nviso

BelgoMISP Meeting 0x01

Building a trusted MISP user community in Belgium

December 2019

www.nviso.be

Background (1)

- FIRST Cyber Threat Intelligence Symposium
  - March 2019 – London

- "do something" local

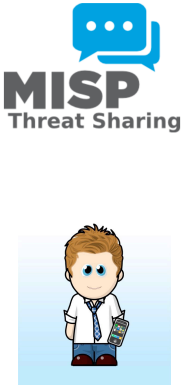
- **Subscribe** to the 2020 Event
  - March 2020 – Zurich
  - https://www.first.org/events/symposium/zurich2020/

Background (2)

- MISP Summit 05
  - October 2019 - Luxembourg

- Presentation "MISP sync process"
  - (or How to make MISP sync 500x faster)
  - Richard van den Berg
  - "RichieB2B"

- nederMISP
  - De Nederlandse MISP-gebruikersgroep



MISP Communities

- **Communities**
  - https://www.misp-project.org/communities/
  - CIRCL MISP
  - CiviCERT MISP
  - Fidelis Malware / RAT community
  - CSSA
  - FIRST and NATO
- **Feeds**
  - CIRCL OSINT Feed
  - Botvrij.eu OSINT feed

MISP Communities

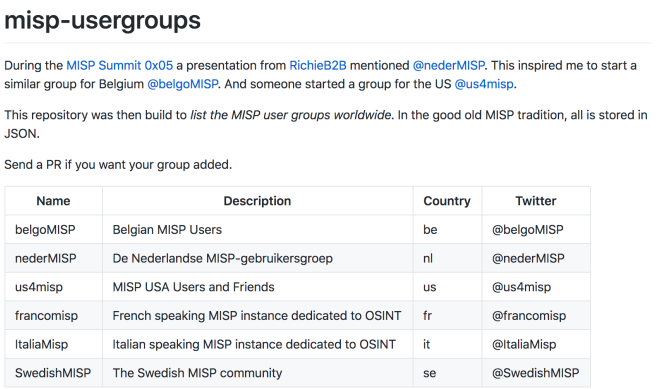
Known Existing and Public MISP Communities

- CIRCL MISP Community
- CiviCERT MISP Community
- Fidelis malware/RAT Community
- CSSA Cyber Security Sharing & Analytics (CSSA)
- FIRST MISP Community
- NATO MISP Community
- MISP Feed Communities
  - CIRCL OSINT Feed
  - Botvrij.eu OSINT feed

"misp-usergroups"

Create a Github Repository. Talk JSON.

- https://**github.com**/cudeso/misp-usergroups
  - Collaborative effort



misp-usergroups

During the MISP Summit 0x05 a presentation from RichieB2B mentioned @nederMISP. This inspired me to start a similar group for Belgium @belgoMISP. And someone started a group for the US @us4misp.

This repository was then build to *list the MISP user groups worldwide*. In the good old MISP tradition, all is stored in JSON.

Send a PR if you want your group added.

Name	Description	Country	Twitter
belgoMISP	Belgian MISP Users	be	@belgoMISP
nederMISP	De Nederlandse MISP-gebruikersgroep	nl	@nederMISP
us4misp	MISP USA Users and Friends	us	@us4misp
francomisp	French speaking MISP instance dedicated to OSINT	fr	@francomisp
ItaliaMisp	Italian speaking MISP instance dedicated to OSINT	it	@ItaliaMisp
SwedishMISP	The Swedish MISP community	se	@SwedishMISP

- **JSON** schema to describe user groups
  - name, contact, geometry, services, community

