Trellix

FOSS enterprise malware analysis

Threat Intelligence Group
Advanced Research Center

Max Kersten
Malware Analyst

Table of contents

About me

Goals and expectations

The pipeline

Collections

Detections

Manual analysis

Resources

Q&A

About me

- Max ‘Libra’ Kersten (@Libranalysis, @libra@infosec.exchange)

- Malware analyst and reverse engineer

- Working for Trellix’ Advanced Research Center
  - Published DotDumper

- I write blogs about reverse engineering
  - Including my free Binary Analysis Course

- My tools are open-sourced on GitHub
  - Such as AndroidProjectCreator and the Mobile Malware Mimicking Framework

Goals and expectations

Premium services provide premium quality

Only accessible if premiums are paid

This is not meant to discredit any premium service in any way, shape, or form

There is no affiliation with any of the mentioned services, other than my subjective personal preferences

Trellix

Goals and expectations

Should run on a Raspberry Pi 3B

60-day sample retention period

Scan and search locally, running 24/7

Traffic Light Protocol

The pipeline

Do not focus on manual analysis yet

Rely on the community and pattern matching

Understanding data does not require expensive hardware

Scale by outsourcing

Collections

What to expect

Premium services offer an overwhelming number of fresh samples

The goal is to find trends and learn along the way

Collections

Please adhere to rate limits and fair use

MalShare

- Free access upon registering
- 2000 API requests per day

Malware Bazaar

- Requires a Twitter account to login
- API requests with a rate limit
- Allows batch downloading of recent files

Malpedia

- Public and invite-only sections
- Requires vouches from existing members
- Contains (unpacked) samples and Yara rules

Triage

- Free access for non-commercial usage
- Sandbox
- Extensive and free to use API
- Implements config extractors

Collections

Local set-up

- Attach external storage
- Store samples
- Store metadata in a database

Trellix

Collections

Possible folder structure

/samples/[year]/[month]/[day]

/samples/[year]/[dayOfYear]

Trellix

Detections

Scanning files with Yara

- Optimise your Yara rules
- Offload the scanning to a public platform such as Yaraify

Manual analysis

Free and open-source tools are readily available

- Ghidra
- Cutter/Rizin
- IDA Free (or Home if your budget allows)
- dnSpyEx for DotNet
- JADX for Java and Android

Manual analysis

Automate as much as possible

RUN TOOLS HEADLESS ON INTERESTING SAMPLES

GET NOTIFIED VIA SLACK/DISCORD/TELEGRAM FOR INTERESTING SAMPLES

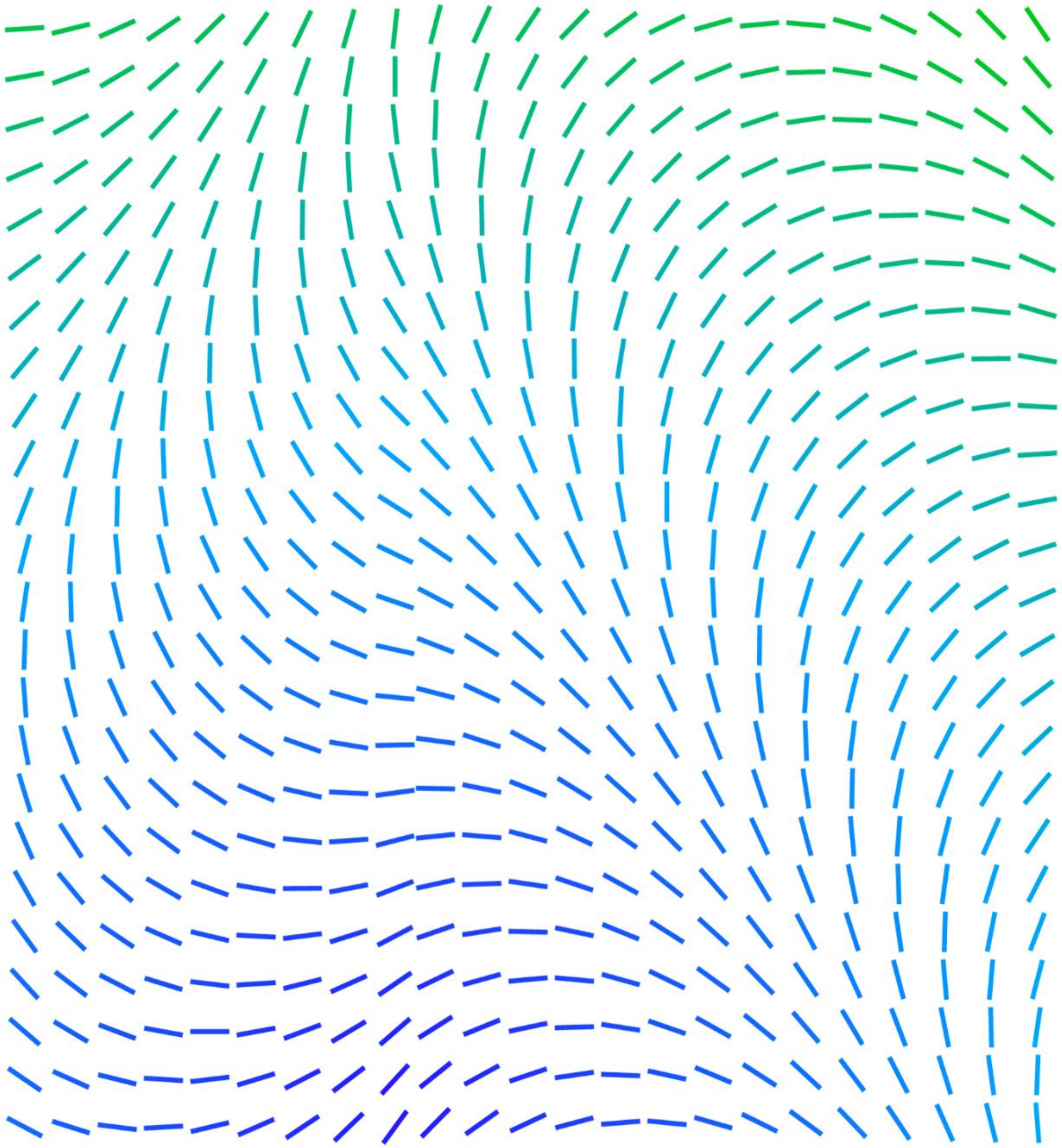
Resources

Do not reinvent the wheel

MY FREE BINARY ANALYSIS COURSE

API CLIENT LIBRARIES

COLLABORATE WITH THE COMMUNITY



Q&A

For questions, you can also reach out to me via @Libranalysis, @libra@infosec.exchange, or Max Kersten on LinkedIn