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

CSIRT network information exchange

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

Main objectives of information sharing from a CSIRT perspective

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

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

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

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

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)

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

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

Takedown requests

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

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)

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