

Identifying malware campaigns on a budget

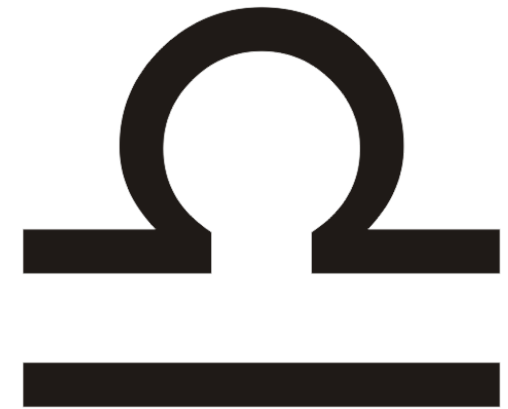
MAX 'LIBRA' KERSTEN & RENS VAN DER LINDEN

Table of contents

- Who are we?
- Goal
- Audience
- Budget
- Used data
- Data normalisation
- Modules
- Questions

Who am we?

- Max 'Libra' Kersten ([@Libranalysis](#))
- Working for Trellix' Advanced Threat Research team
 - During the research I was part of ABN AMRO's Threat Intelligence team
- Spoke at several conferences
 - Botconf, BlackHat, CONFidence, atHack, and others
- I write [blogs](#) about reverse engineering
 - Including my own free [Binary Analysis Course](#)
- My tools are open-sourced on [Github](#)
 - Such as [m3](#) or [AndroidProjectCreator](#)



Trellix

Who are we?

- Rens van der Linden
- Working at RSecure
 - Penetration tester
- ABN AMRO's Threat Intelligence team
 - Graduation internship
- [Blog](#)
- Tooling open sourced on [Github](#)

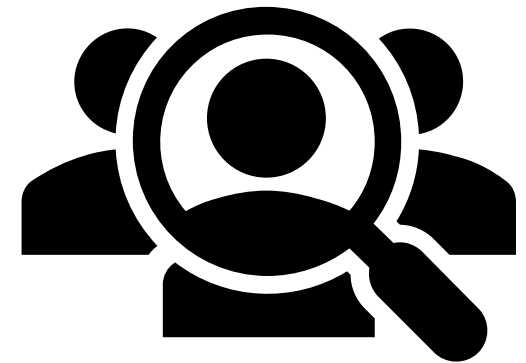
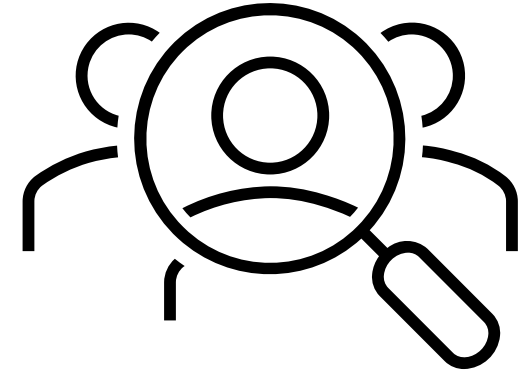


Goal

- “Gain continuous insight into malware campaigns on a budget”
- Selected criteria
 - Cross platform
 - Use as few resources as possible
 - Scalable
 - Reusable and repurposable
 - Pareto principle
 - Applicable in the real world

Audience

- Applicable to
 - Students
 - Start-ups
 - Independent researchers
 - Corporations
- Useful in
 - Malware analysis
 - Threat intelligence
 - Incident response



Budget

- Depends on the user's needs and background
 - I.e. a corporate budget or a student
- Scaling requires improved hardware
- The Raspberry Pi 3B+ can still be used for other projects

ITEM	COST
Raspberry Pi 3B+	€65
Raspberry Pi 3B+ power <u>usage</u>	€5 (3.5W, yearly 31 kWh, €0.15 per kWh)
Software	FOSS

