RansomCoin

A quarterly report of ransomware analysis and blackmarket economic analysis

Eireann Leverett & Juriaan Bremer

EXAMPLE QUARTERLY REPORT: CONCINNITY RISKS & CUCKOO

HTTPS://GITHUB.COM/JBREMER/RANSOMCOIN

This research was done under contract for CCDP February 10 to September 30th of 2018.

First release, February 2018

Contents

1. Introduction

1.1 Motivation

Lorem ipsum dolor sit amet, an verterem probatus qualisque eam, inani habemus mei at. Pri ut pericula accommodare, qui nibh petentium eu. Senserit honestatis cotidieque ut pri, quodsi voluptua referrentur sit at. Est nisl assum id, an odio veniam ceteros mei, ne abhorreant concludaturque vel.

Per quot vidit disputationi ex, fugit tantas volumus nam et. Eu omittam torquatos vim. Ei nihil vitae quando vis, omnium commune facilisi in his. Harum definiebas assueverit mel id, te mediocrem adolescens vel. Agam omnium no his. Et nec feugait fabellas, vel cu inimicus inciderint repudiandae.

1.2 Objective

- Write code that helps analyse and extract metadata from ransomware
  - Altcoin addresses
  - Altcoin prices
  - jpeg/png/gif images
  - ransomware notes
  - screenshots
  - C2 servers
  - different behaviour on language settings, or timestamps
- Alter Cuckoo to regularly use the new code and extract these indicators
- Gather a large corpus of ransomware to produce data from
- upload as Indicators of Compromise to many defense threat intel streams (such as MISP)
- report on any trends discovered, such as distribution of samples across crypto currency

Lorem ipsum dolor sit amet, an verterem probatus qualisque eam, inani habemus mei at. Pri ut pericula accommodare, qui nibh petentium eu. Senserit honestatis cotidieque ut pri, quodsi voluptua referrentur sit at. Est nisl assum id, an odio veniam ceteros mei, ne abhorreant concludaturque vel.

Per quot vidit disputationi ex, fugit tantas volumus nam et. Eu omittam torquatos vim. Ei nihil vitae quando vis, omnium commune facilisi in his. Harum definiebas assueverit mel id, te mediocrem adolescens vel. Agam omnium no his. Et nec feugait fabellas, vel cu inimicus inciderint repudiandae.

Lorem ipsum dolor sit amet, an verterem probatus qualisque eam, inani habemus mei at. Pri ut pericula accommodare, qui nibh petentium eu. Senserit honestatis cotidieque ut pri, quodsi voluptua referrentur sit at. Est nisl assum id, an odio veniam ceteros mei, ne abhorreant concludaturque vel.

Per quot vidit disputationi ex, fugit tantas volumus nam et. Eu omittam torquatos vim. Ei nihil vitae quando vis, omnium commune facilisi in his. Harum definiebas assueverit mel id, te mediocrem adolescens vel. Agam omnium no his. Et nec feugait fabellas, vel cu inimicus inciderint repudiandae.

1.3 A bit of context

Lorem ipsum dolor sit amet, an verterem probatus qualisque eam, inani habemus mei at. Pri ut pericula accommodare, qui nibh petentium eu. Senserit honestatis cotidieque ut pri, quodsi voluptua referrentur sit at. Est nisl assum id, an odio veniam ceteros mei, ne abhorreant concludaturque vel.

