AIL Framework for Analysis of Information Leaks

Practical and Efficient Data-Mining of Suspicious Websites, Forums and Tor Hidden-Services

CIRCL
Computer Incident
Response Center
Luxembourg

Alexandre Dulaunoy
alexandre.dulaunoy@circl.lu
Aurelien Thirion
aurelien.thirion@circl.lu

info@circl.lu

July 10, 2024

Links

- AIL project website `https://ail-project.org`
- AIL project open source framework `https://github.com/ail-project`
- AIL framework `https://github.com/ail-project/ail-framework`
- Training materials `https://github.com/ail-project/ail-training`
- Mastodon `https://infosec.exchange/@ail_project`
- Online chat `https://gitter.im/ail-project/community`

Legal and Ethics

Privacy, AIL and GDPR (PII)

- Many modules in AIL can process personal data and even special categories of data as defined in GDPR (Art. 9).
- The data controller is often the operator of the AIL framework (limited to the organisation) and has to define **legal grounds for processing personal data**.
- To help users of AIL framework, a document is available which describe points of AIL in regards to the regulation[1].

[1] `https://www.circl.lu/assets/files/information-leaks-analysis-and-gdpr.pdf`

Potential legal grounds

- **Consent of the data subject** is in many cases not feasible in practice and often impossible or illogical to obtain (Art. 6(1)(a)).
- Legal obligation (Art. 6(1)(c)) - This legal ground applies mostly to CSIRTs, in accordance with the powers and responsibilities set out in CSIRTs mandate and with their constituency, as they may have the legal obligation to collect, analyse and share information leaks without having a prior consent of the data subject.
- Art. 6(1)(f) - Legitimate interest - Recital 49 explicitly refers to CSIRTs' right to process personal data provided that they have a legitimate interest but not colliding with fundamental rights and freedoms of data subject.

Ethics in Information Security and Cybersecurity

- The materials and tools presented can open a significant numbers of questions regarding ethics;
- Our researches and tools are there for education, supporting the public good and improve incident response;
- We ask all users and participants to **follow ethical principles and act professionaly**[2].

[2] https://www.acm.org/code-of-ethics
https://www.first.org/global/sigs/ethics/ethics-first

Introduction

Concepts - Deep Web

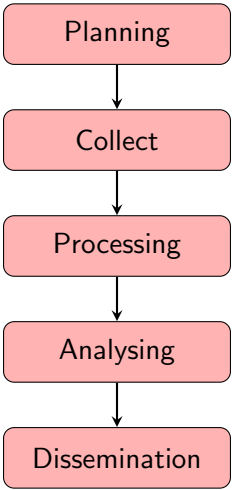
- **Deep Web** is the part of World Wide Web not indexed or directly accessible by standard web search-engines;
- This can be content hidden from **crawlers** by requiring a specific access and this can includes private social media, password-protected forums or content protected by different measures such as paywalls or specific security interface to access the information;
- A large portion of content accessible via Internet is part of the deep web[3].

[3] also called invisible web, hidden web or non-indexed web

Concepts - darknet

- **Darknet** is an overlay network running on top of Internet requiring specific software to access the network and its services;
- Tor, I2P and Freenet are the most commonly used ones. Many are used for hidden services access and some for proxy access to the Internet;
- There are **legitimate use-cases** for such network but also many **illegal or criminal usage**.

Lifecycle of collection and analysis



Collecting, processing and analysing content - web pages

- Building a search engine on the web is a challenging task because:
  - it has to crawl webpages,
  - it has to to make sense of **unstructured data**,
  - it has to **index** these data,
  - it has to provide a way to retrieve data and structure data (e.g. correlation).
- Doing so on Tor is even more challenging because:
  - services don't always want to be found,
  - parts of the dataset have to be discarded.
- in each case, it requires a lot of bandwidth, storage and computing power.

Collecting, processing and analysing content - structured data

- Some data are structured and are easy to process:
  - metadata!
  - API responses.
- Some even provide cryptographic evidences:
  - authentication mechanisms between peers,
  - OpenGPG can leak a lot of metadata
    - key ids,
    - subject of email in thunderbird,
  - Bitcoin's Blockchain is public,
  - pivoting on these data with external sources yields interesting results.

AIL design Objectives

Objectives of the session

- Show how to use and extend an open source tool to monitor web pages, pastes, chats, forums and hidden services
- Explain challenges and the design of the AIL open source framework
- Review different **collection mechanisms** and **sources**
- Learn how to create new modules
- Learn how to use, install and start AIL
- **Supporting investigation using the AIL framework** and including it in cyber threat intelligence life cycle

AIL Framework

From a requirement to a solution: AIL Framework

History:

- AIL initially started as an **internship project** (2014) to evaluate the feasibility to automate the analysis of (un)structured information to find leaks.
- In 2019, AIL framework is an **open source software** in Python. The software is actively used (and maintained) by CIRCL and many organisations.
- In 2020, AIL framework is now a complete project called **ail project**[4].
- In 2023, AIL framework version 5.0 released with new datastorage back-end.

[4] `https://github.com/ail-project/`

Capabilities Overview

Common usage

- **Check** if mail/password/other sensitive information (terms tracked) leaked
- **Detect** reconnaissance of your infrastructure
- **Search** for leaks inside an archive
- **Monitor** and crawl chats/websites

Support CERT and Law Enforcement activities

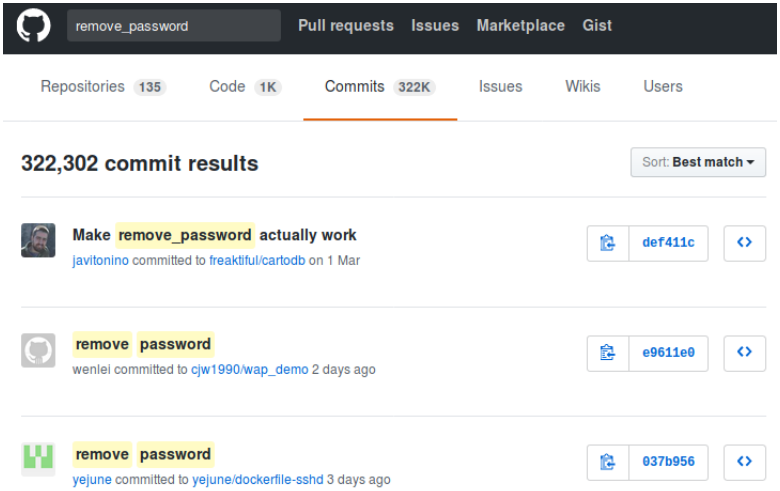
- Proactive investigation: leaks detection
  - List of emails and passwords
  - Leaked database
  - AWS Keys
  - Credit-cards
  - PGP private keys
  - Certificate private keys
- Feed Passive DNS or any passive collection system
- CVE and PoC of vulnerabilities most used by attackers

Support CERT and Law Enforcement activities

- Website monitoring
  - monitor booters
  - Detect encoded exploits (WebShell, malware encoded in Base64, ...)
  - SQL injections
- Chat/Channel monitoring
  - Monitor Threat Actor Chat and Community Activities
- Automatic and manual submission to threat sharing and incident response platforms
  - MISP
  - TheHive
- Term/Regex/YARA monitoring for local companies/government

Sources of leaks

Mistakes from users:

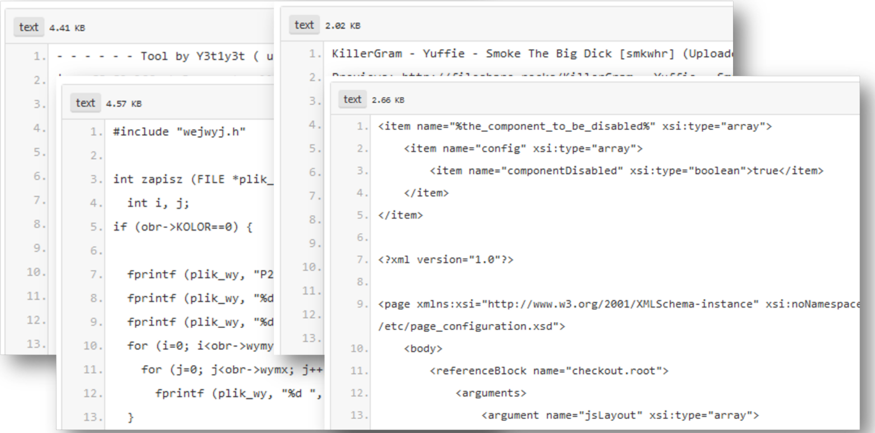


Sources of Leaks: Paste Monitoring

- **Example:** `https://gist.github.com/`
  - Easily stores and shares text online
  - Used by programmers and legitimate users
    → Source code & configuration information

- **Abused by attackers to store:**
  - Lists of vulnerable/compromised sites
  - Software vulnerabilities (e.g., exploits)
  - Database dumps
    → User data
    → Credentials
    → Credit card details
  - Increasingly more sensitive information

Examples of pastes (items)



Why So Many Leaks?