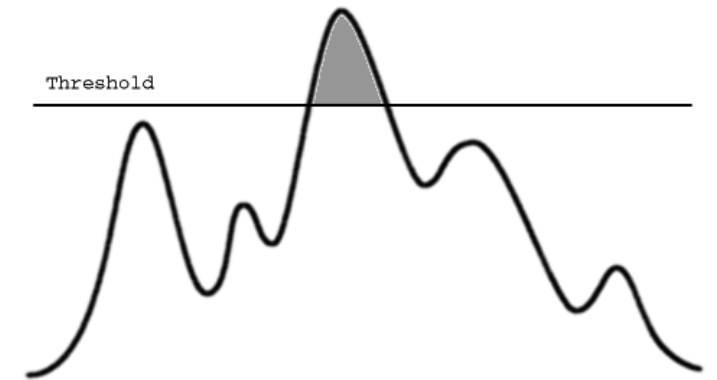


Used data

- Anonymous source provided 500 000 malicious e-mails
 - Unable to publish the given data set
 - The e-mails did not contain the mail body
- One can replicate the shown techniques with other e-mails
- Public services are used to enrich the obtained data

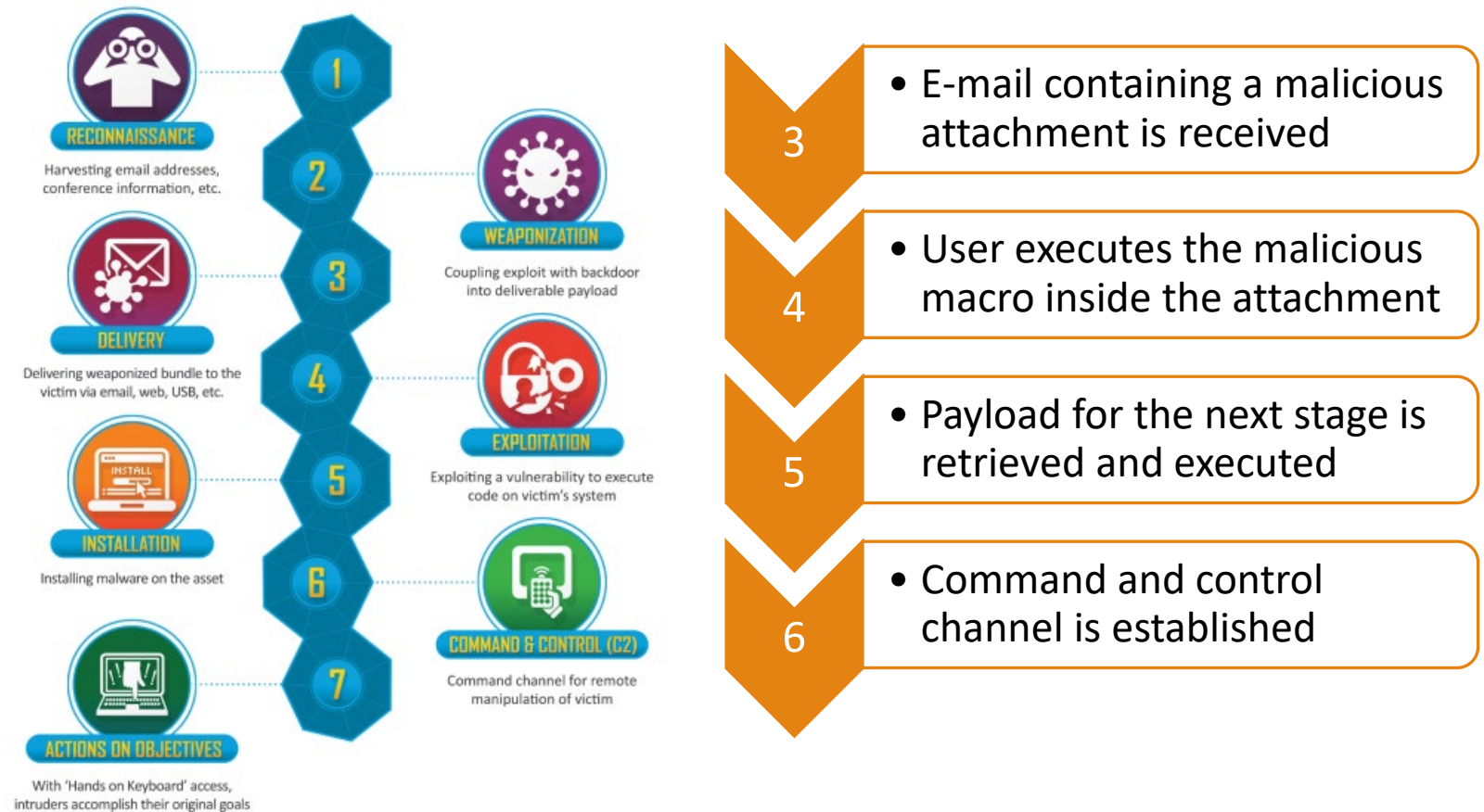
Data normalisation

- Combine modules to increase granularity
 - Reduce false positives
- User-controllable threshold
 - Flexible
 - Use-case of results