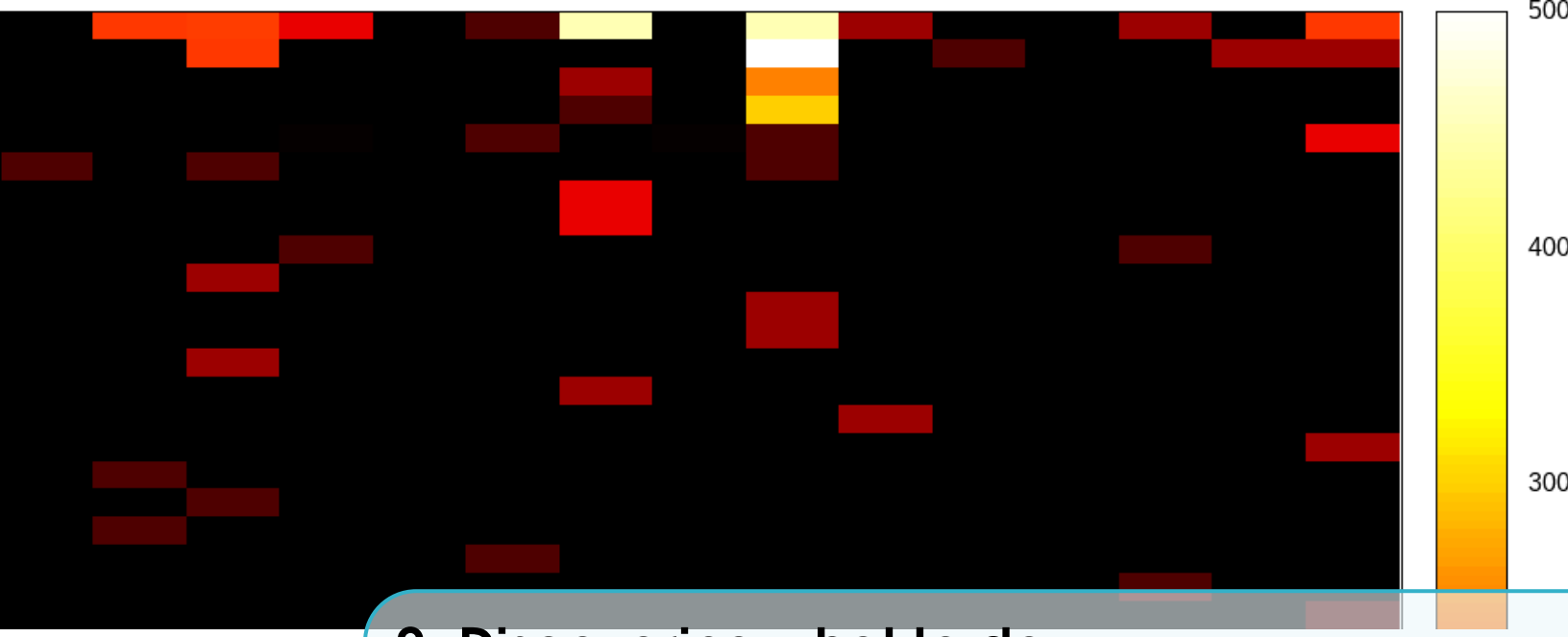
Per quot vidit disputationi ex, fugit tantas volumus nam et. Eu omittam torquatos vim. Ei nihil vitae quando vis, omnium commune facilisi in his. Harum definiebas assueverit mel id, te mediocrem adolescens vel. Agam omnium no his. Et nec feugait fabellas, vel cu inimicus inciderint repudiandae.

1.3.1 References

Lorem ipsum dolor sit amet, an verterem probatus qualisque eam, inani habemus mei at. Pri ut pericula accommodare, qui nibh petentium eu. Senserit honestatis cotidieque ut pri, quodsi voluptua referrentur sit at. Est nisl assum id, an odio veniam ceteros mei, ne abhorreant concludaturque vel.

Per quot vidit disputationi ex, fugit tantas volumus nam et. Eu omittam torquatos vim. Ei nihil vitae quando vis, omnium commune facilisi in his. Harum definiebas assueverit mel id, te mediocrem adolescens vel. Agam omnium no his. Et nec feugait fabellas, vel cu inimicus inciderint repudiandae.

For more information about malware analysis see page 10, from **21st Century Malware**, *Hester* | *Smith* | *Blumenthal* | *Kay* | *Voss*, Third Edition, 2010.



