Writing YARA rules

An introduction to YARA for AIL usage

CIRCL
Computer Incident
Response Center
Luxembourg

Alexandre Dulaunoy
alexandre.dulaunoy@circl.lu

Jean-Louis Huynen
jean-louis.huynen@circl.lu

info@circl.lu

October 19, 2021

Links

- AIL project: `https://github.com/ail-project`
- AIL framework: `https://github.com/ail-project/ail-framework`
- Training materials: `https://github.com/ail-project/ail-training`
- YARA doc: `https://yara.readthedocs.io/en/stable/`
- YARA download: `http://virustotal.github.io/yara/`

What's YARA?

- *The pattern matching swiss knife for malware researchers (and everyone else)*;
- It's an improved **grep** to create pattern matching rule to search for **strings**, **binary patterns**, **regular expressions**;
- A YARA rule can be contextualised with metadata and tags describing a specific set of pattern matching rules.