CSIRTs network, notification and sharing scenarios

E.104

CIRCL Computer Incident Response Center Luxembourg

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

March 25, 2022 - v0.7

CSIRTs network, notification and sharing scenarios
E.104
CIRCL Computer Incident Response Center Luxembourg
MISP Project
https://www.misp-project.org/
March 25, 2022 - v0.7
MISP
Threat Sharing

CSIRT NETWORK INFORMATION EXCHANGE

- Well **established methodologies and rule-sets**
- Reliance on a **common understanding of information releasability**
- Network wide exchange - **tooling and practices**

CSIRT NETWORK INFORMATION EXCHANGE
- Well **established methodologies and rule-sets**
- Reliance on a **common understanding of information releasability**
- Network wide exchange - **tooling and practices**

1. Here we just quickly give an overview and explanation of the main factors that enable the sharing for the CSIRT network.

Main objectives of information sharing from a CSIRT perspective

- **Incident response**
- **Proactive information sharing** for detection and prevention
- **Takedown notifications**

Main objectives of information sharing from a CSIRT perspective
- Incident response
- Proactive information sharing for detection and prevention
- Takedown notifications

1. Information sharing happens for different reasons and at different layers.
2. Before diving into each objective, here we list them as an overview

The incident response use-cases

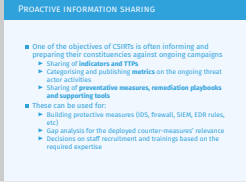
- Collaboration during **incident repsonse**
  - **Multiple CSIRTs** involved in the **IR** of a single victim
  - Ongoing campaigns against multiple victims in **different constituencies**
- Building **baseline rulesets** for hunting / IR

The incident response use-cases
- Collaboration during incident repsonse
  - Multiple CSIRTs involved in the IR of a single victim
  - Ongoing campaigns against multiple victims in different constituencies
- Building baseline rulesets for hunting / IR

1. During incident response, there are multiple scenarios where information sharing becomes crucial.
2. It is quite frequent that victims span organisations of multiple countries or sectors, in which case collaboration saves time and effort.
3. Besides individual IR cases, having a well maintained and relevant indicator repository is vital for bootstrapping the IR / hunting workflows.

Proactive information sharing

- One of the objectives of CSIRTs is often informing and preparing their constituencies against ongoing campaigns
  - Sharing of **indicators and TTPs**
  - Categorising and publishing **metrics** on the ongoing threat actor activities
  - Sharing of **preventative measures, remediation playbooks and supporting tools**
- These can be used for:
  - Building protective measures (IDS, firewall, SIEM, EDR rules, etc)
  - Gap analysis for the deployed counter-measures' relevance
  - Decisions on staff recruitment and trainings based on the required expertise



1. CSIRTs often act as central hubs for the national / sectorial information flow for ongoing attacker trends.
2. In contrast to commercial feed providers, the main importance attributed to the data shared by the CSIRTs is that their focus is on attacks targeting their constituency, making it additionally relevant for them.
3. What is important to explain here is the type of information that is relevant here (Indicators, TTPs, preventative measures and playbooks) and what effect they can have on an organisation.

Takedown notifications

- **Abuse handling** often delegated to the CSIRTs who
  - The contact providers to issue takedown requests
  - Potentially liaise with law enforcement on more drastic measures
- Takedown requests can be **difficult due attacks originating in another country**
- A **working relationship with operators and hosting providers** can speed up the process
- **Contacts to local law enforcement** also help
- Involving the responsible CSIRT therefore is customary

Takedown notifications
Abuse handling often delegated to the CSIRTs who
The contact providers to issue takedown requests
Potentially liaise with law enforcement on more drastic measures
Takedown requests can be difficult due attacks originating in another country
A working relationship with operators and hosting providers can speed up the process
Contacts to local law enforcement also help
Involving the responsible CSIRT therefore is customary

1. The focus of this slide should be on the difficulty of successful takedown requests when dealing with providers / hosts abroad and how contacting the local CSIRTs can help the process along.
2. Also explain how the CSIRT getting the request forwarded would potentially involve law enforcement.

Sharing in practice

- The actual sharing happens over different layers (from most to least stricly formalised)
  - **Automated information sharing** for **structured intelligence** (via for example MISP)
  - **Recurring report** on trends based on **surveys** conducted in the network (for example ENISA Cyber Weather)
  - **Takedown notifications** assistance requests to the responsible CSIRTs
  - **Conference calls** for certain **high priority campaigns** (via for example BBB, Jitsi, webex, etc)
  - **Ad-hoc discussions** and information requests (via mailing lists, chat applications such as mattermost)

Sharing in practice
- The actual sharing happens over different layers (from most to least stricly formalised)
  - **Automated information sharing** for **structured intelligence** (via for example MISP)
  - **Recurring report** on trends based on **surveys** conducted in the network (for example ENISA Cyber Weather)
  - **Takedown notifications** assistance requests to the responsible CSIRTs
  - **Conference calls** for certain **high priority campaigns** (via for example BBB, Jitsi, webex, etc)
  - **Ad-hoc discussions** and information requests (via mailing lists, chat applications such as mattermost)

1. The actual exchanges use a variety of tools and mechanisms for the exchange, ranging from ad-hoc discussions to well modeled, automated intel sharing.

