MISP

Information Sharing using MISP in 2019

CIRCL
Computer Incident
Response Center
Luxembourg

Team CIRCL

TLP:WHITE

MISP in 20 Minutes @
MNSEC-2019

20191004

Plan for this session

- Who am I, what is a Luxembourg and have you heard of CIRCL?
- Quick .lu and .in relations brief.
- What is MISP and where does it come from?
- Building an information sharing community in 2019
- Various random rants along the way

whoami, whereis steve

about CIRCL

The Computer Incident Response Center Luxembourg (CIRCL) is a government-driven initiative designed to provide a systematic response facility to computer security threats and incidents. CIRCL is the CERT for the private sector, communes and non-governmental entities in Luxembourg and is operated by securitymadein.lu g.i.e.

MISP and CIRCL

- CIRCL is mandated by the Ministry of Economy and acting as the Luxembourg National CERT for private sector.
- CIRCL leads the development of the Open Source MISP threat intelligence platform which is used by a wide range of communities.
- **CIRCL runs multiple large MISP communities performing active daily threat-intelligence sharing**.

Co-financed by the European Union

Connecting Europe Facility

Luxembourg quo vadis?

Luxembourg quo vadis?

Official name: Grand Duchy of Luxembourg
Capital: Luxembourg City
Neighbouring countries: Germany, Belgium, France
Population: 602k inhabitants (Oct, 2018), of whom 47,9% foreigners, over 170 nationalities
Form of government: constitutional monarchy functioning as a parliamentary democracy
Head of State: HRH Grand Duke Henri
Head of Government: Xavier Bettel, Prime Minister, Min. of State
National language: Luxembourgish (Lëtzebuergesch, but)
Administrative languages: French, German and Luxembourgish

Luxembourg quo vadis?

Currency: Euro (1 euro = 100 cents)
International Dialing Code: +352
TLD: .lu
Time zone: Central European Standard Time (CET) = GMT/UTC +1; Central European Summer Time (CEST) = GMT/UTC +2
Electricity supply: 220-240V, 50 Hz
Units of weight and measure: kilogram and metre

What is MISP

- Threat Intelligence Sharing Platform
- IoC aggregator
- A standardised format that makes (pragmatic) sense and allows itself to change
- Tool to make sense of all the random mess we see in our digital flows and puts it into context(s)

MISP and starting from a practical use-case

- During a malware analysis workgroup in 2012, we discovered that we worked on the analysis of the same malware.
- We wanted to share information in an easy and automated way **to avoid duplication of work**.
- Christophe Vandeplas (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**.

Bigger changes 2019

- Indicator Decaying
- ATT&CK sighting
- UI Improvements (but)
- Performance and Security Fixes
- Community Listings
- Sync updates
- Translations
- Tag collections (time-to-contextualise)
- MISP Modules (PDF, PPT, XLS importer) VMRay import, QR Code extract...
- DFIR improvements

Le Demo

What does it look like?

Communities operated by CIRCL

- Private sector community
  - Our largest sharing community
  - Over **1000 organisations**
  - **3000 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

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

Communities operated by CIRCL

- National/Governmental/Military CSIRTs
- NATO (NCIRC and NICP)
- ISACs/ISAOs (Information Sharing and Analysis Center)
- along with many large private organisations
- Security researchers and SMEs in the ICT field
- Security vendors
- Telecom, Medical, Financial ...

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 (3rd year MISP was used)
  - Open for other events

Advantages of cross sectorial sharing

City | Bengaluru | Mumbai | Delhi | Hyderabad | Kolkata | Chennai | Agartala | Agra | Ajmer | Amaravati | Ahmedabad | Allahabad | Amritsar

Aero India: Special focus on cyber security to thwart digital threats

Chethan Kumar | TNN | Updated: Feb 16, 2019, 06:10 IST

BENGALURU: With a digital threat looming large, intelligence agencies and armed forces personnel responsible for maintaining security at Aero India 2019 have, for the first time, pinned special focus on cyber security

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`