2. Discovering what to do

2.1 First ideas

Can we measure threat actor capabilities? Does one threat actor manage more domains, or another produce more unique malware samples? [1] This is part of a project we call LogisticalBurden which reverse engineers the quantification of threat actors into groupings based on their capabilities to manage domains/urls, IP addresses, and produce malicious files.

Lorem ipsum dolor sit amet, an verterem probatus qualisque eam, inani habemus mei at. Pri ut pericula accommodare, qui nibh petentium eu. Senserit honestatis cotidieque ut pri, quodsi voluptua referrentur sit at. Est nisl assum id, an odio veniam ceteros mei, ne abhorreant concludaturque vel.

Per quot vidit disputationi ex, fugit tantas volumus nam et. Eu omittam torquatos vim. Ei nihil vitae quando vis, omnium commune facilisi in his. Harum definiebas assueverit mel id, te mediocrem adolescens vel. Agam omnium no his. Et nec feugait fabellas, vel cu inimicus inciderint repudiandae.

2.1.1 Altcoin address regular expressions

Lorem ipsum dolor sit amet, an verterem probatus qualisque eam, inani habemus mei at. Pri ut pericula accommodare, qui nibh petentium eu. Senserit honestatis cotidieque ut pri, quodsi voluptua referrentur sit at. Est nisl assum id, an odio veniam ceteros mei, ne abhorreant concludaturque vel.

Per quot vidit disputationi ex, fugit tantas volumus nam et. Eu omittam torquatos vim. Ei nihil vitae quando vis, omnium commune facilisi in his. Harum definiebas assueverit mel id, te mediocrem adolescens vel. Agam omnium no his. Et nec feugait fabellas, vel cu inimicus inciderint repudiandae.

Lorem ipsum dolor sit amet, an verterem probatus qualisque eam, inani habemus mei at. Pri ut pericula accommodare, qui nibh petentium eu. Senserit honestatis cotidieque ut pri, quodsi voluptua referrentur sit at. Est nisl assum id, an odio veniam ceteros mei, ne abhorreant concludaturque vel.

Per quot vidit disputationi ex, fugit tantas volumus nam et. Eu omittam torquatos vim. Ei nihil vitae quando vis, omnium commune facilisi in his. Harum definiebas assueverit mel id, te mediocrem adolescens vel. Agam omnium no his. Et nec feugait fabellas, vel cu inimicus inciderint repudiandae.

[1] For example purposes the image selected is a heatmap of number of malicious binaries detected per threat actor, which gives a ranking of who produces more malware in a given timeframe.

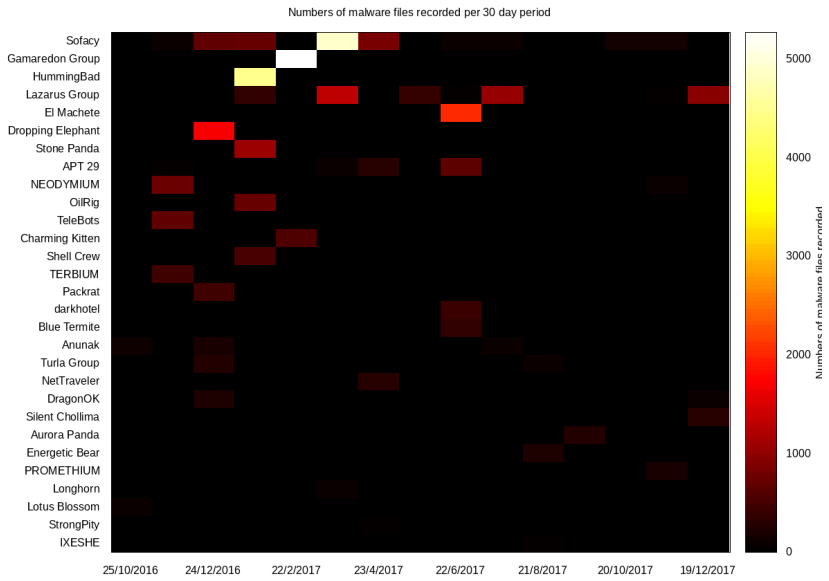


Figure 2.1: Heatmap of malicious file activity by threat actor (detection time)

Lorem ipsum dolor sit amet, an verterem probatus qualisque eam, inani habemus mei at. Pri ut pericula accommodare, qui nibh petentium eu. Senserit honestatis cotidieque ut pri, quodsi voluptua referrentur sit at. Est nisl assum id, an odio veniam ceteros mei, ne abhorreant concludaturque vel.

