Detecting Information Leaks and Notify Victims

Relying on AIL and MISP open source tooling

CIRCL
Computer Incident
Response Center
Luxembourg

Team CIRCL - *TLP:WHITE*
Demo *TLP:GREEN*

June 27, 2019

CIRCL
Computer Incident
Response Center
Luxembourg

- 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**
- CIRCL **develops and maintains a set of open source software** used by CERTs, SOCs and multiple organisations worldwide

Open Source Tooling

- **Automation is a key factor in incident response**
- 8 years ago, CIRCL started to build and maintain software to support our internal activities
- We release these tools as open source to support and help other organisations facing similar challenges

MISP
Threat Sharing

CIRCL
AIL
Analysis of Information Leaks

MISP - Threat Intelligence and Sharing Platform

- MISP[1] is an open source software (can be self-hosted or cloud-based) **information sharing and exchange platform**
- It enables analysts from various different sectors to create, collaborate on and share information
- The information shared can then be used to find correlations as well as automatically be fed into **protective tools or processes**
- The software is widely used by CERTs (e.g. CSIRTs network), law enforcement, private sector, military organisations and researchers since 2012
- CIRCL is both the main driving force behind the tool's **development** as well as some of the largest information **sharing communities** worldwide

[1] `https://www.misp-project.org/`

AIL - AIL framework - Analysis Information Leak framework

- AIL[2] is a modular framework to **discover potential information leaks from unstructured data sources** (e.g. Pastebin or similar services, unstructured data streams such as Tor onion services)
- AIL framework is flexible and can be extended to support other functionalities to mine, detect or process sensitive information (e.g. detecting IBAN numbers, credit-cards, personal information, credentials, ...)

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

Demo!

Content from the demo might include personal information. So the screencasts are classified as TLP:GREEN.

Information given to a community or a group of organizations at large. The information cannot be publicly released.

Conclusion

- Sharing personal information is easier for cyber-criminals than for organisations protecting the victims (e.g. **legal complexity**)
- Information sharing, in the scope of security, **lacks economical and legal incentive** (e.g. the complaints are often too much towards the organisation sharing and not the ones hidding/not sharing)
- Automation improved the time-to-notify the victims and reduce the ”analyst fatigue”
- Continuing the effort in Open Source for European CSIRT tooling to ensure independence, autonomy and security for CSIRTs in Europe

Contact

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