

AIL Framework for Analysis of Information Leaks

API



CIRCL

Computer Incident
Response Center
Luxembourg

Alexandre Dulaunoy

alexandre.dulaunoy@circl.lu

Aurélien Thirion

aurelien.thirion@circl.lu

info@circl.lu

IHAP 20190522

AIL¹ is a framework to find leaks and sensitive information from stream of data such as crawler website (e.g. Tor hidden services or pastebin-like website). The current version 1.6 is functional via the user-interface. This presentation presents the **roadmap to expose the UI functionalities via the API**.

¹<https://github.com/CIRCL/AIL-framework>
2 of 10

API - Roadmap

API - v1.8

The first step is to have a solid user management interface before exposing the complete API.

- Basic users management
- Roles management: Admin, Analyst, ...
- API: create and manage tokens

API - step 1

- Get item tags (e.g. credential leaks)
- Set item tags (e.g. to reclassify items)
- Get item metadata
- Get item content

API - step 2

- Text search by date range
- Get all tags list
- Get tagged items by date range
- Submit a paste or text blob
- Submit a domain to crawl
- Create a term/set/regex tracker
- Get tracker items list

API - step 3

- Check if a tor/regular domain has been crawled
- Get domain tags
- Get domain history
- Get domain list of items
- Create auto-crawlers

API - step 4

- Check if a decoded item exists (via sha1)
- Get decoded item metadata
- Get VT result
- Send this item to VT
- Get items list
- Get decoded item correlation (1 depth)

API - step 5

- Check if a cryptocurrency address (bitcoin, ..) exists
- Get cryptocurrency address metadata
- Get item list
- Item correlation (1 depth)

API - step 6++

- Create MISP event from item
- Create TheHive case from item
- ...
- Complex tags search
- Advanced search

How can I contribute?

- Provide ideas to the API roadmap for AIL (don't forget to open an issue²).
- Contribute new modules or extension to the framework.
- Don't hesitate to contact us via <mailto:info@circl.lu> if you have any question or idea.

²<https://github.com/CIRCL/AIL-framework/issues>