Per quot vidit disputationi ex, fugit tantas volumus nam et. Eu omittam torquatos vim. Ei nihil vitae quando vis, omnium commune facilisi in his. Harum definiebas assueverit mel id, te mediocrem adolescens vel. Agam omnium no his. Et nec feugait fabellas, vel cu inimicus inciderint repudiandae.

Lorem ipsum dolor sit amet, an verterem probatus qualisque eam, inani habemus mei at. Pri ut pericula accommodare, qui nibh petentium eu. Senserit honestatis cotidieque ut pri, quodsi voluptua referrentur sit at. Est nisl assum id, an odio veniam ceteros mei, ne abhorreant concludaturque vel.

Per quot vidit disputationi ex, fugit tantas volumus nam et. Eu omittam torquatos vim. Ei nihil vitae quando vis, omnium commune facilisi in his. Harum definiebas assueverit mel id, te mediocrem adolescens vel. Agam omnium no his. Et nec feugait fabellas, vel cu inimicus inciderint repudiandae.

2.1.2 PCA

Lorem ipsum dolor sit amet, an verterem probatus qualisque eam, inani habemus mei at. Pri ut pericula accommodare, qui nibh petentium eu. Senserit honestatis cotidieque ut pri, quodsi voluptua referrentur sit at. Est nisl assum id, an odio veniam ceteros mei, ne abhorreant concludaturque vel.

Per quot vidit disputationi ex, fugit tantas volumus nam et. Eu omittam torquatos vim. Ei nihil vitae quando vis, omnium commune facilisi in his. Harum definiebas assueverit mel id, te mediocrem adolescens vel. Agam omnium no his. Et nec feugait fabellas, vel cu inimicus inciderint repudiandae.

Lorem ipsum dolor sit amet, an verterem probatus qualisque eam, inani habemus mei at. Pri ut pericula accommodare, qui nibh petentium eu. Senserit honestatis cotidieque ut pri, quodsi voluptua referrentur sit at. Est nisl assum id, an odio veniam ceteros mei, ne abhorreant concludaturque vel.

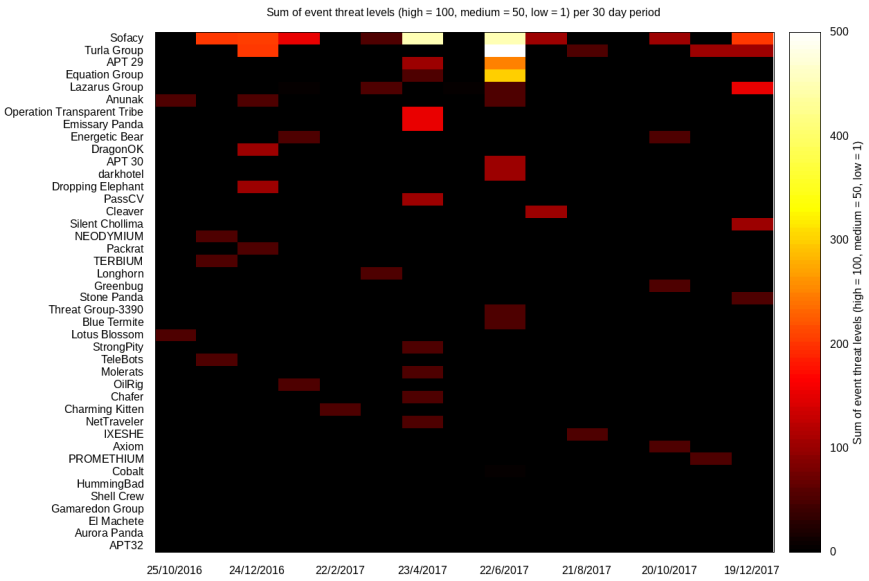


Figure 2.2: Heatmap of malicious activity by threat actor (detection time) across multiple attributes

