

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

September 11, 2024

Background

- Over the past five years, we have developed the AIL project¹ to meet the intelligence gathering and analysis needs at CIRCL.
- As AIL gained popularity, an increasing number of users have integrated it into their **threat intelligence processes and workflows**.
- In this presentation, we will outline several processes where AIL can be a valuable tool, **facilitating and enhancing the work of intelligence analysts**².

¹<https://www.ail-project.org/>

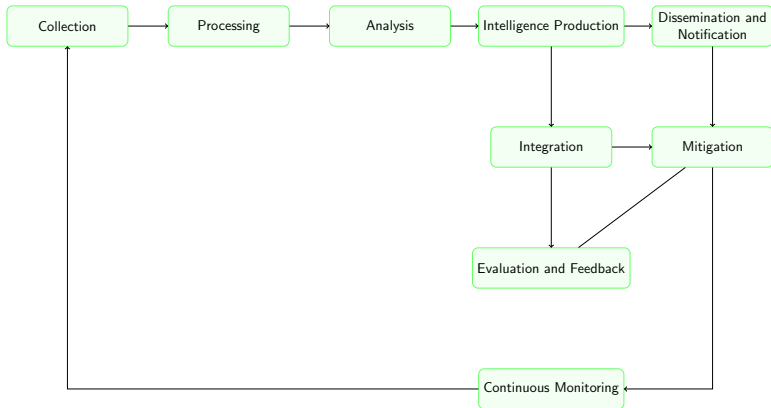
²Including those working in SOCs, CSIRTs, or any organizations dealing with threat intelligence.

AIL overview

- The AIL Project is an open-source framework³ 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.

³<https://github.com/ail-project>

Threat Intelligence Process at CIRCL



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 :





1228309110

Icon	Name	ID	First Seen	Last Seen	NB Sub-Channels
	DDosia Project	1228309110	2023-10-20	2023-11-06	5

Sub-Channels:

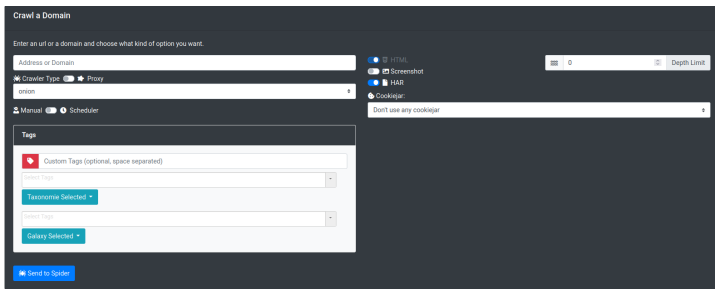
Show 10 entries

Search:

Icon	Name	ID	First Seen	Last Seen	NB Messages
	Общий чат	1228309110/1	2023-10-20	2023-11-06	1498
	Полезные материалы	1228309110/34221	2023-10-21	2023-11-06	360
	DDoSia - поддержка	1228309110/34219	2023-10-20	2023-11-05	417
	Предложение целей	1228309110/34217	2023-10-24	2023-11-05	26

Collection - automate crawling

- Crawling can be a challenging task, for example, gathering all the blog posts from ransomware groups⁴, which can be demanding for an analyst.
- AIL offers a crawling feature that can **initiate regular crawls using a standard spawned browser**.



Crawl a Domain

Enter an url or a domain and choose what kind of option you want.

Address or Domain

Crawler Type: ☐ HTML ☐ Screenshot ☐ HAR

prion

Manual ☐ Scheduler

Tags

Custom Tags (optional, space separated)

Select Tags

Tazomine Selected

Select Tags

Galaxy Selected

Send to Spider

Depth Limit

Cookiejar: Don't use any cookiejar

⁴<https://www.ransomlook.io/>

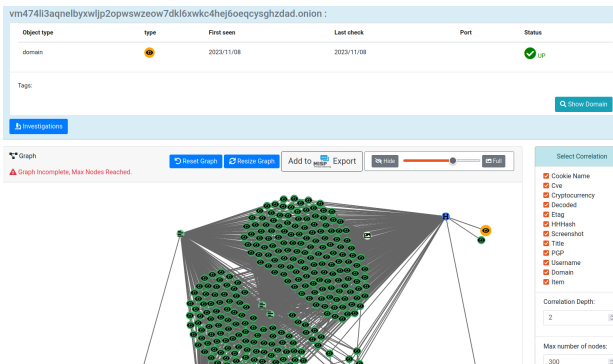
Processing - extracting selector/patterns

- 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.

