Usually a MISP workshop

Introduction into Information Sharing using MISP for CSIRTs

CIRCL
Computer Incident
Response Center
Luxembourg

MISP
Threat Sharing

Team CIRCL
TLP:WHITE

MNSEC 2018
20181004

Plan for this session

- Explanation of the CSIRT use case for information sharing and what CIRCL does
- Building an information sharing community and best practices

Communities operated by CIRCL

- As a CSIRT, CIRCL operates a wide range of communities
- We use it as an **internal tool** to cover various day-to-day activities
- Whilst being the main driving force behind the development, we're also one of the largest consumers
- Different communities have different needs and restrictions

Communities operated by CIRCL

- Private sector community
  - Our largest sharing community
  - Over **900 organisations**
  - **2000 users**
  - Functions as a central hub for a lot of sharing communities
  - Private organisations, Researchers, Various SoCs, some CSIRTs, etc
- CSIRT community
  - Tighter community
  - National CSIRTs, connections to international organisations, etc

Communities operated by CIRCL

- Financial sector community
    - Banks, payment processors, etc.
    - Sharing of **mule accounts** and **non-cyber threat infomartion**
- X-ISAC
    - **Bridging the gap** between the various sectorial and georgraphical ISACs
    - New, but ambitious initiative
    - Goal is to **bootstrap the cross-sectorial sharing** along with building the infrastructure to enable sharing when needed
    - `https://www.x-isac.org/`

Need access? np: `mailto:info@circl.lu`

Communities operated by CIRCL

- Coming up - the ATT&CK EU community
  - Work on attacker modelling
  - With the assistance of Mitre themselves
  - Unique opportunity to **standardise on TTPs**
  - Looking for organisations that want to get involved!
  - https://attack.mitre.org

Communities supported by CIRCL

- FIRST.org's MISP community
- Telecom and Mobile operators' community
- Various ad-hoc and time limited communities, exercises for example
  - Most recently the ENISA exercise a few months ago (2nd year MISP was used)
  - Open for other events

Sharing Scenarios in MISP

- Sharing can happen for **many different reasons**. What are the typical CSIRT scenarios?
- We can generally split these activities into 4 main groups when we're talking about traditional CSIRT tasks:
  - Core services
  - Proactive services
  - Advanced services
  - Sharing communities managed by CSIRTs for various tasks

CSIRT core services

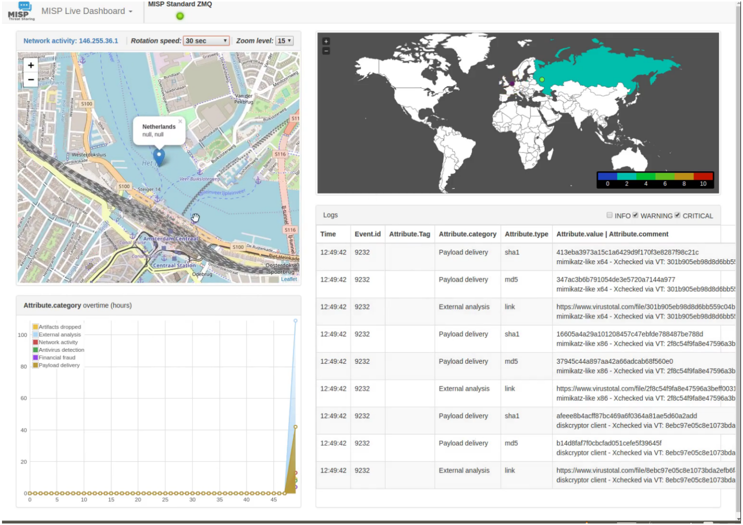
- Incident response
  - **Internal storage** of incident response data
  - Sharing of indicators **derived from incident response**
  - **Correlating data** derived and using the built in analysis tools
  - **Enrichment** services
  - **Collaboration** with affected parties via MISP during IR
  - **Co-ordination** and collaboration
  - **Takedown** requests
- Alerting of information leaks (integration with **AIL**[1])

