

How information sharing is saving us

MISP project perspective

Alexandre Dulaunoy

MISP Project

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

vOPCDE #3



MISP
Threat Sharing

- We build various information sharing communities (one is more than 1500 organisations with more than 4000 users). **sharing and updating daily cybersecurity indicators, financial indicators or threats in both ways**
- To achieve this we actively develop, maintain and support MISP (an open source threat sharing¹ platform)
- Beside the tools, **practices, standard formats and classifications** play an important role
- These practices need to be shared among the communities to support efficient collaboration

¹also called TIP, CTI platform. <http://www.misp-project.org>

*There was never a plan.
There was just a series of
mistakes.*

Robert Caro, journalist.

- During a malware analysis workgroup in 2012, we discovered that we worked on the analysis of the same threat actor
- We wanted to share information in an easy and automated way **to avoid duplication of work**
- Christophe Vandeplass (then working at the CERT for the Belgian MoD) showed us his work on a platform that later became MISP
- A first version of the MISP Platform was used by the MALWG and **the increasing feedback of users** helped us to build an improved platform.
- MISP is now **a community-driven development**

*Don't be abused by the legal
framework.
Use the legal the framework.*

MISP Project²

²<https://www.misp-project.org/compliance/>

RELY ON OUR INSTINCTS TO IMITATE OVER EXPECTING ADHERENCE TO RULES

- **Lead by example** - the power of imitation
- Encourage **improving by doing** instead of blocking sharing with unrealistic quality controls
 - ▶ What should the information look like?
 - ▶ How should it be contextualise
 - ▶ What do you consider as useful information?
 - ▶ What tools did you use to get your conclusions?
- Side effect is that you will end up **raising the capabilities of your constituents**

HOW TO DEAL WITH ORGANISATIONS THAT ONLY "LEECH"?

- From our own communities, only about **30%** of the organisations **actively share data**
- We have come across some communities with sharing requirements
- In our experience, this sets you up for failure because:
 - ▶ Organisations losing access are the ones who would possibly benefit the most from it
 - ▶ Organisations that want to stay above the thresholds will start sharing junk / fake data
 - ▶ You lose organisations that might turn into valuable contributors in the future

SHARED LIBRARIES OF META-INFORMATION (GALAXIES)











- The MISPPProject in co-operation with partners provides a **curated list of galaxy information**
- Can include information packages of different types, for example:
 - ▶ Threat actor information
 - ▶ Specialised information such as Ransomware, Exploit kits, etc
 - ▶ Methodology information such as preventative actions
 - ▶ Classification systems for methodologies used by adversaries
 - ATT&CK or Misinformation Pattern
- Consider improving the default libraries or contributing your own (simple JSON format)
- If there is something you cannot share, run your own galaxies and **share it out of bound** with partners
- Pull requests are always welcome

- COVID-19 MISP is a MISP instance retrofitted for COVID-19³ info sharing
- We are focusing on two areas of sharing:
 - ▶ **Medical** information
 - ▶ **Cyber threats** related to / abusing COVID-19
 - ▶ **Misinformation** related to COVID-19
- Low barrier of entry, aiming for wide spread
- Already a **massive community**

³<https://www.misp-project.org/covid-19-misp/>

- 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

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

WHAT KIND OF INFORMATION SHARING COMMUNITIES EXIST RELYING ON MISP?

- **A plethora of "cyber security"-related** communities in CSIRTs, SOC and private exchange groups
- Specific **financial** sharing communities in the banking sector
- **Border control information** sharing communities
- **Vulnerability disclosure** sharing communities
- **Intelligence community** sharing community

CONTACT US IF YOU WANT TO BUILD YOUR SHARING COMMUNITY

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