- **Economic Interests:**
  - Adversaries promoting services
- **Ransom Model:**
  - To publicly pressure the victims
- **Political Motives:**
  - Adversaries showing off
- **Collaboration:**
  - Criminals need to collaborate
- **Operational Infrastructure:**
  - Malware exfiltrating information on a paste website
- **Mistakes and Errors from Users**

What's your role while discovering such leak?

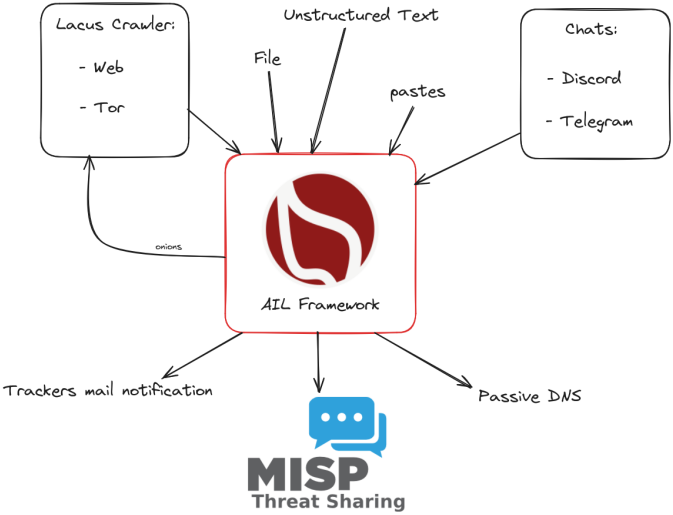
As a CSIRT, we must address this issue.

- **Contacting companies or organizations** responsible for accidental leaks
- **Engaging with the media** about specific leak cases to ensure practical and factual reporting
- **Evaluating the economic landscape** for cyber criminals (e.g., DDoS booters[5] or the resale of personal information - comparing reality versus media coverage)
- **Analyzing collateral effects** of malware, software vulnerabilities, or data exfiltration

[5] https://github.com/D4-project/

Current capabilities

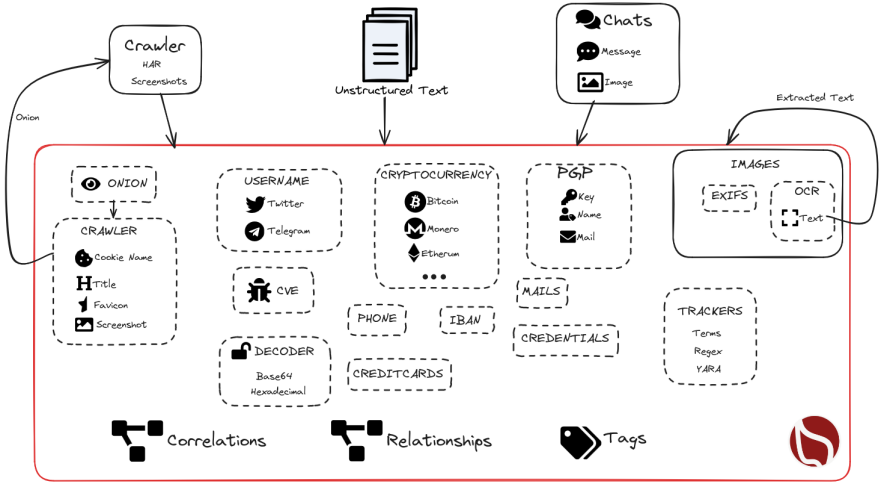
High Level Overview



AIL Framework: Extensible capabilities

- Extending AIL to add a new **analysis module** can be done in 50 lines of Python
- The framework **supports multi-processors/cores by default**. Any analysis module can be started multiple times to support faster processing during peak times or bulk import
- **Multiple** concurrent **data inputs**
- Tor Crawler (handle cookies authentication)
- Feeders: Discord, Telegram, ...

Analysis of unstructured information



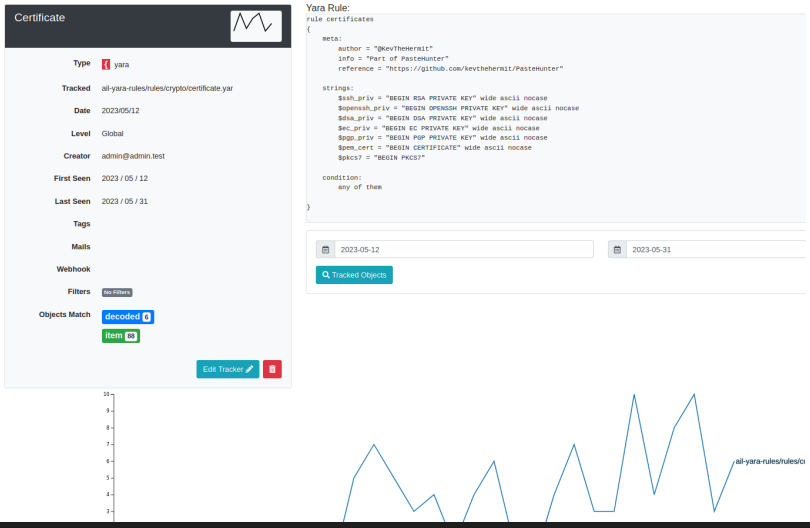
AIL Framework: Features

- Extracting **credit card numbers, credentials, phone numbers, ...**
- Extracting and validating potential **hostnames**
- Keeps track of **duplicates**
- Submission to threat sharing and incident response platforms (**MISP** and **TheHive**)
- **Full-text indexer** to index unstructured information
- **Tagging** for classification and searches
- Terms, sets, regex and YARA **tracking, occurrences, and history**
- Archives, files, and raw **submission** from the UI
- Correlation engine based on PGP ID, cryptocurrencies, decoded (Base64, ...), usernames, cookie names, and many selectors to find relationships
- And many more

Trackers - Retro Hunt

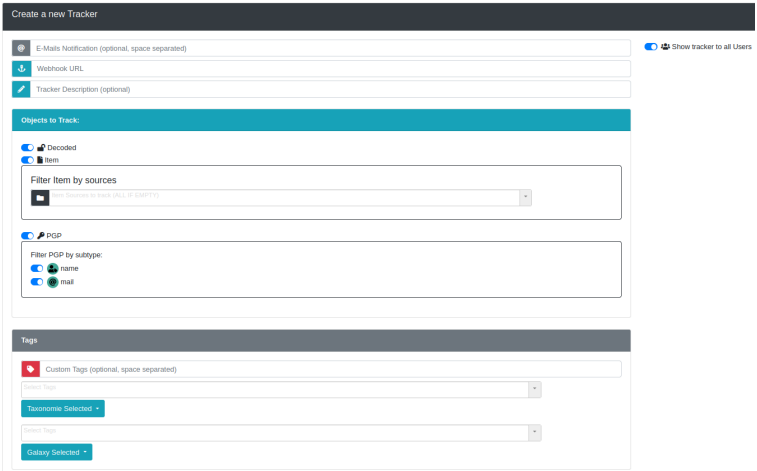
- Search and monitor specific keywords/patterns
  - Automatic Tagging
  - Email Notifications
- Track Word
  - ddos
- Track Set
  - booter,ddos,stresser;2
- Track Regex
  - circl\.lu
- YARA rules
  - https://github.com/ail-project/ail-yara-rules