Per quot vidit disputationi ex, fugit tantas volumus nam et. Eu omittam torquatos vim. Ei nihil vitae quando vis, omnium commune facilisi in his. Harum definiebas assueverit mel id, te mediocrem adolescens vel. Agam omnium no his. Et nec feugait fabellas, vel cu inimicus inciderint repudiandae.

2.2 Hypothesis

Lorem ipsum dolor sit amet, an verterem probatus qualisque eam, inani habemus mei at. Pri ut pericula accommodare, qui nibh petentium eu. Senserit honestatis cotidieque ut pri, quodsi voluptua referrentur sit at. Est nisl assum id, an odio veniam ceteros mei, ne abhorreant concludaturque vel.

Per quot vidit disputationi ex, fugit tantas volumus nam et. Eu omittam torquatos vim. Ei nihil vitae quando vis, omnium commune facilisi in his. Harum definiebas assueverit mel id, te mediocrem adolescens vel. Agam omnium no his. Et nec feugait fabellas, vel cu inimicus inciderint repudiandae.

Lorem ipsum dolor sit amet, an verterem probatus qualisque eam, inani habemus mei at. Pri ut pericula accommodare, qui nibh petentium eu. Senserit honestatis cotidieque ut pri, quodsi voluptua referrentur sit at. Est nisl assum id, an odio veniam ceteros mei, ne abhorreant concludaturque vel.

Per quot vidit disputationi ex, fugit tantas volumus nam et. Eu omittam torquatos vim. Ei nihil vitae quando vis, omnium commune facilisi in his. Harum definiebas assueverit mel id, te mediocrem adolescens vel. Agam omnium no his. Et nec feugait fabellas, vel cu inimicus inciderint repudiandae.

2.2.1 Topics you should review

Lorem ipsum dolor sit amet, an verterem probatus qualisque eam, inani habemus mei at. Pri ut pericula accommodare, qui nibh petentium eu. Senserit honestatis cotidieque ut pri, quodsi voluptua referrentur sit at. Est nisl assum id, an odio veniam ceteros mei, ne abhorreant concludaturque vel.

```
GreyArea@20:21>710 ocamlopt -o testransomware btc.ml
GreyArea@20:21>711 binwalk testransomware

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             ELF, 64-bit LSB shared object, AMD x86-64, version 1 (SYSV)
156028        0x2617C         Unix path: /build/ocaml-KvJJA8/ocaml-4.02.3/stdlib

GreyArea@20:21>712 ./testransomware
15F5FM7qMhLQ44RDxuozbKRwSbHKmq7N39
17VZNX1SN5NtKa8UQFxwQbFeFc3iqRYhem
3EktnHQD7RiAE6uzMj2ZifT9YgRrkSgzQX
5Hwgr3u458GLafKBgxtssHSPqJnYoGrSzgQsPwLFhLNYskDPyyA
L1aW4aubDFB7yfras2S1mN3bqg9nwySY8nkoLmJebSLD5BWv3ENZ
xpub661MyMwAqRbcEYS8w7XLSVeEsBXy79zSzH1J8vCdxAZningWLdN3
zgtU6LBpB85b3D2yc8sfvZU521AAwdZafEz7mnzBBsz4wKY5e4cp9LB
xprv9s21ZrQH143K24Mfq5zL5MhWK9hUhhGbd45hLXo2Pq2oqzMMo63o
StZzF93Y5wvzdUayhgkkFoicQ2cP3y52uPPxFnfoLZB21Teqt1VvEHx
mipcBbFg9gMiCh81Kj8tqqdgoZub1ZJRfn
2MzQwSSnBHWHqSAqtTVQ6v47XtaisrJa1Vc
92Pg46rUhgTT7romnV7iGW6W1gbGdeezqdbJCzShkCsYNzyyNcc
cNJFgoldriFnPcBdBX8BrJrpxchBWXwXCvNH5SoSkdcF6JXXwHMm
tpubD6NzVbkrYhZ4WLczPJWReQycCJdd6YVWXubbVUFnJ5KgU5MDQrD9
98ZJLNGbhd2pq7ZtDiPYfFJ7iBenLVQpYgSQqPjUsQeJXH8VQ8xA67D
tprv8ZgxMBicQKsPcsbCVeqqF1KVdH7gwDJbxbzpCxDUsoXHdb6SnTPY
xdwSAKDC6KKJzv7khnNWRAJQsRA8BBQyiSfYnRt6zuu4vZQGKjeW4YF
GreyArea@20:21>713 python re-search.py "(?#extra=P:BTCValidate)[13][a-km-zA-HJ-NP-Z1-9]{25,34}" testransomware
15F5FM7qMhLQ44RDxuozbKRwSbHKmq7N39
17VZNX1SN5NtKa8UQFxwQbFeFc3iqRYhem
3EktnHQD7RiAE6uzMj2ZifT9YgRrkSgzQX
```

