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 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**.

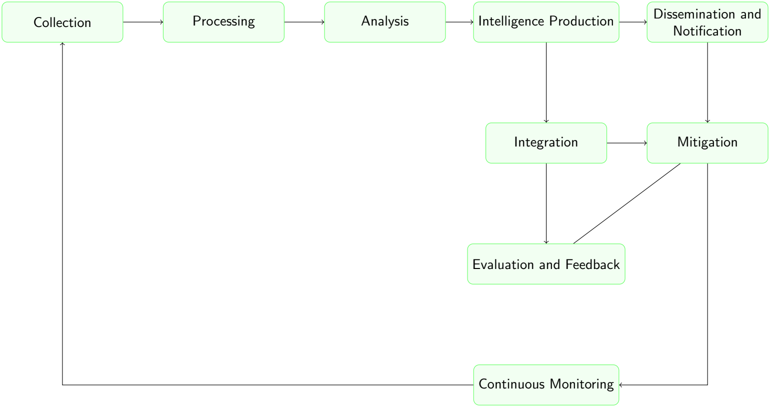
[1] `https://www.ail-project.org/`

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



Common questions from constituents

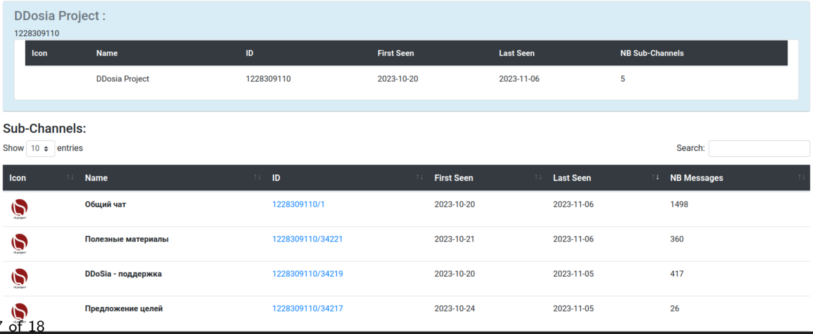
- Do you **know if we are a target** of this adversary group?
- We have **observed a partnering company experiencing a ransomware incident**, and we are concerned about the impact on our organization.
- Can you determine if our **sector is a target** of this threat actor?
- Have you come across phishing 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

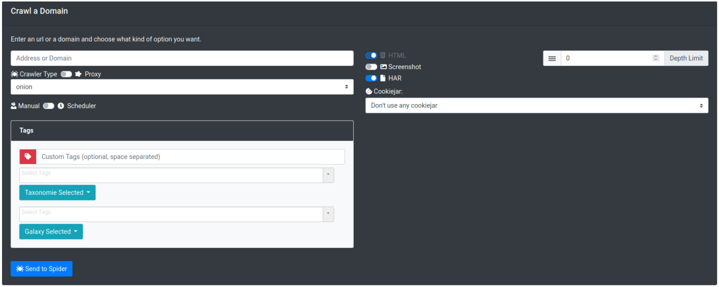
Icon	Name	ID	First Seen	Last Seen	NB Sub-Channels
	DDosia Project	1228309110	2023-10-20	2023-11-06	5

Sub-Channels:

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 groups[3], 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 ○ Proxy

onion

Manual ○ Scheduler

● HTML

○ Screenshot

● HAR

Cookiejar:

Don't use any cookiejar

0 Depth Limit

Tags

Custom Tags (optional, space separated)

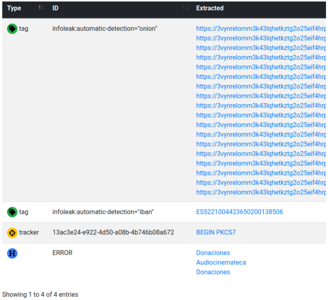
Select Tags

Select Tags

[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.

