Sig • Mal

Meeting 10

Yara

- Powerful Malware Identification and Classification Tool

+ https://virustotal.github.io/yara/

Yara (Installation)

- brew install yara

- pip install yara-python

Yara Rules

- Malware researchers can create YARA rules based on textual and binary info contained within a file.
- Yara rules consist of a set of strings and a Boolean expression (this determines its logic)

+ Once written, you can use it to scan files.

Writing Yara Rules

src:: https://yara.readthedocs.io/en/latest/writingrules.html

LIVE DEMO TIME