YARA Tracker

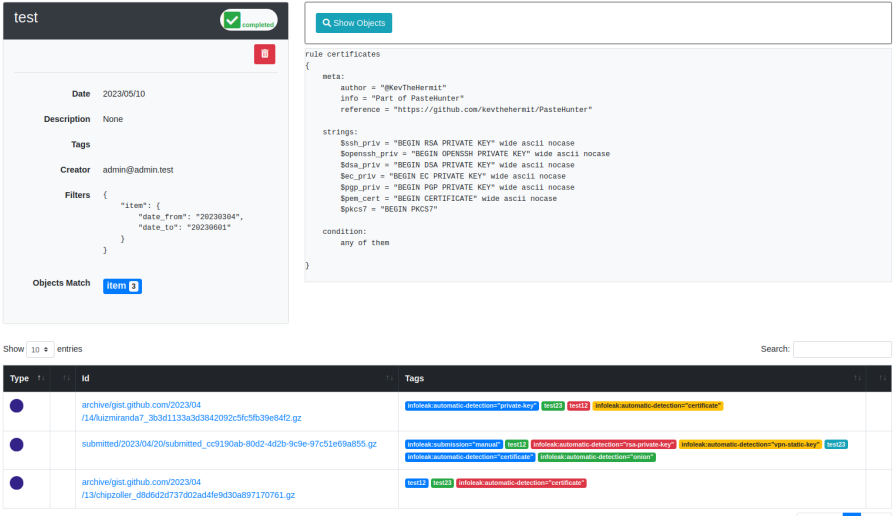


Trackers - Practical part

- **Create and test** your own tracker



Retro Hunt


test
completed
Date
2023/05/10
Description
None
Tags
Creator
admin@admin.test
Filters
{
"item": {
"date_from": "20230304",
"date_to": "20230601"
}
}
Objects Match
item 3
Show Objects
rule certificates
{
meta:
author = "@KevTheHermit"
info = "Part of PasteHunter"
reference = "https://github.com/kevthehermit/PasteHunter"
strings:
$ssh_priv = "BEGIN RSA PRIVATE KEY" wide ascii nocase
$openssh_priv = "BEGIN OPENSSH PRIVATE KEY" wide ascii nocase
$dsa_priv = "BEGIN DSA PRIVATE KEY" wide ascii nocase
$ec_priv = "BEGIN EC PRIVATE KEY" wide ascii nocase
$pgp_priv = "BEGIN PGP PRIVATE KEY" wide ascii nocase
$pem_cert = "BEGIN CERTIFICATE" wide ascii nocase
$pkcs7 = "BEGIN PKCS7"
condition:
any of them
}
Show 10 entries
Search:
Type
Id
Tags
archive/gist.github.com/2023/04/14/luizmiranda7_3b3d1133a3d3842092c5fc5fb39e84f2.gz
infoleak:automatic-detection="private-key"
test23
test12
infoleak:automatic-detection="certificate"
submitted/2023/04/20/submitted_cc9190ab-80d2-4d2b-9c9e-97c51e69a855.gz
infoleak:submission="manual"
test12
infoleak:automatic-detection="rsa-private-key"
infoleak:automatic-detection="vpn-static-key"
test23
infoleak:automatic-detection="certificate"
infoleak:automatic-detection="onion"
archive/gist.github.com/2023/04/13/chipzoller_d8d6d2d737d02ad4fe9d30a897170761.gz
test12
test23
infoleak:automatic-detection="certificate"

Recon and intelligence gathering tools

- **Attacker also share informations**
- Recon tools detected: 94
  - sqlmap
  - dnscan
  - whois
  - msfconsole (metasploit)
  - dnmap
  - nmap
  - ...

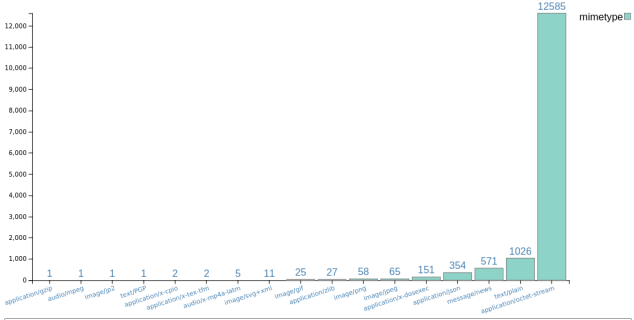
Recon and intelligence gathering tools

```
##############################################################################################
==============================================================================================
Hostname        www.pabloquintanilla.cl                 ISP     Wix.com Ltd.
Continent       North America           Flag
US
Country         United States           Country Code    US
Region  Unknown                 Local time      19 Nov 2019 07:59 CST
City    Unknown                 Postal Code     Unknown
IP Address      185.230.60.195          Latitude        37.751
                        Longitude       -97.822
==============================================================================================
##############################################################################################
> www.pabloquintanilla.cl
Server:         38.132.106.139
Address:        38.132.106.139#53

Non-authoritative answer:
www.pabloquintanilla.cl canonical name = www192.wixdns.net.
www192.wixdns.net       canonical name = balancer.wixdns.net.
Name:   balancer.wixdns.net
Address: 185.230.60.211
>
##############################################################################################
Domain name: pabloquintanilla.cl
Registrant name: SERGIO TORO
```

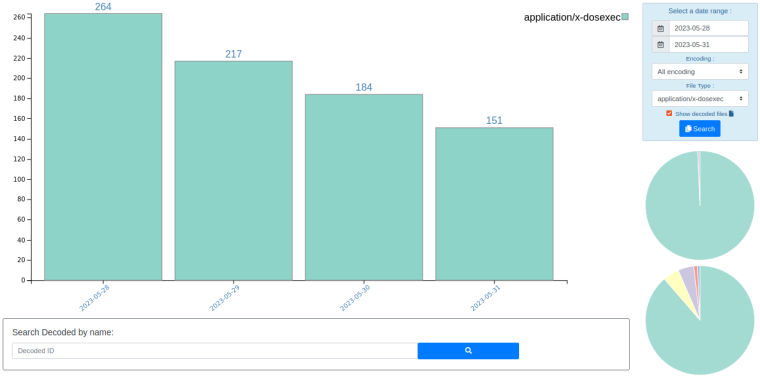
Decoder

- Search for encoded strings
  - Base64
  - Hexadecimal
  - Binary
- Guess Mime-type
- Items/Domains Correlation

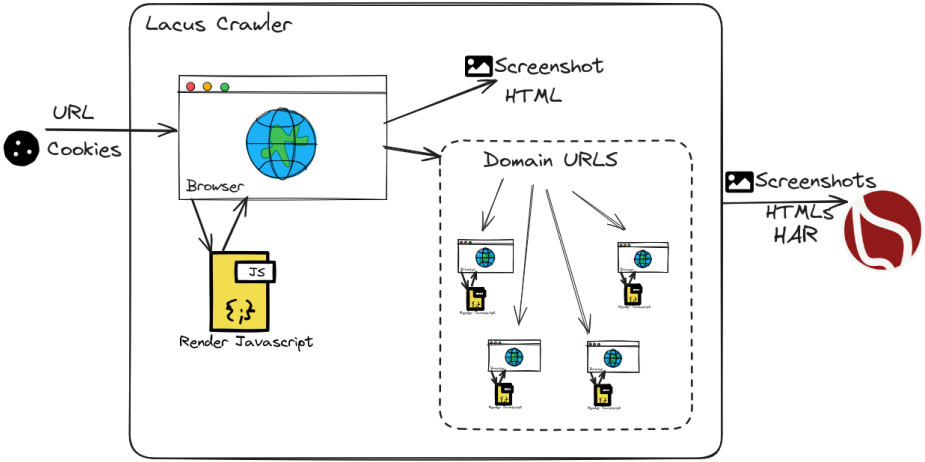
Decoder:


mimetype
12585
1026
571
354
151
65
58
27
25
11
5
2
2
1
1
1
Select a date range :
2023-05-31
2023-05-31
Encoding :
All encoding
File Type :
All types
show decoded files
Search
Search Decoded by name:
Decoded ID
20230531 Decoded files:
Show 10 entries
Search:
estimated type
hash
first seen
last seen
nb item
size
Virus Total
Sparkline
image/gif
ee0bc07fef6baeb22c8ec1364a4bef2df840dc3e05
20230404
20230531
214708
1108
Virus Total submission is disabled
image/png
b009399cefaa0e82086453da04a887105ca2f6a4
20230404
20230531
8404
1054
Virus Total submission is disabled
application/json
f9f918ba5b0a35f5e2523bdbf4ece6bd2cda11f9
20230410
20230531
3947
44
Virus Total submission is disabled

