March 18 & 19, 2019

Ransomware Payments in the Bitcoin Ecosystem

Masarah Paquet-Clouston
GoSecure Powered by Countertack

BSides Vancouver 2019

GoSecure
POWERED BY COUNTERTACK

Who am I?

- Security researcher at GoSecure Powered by CounterTack
- PhD Student in Criminology at Simon Fraser University
- Part of the NorthSec council (www.nsec.io)

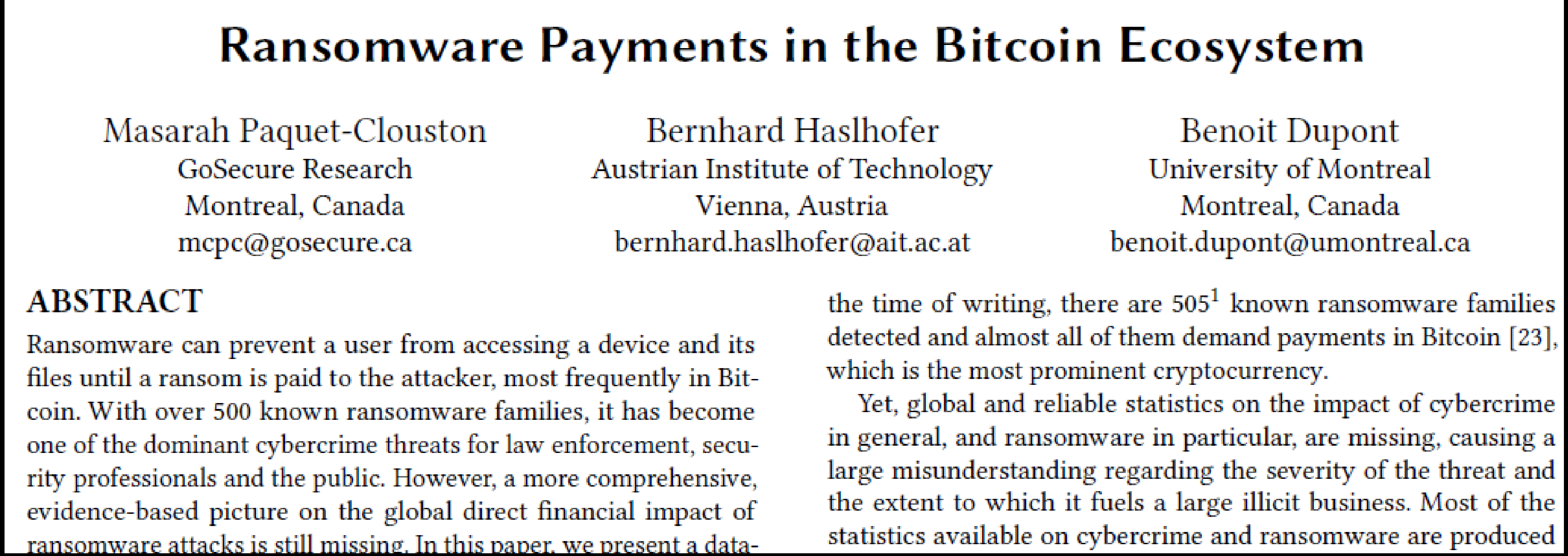
Agenda

- Research goal
- Tracing ransomware payments in the bitcoin ecosystem
- Quantifying the direct financial impact of ransomware
- The market with kingpins
- Future work

Ransomware Payments in the Bitcoin Ecosystem

Workshop on the Economics of Information Security (WEIS2018)

https://weis2018.econinfosec.org/program/



Ransomware Payments in the Bitcoin Ecosystem

Masarah Paquet-Clouston
GoSecure Research
Montreal, Canada
mcpc@gosecure.ca

Bernhard Haslhofer
Austrian Institute of Technology
Vienna, Austria
bernhard.haslhofer@ait.ac.at

Benoit Dupont
University of Montreal
Montreal, Canada
benoit.dupont@umontreal.ca

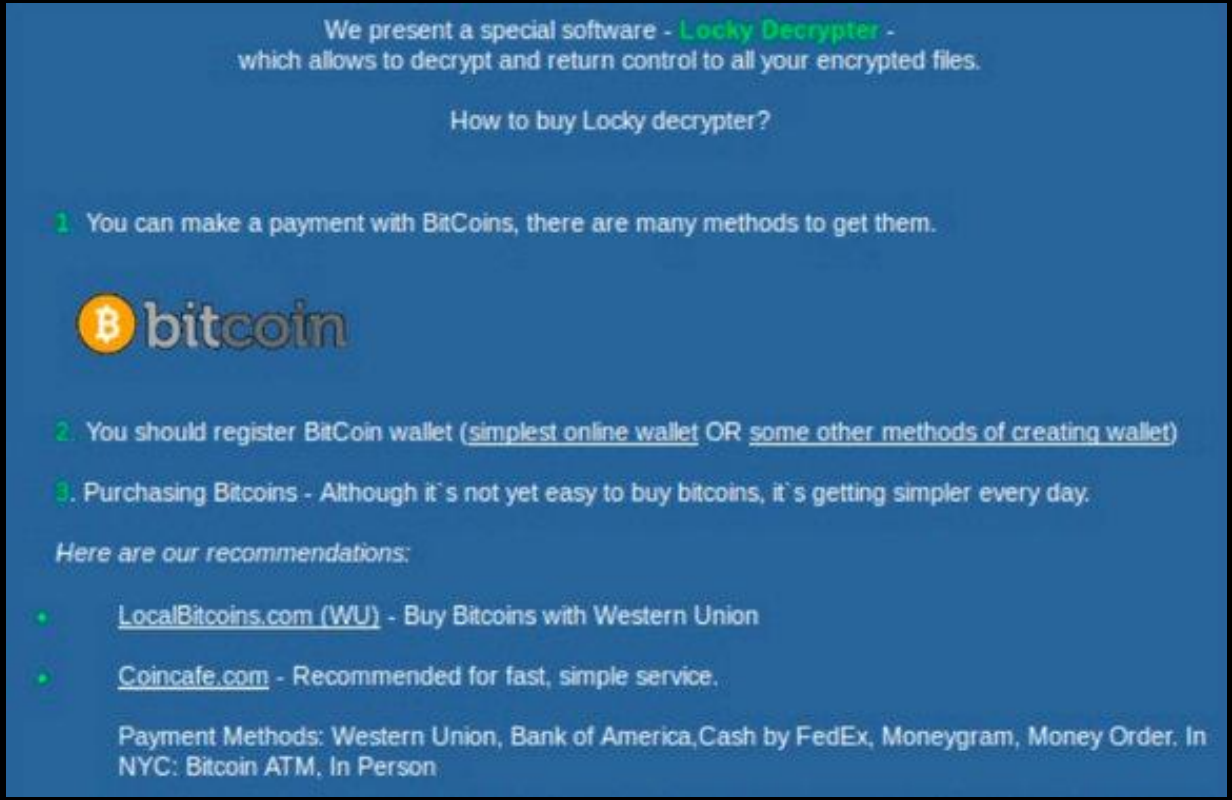
ABSTRACT

Ransomware can prevent a user from accessing a device and its files until a ransom is paid to the attacker, most frequently in Bitcoin. With over 500 known ransomware families, it has become one of the dominant cybercrime threats for law enforcement, security professionals and the public. However, a more comprehensive, evidence-based picture on the global direct financial impact of ransomware attacks is still missing. In this paper, we present a data-

the time of writing, there are 505[1] known ransomware families detected and almost all of them demand payments in Bitcoin [23], which is the most prominent cryptocurrency.

Yet, global and reliable statistics on the impact of cybercrime in general, and ransomware in particular, are missing, causing a large misunderstanding regarding the severity of the threat and the extent to which it fuels a large illicit business. Most of the statistics available on cybercrime and ransomware are produced

Ransomware



We present a special software - Locky Decrypter - which allows to decrypt and return control to all your encrypted files.

How to buy Locky decrypter?

