# AIL – Analysis Information Leak framework

## Track pasties with no hassle

CIRCL
Computer Incident
Response Center
Luxembourg

Raphaël Vinot - *TLP:WHITE*

CIRCL

September 20, 2016

# Who am I

- Raphaël Vinot - @rafi0t
- CERT operator @ Computer Incident Response Center Luxembourg (CIRCL)
- Core team working on **MISP ecosystem** - https://github.com/MISP/
- Co-organiser of **hack.lu** - 18th to 20th of October in Luxembourg

# Why a pastes monitoring system?

- Attackers need a may to communicate, and to **brag**
- Reasonably **anonymous** (no registration/moderation)
- Contains a bit of everything
- Can store big text blobs

# Unstructured dataset

- Databases dumps
- Credit cards leaks
- **Login informations**
- IRC logs
- Source code, exploits
- Emails

# Main functionalities

- **Full text indexing**
- **Pastes browsing**
- Statistics on content
- Trends and evolution
- Terms frequency

# Enough slides...

- Let's have a demo !

# Resources

- Source code: https://github.com/CIRCL/AIL-framework
- Source code Pystemon: https://github.com/CIRCL/pystemon
- We can provide a feed for raw pastes
- **Contact us**: info@circl.lu
  - 3B12 DCC2 82FA 2931 2F5B 709A 09E2 CD49 44E6 CBCD