Decoder:


application/x-dosexec
264
217
184
151
260
240
220
200
180
160
140
120
100
80
60
40
20
0
2023-05-28
2023-05-29
2023-05-30
2023-05-31
Select a date range :
2023-05-28
2023-05-31
Encoding :
All encoding
File Type :
application/x-dosexec
Show decoded files
Search
Search Decoded by name:
Decoded ID
20230528 to 20230531 Decoded files:
Show 10 entries
Search:
estimated type
hash
first seen
last seen
nb item
size
Virus Total
Sparkline
application/x-dosexec
c408501f7f2bd8279704c380dd61d329c6119fc2
20230421
20230529
76
64
Virus Total submission is disabled
application/x-dosexec
a9ecbb74ce7d22b70f0dc0f57299f31ce570161
20230405
20230530
56
55666
Virus Total submission is disabled
application/x-dosexec
e5805aa6a66c6e013d5ebddbab4fbc45b4c84127
20230529
20230531
4
32
Virus Total submission is disabled

Collection - Lacus Crawler



Crawler

- Crawlers are used to navigate on regular website as well as .onion addresses (via automatic extraction of urls or manual submission)
- Lacus[6] ("scriptable" browser) is rending the pages (including javascript) and produce screenshots (HAR archive too)
- How a domain is crawled by default:
  1. Fetch the first url
  2. Render javascript (webkit browser)
  3. Extract all urls
  4. Filter url: keep all url of this domain
  5. crawl next url (max depth = 1)

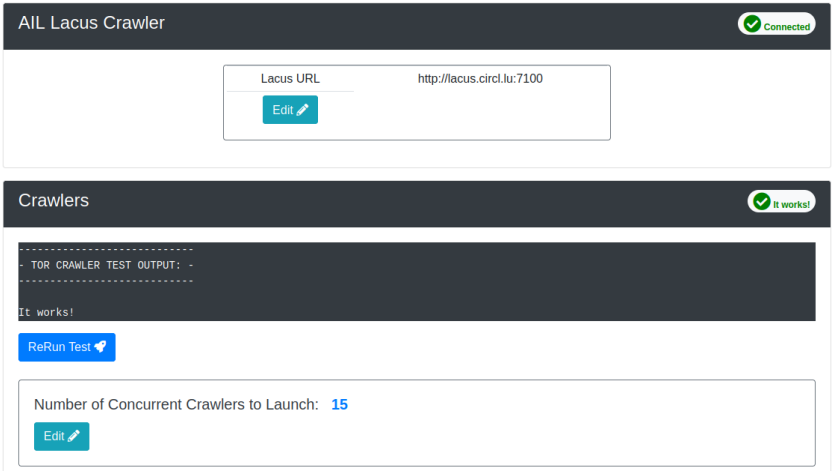
[6] `https://github.com/ail-project/lacus`

Lacus

- Lacus[7] is a capturing system using playwright, as a web service
- AIL utilizes Lacus for fetching and rendering domains.
  - Lacus can be installed and executed outside of AIL,
  - Enqueue what you want to capture,
  - Trigger the capture,
  - Get the capture result,

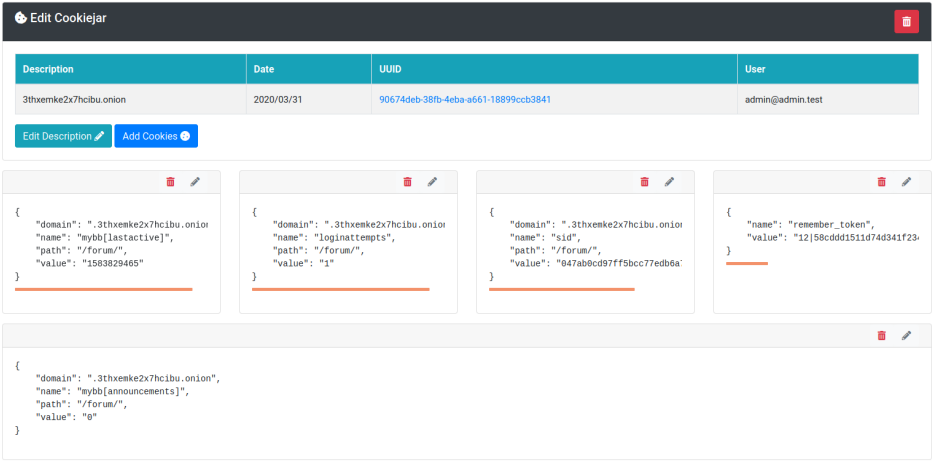
[7] `https://github.com/ail-project/lacus`

Crawler Settings - Lacus

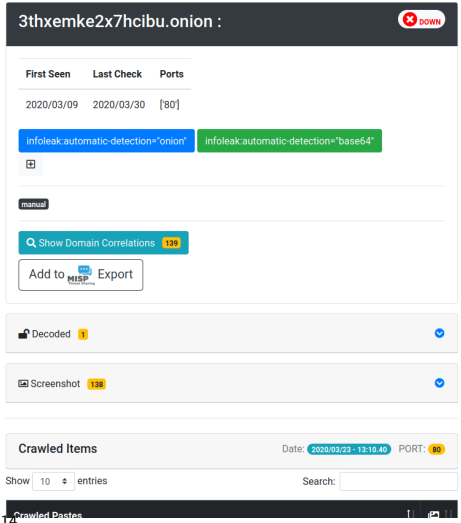


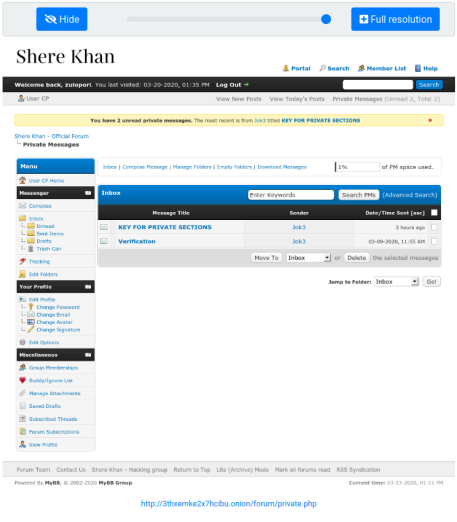
Crawler: Cookiejar

Use your cookies to login and bypass captcha



Crawler: Cookiejar

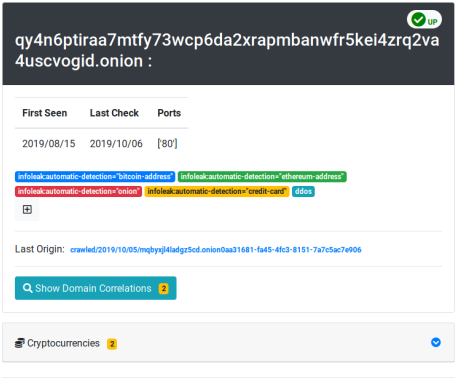


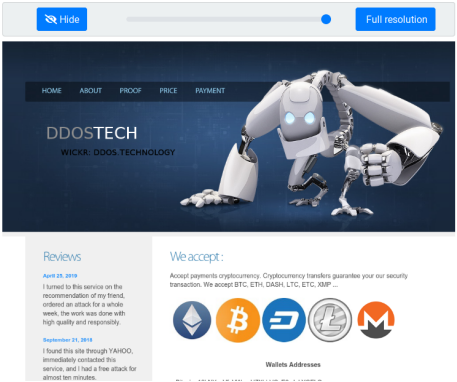


http://3thxemke2x7hcibu.onion/forum/private.php

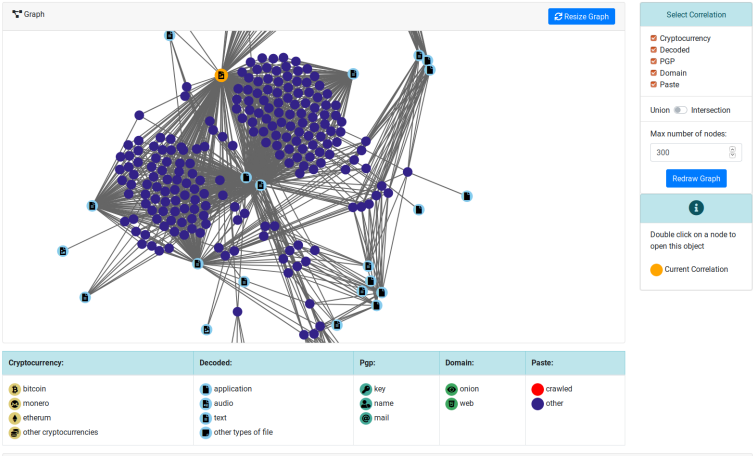
Live demo!