[1] https://github.com/CIRCL/AIL-framework

CSIRT proactive services

- **Contextualising** both internal and external data
- **Collection** and **dissimination** of data from various sources (including OSINT)
- Storing, correlating and sharing own manual research (**reversing, behavioural analysis**)
- Aggregating automated collection (**sandboxing, honeypots, spamtraps, sensors**)
  - MISP allows for the creation of **internal MISP "clouds"**
  - Store **large specialised datasets** (for example honeypot data)
  - MISP has **interactions with** a large set of such **tools** (Cuckoo, Mail2MISP, etc)
- **Situational awareness** tools to monitor trends and adversary TTPs within my sector/geographical region (MISP-dashboard, built in statistics)

CSIRT proactive services - MISP dashboard

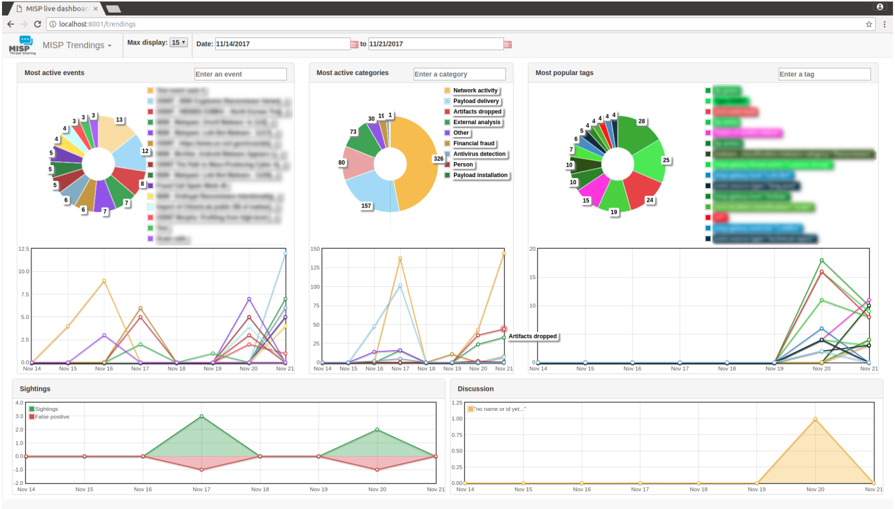


Network activity: 146.255.36.1 | Rotation speed: 30 sec | Zoom level: 15

Logs ☐ INFO ☑ WARNING ☑ CRITICAL

Time	Event.id	Attribute.Tag	Attribute.category	Attribute.type	Attribute.value | Attribute.comment
12:49:42	9232		Payload delivery	sha1	413eba3973a15c1a6429d9f170f3e8287f98c21c mimikatz-like x64 - Xchecked via VT: 301b905eb98d8d6bb5
12:49:42	9232		Payload delivery	md5	347ac3b6b791054de3e5720a7144a977 mimikatz-like x64 - Xchecked via VT: 301b905eb98d8d6bb5
12:49:42	9232		External analysis	link	https://www.virustotal.com/file/301b905eb98d8d6bb559c04b mimikatz-like x64 - Xchecked via VT: 301b905eb98d8d6bb5
12:49:42	9232		Payload delivery	sha1	16605a4a29a101208457c47ebfde788487be788d mimikatz-like x86 - Xchecked via VT: 2f8c54f9fa8e47596a3b
12:49:42	9232		Payload delivery	md5	37945c44a897aa42a66adcab68f560e0 mimikatz-like x86 - Xchecked via VT: 2f8c54f9fa8e47596a3b
12:49:42	9232		External analysis	link	https://www.virustotal.com/file/2f8c54f9fa8e47596a3beff0031 mimikatz-like x86 - Xchecked via VT: 2f8c54f9fa8e47596a3b
12:49:42	9232		Payload delivery	sha1	afeee8b4acff87bc469a6f0364a81ae5d60a2add diskcryptor client - Xchecked via VT: 8ebc97e05c8e1073bda
12:49:42	9232		Payload delivery	md5	b14d8faf7f0cbcfad051cefe5f39645f diskcryptor client - Xchecked via VT: 8ebc97e05c8e1073bda
12:49:42	9232		External analysis	link	https://www.virustotal.com/file/8ebc97e05c8e1073bda2efb6f diskcryptor client - Xchecked via VT: 8ebc97e05c8e1073bda

CSIRT proactive services - MISP dashboard



MISP live dashboar

localhost:8001/trendings

MISP Trendings

Max display: 15

Date: 11/14/2017 to 11/21/2017

Most active events Enter an event

Most active categories Enter a category

- 🟧 Network activity
- 🟦 Payload delivery
- 🟥 Artifacts dropped
- 🟩 External analysis
- 🟪 Other
- 🟫 Financial fraud
- 🟦 Antivirus detection
- 🟥 Person
- 🟩 Payload installation

Most popular tags Enter a tag

Sightings

- 🟩 Sightings
- 🟥 False positive

Discussion

- 🟧 "no name or id yet..."

