matter [including]								
2020-04-13		Relationships [1, 1]								
2020-04-13		Relationships [1, 1]								
2020-04-13		External analysis	link	https://www.facebook.com/RealNewsStudioOfficial/posts/112020020401008						
2020-04-13		External analysis	article	https://m.facebook.com/RealNewsStudioOfficial/posts/112020020401008						
2020-04-13		External analysis	advertisement							

DISINFORMATION "OPERATION GRIDLOCK"

Operation Gridlock

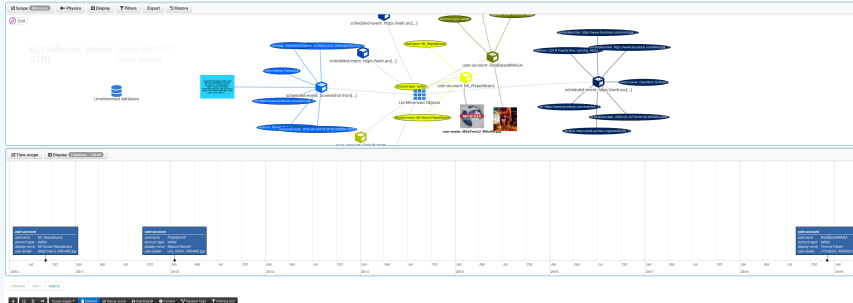
Event ID	105
UUID	bcf90535-6346-4526-ba3c-3dd639c98193
Created by	Malware Analyst
Owner by	Malware Analyst
Created on	2015-04-28 17:12:16
Created by	Malware Analyst
Time	2015-04-28 17:12:16
Host Label	301303184
Analysis	Static
Distribution	Command execution
File	Operation Gridlock
Analysis	Detected
File name	Operation Gridlock
File size	4096 bytes
File recorded change	2015-04-28 17:12:16
Last change	2015-04-28 17:12:16
Modification time	
Signature	Malware Analyst

Related Events

- 2015-04-28 17:12:16
- 2015-04-28 17:12:16
- 2015-04-28 17:12:16

Warning: Potential false positives (show)

Top 100 related files (hide)



DISINFORMATION AND CORRELATION



WHAT DID WE LEARN?

- Creating ad-hoc collaboration is an incredible laboratory for experimenting
- **Removing control provides freedom** to collaborate and share information is possible
- Building community up without any prior planning / any existing structure can be succesful
- Self-organisation and filtering came very early due to early abusers of the freedom
- New information and topics shared moved the community towards different fields

HOW CAN YOU GET INVOLVED?

- Join the COVID-19 community
- Either just use the data, or contribute data back, examples:
 - ▶ Ongoing Covid-19 phishing campaigns
 - ▶ Sharing warninglists of known valid covid-19 related websites
 - ▶ Local articles about the situation in your area
 - ▶ Best practice recommendations
 - ▶ Informations on travel restrictions
 - ▶ Analysis and further **research of a live information sharing community**
- Create **pull requests** on data models, dashboards, taxonomies...
- Share your ideas

- <https://www.misp-project.org/>
- <https://www.misp-standard.org/>
- <https://github.com/MISP>
- info@misp-project.org
- <https://twitter.com/MISPProject>