Adhering to releasability

- Simple to understand sharing models
  - **TLP** is understood to be authoritative in the network
  - **PAP** used less frequently, it is an additional way to mark the accepted actions to be carried out on the information
- Besides data, meetings and individual discussion channels all can have an indicated baseline TLP level
- Networks such as this are built on trust that needs to be fostered

Adhering to releasability
Simple to understand sharing models
TLP is understood to be authoritative in the network
PAP used less frequently, it is an additional way to mark the accepted actions to be carried out on the information
Besides data, meetings and individual discussion channels all can have an indicated baseline TLP level
Networks such as this are built on trust that needs to be fostered

1. A quick explanation of TLP and PAP is required at this point, especially in regards to their differences.
2. TLP: Who can I share it with?
3. PAP: What sort of actions are permitted with regards to the information?

Automated information sharing

- **Indicators, context, enrichments, sightings**
- The objectives of the data are **automation** as well as building **knowledge-bases** for future use
- Strong **validation and contextualisation** is crucial
- **Parts** of the data will end up in the **proactive sharing** with the constituency
- Information about the Victim is excluded
- Information about the attacker beyond the attacker modus operandi are also excluded
- The objective is protection / remediation rather than dealing with the attacker

Automated information sharing
- Indicators, context, enrichments, sightings
- The objectives of the data are automation as well as building knowledge-bases for future use
- Strong validation and contextualisation is crucial
- Parts of the data will end up in the proactive sharing with the constituency
- Information about the Victim is excluded
- Information about the attacker beyond the attacker modus operandi are also excluded
- The objective is protection / remediation rather than dealing with the attacker

1. It is important to note here that CSIRTs in general don't focus at all on attribution beyond being able to differentiate and anticipate potential attacker actions to help with the incident response and detection. Attributing attacks to individuals, groups, nationalities are not in scope beyond this.
2. As for the sanitisation process, it should also be mentioned that data is shared with different releasability levels depending on sensitivity.
3. The sharing is often broader and less filtered with the network than it is with the constituencies.

Takedown requests

- **Malicious infrastructure** IPs, IP ranges, domains
- **Timeline** of the malicious activities
- **Network logs** for verification and evidence towards the provider

Takedown requests
- **Malicious infrastructure** IPs, IP ranges, domains
- **Timeline** of the malicious activities
- **Network logs** for verification and evidence towards the provider

1. Whilst not standardised globally, takedown request notifications are kept similar in scope, with information backing up the claim of malicious activity being provided from the get go to speed up the process.
2. Besides the target of the takedown request, timestamps and logs are crucial.

Ad-hoc communications

- E-mails, chats, video conferences
- Network wide vs ad-hoc exchanges
- Inter-personal trust relationships go a long way
- **Request for information** (has anyone else also seen... ?)
- Updates on **conclusions drawn** during incidents (we are seeing a rise in a specific type of attacks abusing a given vulnerability)

Ad-hoc communications
- E-mails, chats, video conferences
- Network wide vs ad-hoc exchanges
- Inter-personal trust relationships go a long way
- **Request for information** (has anyone else also seen... ?)
- Updates on **conclusions drawn** during incidents (we are seeing a rise in a specific type of attacks abusing a given vulnerability)

1. Besides the network wide communication, familiarity and trust in individual other members is often a starting point in ad-hoc discussions, especially for requests for information and assistance.
2. It's important to emphasise here that timeliness is of the essence for incident response, leading to these networks being often active around the clock.

CSIRT exchanges with law enforcement

- Sharing information during the rendering of **assistance to law enforcement during an ongoing forensics case**
- Creating data-sets to **bootstrap the forensics investigations** of law enforcement
- **Attacker trends** being shared both ways
- Assistance in the **takedown** process

CSIRT exchanges with law enforcement
- Sharing information during the rendering of **assistance to law enforcement during an ongoing forensics case**
- Creating data-sets to **bootstrap the forensics investigations** of law enforcement
- **Attacker trends** being shared both ways
- Assistance in the **takedown** process

1. There are numerous reasons why exchanges between LEAs and CSIRTs would take place, be it an off-loading of certain tasks where the others can offer expertise, or simply assisting in the creation of working information knowledge bases / rules to be used during day-to-day activities.