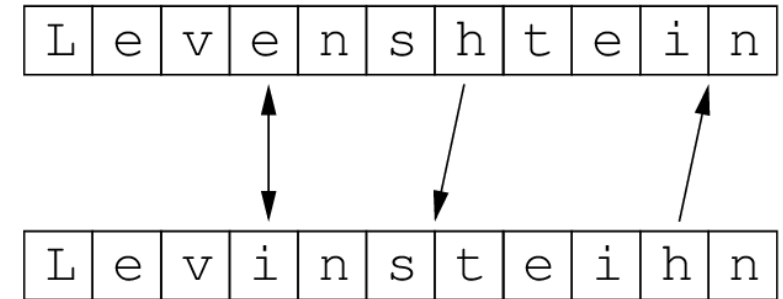
Modules

- Widely adopted
 - Modeling intrusion attempts
- Devises seven steps
 - Achieve objectives
- Malware
 - Steps 3 / 6



E-mail subjects

- Identify e-mails sent out in bulk
- Proactive search
 - In contrast to a literal search
- Levenshtein distance
 - Number of character changes



Source: [researchgate](https://researchgate.net/publication/310111111)

SUBJECTS

Do you want to extend your free period #####?
Do you want to extend your free trial #####?
Free period for ##### will come to the end end in 3 days
Free trial period for ##### ends in three days
Free trial period for ##### will end in 3 days
Your free period ##### is about to end!
Your free trial ##### is about to end!

Source: [ExecuteMalware](https://www.execute-malware.com/)

Lure images

- Disabling Office's Protected View
 - Enabling Macros
- Small changes
 - Cryptographic hashes
- Perceptual hashing algorithm
 - Average Hash
- Malicious document builders
 - Include pre-made lure image



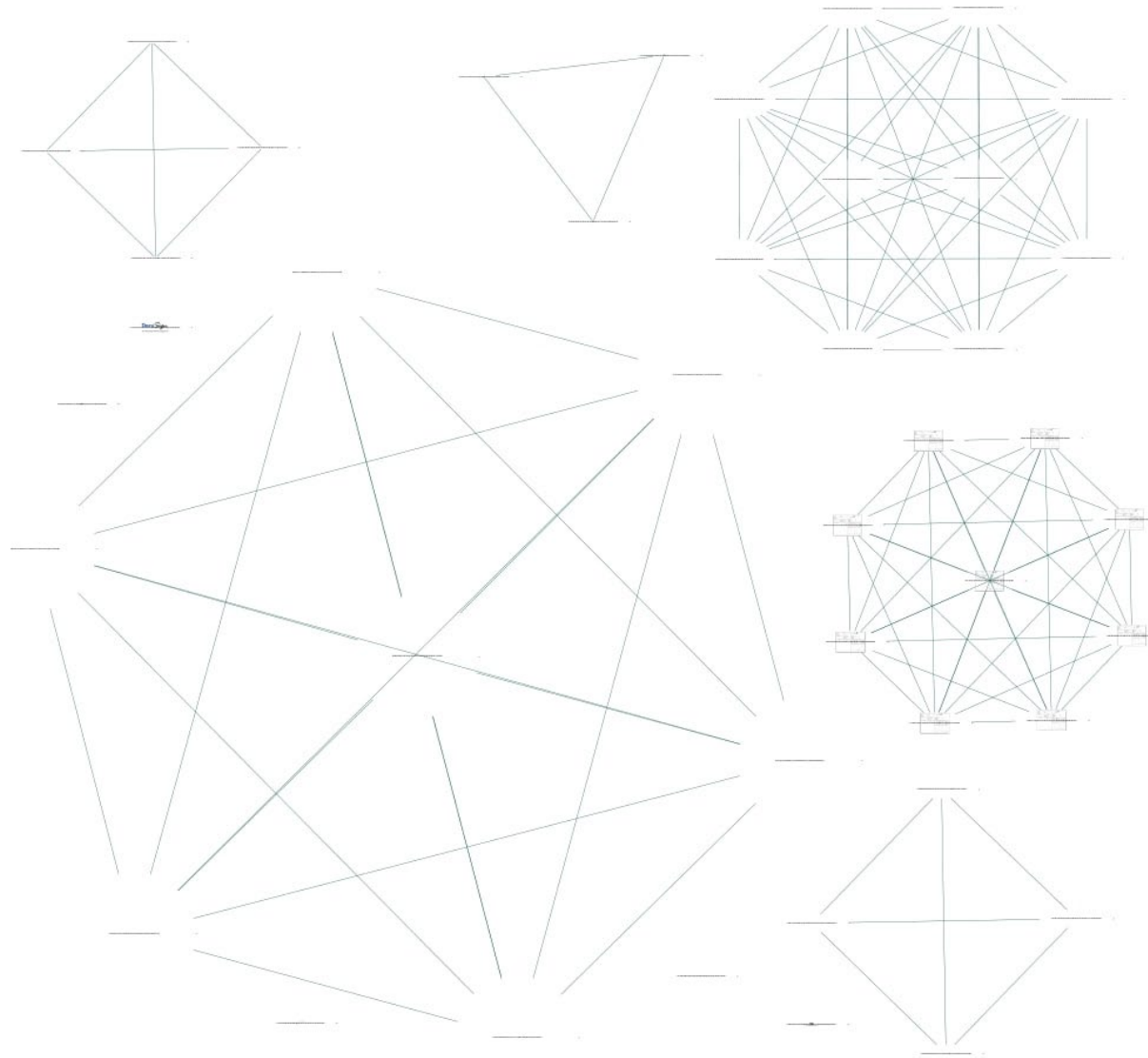
Questo file è stato creato con una versione precedente di Microsoft Office Word.