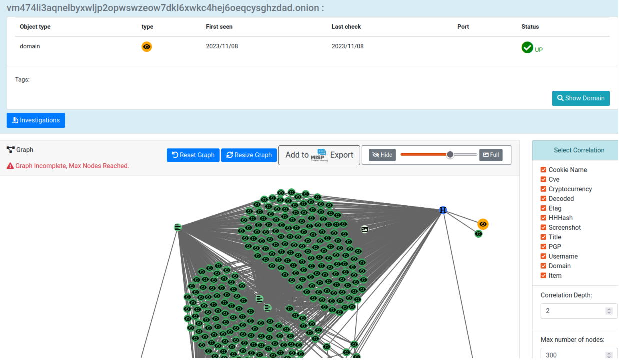


Type	ID	Extracted
tag	infoleak:automatic-detection="onion"	https://3vynrelomm3k43lqhetkztg2o25eif4hrp https://3vynrelomm3k43lqhetkztg2o25eif4hrp https://3vynrelomm3k43lqhetkztg2o25eif4hrp https://3vynrelomm3k43lqhetkztg2o25eif4hrp https://3vynrelomm3k43lqhetkztg2o25eif4hrp https://3vynrelomm3k43lqhetkztg2o25eif4hrp https://3vynrelomm3k43lqhetkztg2o25eif4hrp https://3vynrelomm3k43lqhetkztg2o25eif4hrp https://3vynrelomm3k43lqhetkztg2o25eif4hrp https://3vynrelomm3k43lqhetkztg2o25eif4hrp https://3vynrelomm3k43lqhetkztg2o25eif4hrp https://3vynrelomm3k43lqhetkztg2o25eif4hrp https://3vynrelomm3k43lqhetkztg2o25eif4hrp https://3vynrelomm3k43lqhetkztg2o25eif4hrp https://3vynrelomm3k43lqhetkztg2o25eif4hrp https://3vynrelomm3k43lqhetkztg2o25eif4hrp https://3vynrelomm3k43lqhetkztg2o25eif4hrp https://3vynrelomm3k43lqhetkztg2o25eif4hrp
tag	infoleak:automatic-detection="iban"	ES5221004423650200138506
tracker	13ac3e24-e922-4d50-a08b-4b746b08a672	BEGIN PKCS7
H	ERROR	Donaciones Audiocinemateca Donaciones

Showing 1 to 4 of 4 entries

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**.



vm474li3aqnelbyxwljp2opwswzeow7dkl6xwkc4hej6oeqcysghzdad.onion :

Object type	type	First seen	Last check	Port	Status
domain	👁	2023/11/08	2023/11/08		✓ UP

Tags:

Graph

Graph Incomplete, Max Nodes Reached.

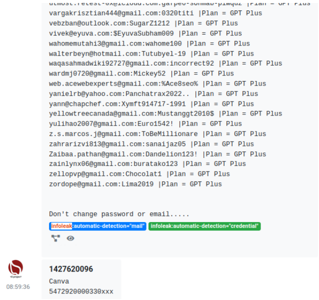
- ☑ Cookie Name
- ☑ Cve
- ☑ Cryptocurrency
- ☑ Decoded
- ☑ Etag
- ☑ HHHash
- ☑ Screenshot
- ☑ Title
- ☑ PGP
- ☑ Username
- ☑ Domain
- ☑ Item

Correlation Depth: 2

Max number of nodes: 300

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**.



```
utmost.retest-0x@icloud.com:garpe0-sohmab-piwquz |Plan = GPT Plus
vargakrisztian444@gmail.com:0320titi |Plan = GPT Plus
vebzban@outlook.com:SugarZ1212 |Plan = GPT Plus
vivek@eyuva.com:$EyuvaSubham009 |Plan = GPT Plus
wahomemutahi3@gmail.com:wahome100 |Plan = GPT Plus
walterbeyn@hotmail.com:Tutubyel-19 |Plan = GPT Plus
waqasahmadwiki92727@gmail.com:incorrect92 |Plan = GPT Plus
wardmj0720@gmail.com:Mickey52 |Plan = GPT Plus
web.acewebexperts@gmail.com:%Ace8seo% |Plan = GPT Plus
yanielrb@yahoo.com:Panchatrax2022.. |Plan = GPT Plus
yann@chapchef.com:Xymft914717-1991 |Plan = GPT Plus
yellowtreecanada@gmail.com:Mustanggt2010$ |Plan = GPT Plus
yulihao2007@gmail.com:Euro1542! |Plan = GPT Plus
z.s.marcos.j@gmail.com:ToBeMillionare |Plan = GPT Plus
zahrarizvi813@gmail.com:sanaijaz05 |Plan = GPT Plus
Zaibaa.pathan@gmail.com:Dandelion123! |Plan = GPT Plus
zainlynx06@gmail.com:buratako123 |Plan = GPT Plus
zellopvp@gmail.com:Chocolat1 |Plan = GPT Plus
zordope@gmail.com:Lima2019 |Plan = GPT Plus


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

infoleak:automatic-detection="mail"
infoleak:automatic-detection="credential"

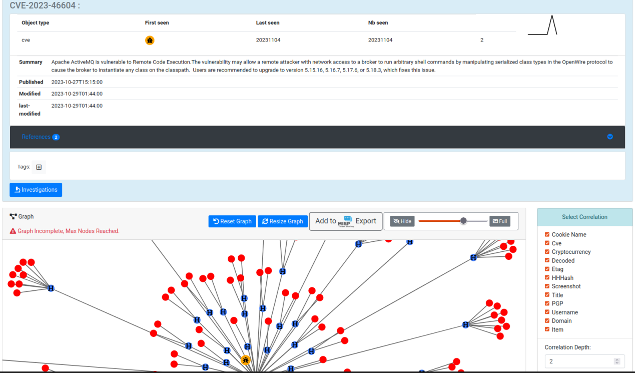
08:59:36

1427620096