BelgoMISP

- **@belgomisp**

- @cudeso
  - Koen Van Impe

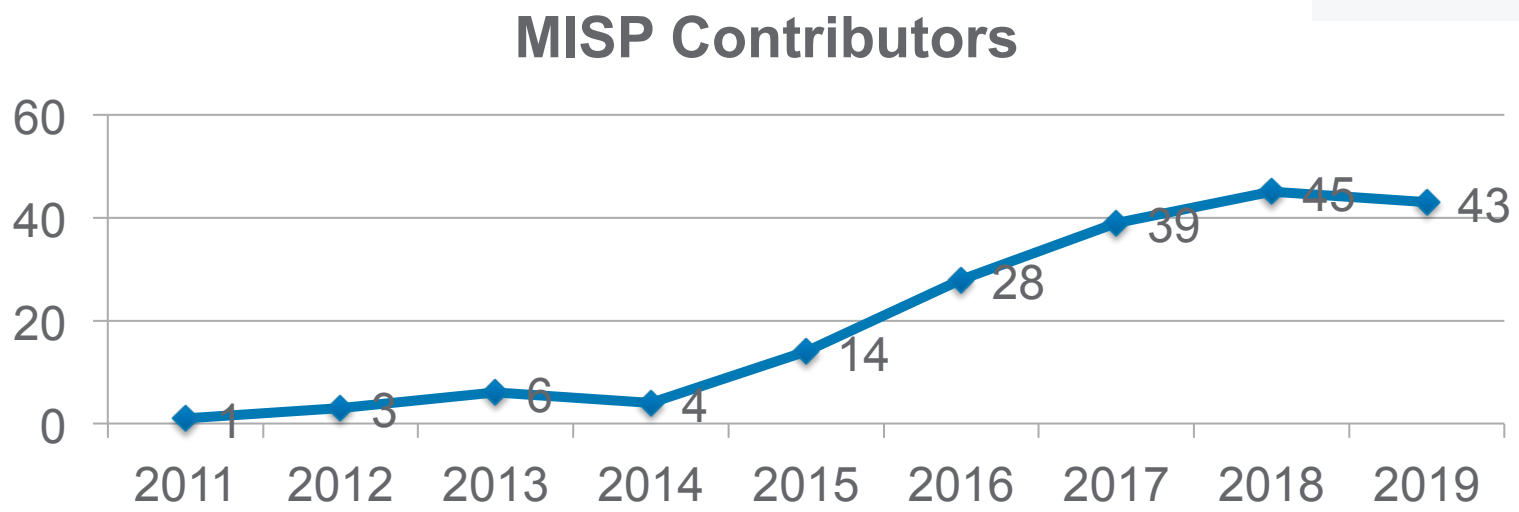
- @treyka
  - Trey Darley

Start Small

Based on Github contributors (Insights statistics)

Members (24)

Attendees (19)



Objectives

- Build a **trusted** MISP user community in Belgium

- All our talks are TLP:White
  - Not recorded
  - English

- MISP usage, also outside traditional threat intelligence cases
- Dealing with threat intelligence in general
- Custom taxonomies and tagging

My background with MISP

- Belnet-CERT / CERT.be
- End 2013 / early 2014

- Let's host a web application
- In the DMZ
- It runs PHP
- It's managed by someone externally

Continue

- First commits 2014
  - (less than a year!)

Commits on Nov 16, 2014

Example script to download MISP network activity

cudeso committed on 16 Nov 2014

Commits on Feb 1, 2015

Merge pull request #1 from MISP/master ...

cudeso committed on 1 Feb 2015

- Extensions
  - VMray
  - VulnDB
- OSINT feed
  - Botvrij.eu

Commits on Nov 18, 2016

Submit malware samples ...

cudeso committed on 18 Nov 2016

Commits on Nov 6, 2017

VulnDB Queries ...

cudeso committed on 6 Nov 2017

Logistics

- **No coffee** in this room
  - Water is OK
- Coffee is in the breakout room
- Toilets
- Emergency exit

Agenda

Koen Van Impe	What's BelgoMISP about?
Borce Stojkovski	UX
Break	
Andras Iklody / Alexandre Dulaunoy	MISP AMA
Nathalie Van Raemdonck	How are states taking up their international infosec role?
All	Open discussion on MISP usage and integrations

www.nviso.be

nviso