AIL Project

How to Improve and Support Your Threat Intelligence Process

Alexandre Dulaunoy
alexandre.dulaunoy@circl.lu

info@circl.lu

November 8, 2023
Background

- Over the past five years, we have developed the AIL project\(^1\) 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\(^2\) 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.

\(^2\)https://github.com/ail-project
Threat Intelligence Process at CIRCL

1. Collection
2. Processing
3. Analysis
4. Intelligence Production
5. Dissemination and Notification
6. Integration
7. Mitigation
8. Evaluation and Feedback
9. Continuous Monitoring

The process flows from Collection to Processing to Analysis to Intelligence Production to Dissemination and Notification. Integration and Mitigation are connected to Evaluation and Feedback, which in turn connects to Continuous Monitoring.
Common questions from constituents

• Do you **know if we are a target** of this adversary group?
• We have **observed a partnering company experiencing a ransomware incident**, and we are concerned about the impact on our organization.
• Can you determine if our **sector is a target** of this threat actor?
• Have you come across phishing kits targeting our bank/service or any instances of our **data being stolen** on the ”dark web”? 
Challenges and opportunity

- **Reducing repetitive tasks** for the analysts.
- **Preparing factual intelligence evidence** for intelligence production, including human-readable reports and MISP structured intelligence.
- **Correlating information** from multiple sources, especially when different analysts are working with different sources on their end.
- **Facilitating the integration** of "intelligence requests" from our constituents.
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.

### DDosia Project:

<table>
<thead>
<tr>
<th>Icon</th>
<th>Name</th>
<th>ID</th>
<th>First Seen</th>
<th>Last Seen</th>
<th>NB Sub-Channel</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>DDosia Project</td>
<td>1228309110</td>
<td>2023-10-20</td>
<td>2023-11-06</td>
<td>5</td>
</tr>
</tbody>
</table>

### Sub-Channels:

<table>
<thead>
<tr>
<th>Icon</th>
<th>Name</th>
<th>ID</th>
<th>First Seen</th>
<th>Last Seen</th>
<th>NB Messages</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Общий чат</td>
<td>1228309110/1</td>
<td>2023-10-20</td>
<td>2023-11-06</td>
<td>1498</td>
</tr>
<tr>
<td></td>
<td>Полезные материалы</td>
<td>1228309110/34221</td>
<td>2023-10-21</td>
<td>2023-11-06</td>
<td>360</td>
</tr>
<tr>
<td></td>
<td>DDoSia - поддержка</td>
<td>1228309110/34219</td>
<td>2023-10-20</td>
<td>2023-11-05</td>
<td>417</td>
</tr>
<tr>
<td></td>
<td>Предложение целей</td>
<td>1228309110/34217</td>
<td>2023-10-24</td>
<td>2023-11-05</td>
<td>26</td>
</tr>
</tbody>
</table>
Collection - automate crawling

- Crawling can be a challenging task, for example, gathering all the blog posts from ransomware groups\(^3\), which can be demanding for an analyst.
- AIL offers a crawling feature that can initiate regular crawls using a standard spawned browser.

\(^3\)https://www.ransomlook.io/
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.
Processing - deduplicating source/information

- When collecting data from numerous sources, encountering duplicate information is common, and distinguishing between them can be challenging.
- AIL’s correlation between page titles, screenshots, and HTTP headers matching helps identify copy-cat sources.
Analysis - automatic detection from collection

- Processing automatically collected information can be a challenging task.
- AIL processes all the collected items for any **hunting rules and utilizes MISP taxonomies to tag the matching information.**
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).
Analysis - Standardising labels and taxonomies

- Attribution and classification can be challenging for analysts. Facilitating integration with other tools, processes, and teams.
- AIL leverages the entire MISP galaxy, including threat actor data, taxonomies, and the ability to assign tags to every item.
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.
Evaluation/Integration - review search rules on real dataset

- Reviewing matching rules on a large dataset, such as extensive ransomware leaks, can be cumbersome.
- AIL provides a "retro-hunt" functionality to search and evaluate your YARA rules.
Production collecting evidences

- Analysts need to gather evidence, insights, and intelligence to produce intelligence reports.
- AIL can support the creation of reports by offering a straightforward method to organize discoveries for investigation.
Improving internal capabilities

Whilst buying ready made intelligence is easy, you see here that going from a black box solution of questionable quality to something that you can vet and validate can be easily implemented - the costs will also be invested in your internal experts rather than an opaque supplier.
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.

• Establishing consistent and reproducible intelligence processes throughout your organization.
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.

• Co-funded by European Union under joint threat analysis network (JTAN) project.