1. You can make a payment with BitCoins, there are many methods to get them.

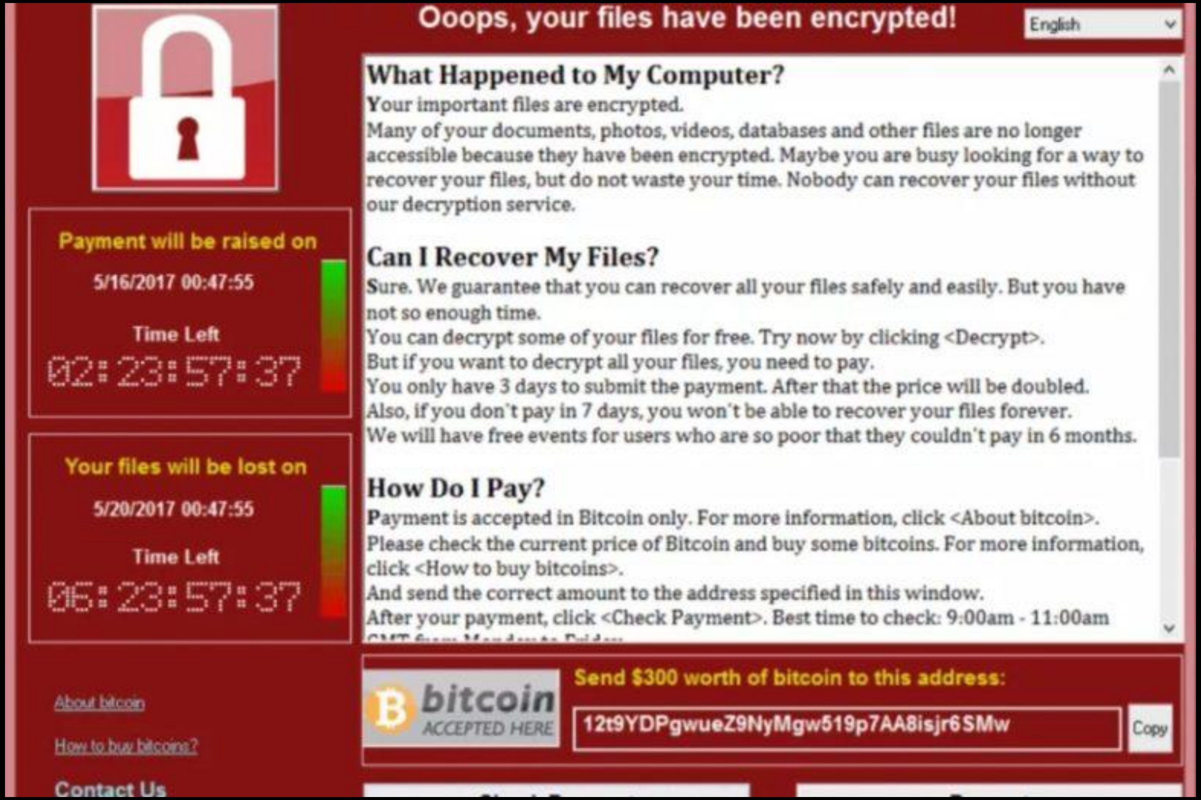
2. You should register BitCoin wallet (simplest online wallet OR some other methods of creating wallet)

3. Purchasing Bitcoins - Although it`s not yet easy to buy bitcoins, it`s getting simpler every day.

Here are our recommendations:

- LocalBitcoins.com (WU) - Buy Bitcoins with Western Union
- Coincafe.com - Recommended for fast, simple service.

  Payment Methods: Western Union, Bank of America,Cash by FedEx, Moneygram, Money Order. In NYC: Bitcoin ATM, In Person



Ooops, your files have been encrypted!

Payment will be raised on
5/16/2017 00:47:55
Time Left
02:23:57:37

Your files will be lost on
5/20/2017 00:47:55
Time Left
06:23:57:37

What Happened to My Computer?

Your important files are encrypted.

Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.

You can decrypt some of your files for free. Try now by clicking <Decrypt>.

But if you want to decrypt all your files, you need to pay.

You only have 3 days to submit the payment. After that the price will be doubled.

Also, if you don't pay in 7 days, you won't be able to recover your files forever.

We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.

Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.

And send the correct amount to the address specified in this window.

After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am GMT from Monday to Friday

Send $300 worth of bitcoin to this address:

12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

Ransomware

- Serious threat: raises fear and concern among potential victims
- Potentially highly profitable for ransomware authors

“Ransomware: Too Profitable to Go Away”

(CSO online, 2017)

- Yet, global and reliable statistics are missing
- Most of the statistics are produced by private corporations

Ransomware

1. Kharraz et al. (2015)

- Analyzed 1,359 samples from 15 ransomware families
- Found that the number of families with sophisticated destructive capabilities remains quite small

2. Gazet (2010)

- Conducted a comparative analysis of 15 ransomware
- Concluded that ransomware attackers followed a low-cost/low-risk business model

Unique Opportunity

To quantify the lower bound direct financial impact of ransomware attacks

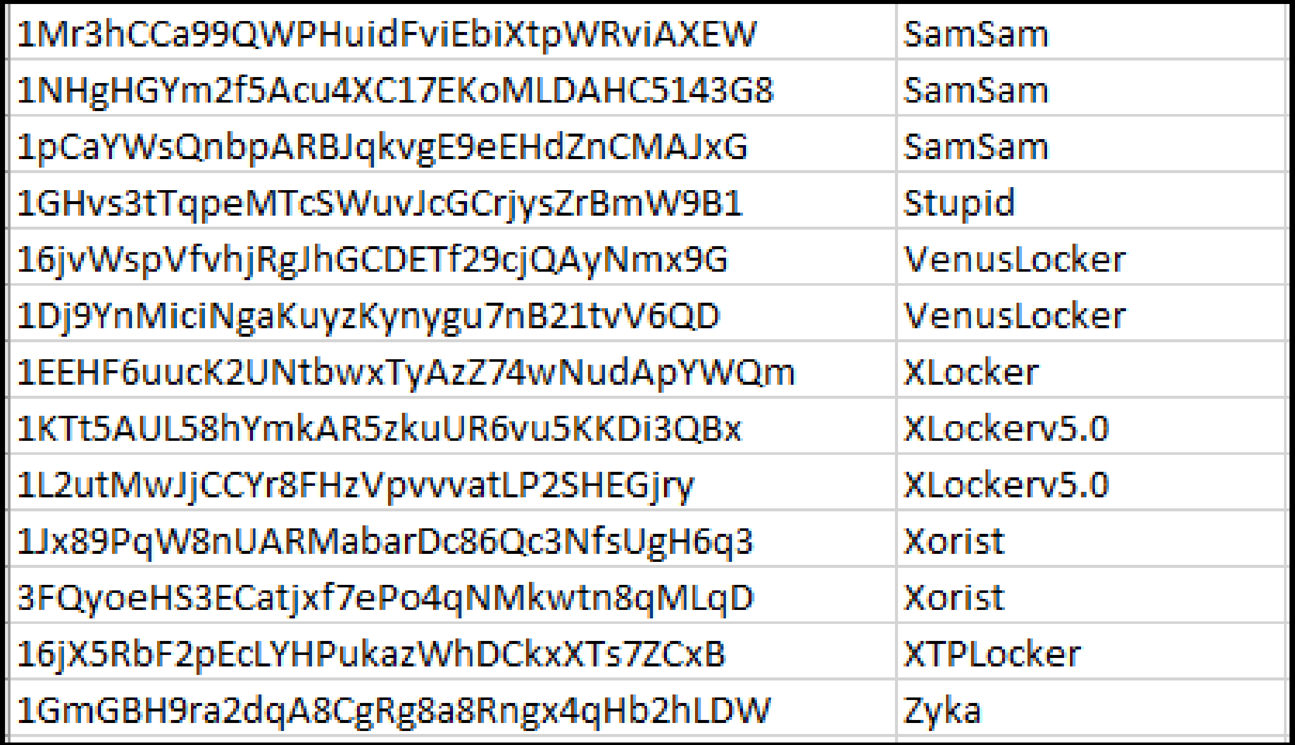
- Most ransoms are paid in Bitcoin
- Bitcoin transactions are publicly available
- Clustering heuristics and tools have been developed to extract information from each bitcoin transaction

Research Goal

Develop a data-driven method for identifying, quantifying, and comparing payments and revenues of given ransomware families

Seed Dataset

We gathered 7,118 Bitcoin addresses related to 35 ransomware families



1Mr3hCCa99QWPHuidFviEbiXtpWRviAXEW	SamSam
1NHgHGYm2f5Acu4XC17EKoMLDAHC5143G8	SamSam
1pCaYWsQnbpARBJqkvgE9eEHdZnCMAJxG	SamSam
1GHvs3tTqpeMTcSWuvJcGCrjysZrBmW9B1	Stupid
16jvWspVfvhjRgJhGCDETf29cjQAyNmx9G	VenusLocker
1Dj9YnMiciNgaKuyzKynygu7nB21tvV6QD	VenusLocker
1EEHF6uucK2UNtbwxTyAzZ74wNudApYWQm	XLocker
1KTt5AUL58hYmkAR5zkuUR6vu5KKDi3QBx	XLockerv5.0
1L2utMwJjCCYr8FHzVpvvvatLP2SHEGjry	XLockerv5.0
1Jx89PqW8nUARMabarDc86Qc3NfsUgH6q3	Xorist
3FQyoeHS3ECatjxf7ePo4qNMkwtn8qMLqD	Xorist
16jX5RbF2pEcLYHPukazWhDCkxXTs7ZCxB	XTPLocker
1GmGBH9ra2dqA8CgRg8a8Rngx4qHb2hLDW	Zyka

Dataset Expansion:
Multi-Input Heuristic

Meiklejohn, 2013; Ortega; 2013; Biryukov et al., 2014; Fleder et. al, 2015; Haslhofer et. al, 2016; Möser and Böhme, 2016

Key Understanding about bitcoin transactions

Each bitcoin address is related to a public/private key pair

Private key:

5Jtr4hBXP2hPedtcFfcMFQK79YGhkJejjgduHy3oLSTuTiYbhrq

Public key:

04869B9A9D4FF58006B5BAB2253EF3C2CD1C8607007172D0493A
AA9BDD4E17E90FEDF740C2B2068C6F24AE6CC38B85EB8D54185
A2B87E790DA9259F8996A17CF26

Public Address:

14geEFfPXT9K5Vao9DcoFeikPDJyc7QZUM

Key Understanding about bitcoin transactions

Private key

Kx4JXfodisMpQEij9momeA5aWuEf7bnr5FjiQtsQP2UxqagWrVUY

Generate a bitcoin address

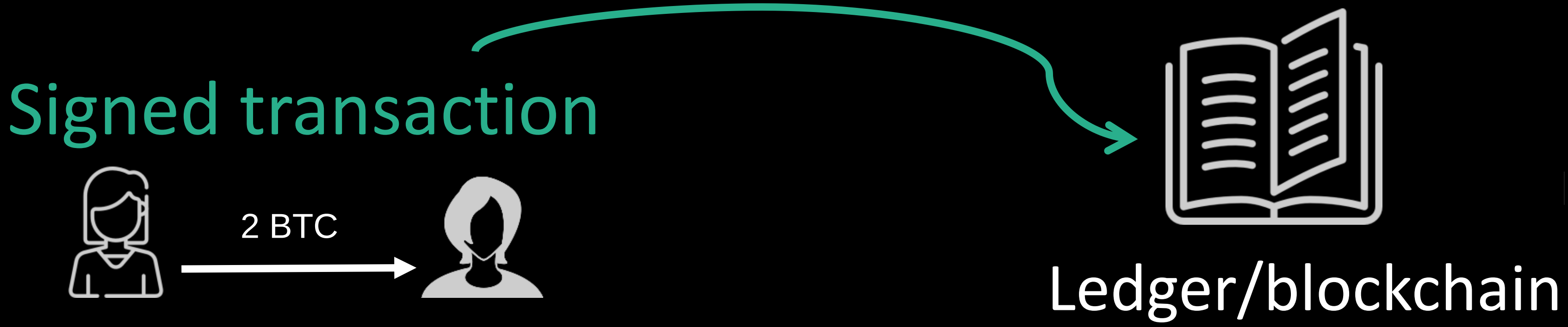
12HMwtYw9ctZCPaPHiFBbF
PqF9wiEgNND2

Sign a transaction

Key Understanding about bitcoin transactions

Private key

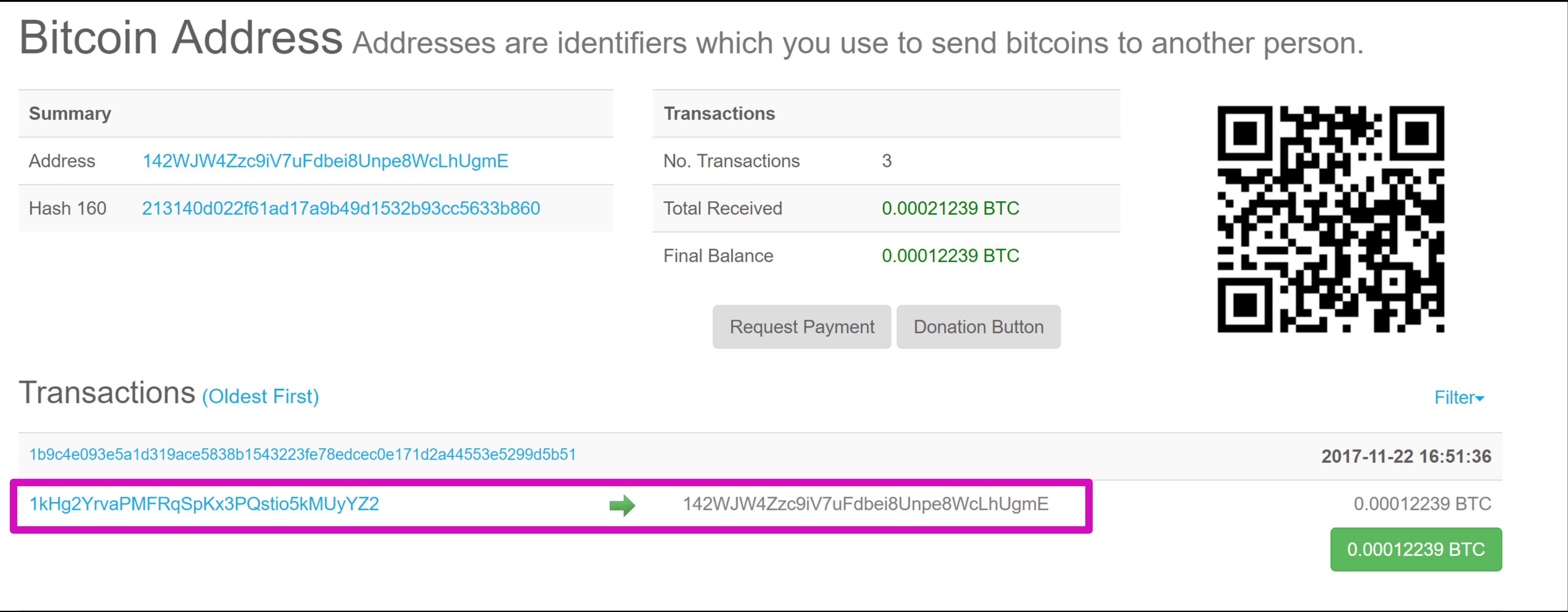
Kx4JXfodisMpQEij9momeA5aWuEf7bnr5FjiQtsQP2UxqagWrVUY



Signed transaction

Ledger/blockchain

Key Understanding about bitcoin addresses



Bitcoin Address Addresses are identifiers which you use to send bitcoins to another person.

Summary	
Address	142WJW4Zzc9iV7uFdbei8Unpe8WcLhUgmE
Hash 160	213140d022f61ad17a9b49d1532b93cc5633b860

Transactions	
No. Transactions	3
Total Received	0.00021239 BTC
Final Balance	0.00012239 BTC

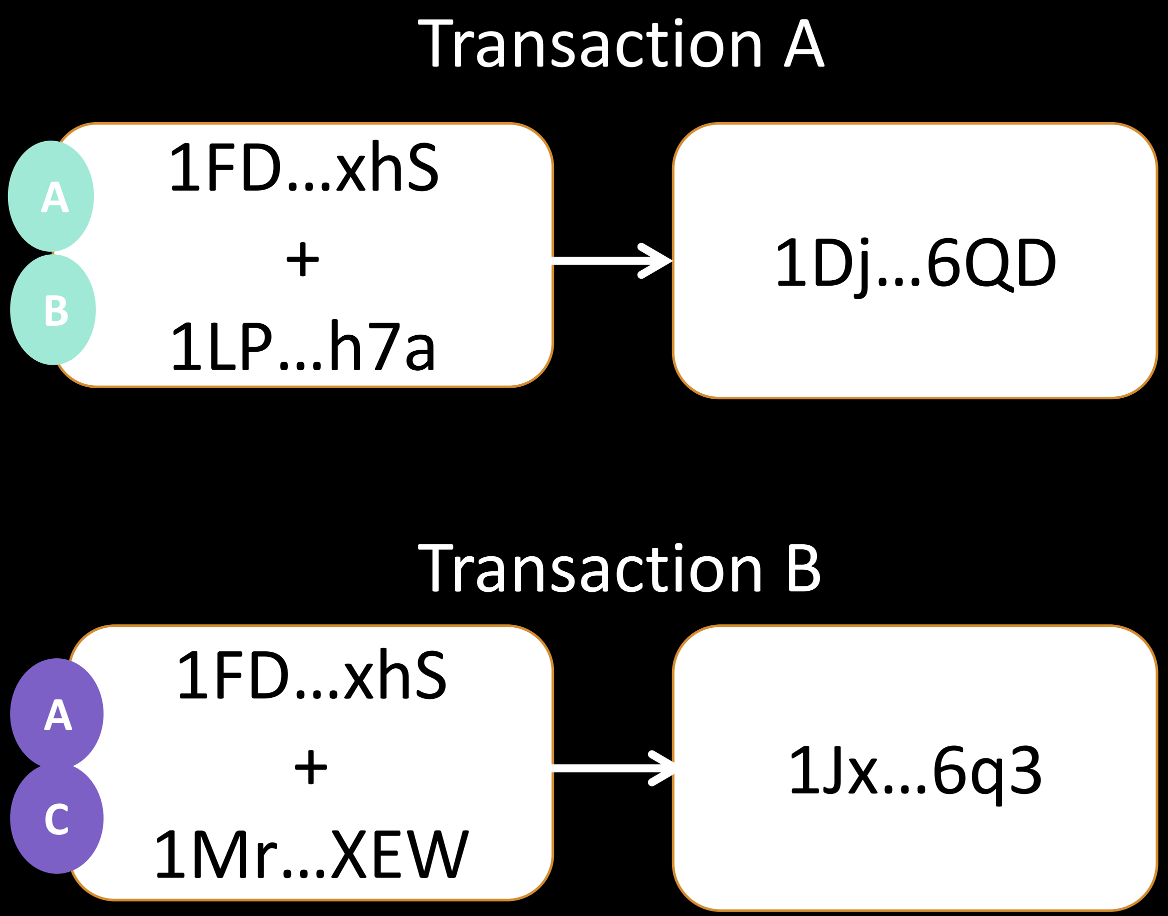
Transactions (Oldest First)