[illegible]

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.**

```
vargakrisztian44@gmail.com:8320111 |Plan = GPT Plus  
vebzbaooutlook.com:Sugar21212 |Plan = GPT Plus  
vivek@eyuva.com:$EyuvuSubhas009 |Plan = GPT Plus  
wahomeemutah13@gmail.com:wahomee100 |Plan = GPT Plus  
walterbeyn@hotmail.com:Tutubey1-19 |Plan = GPT Plus  
waqasahmadwik192727@gmail.com:incorrect92 |Plan = GPT Plus  
wardnj0720@gmail.com:Mickey52 |Plan = GPT Plus  
web.acwebexperts@gmail.com:$Ac08se0K |Plan = GPT Plus  
yaniele1@yahoo.com:Panchatras2022.. |Plan = GPT Plus  
yanq@chapchef.com:Kxft914717-1991 |Plan = GPT Plus  
yellowtreecanada@gmail.com:Mustanggt12019$ |Plan = GPT Plus  
yulihao2007@gmail.com:Euro15421 |Plan = GPT Plus  
z.s.marcos.j@gmail.com:ToBeMillionaire |Plan = GPT Plus  
zahrarizvi813@gmail.com:sana1jaz05 |Plan = GPT Plus  
Zaibaa.pathan@gmail.com:Dandelion1231 |Plan = GPT Plus  
zainlynx06@gmail.com:buratako123 |Plan = GPT Plus  
zellopvp@gmail.com:Chocolati1 |Plan = GPT Plus  
zordope@gmail.com:Lisa2019 |Plan = GPT Plus
```

Don't change password or email.....

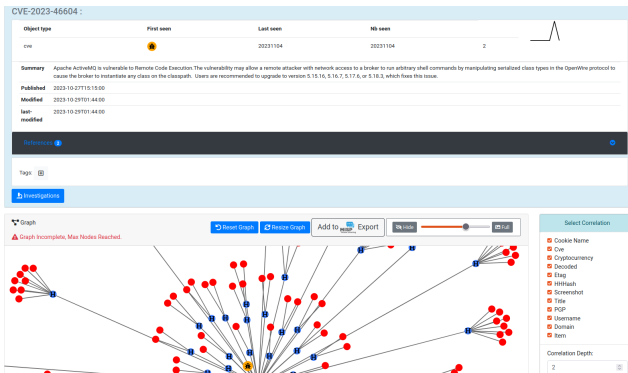
Infoleak automatic-detection=nsa **Infoleak** automatic-detection=credential



1427620096
Camva
5472920000338xxx

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

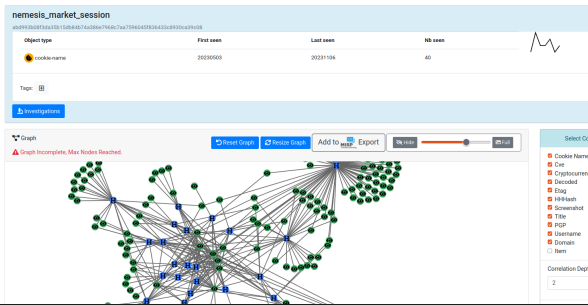
- Attribution and classification can be challenging for analysts. Facilitating integration with other tools, processes, and teams.
- **ALL leverages the entire MISP galaxy, including threat actor data, taxonomies, and the ability to assign tags to every item.**

