

AIL Project

How to Improve and Support Your Threat Intelligence Process



CIRCL

Computer Incident
Response Center
Luxembourg

Alexandre Dulaunoy

alexandre.dulaunoy@circl.lu

info@circl.lu

November 6, 2023

Background

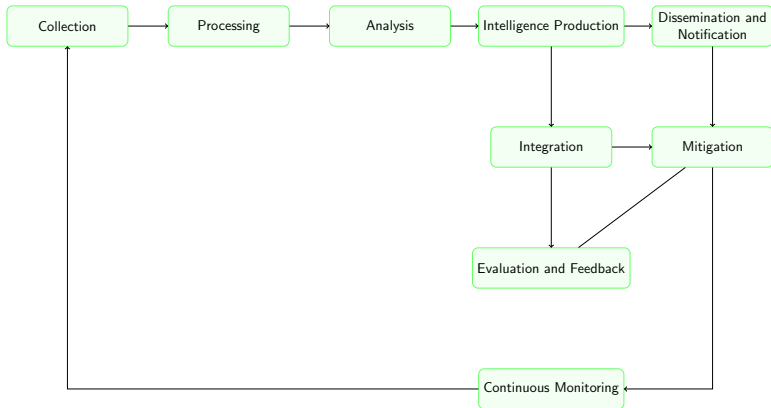
- Over the past five years, we have developed the AIL project¹ to fulfill our needs at CIRCL in intelligence gathering and analysis.
- As AIL gained popularity, an increasing number of users began integrating it into their **threat intelligence processes and workflows**.
- In this presentation, we outline some of the processes where AIL can serve as a valuable tool, **facilitating and enhancing the work of intelligence analysts**.

¹<https://www.ail-project.org/>

AIL overview

- The AIL Project is an open-source framework comprising various modules designed for the **collection, crawling, digging, and analysis of unstructured data**.
- AIL features an extensible Python-based framework for the **analysis of unstructured information**, collected either through an advanced Crawler manager or from various feeders, including social networks and custom feeders.
- AIL also provides support for actively **crawling Tor** hidden services, as well as crawling protected websites and forums by utilizing pre-recorded session cookies.

Threat Intelligence Process at CIRCL



Collection - automate collection




- Collecting data from various chat sources can be a **tedious task for analysts**.
- AIL offers a set of feeders (e.g., Telegram, Discord, etc.) that can be used to subscribe to chat channels.
- All the **collected messages are then processed and analyzed** within the AIL's *processing* and *analysis* stages.

telegram :

Chat Instance	Network	Address	Nb Chats
00098785-7e70-5d12-a120-c5cdc1252b2b			4

Show 10 entries

Search:

Icon	Name	ID	First Seen	Last Seen	NB Chats
	DARKNET DISCUSSION	1492939275	2023-10-06	2023-11-06	0
	H4Fun Bins	1427620096	2023-03-01	2023-11-06	0
	DDosia Project	1228309110	2023-10-19	2023-11-06	5

Showing 1 to 4 of 4 entries

Previous **1** Next

Processing - extracting selector/patterns

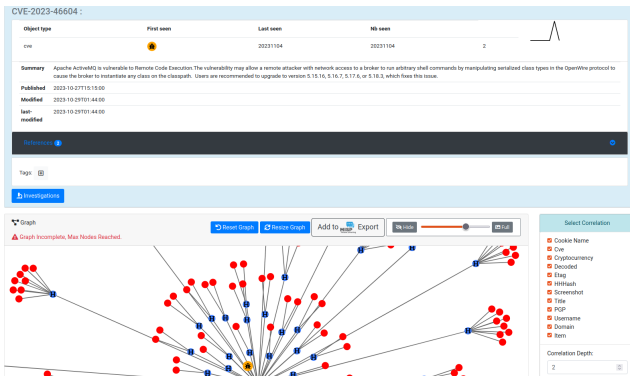
- Detecting specific search patterns in a large dataset, such as a significant ransomware leak, can be challenging for analysts.
- AIL includes a **rich set of existing search patterns** (e.g. IBAN) along with default Yara rules, and you have the ability to create custom ones.

Type	ID	Extracted
tag	infoleak-automatic-detection~"orion"	https://3yrirelomm3k43qhektzg025eif4h/ https://3yrirelomm3k43qhektzg025eif4h/ https://3yrirelomm3k43qhektzg025eif4h/ https://3yrirelomm3k43qhektzg025eif4h/ https://3yrirelomm3k43qhektzg025eif4h/ https://3yrirelomm3k43qhektzg025eif4h/ https://3yrirelomm3k43qhektzg025eif4h/ https://3yrirelomm3k43qhektzg025eif4h/ https://3yrirelomm3k43qhektzg025eif4h/ https://3yrirelomm3k43qhektzg025eif4h/ https://3yrirelomm3k43qhektzg025eif4h/ https://3yrirelomm3k43qhektzg025eif4h/ https://3yrirelomm3k43qhektzg025eif4h/ https://3yrirelomm3k43qhektzg025eif4h/ https://3yrirelomm3k43qhektzg025eif4h/
tag	infoleak-automatic-detection~"iban"	ES522100442365020138506
tracker	13ac3e24-e922-4d50-a0f0-4b746b08a672	BEGIN PROCS7
ERROR		Donaciones Audioconferencia Donaciones

Showing 1 to 4 of 4 entries

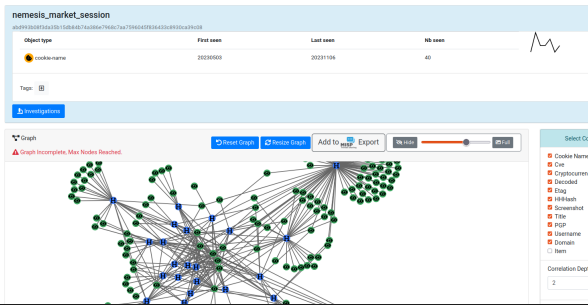
Analysis - evaluating vulnerability severity/risk

- What is the visibility, usage, mentions, or risk of a vulnerability observed in forums, channels, pastes, or websites?
- AIL can assist you in determining the severity/risk level or in **reviewing the usage of a vulnerability** (e.g., the number of PoCs).



Dissemination - distributing analysis

- AIL exports data using the **MISP standard format** and offers complete integration with MISP to facilitate the dissemination of data.
- All the context within AIL uses the **MISP taxonomies and galaxy**.
- The insights provided by AIL are often used as complementary information for threat intelligence reports and landscapes.



Conclusion

- While AIL can be a valuable tool for **organisations dealing with data leaks and information breaches**, it's important to remember that it is primarily designed for information leak analysis and not for the entire threat intelligence process.
- Organizations should use **AIL in conjunction with other threat intelligence solutions** and processes to establish a comprehensive threat intelligence strategy.
- AIL is an open-source project, and if you discover modules that could assist in your processes, please let us know or contribute directly.

Links

- AIL project <https://github.com/ail-project> (**all components including feeders and crawler infrastructure**)
- AIL framework
<https://github.com/ail-project/ail-framework> (**analysis framework**)
- Training materials and slide deck
<https://github.com/ail-project/ail-training>