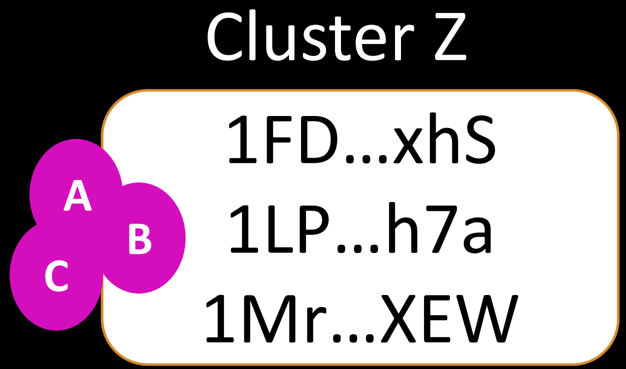
1b9c4e093e5a1d319ace5838b1543223fe78edcec0e171d2a44553e5299d5b51 **2017-11-22 16:51:36**

1kHg2YrvaPMFRqSpKx3PQstio5kMUyYZ2 → 142WJW4Zzc9iV7uFdbei8Unpe8WcLhUgmE 0.00012239 BTC

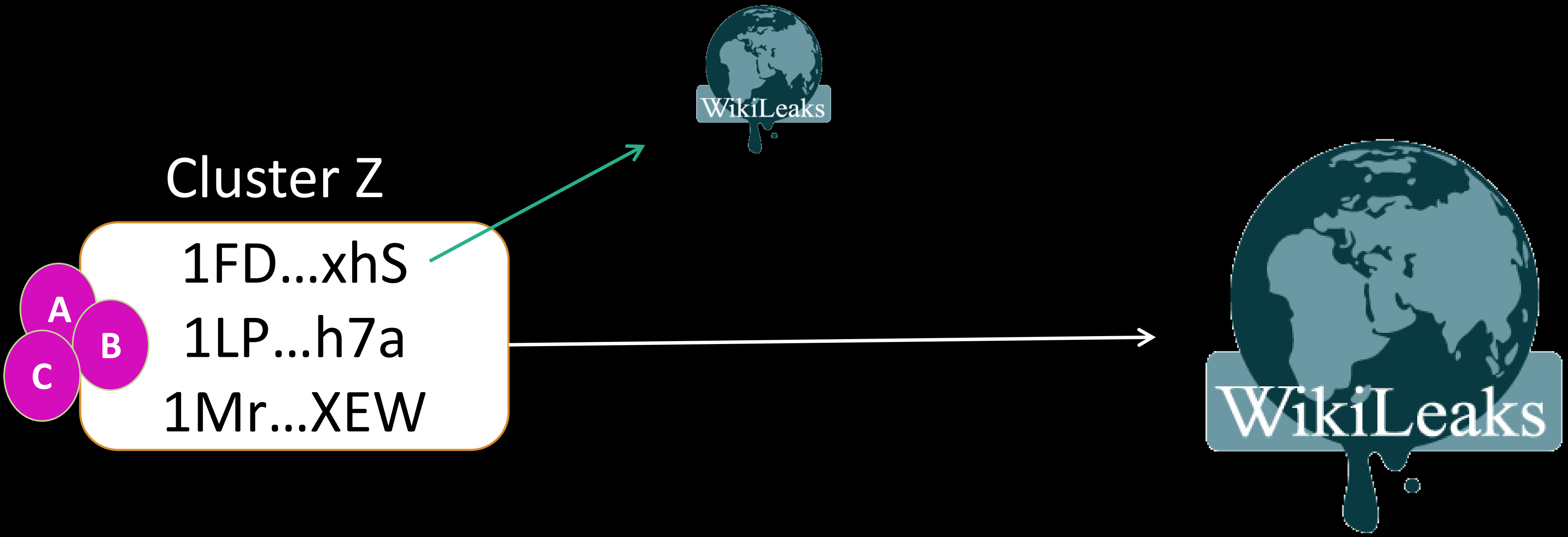
0.00012239 BTC

Multi-Input Heuristic





Deanonymization



Cluster Z

1FD…xhS

1LP…h7a

1Mr…XEW

GraphSense: Cryptocurrency Open-Source Platform

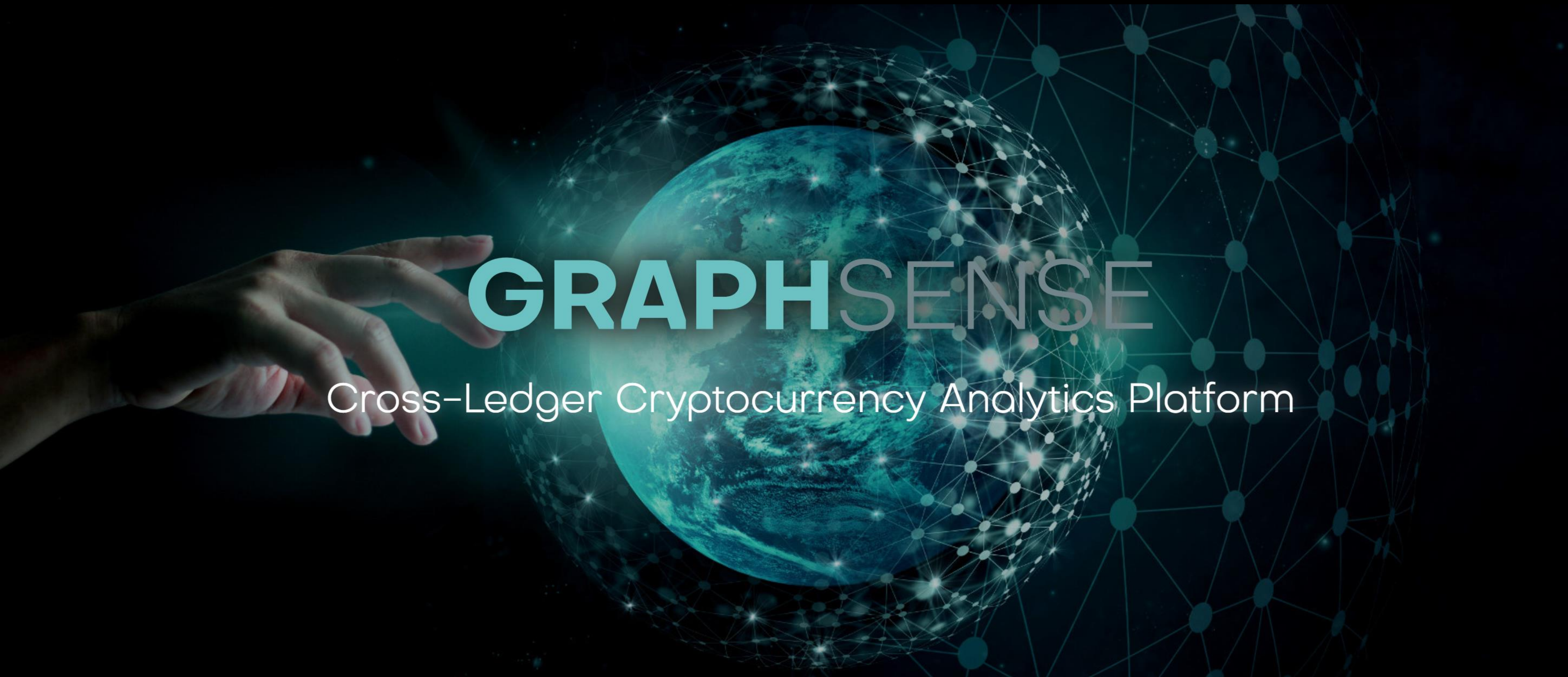
Authors

- Bernhard Haslhofer
- Roman Karl
- Mihai Bartha
- Rainer Stütz

AUSTRIAN INSTITUTE OF TECHNOLOGY

http://graphsense.info/

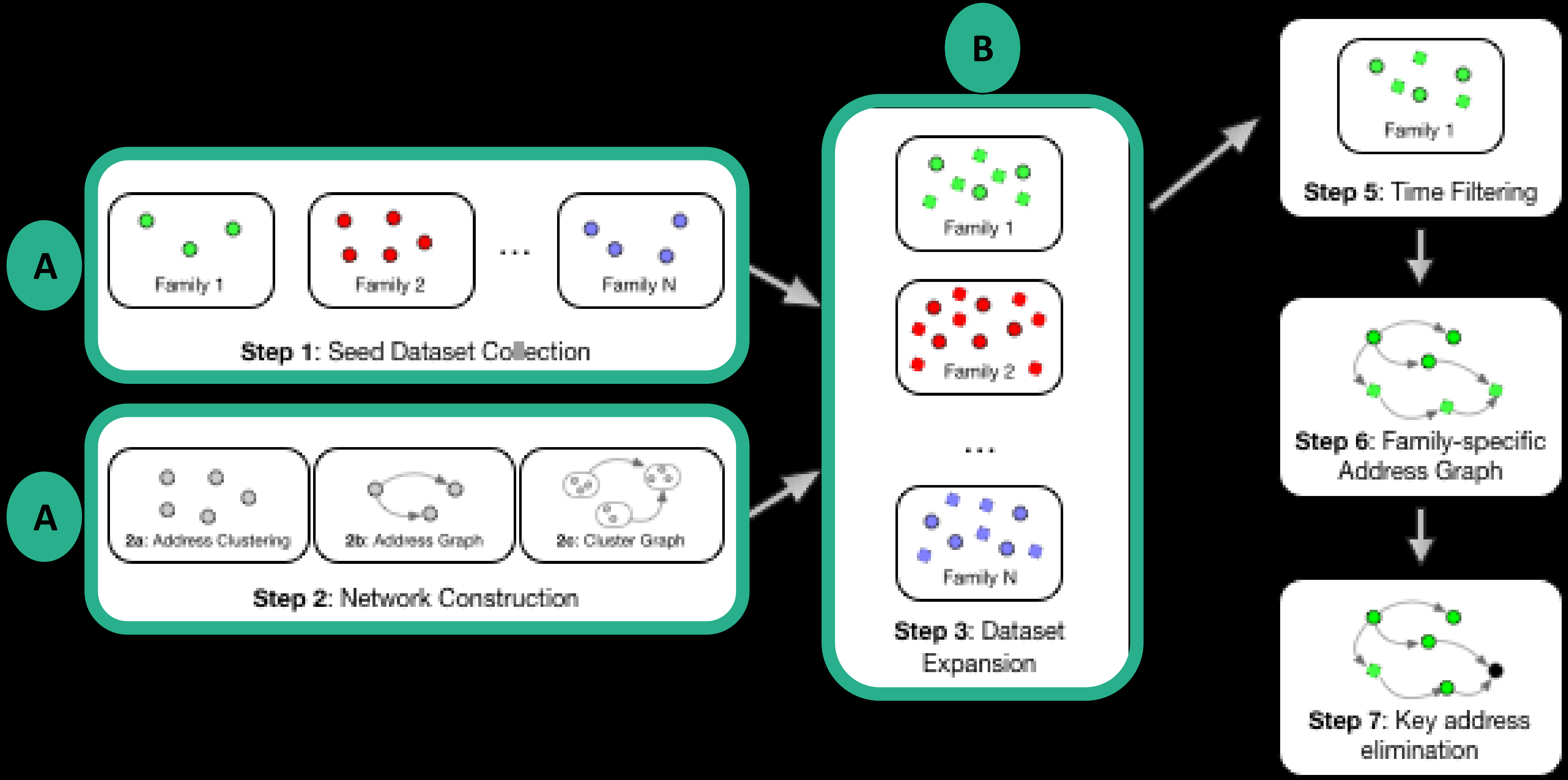
DEMO


GRAPHSENSE
Cross-Ledger Cryptocurrency Analytics Platform

GraphSense REST API

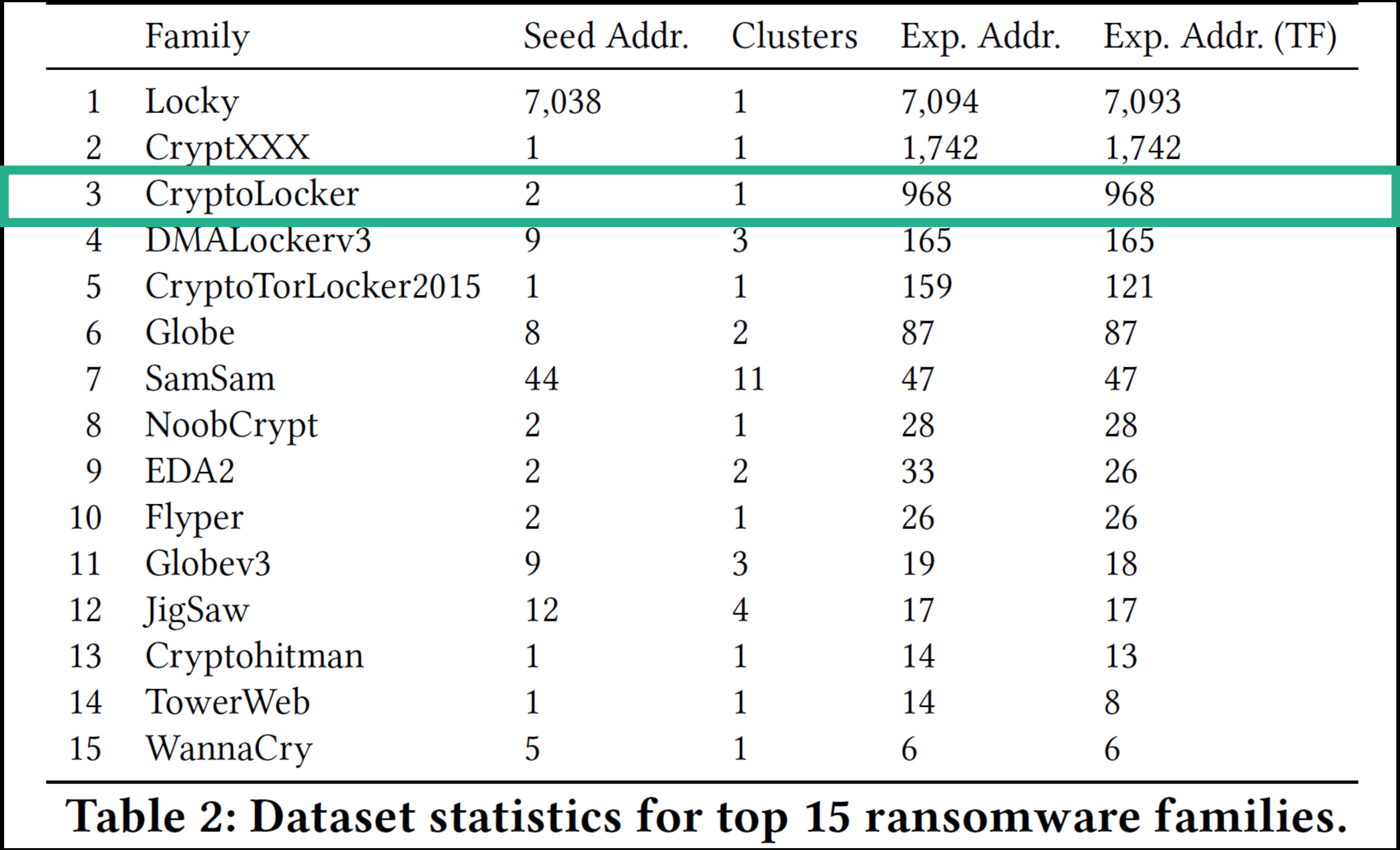
```
"address": "142WJW4Zzc9iV7uFdbei8Unpe8WcLhUgmE",
"address_prefix": "142WJ",
"balance": {
    "eur": 0.39,
    "satoshi": 12239,
    "usd": 0.44
},
"firstTx": {
    "height": 425445,
    "timestamp": 1471338256,
    "tx_hash": "db0defef3acc20e74ad55ec29c1d1fb63d4183941081166f0b4ba4e1e5914b48"
},
"inDegree": 2,
"lastTx": {
    "height": 495722,
    "timestamp": 1511437163,
    "tx_hash": "1b9c4e093e5a1d319ace5838b1543223fe78edcec0e171d2a44553e5299d5b51"
},
"noIncomingTxs": 2,
"noOutgoingTxs": 1,
"outDegree": 2,
"totalReceived": {
    "eur": 0.88,
    "satoshi": 21239,
    "usd": 1.03
},
"totalSpent": {
    "eur": 0.05,
    "satoshi": 9000,
    "usd": 0.05
}
```

The Method



B
A
Family 1
Family 2
. . .
Family N
Step 1: Seed Dataset Collection
A
2a: Address Clustering
2b: Address Graph
2c: Cluster Graph
Step 2: Network Construction
Family 1
Family 2
. . .
Family N
Step 3: Dataset Expansion
Family 1
Step 5: Time Filtering
Step 6: Family-specific Address Graph
Step 7: Key address elimination