Per visualizzare il contenuto è necessario fare click sul pulsante "Abilita modifiche", situato sulla barra gialla in alto, e poi cliccare su "Abilita contenuto"



Questo file è stato creato con una versione precedente di Microsoft Office Word.

Per visualizzare il contenuto è necessario fare click sul pulsante "Abilita modifiche", situato sulla barra gialla in alto, e poi cliccare su "Abilita contenuto"



Lure images

- Cluster example

URLs

- Purpose of the website
- Breached website
 - Correlation does not mean causation
- Enumeration
 - WHOis information
 - WordPress
 - URLHaus

```
Domain name: benvenuti.rs
Domain status: Active https://www.rnids.rs/en/domain-name-status-codes#Active
Registration date: 19.11.2019 16:15:58
Modification date: 20.10.2020 21:44:13
Expiration date: 19.11.2021 16:15:58
Confirmed: 20.11.2019 14:50:52
Registrar: Eutelnet d.o.o.
```

2021-06-21 12:04:12	https://scriptcaseblog.net/neha-schiller/Noah.S...	Online	html	Qakbot	qbot	SilentBuilder	TR	zip	@Cryptolaemus1
2021-06-21 12:04:12	https://bigpms.in/carol-emard/Sophia.Jones-46.zip	Online	html	Qakbot	qbot	SilentBuilder	TR	zip	@Cryptolaemus1
2021-06-21 12:04:11	https://j-metalogradnja.rs/reece-tromp/Ava.Brow...	Online	html	Qakbot	qbot	SilentBuilder	TR	zip	@Cryptolaemus1

Source: [Abuse.ch's URLHaus](#)

Demo

**When project is not ready
but the client wants a demo**



Malware families

- Group of malware
 - Same codebase
 - Generic C&C traffic
- Actionable intelligence
- Increases context

Signatures

AgentTesla

AgentTesla Payload


Reads data files stored by FTP clients

Reads user/profile data of local email clients

Reads user/profile data of web browsers

Suspicious use of SetThreadContext

Extracted

Family	asynrat
Version	0.5.7B
Botnet	2
C2	212.193.30.54:9524 
Attributes	delay 3
	install false
	install_folder %AppData%
aes.plain	1 h6C3f3gAHSTQXa9tyJWg46l109gZ9JqC

Source: [Hatching Triage](#)



Questions

Contact us!

 [@Libranalysis](https://twitter.com/Libranalysis)

 [/in/ThisIsLibra](https://www.linkedin.com/company/thisislibra)

 [@KuulSec](https://twitter.com/KuulSec)

 [/in/RensvdLinden](https://www.linkedin.com/company/rensvdLinden)