The screenshot displays the MISP Galaxies interface. On the left is a sidebar with navigation options: Toggle Sidebar, Tags Search (with sub-options for Search Items by Tags, Search Domains by Tags, Search Decoded Items by Tags, and Search Screenshots by Tags), Tags Management (with sub-options for Taxonomies and Galaxies), Tags Export (with sub-option for MISP and Hive, auto push), Quick Search, and Credentials. The main content area is titled 'Galaxies:' and includes a 'Show' dropdown set to 'entries' and a search bar. Below this is a table with columns: Name, Description, Namespace, Enabled, Active Tags, and a settings icon. The table lists five galaxies:

Name	Description	Namespace	Enabled	Active Tags	
Backdoor	Malware Backdoor galaxy.	misp	✓	12/12	
360.net Threat Actors	Known or estimated adversary groups as identified by 360.net.	360net	✗	0/42	
Android	Android malware galaxy based on multiple open sources.	misp	✗	0/431	
Assets	ATT&CK for ICS Assets	mitre-attack-ics	✗	0/7	
Attack Pattern	ATT&CK Tactic	mitre-attack	✗	0/1086	

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**.

CSSF entities name search (mammouth)



Type  yara

Tracked custom-rules/2e3cbbb8-d093-49f4-9459-17138e38cae2.yar


Date 2023/09/12

Level Global

Yara Rule:

```
rule mammoth_CSSF {  
  
  meta:  
    description = "detect CSSF entities names"  
    author = "gallypette"  
  
  strings:  
    $x1 = "ALTRO LINK" nocase  
    $x2 = "ARVIRA S.à r.l." nocase  
    $x3 = "Alsages S.à r.l." nocase  
    $x4 = "DB2 CONSULT" nocase  
    $x5 = "DOORNBOS LAGERVELD & PARTNERS S.À R.L." nocase  
    $x6 = "EM Wealth Office S.A." nocase  
    $x7 = "FC Consult S.A." nocase  
    $x8 = "FINANCE ET PATRIMOINE S.A." nocase
```

NATO



Date 2023/06/06

Description None

Tags [Add tag](#)

Creator aduba@qirliu

Filters {
 "item": {}
}

Objects Match [Item](#)

[Show Objects](#)

```
rule nato  
{  
  meta:  
    author = "hoblar"  
    info = "Part of all-yara-rules"  
    reference = "https://github.com/all-project/all-yara-rules"  
  
  strings:  
    $s1 = "COSMIC TOP SECRET" fullword wide ascii nocase  
    $s2 = "NATO SECRET" fullword wide ascii nocase  
    $s3 = "ATOTAL" fullword wide ascii nocase  
    $s4 = "NATO CONFIDENTIAL" fullword wide ascii nocase  
    $s5 = "NATO RESTRICTED" fullword wide ascii nocase  
    $s6 = "THIS DOCUMENT CONTAINS NATO CLASSIFIED INFORMATION" fullword wide ascii nocase  
    $s7 = "NATO UNCLASSIFIED - INTERNAL" fullword wide ascii nocase  
    $s8 = "Secret OTAN" fullword wide ascii nocase  
    $s9 = "Confidential OTAN" fullword wide ascii nocase  
    $s10 = "Diffusion restreinte OTAN" fullword wide ascii nocase  
  
  condition:  
    1 of ($s*)
```

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**.

Father: crawled/2023/10/01/zerodayhukmtc56zualcmtvtto5xfz7gytgt7poxgkmgqgnq34p3xcyd.onion139a3549-5892-4dc1-91b3-4016e9b2c931

[Add to MISP](#) [Export](#) [Investigations](#) [Correlations Graph](#)

Crawler

Last Origin:

crawled/2023/10/01/zerodayhukmtc56zualcmtvtto5xfz7gytgt7poxgkmgqgnq34p3xcyd.onion139a3549-5892-4dc1-91b3-4016e9b2c931

zerodayhukmtc56zualcmtvtto5xfz7gytgt7poxgkmgqgnq34p3xcyd.onion139a3549-5892-4dc1-91b3-4016e9b2c931

url <http://zerodayhukmtc56zualcmtvtto5xfz7gytgt7poxgkmgqgnq34p3xcyd.onion139a3549-5892-4dc1-91b3-4016e9b2c931>

politics-military-technology-intelligence-well-paid?pid=1468609#pid1

Full resolution

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 and MISP-LEA.