Crawler: DDoS Booter

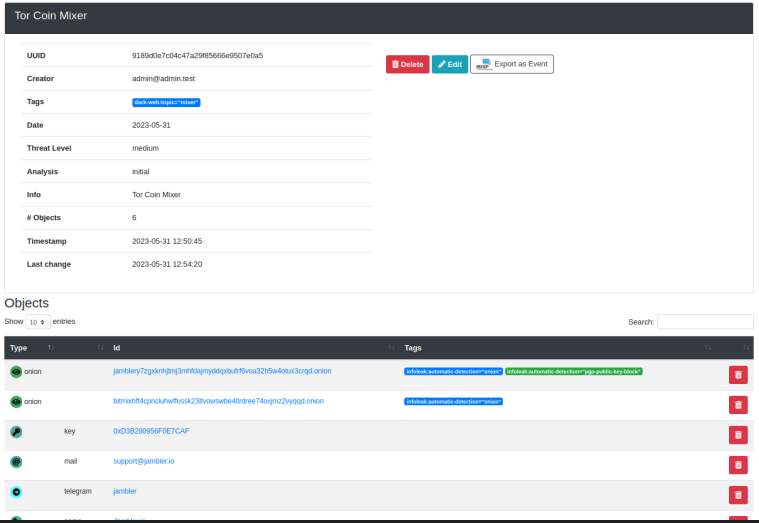




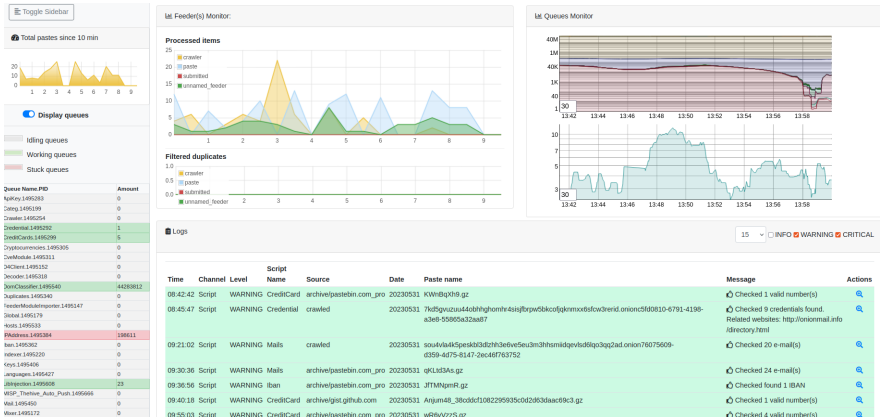
Correlations and relationship



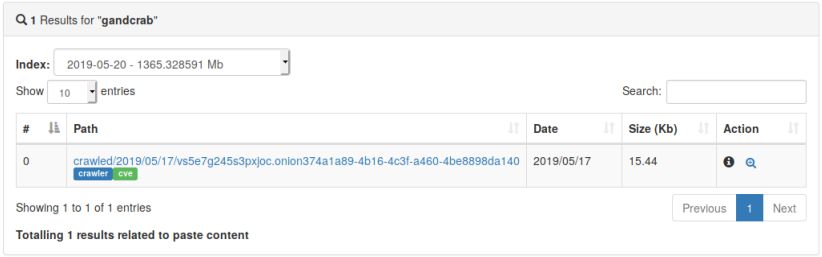
Investigations



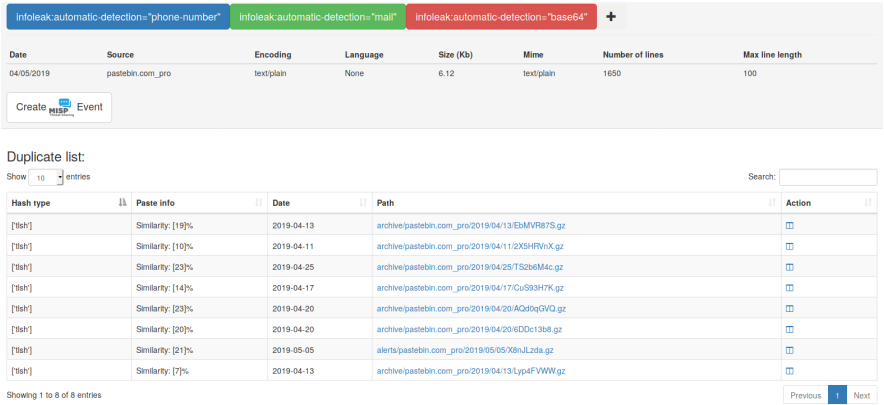
Example: Dashboard



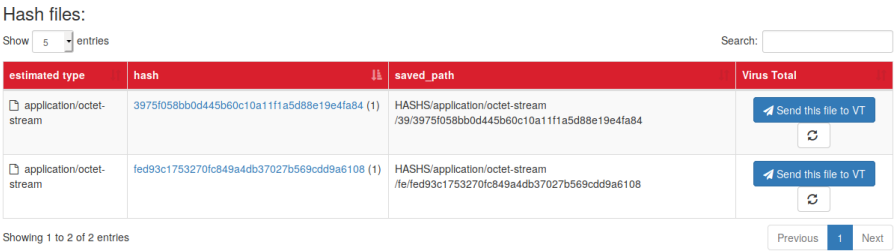
Example: Text search



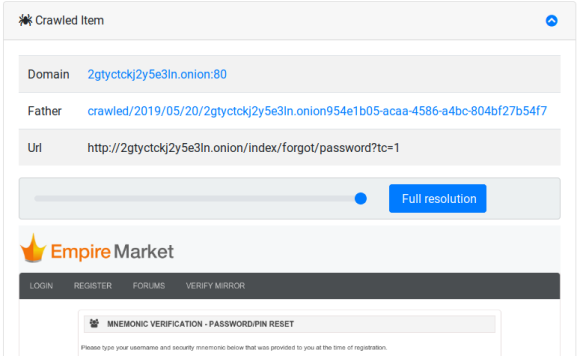
Example: Items Metadata (1)



Example: Items Metadata (2)



Example: Items Metadata (3)



Example: Browsing content

Content:

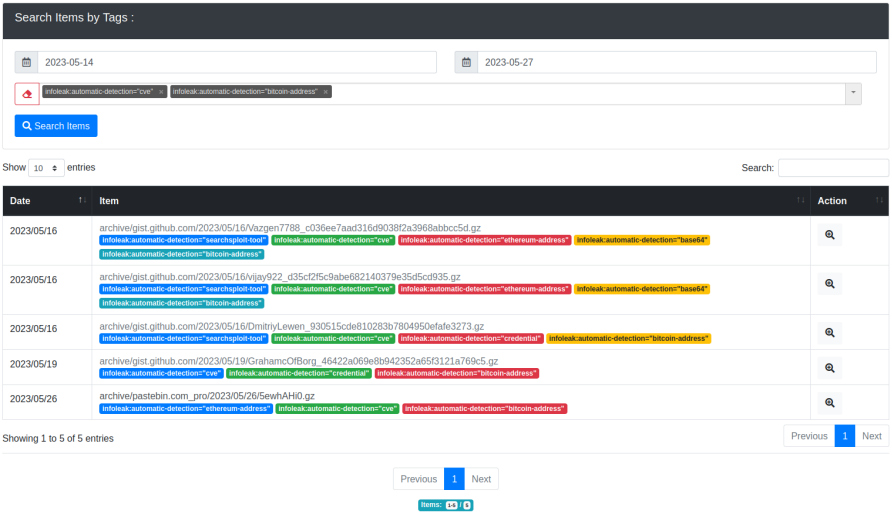
```
http://members2.mofosnetwork.com/access/login/
somosextremos:buddy1990
brazzers_glenn:cocklick
brazzers61:braves01

http://members.naughtyamerica.com/index.php?m=login
gernblanston:3unc2352
Janhuss141200:310575
igetalliwant:1377zeph
pwilks89:mon22key
Bman1551:hockey

MoFos IKnowThatGirl PublicPickUps
http://members2.mofos.com
Chrismagg40884:loganm40
brando1:zzbrando1
aacoen:1q2w3e4r
1rstunkle23:my8self

BraZZers
http://ma.brazzers.com
gcjensen:gcj21pva
skycsc17:rbcdnd

                                ##########################################################
                                    >| Get Daily Update Fresh Porn Password Here |<

                                          =>   http://www.erq.io/4mF1
```

Example: Browsing content

Content:

```
Over 50000+ custom hacked xxx passwords by us! Thousands of free xxx passwords to the hottest paysites!

############################################################
 >| Get Fresh New Premium XXX Site Password Here |<

  =>   http://www.erq.io/4mF1


############################################################



http://ddfnetwork.com/home.html
eu172936:hCSBgKh
UecwB6zs:159X0$!r#6K78FuU

http://pornxn.stiffia.com/user/login
feldwWek8939:RObluJ8XtB
dabudka:17891789
brajits:brajits1

http://members.pornstarplatinum.com/sblogin/login.php/
gigiriveracom:xxxjay
jayx123:xxxjay69

http://members.vividceleb.com/
Rufio99:fairhaven
ScHiFRvi:102091
Chaos84:HOLE5244
Riptor795:blade7
Domi80:harkonnen
```

Example: Search by tags



MISP

MISP Taxonomies

- **Tagging** is a simple way to attach a classification to an event or attribute.
- **Classification must be globally used to be efficient.**
- Provide a set of already defined classifications modeling estimative language
- Taxonomies are implemented in a simple JSON format [8].
- Can be easily cherry-picked or extended

[8] https://github.com/MISP/misp-taxonomies

Taxonomies useful in AIL

- **infoleak**: Information classified as being potential leak.
- **estimative-language**: Describe quality and credibility of underlying sources, data, and methodologies.
- **admiralty-scale**: Rank the reliability of a source and the credibility of an information
- **fpf**[9]: Evaluate the degree of identifiability of personal data and the types of pseudonymous data, de-identified data and anonymous data.