Figure 2.3: Example of current BTC address regex tools failing to detect all address types

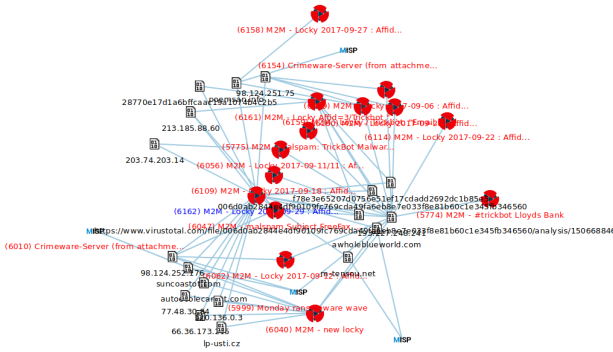


Figure 2.4: Locky IoC clusters

Per quot vidit disputationi ex, fugit tantas volumus nam et. Eu omittam torquatos vim. Ei nihil vitae quando vis, omnium commune facilisi in his. Harum definiebas assueverit mel id, te mediocrem adolescens vel. Agam omnium no his. Et nec feugait fabellas, vel cu inimicus inciderint repudiandae.

- Malware and computer science
  - Data mining
  - Machine Learning
  - Big Data Analysis
  - Neural Networks
  - Visualization Resources
- Statistics and Image Processing
  - Probability Density Function
  - Point Spread Function
  - Full width at half maximum
  - Convolution

Lorem ipsum dolor sit amet, an verterem probatus qualisque eam, inani habemus mei at. Pri ut pericula accommodare, qui nibh petentium eu. Senserit honestatis cotidieque ut pri, quodsi voluptua referrentur sit at. Est nisl assum id, an odio veniam ceteros mei, ne abhorreant concludaturque vel.

Per quot vidit disputationi ex, fugit tantas volumus nam et. Eu omittam torquatos vim. Ei nihil

vitae quando vis, omnium commune facilisi in his. Harum definiebas assueverit mel id, te mediocrem adolescens vel. Agam omnium no his. Et nec feugait fabellas, vel cu inimicus inciderint repudiandae.

Lorem ipsum dolor sit amet, an verterem probatus qualisque eam, inani habemus mei at. Pri ut pericula accommodare, qui nibh petentium eu. Senserit honestatis cotidieque ut pri, quodsi voluptua referrentur sit at. Est nisl assum id, an odio veniam ceteros mei, ne abhorreant concludaturque vel.