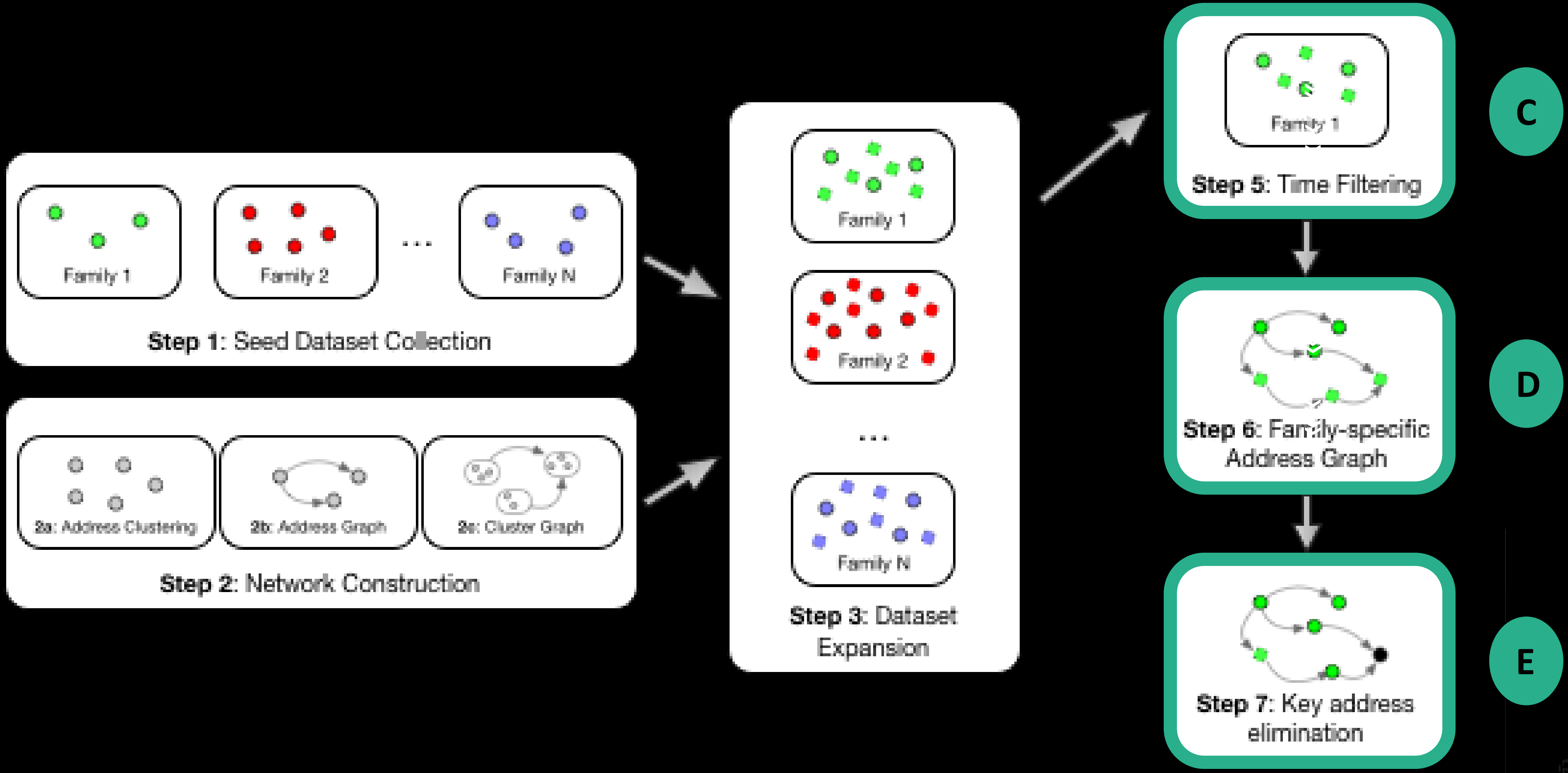
Sample



	Family	Seed Addr.	Clusters	Exp. Addr.	Exp. Addr. (TF)
1	Locky	7,038	1	7,094	7,093
2	CryptXXX	1	1	1,742	1,742
3	CryptoLocker	2	1	968	968
4	DMALockerv3	9	3	165	165
5	CryptoTorLocker2015	1	1	159	121
6	Globe	8	2	87	87
7	SamSam	44	11	47	47
8	NoobCrypt	2	1	28	28
9	EDA2	2	2	33	26
10	Flyper	2	1	26	26
11	Globev3	9	3	19	18
12	JigSaw	12	4	17	17
13	Cryptohitman	1	1	14	13
14	TowerWeb	1	1	14	8
15	WannaCry	5	1	6	6

Table 2: Dataset statistics for top 15 ransomware families.

The Method


Family 1
Family 2
...
Family N
Step 1: Seed Dataset Collection
2a: Address Clustering
2b: Address Graph
2c: Cluster Graph
Step 2: Network Construction
Family 1
Family 2
...
Family N
Step 3: Dataset Expansion
Family 1
Step 5: Time Filtering
Step 6: Family-specific Address Graph
Step 7: Key address elimination
C
D
E