CSIRT advanced services

- Supporting **forensic analysts**
- Collaboration with **law enforcement**
- **Vulnerability** information sharing
  - **Notifications** to the constituency about relevant vulnerabilities
  - **Co-ordinating** with vendors for notifications (*)
  - Internal / closed community sharing of pentest results
  - We're planning on starting a series of hackathons to find

CSIRTs’ management of sharing communities for constituent actions:

- **Reporting** non-identifying information about incidents (such as outlined in NISD)
- **Seeking** and engaging in **collaboration** with CSIRT or other parties during an incident
- Pre-sharing information to **request for help** / additional information from the community
- **Pseudo-anonymised sharing** through 3rd parties to **avoid attribution** of a potential target
- Building processes for **other types of sharing** to get the community engaged and acquainted with the methodologies of sharing (mule account information, border control, etc)

A quick note on compliance...

- Collaboration with Deloitte as part of a CEF project for creating compliance documents
  - Information sharing and cooperation **enabled by GDPR**
  - How MISP enables stakeholders identified by the **NISD** to perform key activities
  - **AIL** and MISP
- For more information: https://github.com/CIRCL/compliance

Getting started with building your own sharing community

- Starting a sharing community is **both easy and difficult** at the same time
- Many moving parts and most importantly, you'll be dealing with a diverse group of people
- Understanding and working with your constituents to help them face their challenges is key

Getting started with building your own sharing community

- When you are starting out - you are in a unique position to drive the community and set best practices...

Running a sharing community using MISP - How to get going?

- Different models for constituents
  - Connecting to a MISP instance hosted by a CSIRT
  - Hosting their own instance and connecting to CSIRT's MISP
  - Becoming member of a sectorial MISP community that is connected to CSIRT's community
- Planning ahead for future growth
  - Estimating requirements
  - Deciding early on common vocabularies
  - Offering services through MISP

Rely on our instincts to immitate over expecting adherence to rules

- Lead by example - the power of immitation
- 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

What counts as valuable data?

- Sharing comes in many shapes and sizes
  - Sharing results / reports is the classical example
  - Sharing enhancements to existing data
  - Validating data / flagging false positives
  - Asking for support from the community
- Embrace all of them. Even the ones that don't do either, you'll never know when they change their minds...

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 will lose protection who would possibily 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

So how does one convert the passive organisations into actively sharing ones?

- Rely on organic growth
- Help them increase their capabilities
- As mentioned before, lead by example
- Rely on the inherent value to one's self when sharing information (validation, enrichments, correlations)
- Give credit where credit is due, never steal the accolades of your community (that is incredibly demotivating)

Dispelling the myths around blockers when it comes to information sharing

- Sharing difficulties are not really technical issues but often it’s a matter of **social interactions** (e.g. **trust**).
    - You can play a role here: organise regular workshops, conferences, have face to face meetings
- Legal restrictions
    - "Our legal framework doesn’t allow us to share information."
    - "Risk of information leak is too high and it’s too risky for our organization or partners."
- Practical restrictions
    - "We don’t have information to share."
    - "We don’t have time to process or contribute indicators."
    - "Our model of classification doesn’t fit your model."
    - "Tools for sharing information are tied to a specific format, we use a different one."

Get in touch if you need some help to get started

- Getting started with building a new community can be daunting. Feel free to get in touch with us if you have any questions!
- Contact: info@circl.lu
- `https://www.circl.lu/`
- `https://github.com/MISP` - `https://gitter.im/MISP/MISP` - `https://twitter.com/MISPProject`

One final #rant

GitHub
stackoverflow
How to upload a Photo
How to fix error
How to Print
GUI library
How to
RUN
He is Alive