Per quot vidit disputationi ex, fugit tantas volumus nam et. Eu omittam torquatos vim. Ei nihil vitae quando vis, omnium commune facilisi in his. Harum definiebas assueverit mel id, te mediocrem adolescens vel. Agam omnium no his. Et nec feugait fabellas, vel cu inimicus inciderint repudiandae.

/subsectionSamples Analysed

event id	category	type	value	comment	ids	date
6733	Social network	email-src	"info@scentreqroup.com"	""	0	20180212
6733	Payload delivery	md5	"ebb76124726 85e43069 11c6efcf29391"	""	1	20180212
6733	Payload delivery	sha1	"5bf5a94015519fe70f2747deb99532b22af9e2af"	""	1	20180212
6733	Payload delivery	sha256	"28e0cb78f8db8da3b4fc7fdf9bf6e28cb40d8019fe23572b9a644b0910a25dc3"	""	1	20180212

Lorem ipsum dolor sit amet, an verterem probatus qualisque eam, inani habemus mei at. Pri ut pericula accommodare, qui nibh petentium eu. Senserit honestatis cotidieque ut pri, quodsi voluptua referrentur sit at. Est nisl assum id, an odio veniam ceteros mei, ne abhorreant concludaturque vel.

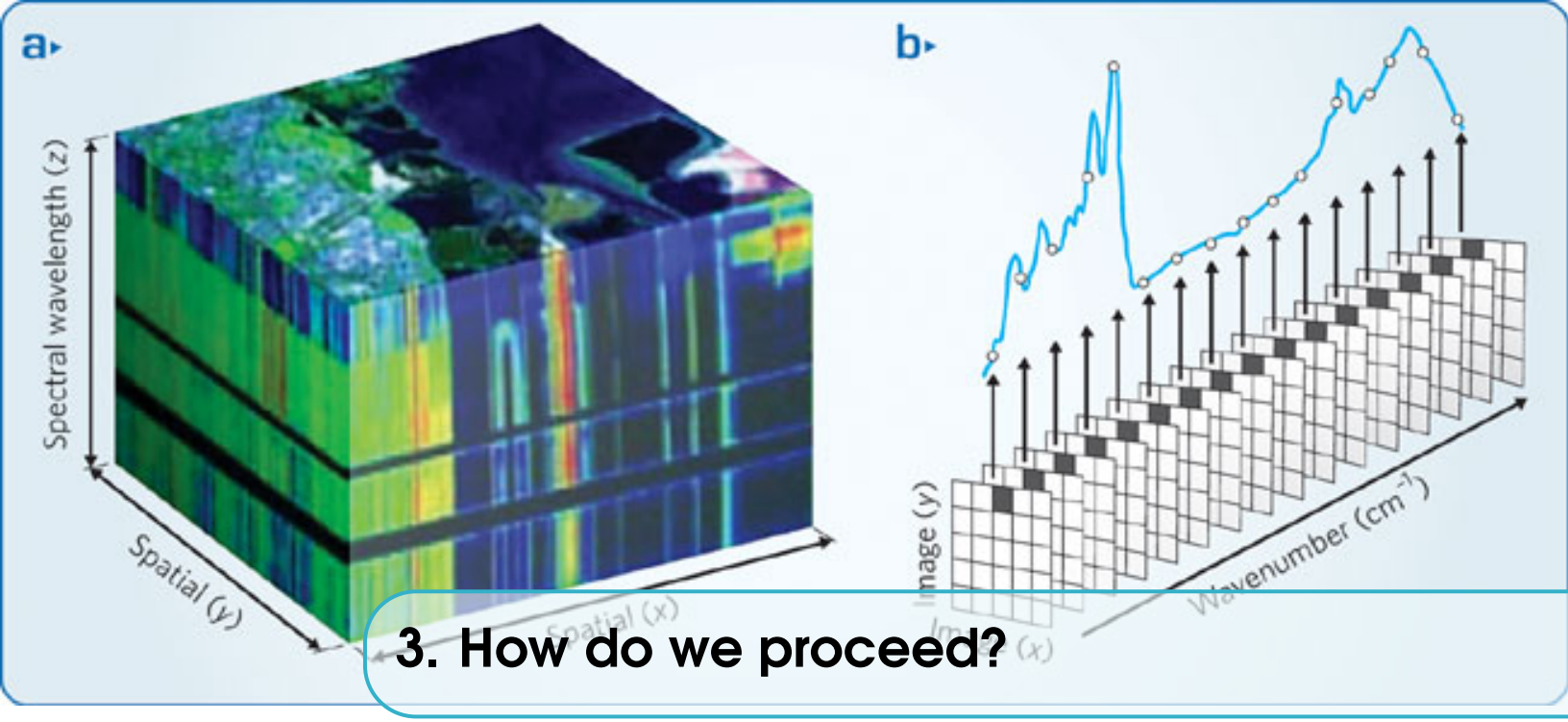
Per quot vidit disputationi ex, fugit tantas volumus nam et. Eu omittam torquatos vim. Ei nihil vitae quando vis, omnium commune facilisi in his. Harum definiebas assueverit mel id, te mediocrem adolescens vel. Agam omnium no his. Et nec feugait fabellas, vel cu inimicus inciderint repudiandae.

