The Good, the Bad & the Ugly

Information sharing experience - 2 years of challenges resumed in 15 minutes

CIRCL
Computer Incident
Response Center
Luxembourg

TLP:WHITE

alexandre.dulaunoy@circl.lu

February 12, 2014

Background

- We operated in the past 2-3 years various sharing platforms including MISP[1]
- We have partnerships with bilateral/"unilateral" sharing agreement
  - CERTs
  - Private or public organizations
  - Companies
  - Security researchers and universities
- The presentation is not to blame anyone but to improve information sharing

[1] https://github.com/MISP

The Good

- Reduced time of reversing or analysis when we found similar indicators
- Finding relationships between malware which keeps us focused on specific group of malware
- Improving relationships between sharing partners (e.g. working together on same cases)
- Common ground for OSINT sharing (cf. the new misp.be initiative that should be launched in the next days)

The Bad

- Some partners might reuse the information shared into a report and reference you as an origin of the information
  - It's sometime very good and part of the good practices except for some sensitive malware analysis
  - $\rightarrow$ We need to find a way to follow "Chatham house rule"[2] for some indicators while keeping the reporting organization accountable
- Different classification scheme in the same information sharing platform
  - Each time you introduce an additional classification label, the sharing interest is reduced by a double factor

[2]When a meeting, or part thereof, is held under the Chatham House Rule, participants are free to use the information received, but neither the identity nor the affiliation of the speaker(s), nor that of any other participant, may be revealed".

The Ugly

- When do you share information? Before the complete analysis? at the end of the analysis?
  - If you share late, nobody benefits from the sharing
  - If you share too early, "partners" might do actions on the shared indicators (e.g. you are still working on the analysis and you don't want any take-down action)
    - $\rightarrow$ Add "actionable" flag in information sharing platforms
- Indicators acquired in questionable ways
  - Unintended leak from third parties (e.g. available in the Google cache but nowhere else)
  - Found in the attackers infrastructure by gathering actions
  - $\rightarrow$ Information sharing platforms should be able to separate clean/grey indicators

Contact

- alexandre.dulaunoy@circl.lu - info@circl.lu
- https://www.circl.lu/
- OpenPGP fingerprint: CA57 2205 C002 4E06 BA70 BE89 EAAD CFFC 22BD 4CD5