FOLLOWING THE MONEY TRACE

Payments to Locky bitcoin addresses

🟢 Ransomware addresses

🔵 Victim addresses

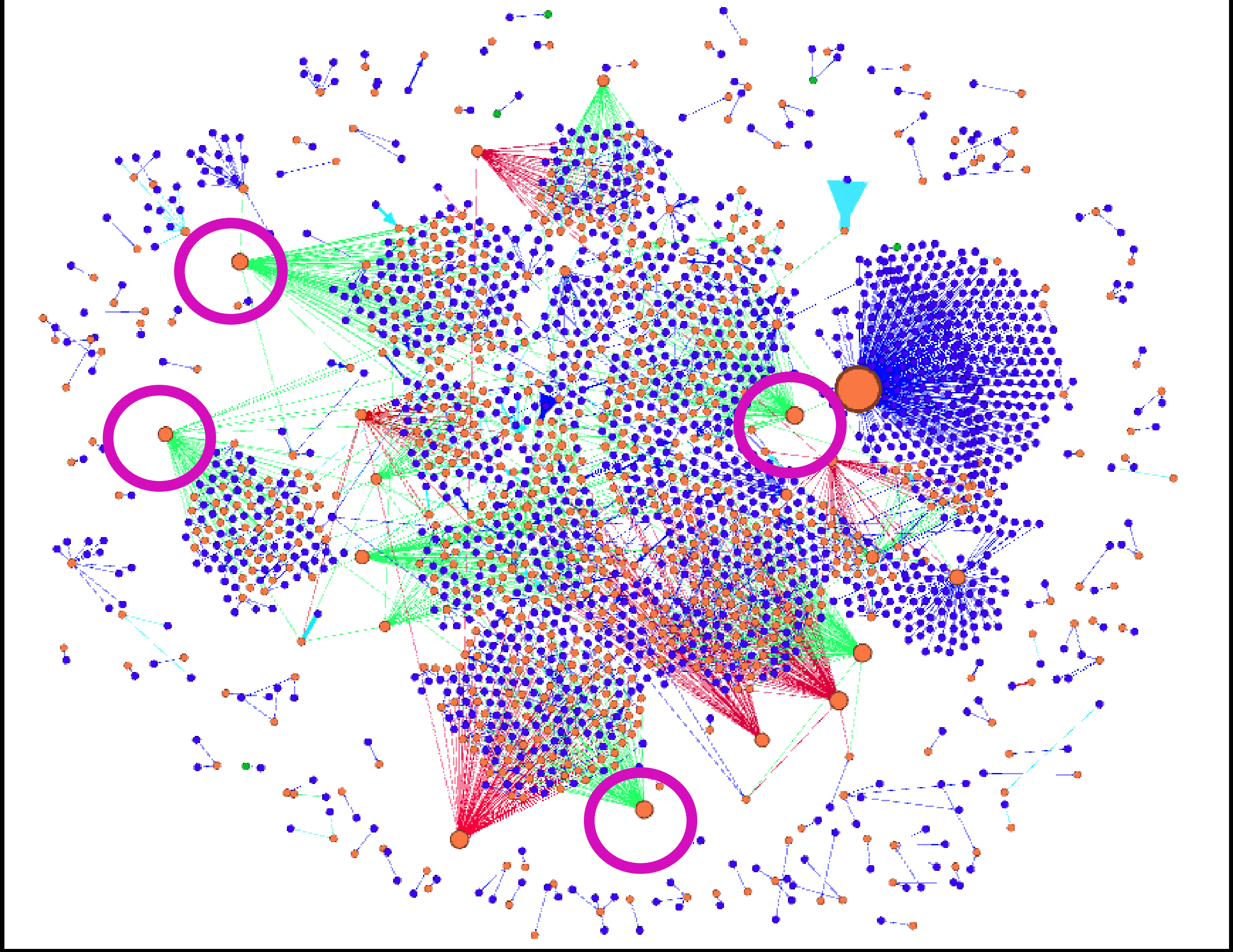
🟠 Both ransomware and victim addresses

🟩 <1 BTC

🟦 1 BTC

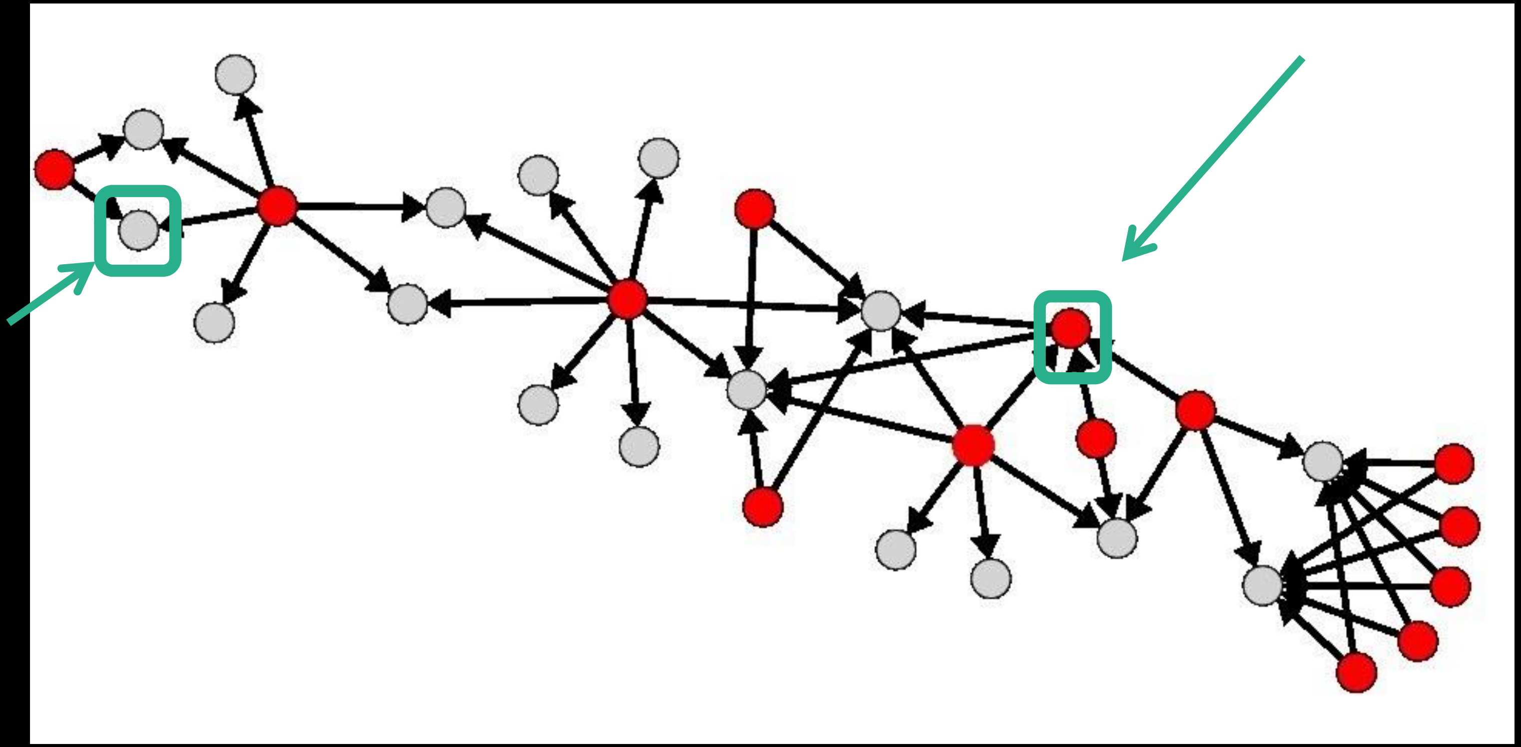
▬ 2-5 BTC

🟥 < 10 BTC



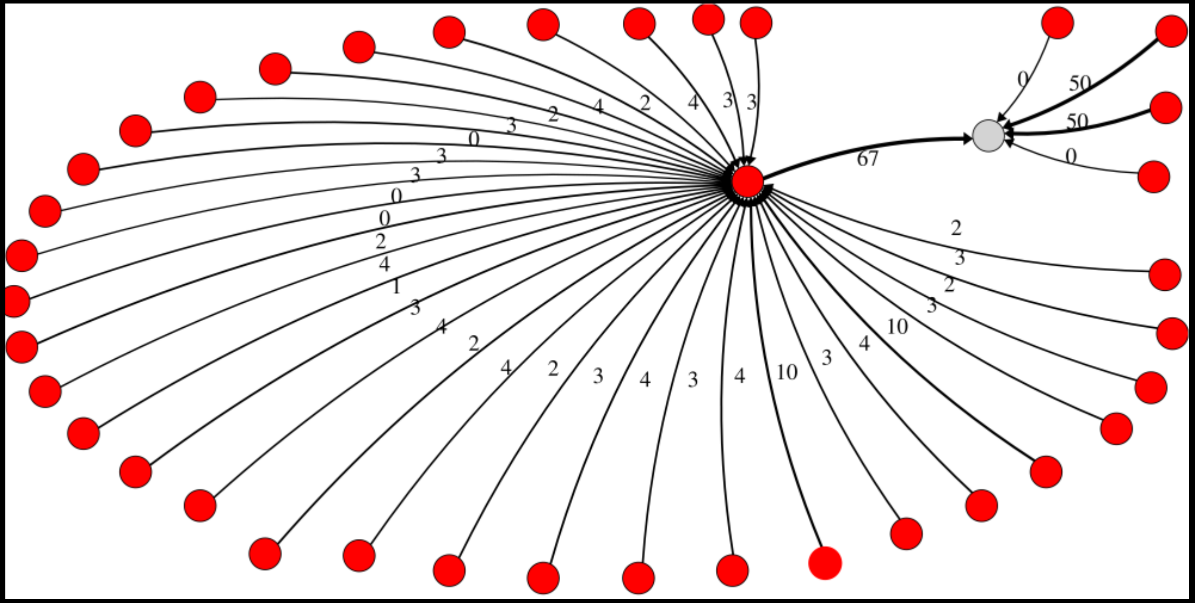
The Method

Analyze only outgoing relationships for each ransomware family



Collectors

“an address used to collect or aggregate payments from”



Collectors

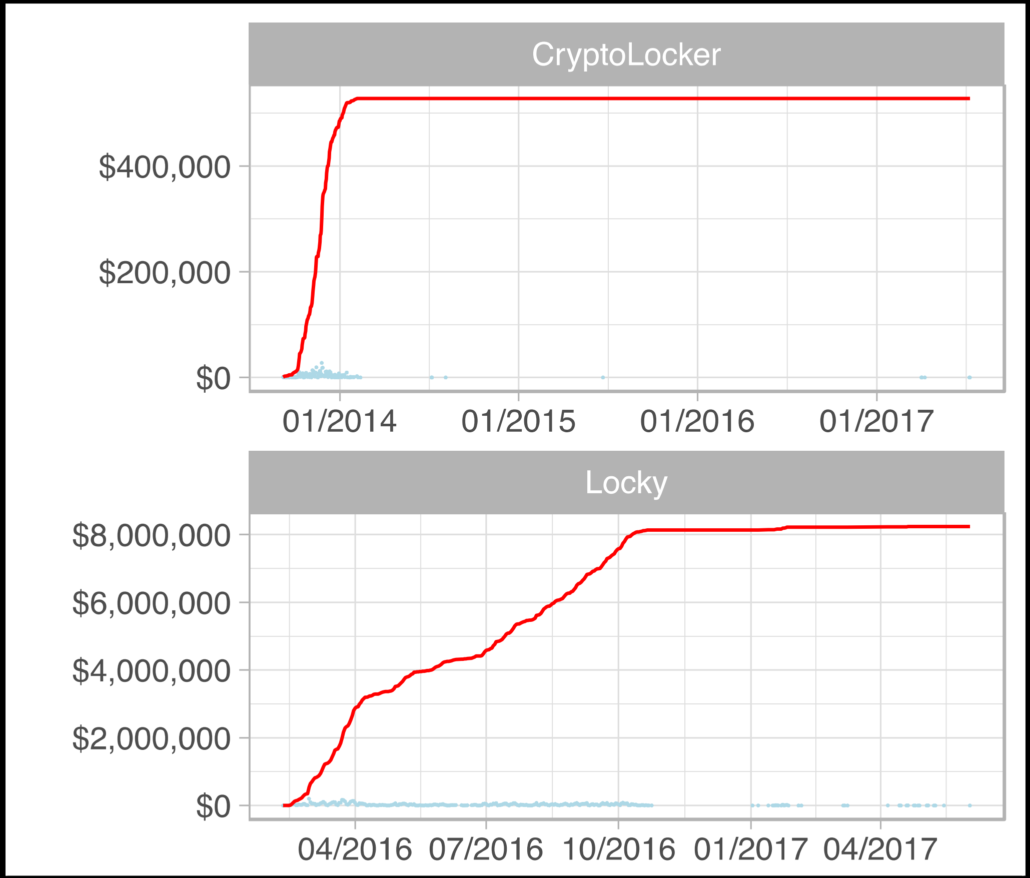
Collectors associated with large "clusters" (thousands of transactions) can be considered the end route of tracing ransomware payments

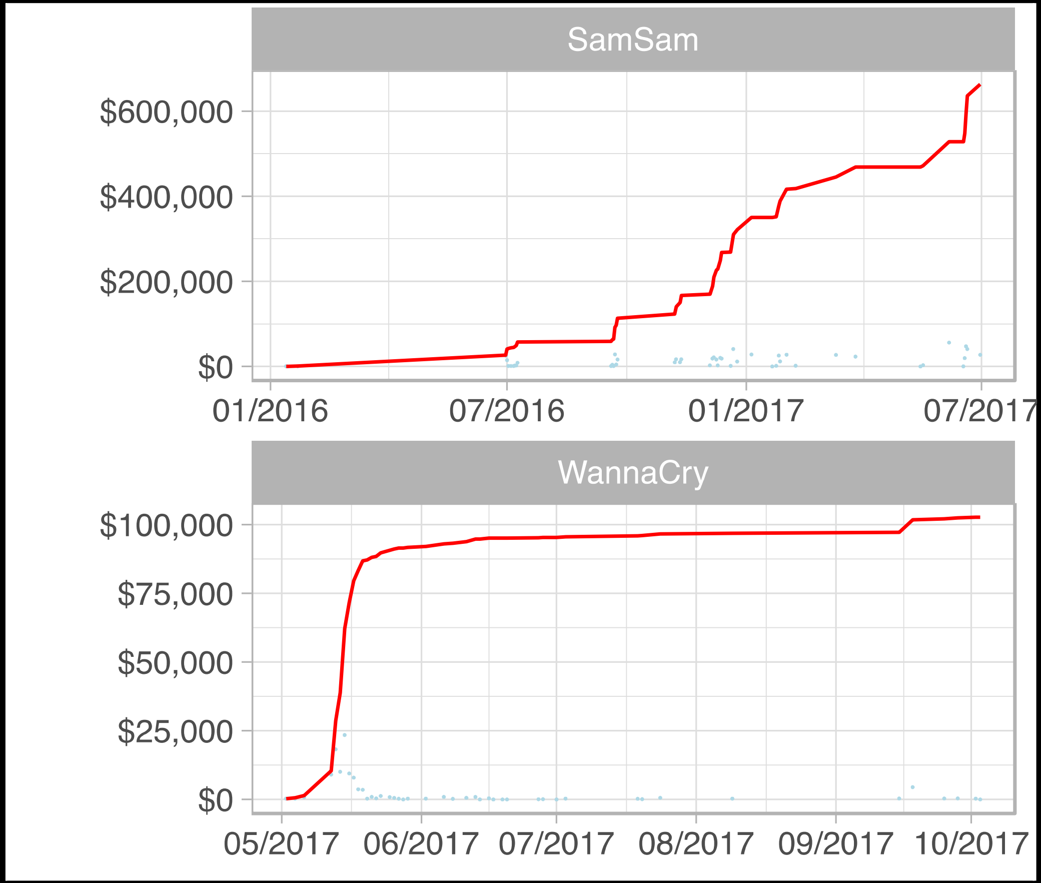
Investigation of tagged collector addresses:

- 86 exchange organizations (i.e. BTC-e.com, LocalBitcoin.com, Kraken.com)
- 47 gambling sites (i.e. SatoshiDice.com, Bitzillions.com, SatoshiMines.com)
- 12 mixing services (i.e. BitcoinFog.info, Helix Mixer)

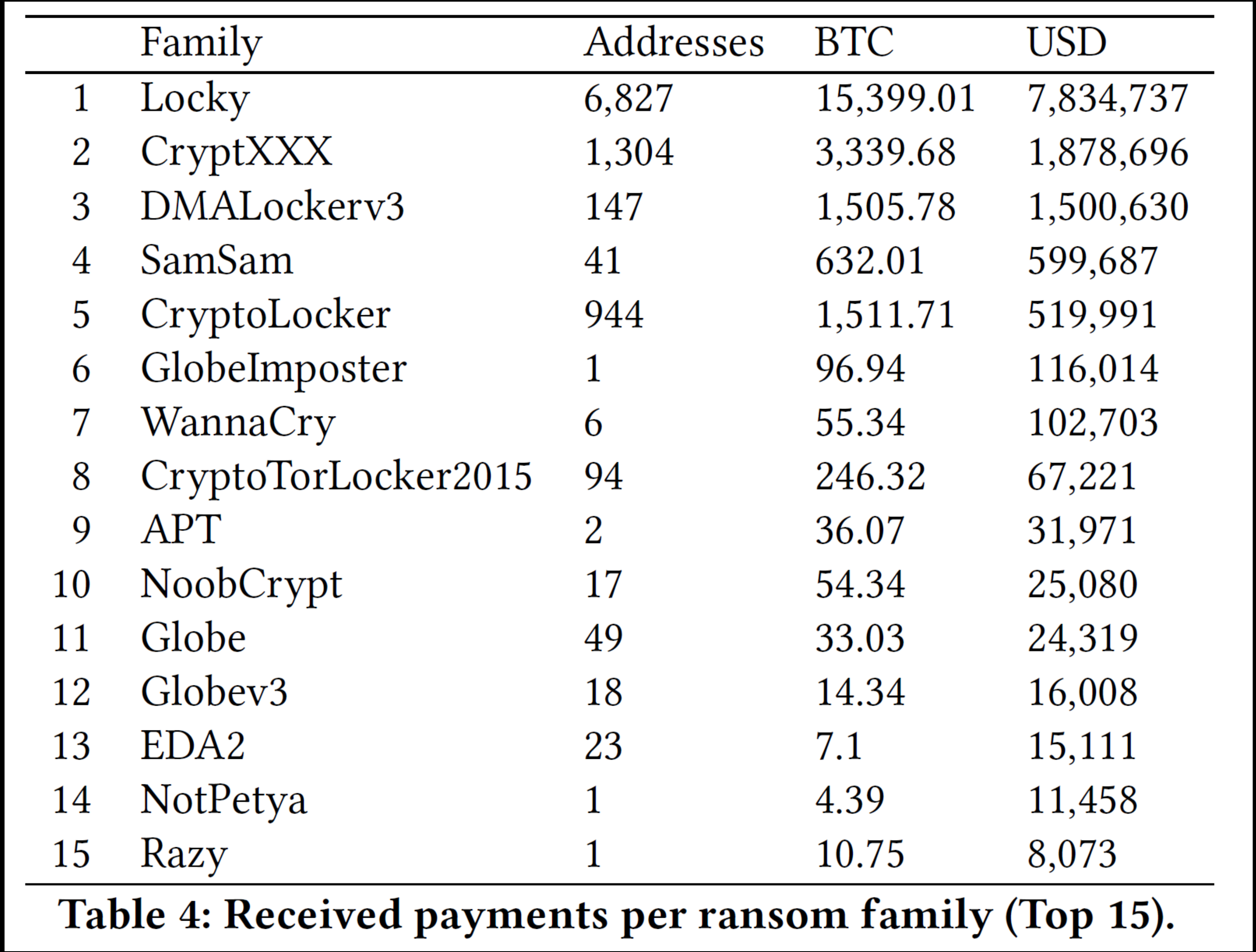
LOWER BOUND FINANCIAL IMPACTS

The Impacts of Ransomware





The Impacts of Ransomware



	Family	Addresses	BTC	USD
1	Locky	6,827	15,399.01	7,834,737
2	CryptXXX	1,304	3,339.68	1,878,696
3	DMALockerv3	147	1,505.78	1,500,630
4	SamSam	41	632.01	599,687
5	CryptoLocker	944	1,511.71	519,991
6	GlobeImposter	1	96.94	116,014
7	WannaCry	6	55.34	102,703
8	CryptoTorLocker2015	94	246.32	67,221
9	APT	2	36.07	31,971
10	NoobCrypt	17	54.34	25,080
11	Globe	49	33.03	24,319
12	Globev3	18	14.34	16,008
13	EDA2	23	7.1	15,111
14	NotPetya	1	4.39	11,458
15	Razy	1	10.75	8,073

Table 4: Received payments per ransom family (Top 15).

The Impact of Ransomware

From 2013 to mid-2017, the market for ransomware payments has a minimum worth of

USD 12,768,536 (22,967.54 BTC)

The Impact of Ransomware

The ransomware market is top-heavy

Locky, CryptXXX et DMALockerv3 make 86% of the market and the 32 other families share 12% of the market

Conclusion

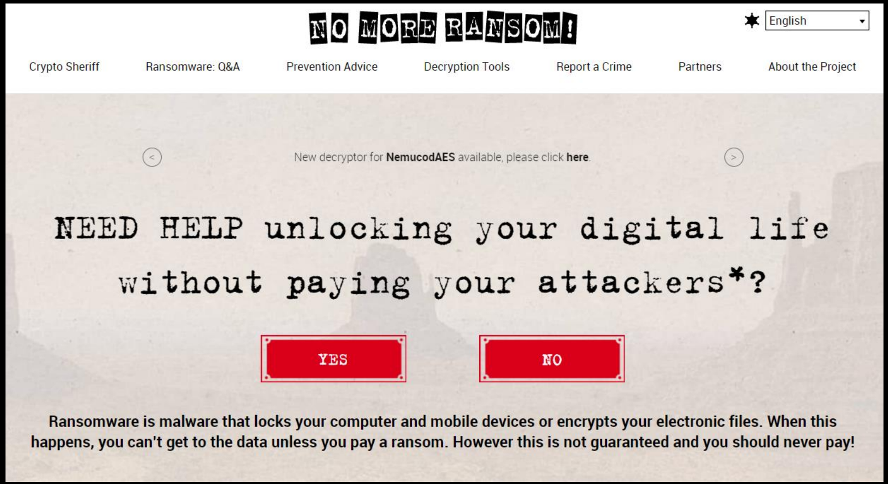
For law enforcement agencies: maybe mobilize resources on a small number of highly capable players ?

Discrepancy between total ransomware payments found and the damages caused by such attacks

- Market of US 12.7 million dollars
- Cryptowall damages estimated at US 325 million dollars (Cyber Threat Alliance, 2015)

Conclusion

- Initiative “No More Ransoms”
- Tools and solutions
- Only need a backup
- Many victims decide not to pay



New decryptor for **NemucodAES** available, please click **here**.

NEED HELP unlocking your digital life without paying your attackers*?

Ransomware is malware that locks your computer and mobile devices or encrypts your electronic files. When this happens, you can't get to the data unless you pay a ransom. However this is not guaranteed and you should never pay!

Future Work

- Extend our analysis to additional ransomware families
- Study other illicit activities channeling financial transactions through the bitcoin network, such as the trafficking of illicit goods or money laundering
- Hands-on workshop at NorthSec on tracing Bitcoin transactions

Summary

- Traced Bitcoin transactions related to ransomware
- Learnt about the open-source platform GraphSense
- Provided insights on ransomware market

Research Reproducibility

GraphSense cryptocurrency analytics platform

http://graphsense.info/

Ransomware seed and complete datasets

https://zenodo.org/record/1238041#.WumE2dNuZR4
https://github.com/behas/ransomware-dataset

Ransomware analytical strategy and code:

https://github.com/behas/ransomware-analytics

March 18 & 19, 2019

THANK YOU !

Masarah Paquet-Clouston
GoSecure Powered by CounterTack

@masarahclouston
Email: mcpc@gosecure.ca

BSides
Vancouver
2019