```
Canva
5472920000330xxx
```

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).



CVE-2023-46604 :

Object type	First seen	Last seen	Nb seen	
cve	🐞	20231104	20231104	2

Summary	Apache ActiveMQ is vulnerable to Remote Code Execution.The vulnerability may allow a remote attacker with network access to a broker to run arbitrary shell commands by manipulating serialized class types in the OpenWire protocol to cause the broker to instantiate any class on the classpath. Users are recommended to upgrade to version 5.15.16, 5.16.7, 5.17.6, or 5.18.3, which fixes this issue.
Published	2023-10-27T15:15:00
Modified	2023-10-29T01:44:00
last-modified	2023-10-29T01:44:00

References 2

Tags: ⊞

Investigations

Graph

Graph Incomplete, Max Nodes Reached.

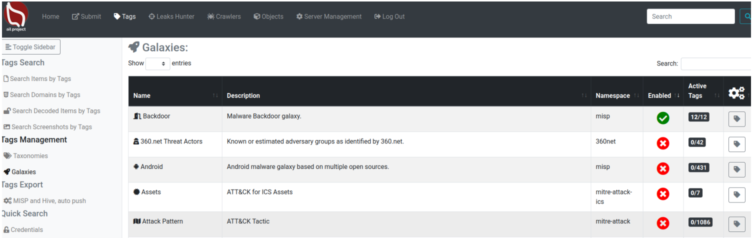
Select Correlation

☑ Cookie Name
☑ Cve
☑ Cryptocurrency
☑ Decoded
☑ Etag
☑ HHHash
☑ Screenshot
☑ Title
☑ PGP
☑ Username
☑ Domain
☑ Item

Correlation Depth: 2

Analysis - Standardising labels and taxonomies

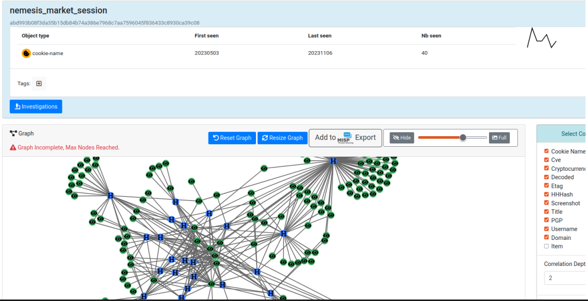
- Attribution and classification can be challenging for analysts. Facilitating integration with other tools, processes, and teams.
- AIL **leverages the entire MISP galaxy, including threat actor data, taxonomies**, and the ability to assign tags to every item.



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.



nemesis_market_session

abd993b08f3da35b15db84b74a386e7968c7aa7596045f836433c8930ca39c08

Object type	First seen	Last seen	Nb seen
cookie-name	20230503	20231106	40

Tags: ⊞

Investigations

Graph

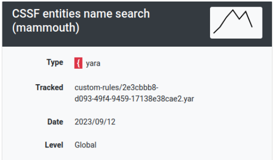
Graph Incomplete, Max Nodes Reached.

☑ Cookie Name
☑ Cve
☑ Cryptocurrenc
☑ Decoded
☑ Etag
☑ HHHash
☑ Screenshot
☑ Title
☑ PGP
☑ Username
☑ Domain
☐ Item

Correlation Dept: 2

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**.



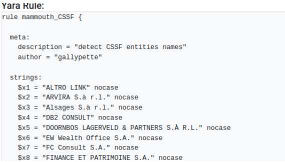
CSSF entities name search (mammouth)

Type yara

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

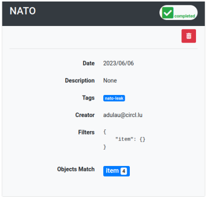
Date 2023/09/12

Level Global



Yara Rule:

```
rule mammouth_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 = "EW Wealth Office S.A." nocase
    $x7 = "FC Consult S.A." nocase
    $x8 = "FINANCE ET PATRIMOINE S.A." nocase
```



NATO

Date 2023/06/06

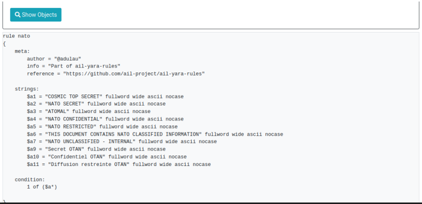
Description None

Tags nato-leak

Creator adulau@circl.lu

Filters
```
{
    "item": {}
}
```

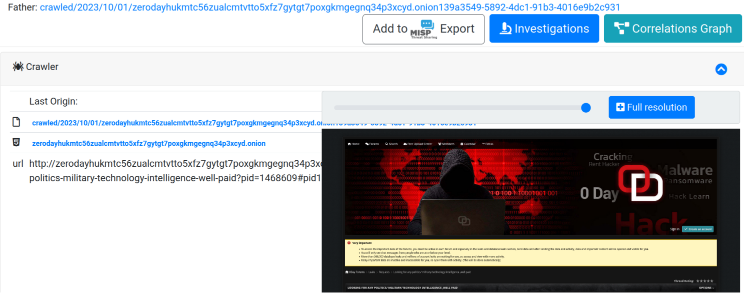
Objects Match item 4



```
rule nato
{
    meta:
        author = "@adulau"
        info = "Part of ail-yara-rules"
        reference = "https://github.com/ail-project/ail-yara-rules"

    strings:
        $a1 = "COSMIC TOP SECRET" fullword wide ascii nocase
        $a2 = "NATO SECRET" fullword wide ascii nocase
        $a3 = "ATOMAL" fullword wide ascii nocase
        $a4 = "NATO CONFIDENTIAL" fullword wide ascii nocase
        $a5 = "NATO RESTRICTED" fullword wide ascii nocase
        $a6 = "THIS DOCUMENT CONTAINS NATO CLASSIFIED INFORMATION" fullword wide ascii nocase
        $a7 = "NATO UNCLASSIFIED - INTERNAL" fullword wide ascii nocase
        $a9 = "Secret OTAN" fullword wide ascii nocase
        $a10 = "Confidentiel OTAN" fullword wide ascii nocase
        $a11 = "Diffusion restreinte OTAN" fullword wide ascii nocase

    condition:
        1 of ($a*)

}
```

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/zerodayhukmtc56zualcmtvtto5xfz7gytgt7poxgkmgegnq34p3xcyd.onion139a3549-5892-4dc1-91b3-4016e9b2c931

Last Origin:

crawled/2023/10/01/zerodayhukmtc56zualcmtvtto5xfz7gytgt7poxgkmgegnq34p3xcyd.o

zerodayhukmtc56zualcmtvtto5xfz7gytgt7poxgkmgegnq34p3xcyd.onion

url http://zerodayhukmtc56zualcmtvtto5xfz7gytgt7poxgkmgegnq34p3x
politics-military-technology-intelligence-well-paid?pid=1468609#pid1

Very important

- To access the important data of the forums, you must be active in each forum and especially in the leaks and database leaks section, send data and after sending the data and activity, data and important content will be opened and visible for you.
- You will only see chat messages from people who are at or below your level.
- More than 500,000 database leaks and millions of account leaks are waiting for you, so access and view with more activity.
- Many important data are inactive and inaccessible for you, so open them with activity. (This will be done automatically)

0Day Forums › Leaks › Requests › Looking for any politics/ military/technology intelligence ,well paid

Thread Rating: ★★★★★

LOOKING FOR ANY POLITICS/ MILITARY/TECHNOLOGY INTELLIGENCE ,WELL PAID

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`