[9] Future of Privacy Forum

Taxonomies useful in AIL

- **tor**: Describe Tor network infrastructure.
- **dark-web**: Criminal motivation on the dark web.
- **copine-scale**[10]: Categorise the severity of images of child sex abuse.

[10] Combating Paedophile Information Networks in Europe

threat sharing and incident response platforms

Goal: submission to threat sharing and incident response platforms.

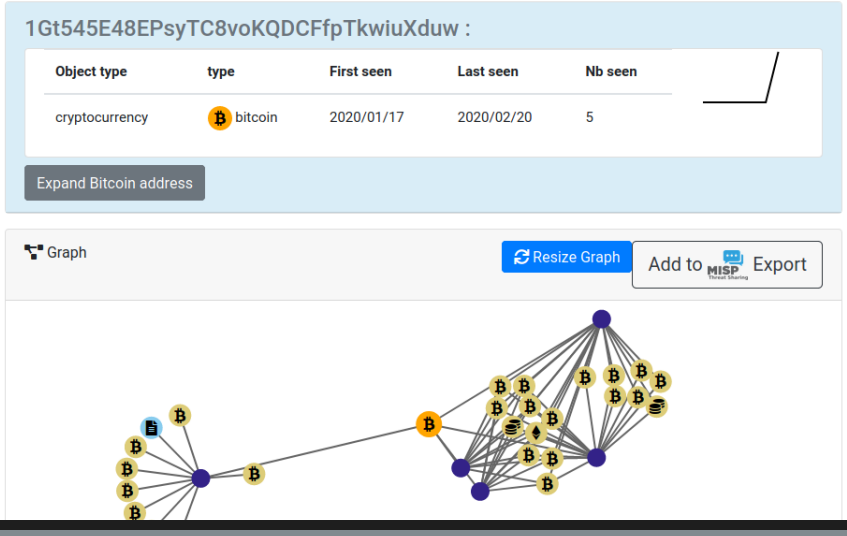
threat sharing and incident response platforms

1. Use infoleak taxonomy[11]
2. Add your own tags
3. Export AIL objects to MISP core format
4. Download it or Create a MISP Event[12]

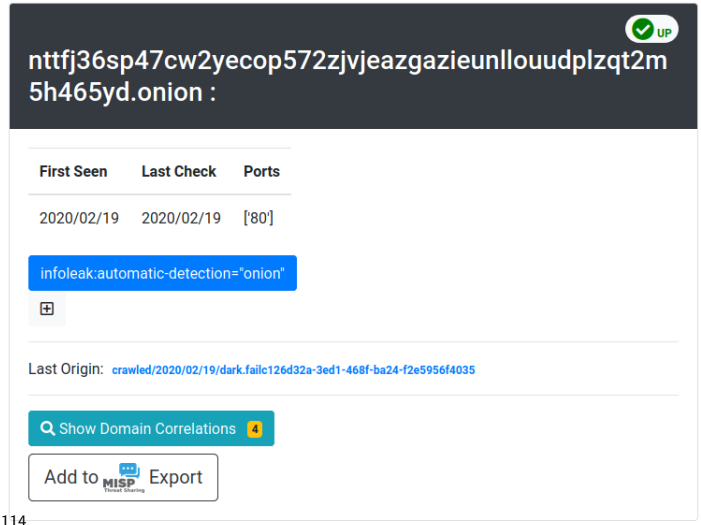
[11] https://www.misp-project.org/taxonomies.html

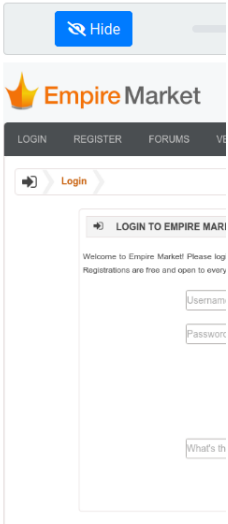
[12] https://www.misp-standard.org/rfc/misp-standard-core.txt

MISP Export

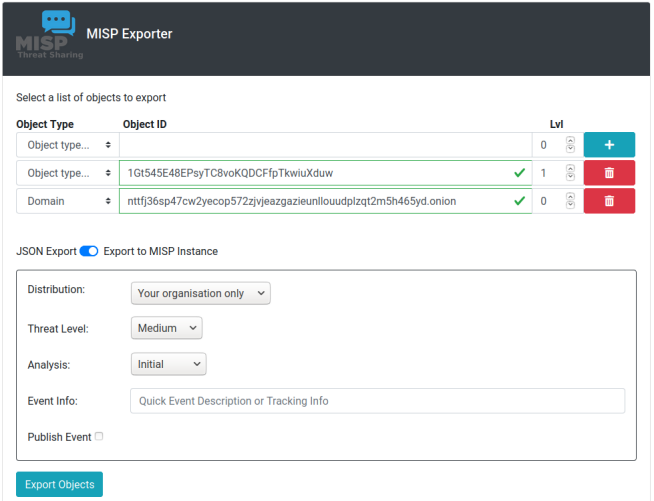

1Gt545E48EPsyTC8voKQDCFfpTkwiuXduw :
Object type
type
First seen
Last seen
Nb seen
cryptocurrency
bitcoin
2020/01/17
2020/02/20
5
Expand Bitcoin address
Graph
Resize Graph
Add to MISP Export

MISP Export

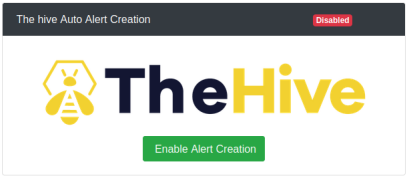

UP
nttfj36sp47cw2yecop572zjvjeazgazieunllouudplzqt2m5h465yd.onion :
First Seen
Last Check
Ports
2020/02/19
2020/02/19
['80']
infoleak:automatic-detection="onion"
Last Origin:
crawled/2020/02/19/dark.failc126d32a-3ed1-468f-ba24-f2e5956f4035
Show Domain Correlations
4
Add to MISP Export

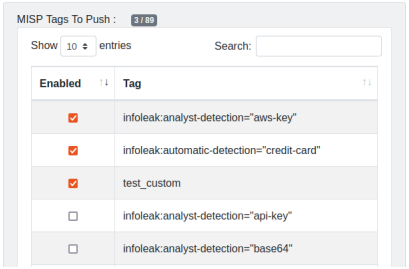

Hide
Empire Market
LOGIN
REGISTER
FORUMS
Login
LOGIN TO EMPIRE MARK
Welcome to Empire Market! Please log
Registrations are free and open to every

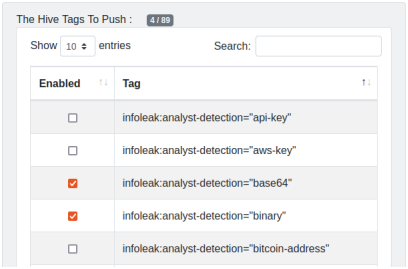
MISP Export


MISP Exporter
Select a list of objects to export
Object Type
Object ID
Lvl
Object type...
0
Object type...
1GtS45E48EPsyTC8voKQDCFfpTkwiuXduw
1
Domain
nttfj36sp47cw2yecop572zjvjeazgazieunllouudplzqt2m5h465yd.onion
0
JSON Export
Export to MISP Instance
Distribution:
Your organisation only
Threat Level:
Medium
Analysis:
Initial
Event Info:
Quick Event Description or Tracking Info
Publish Event
Export Objects