Lorem ipsum dolor sit amet, an verterem probatus qualisque eam, inani habemus mei at. Pri ut pericula accommodare, qui nibh petentium eu. Senserit honestatis cotidieque ut pri, quodsi voluptua referrentur sit at. Est nisl assum id, an odio veniam ceteros mei, ne abhorreant concludaturque vel.

Per quot vidit disputationi ex, fugit tantas volumus nam et. Eu omittam torquatos vim. Ei nihil vitae quando vis, omnium commune facilisi in his. Harum definiebas assueverit mel id, te mediocrem adolescens vel. Agam omnium no his. Et nec feugait fabellas, vel cu inimicus inciderint repudiandae.

Lorem ipsum dolor sit amet, an verterem probatus qualisque eam, inani habemus mei at. Pri ut pericula accommodare, qui nibh petentium eu. Senserit honestatis cotidieque ut pri, quodsi voluptua referrentur sit at. Est nisl assum id, an odio veniam ceteros mei, ne abhorreant concludaturque vel.

Per quot vidit disputationi ex, fugit tantas volumus nam et. Eu omittam torquatos vim. Ei nihil vitae quando vis, omnium commune facilisi in his. Harum definiebas assueverit mel id, te mediocrem adolescens vel. Agam omnium no his. Et nec feugait fabellas, vel cu inimicus inciderint repudiandae.



3. How do we proceed?

Lorem ipsum dolor sit amet, an verterem probatus qualisque eam, inani habemus mei at. Pri ut pericula accommodare, qui nibh petentium eu. Senserit honestatis cotidieque ut pri, quodsi voluptua referrentur sit at. Est nisl assum id, an odio veniam ceteros mei, ne abhorreant concludaturque vel.

Per quot vidit disputationi ex, fugit tantas volumus nam et. Eu omittam torquatos vim. Ei nihil vitae quando vis, omnium commune facilisi in his. Harum definiebas assueverit mel id, te mediocrem adolescens vel. Agam omnium no his. Et nec feugait fabellas, vel cu inimicus inciderint repudiandae.

3.1 Further work

Lorem ipsum dolor sit amet, an verterem probatus qualisque eam, inani habemus mei at. Pri ut pericula accommodare, qui nibh petentium eu. Senserit honestatis cotidieque ut pri, quodsi voluptua referrentur sit at. Est nisl assum id, an odio veniam ceteros mei, ne abhorreant concludaturque vel.

Per quot vidit disputationi ex, fugit tantas volumus nam et. Eu omittam torquatos vim. Ei nihil vitae quando vis, omnium commune facilisi in his. Harum definiebas assueverit mel id, te mediocrem adolescens vel. Agam omnium no his. Et nec feugait fabellas, vel cu inimicus inciderint repudiandae.

Wish you all the best, Eireann Leverett