Best Practices in Threat Intelligence

Gather, document, analyse and contextualise intelligence using MISP

Team CIRCL

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

MISP Training @ CIRCL
20190923

MISP
Threat Sharing

Objectives

- Learning how to use MISP to support common OSINT gathering use-cases as often used by SOC, CSIRTs and CERTs
- By using a list of practical exercise[1]
- The exercises are **practical recent cases to model and structure intelligence** using the MISP standard
- Improving the data models available in MISP by exchanging live improvements and ideas
- Being able to share the results to the community at the end of this session

[1] https://gist.github.com/adulau/8c1de48060e259799d3397b83b0eec4f

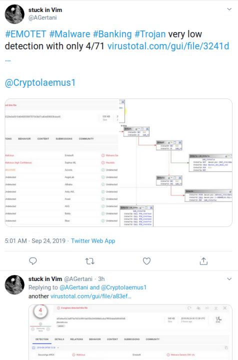
(Threat) Intelligence

- **Cyber threat intelligence (CTI) is a vast concept** which includes different fields such as intelligence as defined in the military community or in the financial sector or the intelligence community.
- **MISP project doesn’t want to lock an organisation or an user into a specific model**. Each model is useful depending of the objectives from an organisation.
- A set of pre-defined knowledge base or data-models are available and organisation can select (or create) what they need.
- During this session, an overview of the most used taxonomies, galaxies and objects will be described.

MICROBLOG OBJECT

Use case

A serie of OSINT tweets from a security researcher. To structure the thread, the information and keep an history.



stuck in Vim
@AGertani

#EMOTET #Malware #Banking #Trojan very low detection with only 4/71 virustotal.com/gui/file/3241d …

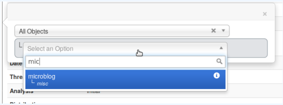
@Cryptolaemus1

5:01 AM · Sep 24, 2019 · Twitter Web App

stuck in Vim @AGertani · 3h
Replying to @AGertani and @Cryptolaemus1
another virustotal.com/gui/file/a83ef...

Object to use

The microblog object can be used for Tweet or any microblog post (e.g. Facebook). Then object can be linked using *followed-by* to describe a serie of post.


All Objects
Select an Option
mic
microblog
misc
Date
Thre
Analysis