Automatic MISP Export on tags







API

AIL exposes a ReST API which can be used to interact with the back-end[13].

```
curl https://127.0.0.1:7000/api/v1/add/crawler/task
        --header "Authorization:
    iHc1_ChZxj1aXmiFiF1mkxxQkzawwriEaZpPqyTQj"
        -H "Content-Type: application/json"
        --data @input.json -X POST

```

[13] https://github.com/ail-project/ail-framework/blob/master/doc/README.md

Setting up the framework

Setting up AIL-Framework from source

Setting up AIL-Framework from source

```
git clone https://github.com/ail-project/ail-framework.git
cd AIL-framework
./installing_deps.sh
```

Feeding the framework

Feeding Data to AIL

There are different ways to feed data into AIL:

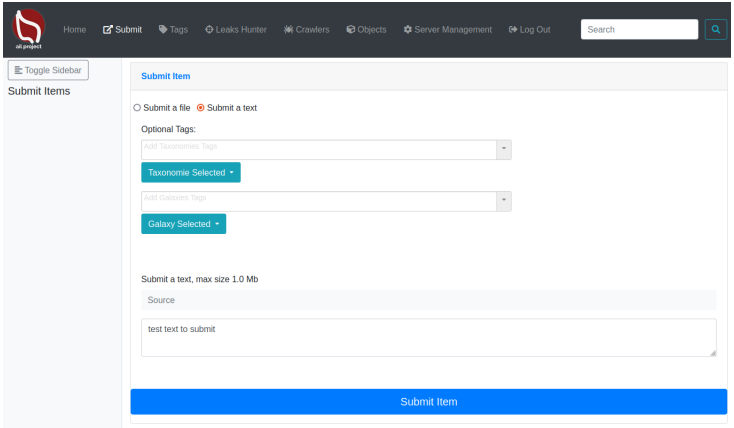
1. AIL Importers:
   - Dir / Files
   - ZMQ
   - *pystemon*
2. AIL Feeders (discord, telegram, ...)
3. Feed your own data using the API
4. Feed your own file/text using the UI (`Submit section`)

Feeding Data to AIL - Limitation

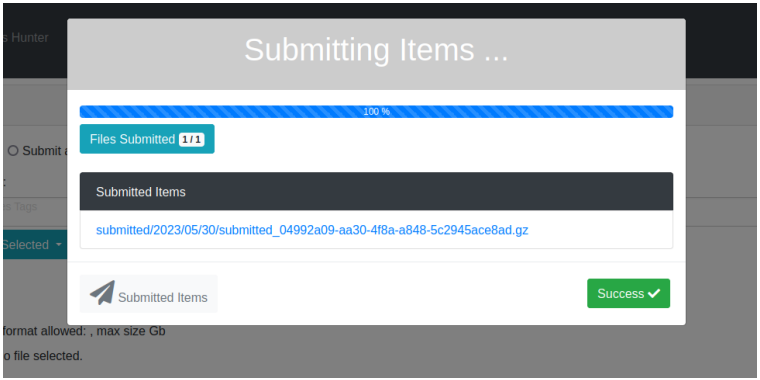
/!\ Limitation:

- Each file to be fed must be of a reasonable size:
  - $\sim$ `3 Mb` / file is already large
  - This is because some modules are doing regex matching (default timeout of 30 seconds)
  - If you want to feed a large file, better split it in multiple ones

Via the UI (1)


Home
Submit
Tags
Leaks Hunter
Crawlers
Objects
Server Management
Log Out
Search
Toggle Sidebar
Submit Items
Submit Item
Submit a file
Submit a text
Optional Tags:
Add Taxonomies Tags
Taxonomie Selected
Add Galaxies Tags
Galaxy Selected
Submit a text, max size 1.0 Mb
Source
test text to submit
Submit Item

Via the UI (2)


Submitting Items ...
100 %
Files Submitted 1 / 1
Submitted Items
submitted/2023/05/30/submitted_04992a09-aa30-4f8a-a848-5c2945ace8ad.gz
Submitted Items
Success
format allowed: , max size Gb
o file selected.

API - Feeding AIL with your own data

api/v1/import/item

```
{
  "type": "text",
  "tags": [
    "infoleak:analyst-detection=\"private-key\""
  ],
  "text": "text to import"
}
```

Importers

- Importers are located in the `/bin/importer` directory
- They are used to import different types of data into AIL
- Adding new Importers is straightforward.
- Available Importers:
  - AIL Feeders
  - ZMQ
  - pystemon
  - Files

File Importer

- `importer/FileImporter.py`

Import File

```
. ./AILENV/bin/activate
cd tools/
./file_dir_importer.py -f MY_FILE_PATH
```

Import Dir

```
. ./AILENV/bin/activate
cd tools/
./file_dir_importer.py -d MY_DIR_PATH
```

AIL feeders Importers

- **12+ feeders are available** for all AIL users to feed from external sources
- External feeders can run anywhere and are completely separated from AIL framework
- The feeder can use their **own internal logic** and even push JSON metadata
- Feeder are then pushing the generated JSON to AIL API

Certificate transparency feeder for AIL

- ail-feeder-cti[14] is a generic software to extract information from a certstream server (certificate transparency)
- All metadata extracted will be processed by AIL
- Onion addresses crawled automatically by AIL if seen in a certificate

[14] `https://github.com/ail-project/ail-feeder-ct`

GitHub archive and GitHub repository

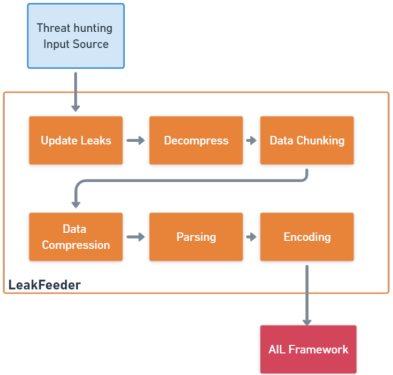
- ail-feeder-gharchive[15] is a generic software to extract informations from **GHArchive**, collect and feed AIL via AIL ReST API
- ail-feeder-github-repo[16] is collecting from a GitHub repository and push everything to AIL
- For monitoring a set of **suspicious git repositories** or finding leaks on existing or managed git repositories, it's a simple way to feed AIL with such source.

[15] `https://github.com/ail-project/ail-feeder-gharchive`

[16] `https://github.com/ail-project/ail-feeder-github-repo`

AIL LeakFeeder

- ail-feeder-leak[17] automates the process to feed leaked large files automatically to AIL



[17] https://github.com/ail-project/ail-feeder-leak

AIL feeder ActivityPub

- ail-feeder-activity-pub[18] is feeder for the ActivityPub standard used in distributed social networks
- Accounts are required on the ActivityPub instance to get the stream

[18] `https://github.com/ail-project/ail-feeder-activity-pub`

AIL feeder telegram

- ail-feeder-telegram[19] is a **Telegram feeder**
- An API ID/hash for Telegram is required and linked to your Telegram phone number

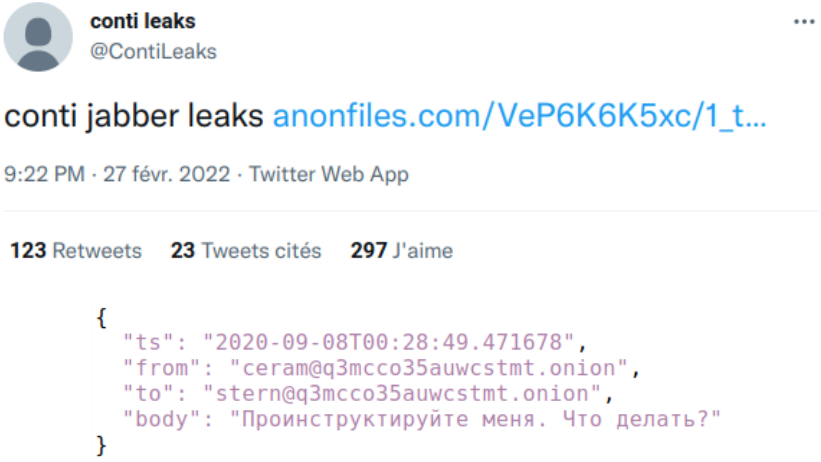
[19] `https://github.com/ail-project/ail-feeder-telegram`

More feeders

- ail-feeder-discord[20] is a generic **Discord** feeder for AIL
- ail-feeder-atom-rss[21] is an **Atom and RSS reader** and feeder for AIL
- ail-feeder-jsonlogs[22] is a **JSON aggregator** to submit generic JSON input into AIL

[20] `https://github.com/ail-project/ail-feeder-discord`
[21] `https://github.com/ail-project/ail-feeder-atom-rss`
[22] `https://github.com/ail-project/ail-feeder-jsonlogs`

Feeding AIL with custom JSON



Feeding AIL with Conti leaks

- Conti jabber leaks are a good candidate for AIL analysis:
  - PGP keys
  - Bitcoin addresses, maybe others,
  - onion hidden services
- first we translated the files on english using deepl.com
- then we created a feeder to import json data in AIL
- Support added in AIL to correlate jabber usernames

Feeding AIL with Conti leaks

```
from pyail import PyAIL
#... imports
#...  setup code
for content in sys.stdin:
    elm = json.loads(content)
    tmp = elm['body']
    tmpmt = {}
    tmpmt['jabber:to'] = elm['to']
    tmpmt['jabber:from'] = elm['from']
    tmpmt['jabber:ts'] = elm['ts']
    tmpmt['jabber:id'] = "{}".format(uuid.uuid4())
    pyail.feed_json_item(tmp, tmpmt, ailfeedertype, source_uuid)
```

feeder.py

```
$ cat ~/conti/* | jq . -c | python ./feeder.py
```

Feeding AIL with Conti leaks

- use grep to limit the noise on an instance by only sending interesting bits:
  - PGP keys

```
$ cat ~/conti/* | jq . -c | grep PGP | python ./feeder.py
```

  - onion hidden services | `grep http://` |
  - telegram addresses | `grep tg://` |
  - bitcoins addresses | `egrep --regexp="[13][a-km-zA-HJ-NP-Z1-9]25,34"` |

Starting the framework

Running your own instance from source

Accessing the environment and starting AIL

```
1
2 # Launch the system and the web interface
3 cd bin/
4 ./LAUNCH -l
```

Updating AIL

Launch the updater:

```
cd bin/
# git pull and launch all updates:
./LAUNCH -u


# PS:
# The Updater is launched by default each time
# you start the framework with
# ./LAUNCH -l
```

Running your own instance using the virtual machine

Login and passwords:

```
# Web interface (default network settings)
   https://127.0.0.1:7000/
# Web interface:
   admin@admin.test
   Password1234
# SSH:
   test
   Password1234
```

AIL ecosystem - Challenges and design

AIL ecosystem: Technologies used

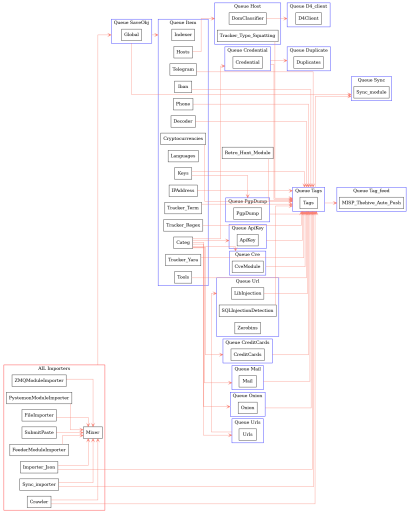
Programming language: Full python3

Databases: Redis and Kvrocks

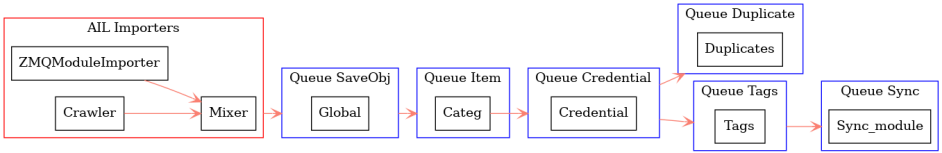
Server: Flask

Data message passing: Redis Set

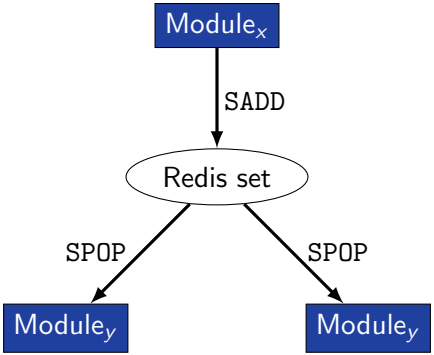
AIL global architecture: Data streaming between module



AIL global architecture: Data streaming between module (Credential example)



Message consuming



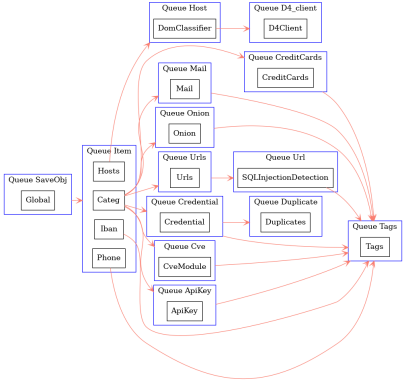
→ No message lost nor double processing

→ Multiprocessing!

Creating new features

Developing new features: Plug-in a module in the system

Choose where to put your module in the data flow:



Then, modify `configs/modules.cfg` accordingly

Writing your own modules - /bin/modules/TemplateModule.py

```
1  from modules.abstract_module import AbstractModule
2
3  class NewModule(AbstractModule):
4
5    def __init__(self):
6          super().__init__()
7      self.logger.info(f'Module {self.module_name} initialized')
8
9    # Do something with the message from the queue
10   def compute(self, message):
11     # Process Message
12
13 # LAUNCH MODULE
14 if __name__ == '__main__':
15     module = NewModule()
16     module.run()
17
18
```

Writing your own Importer - /bin/importer/

```python
from importer.abstract_importer import AbstractImporter
from modules.abstract_module import AbstractModule

class MyNewImporter(AbstractImporter):

    def __init__(self):
        super().__init__()
        # super().__init__(queue=True)   # if it's an one-time run importer
        self.logger.info(f'Importer {self.name} initialized')

    def importer(self, my_var): # import function
        # Process my_var and get content to import
        content = GET_MY_CONTENT_TO_IMPORT
        # if content is not gzipped and/or not b64 encoded,
        # set gzipped and/or b64 to False
        message = self.create_message(item_id, content)
        return message
        # if it's an one-time run, otherwise create an AIL Module
        # self.add_message_to_queue(message)

class MyNewModuleImporter(AbstractModule):
    def __init__(self):
        super().__init__() # init module ...
        # init module ...
```

Writing your own Importer - /bin/importer/

```
1
2       def get_message(self):
3           return self.importer.importer()
4
5       def compute(self, message):
6           self.add_message_to_queue(message)
7
8   if __name__ == '__main__':
9       module = MyNewModuleImporter()
10      module.run()
11
12      # if it's an one-time run:
13      # importer = MyImporter()
14      # importer.importer(my_var)
15
16
```

Contribution rules

How to contribute

Glimpse of contributed features

- Docker
- Ansible
- Email alerting
- SQL injection detection
- Phone number detection

How to contribute

- Feel free to fork the code, play with it, make some patches or add additional analysis modules.

How to contribute

- Feel free to fork the code, play with it, make some patches or add additional analysis modules.
- Feel free to make a pull request for your contribution

How to contribute

- Feel free to fork the code, play with it, make some patches or add additional analysis modules.
- Feel free to make a pull request for your contribution
- That's it!

〈(^.^)ノ

Final words

- Building AIL helped us to find additional leaks which cannot be found using manual analysis and **improve the time to detect duplicate/recycled leaks**.

  $\rightarrow$ Therefore quicker response time to assist and/or inform proactively affected constituents.

Implementation Steps in AIL project

- **Gradual changes** in AIL to add required functionalities to support the objectives.
- **Time-memory trade-off** can be challenging to ensure a functional framework.
- Evaluation and integration of new modules in AIL based on time-memory comparisons.
- Semantic aspects are challenging due to the diverse data sources, unstructured data and languages seen.

Ongoing developments

- Two-Factor Authentication (2FA) - One-Time Password (OTP)
- Bloom filter filtering - PSS
- Relationships and activity between chats: message forwards, replies, etc.
- Improved indexing relying on Solr, Lucene or other components

Annexes

Managing AIL: Old fashion way

Access the script screen

```
1 screen -r Script
```

Table: GNU screen shortcuts

Shortcut	Action
C-a d	detach screen
C-a c	Create new window
C-a n	next window screen
C-a p	previous window screen