Tracking Ransomware End-to-end

Danny Y. Huang

Maxwell Matthaios Aliapoulios, Vector Guo Li
Luca Invernizzi, Elie Bursztein, Kylie McRoberts, Jonathan Levin
Kirill Levchenko, Alex C. Snoeren, Damon McCoy

PRINCETON UNIVERSITY UC San Diego NYU CHAINALYSIS Google

Ransomware causes financial damages

ars TECHNICA SIGN IN

RISK ASSESSMENT —

Two more healthcare networks caught up in outbreak of hospital ransomware

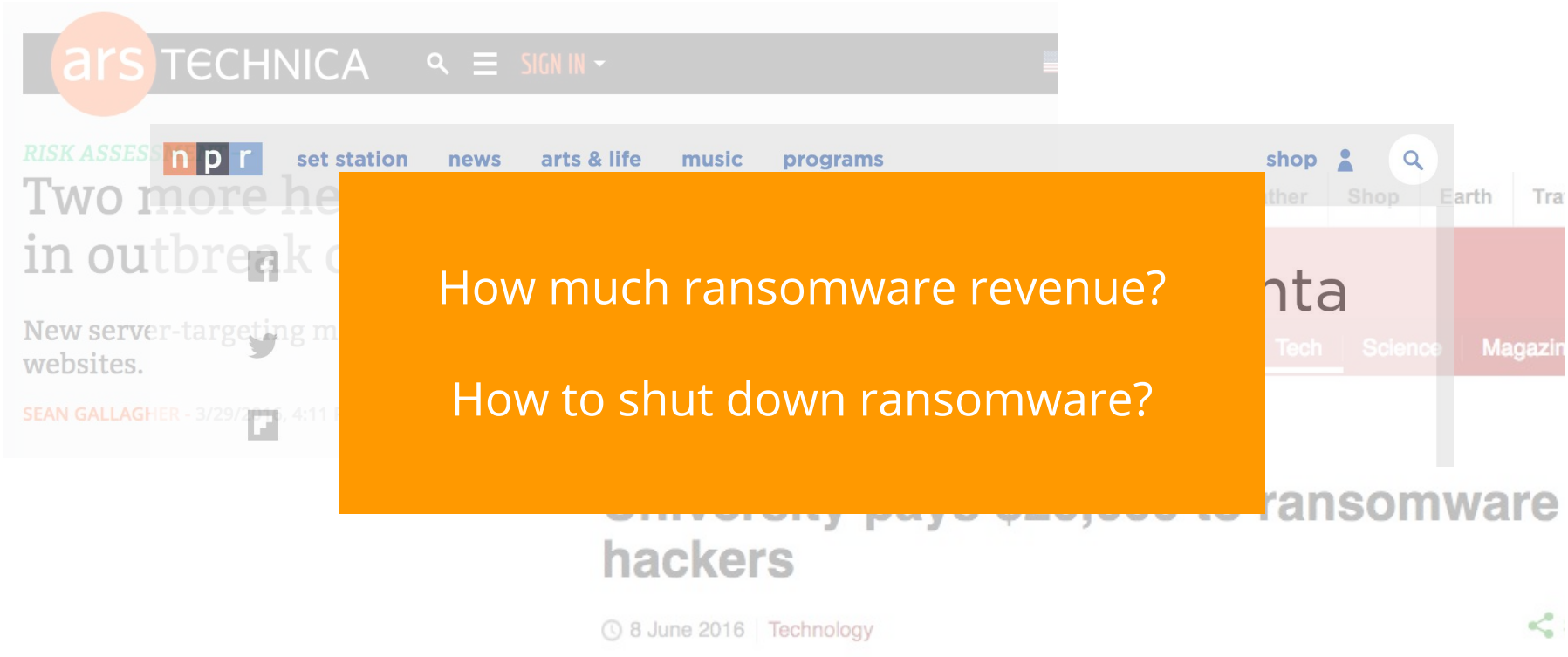
New server-targeting malware hitting healthcare targets with unpatched websites.

SEAN GALLAGHER - 3/29/2016, 4:11 PM

Ransomware causes financial damages

Ransomware causes financial damages

Ransomware causes financial damages



How much ransomware revenue?

How to shut down ransomware?

How typical ransomware works

1. Distribution

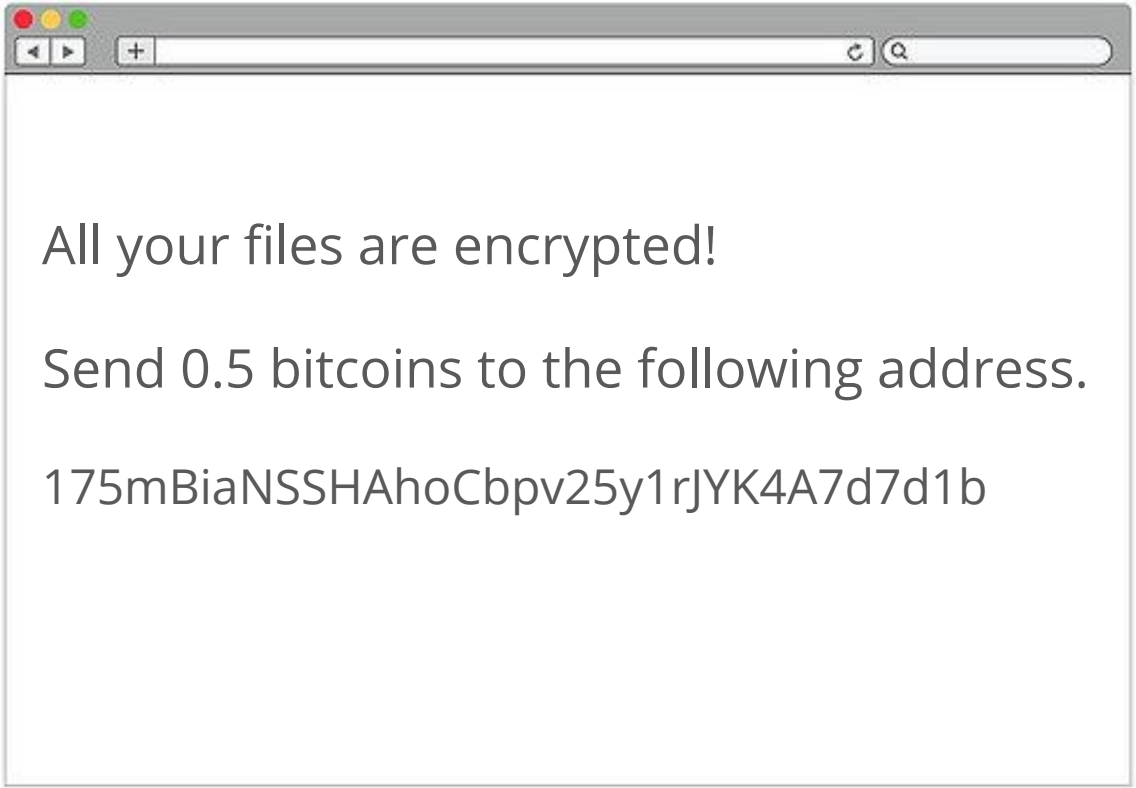
   Spam, compromised websites, etc

How typical ransomware works

1. Distribution
2. Infection

How typical ransomware works

1. Distribution
2. Infection

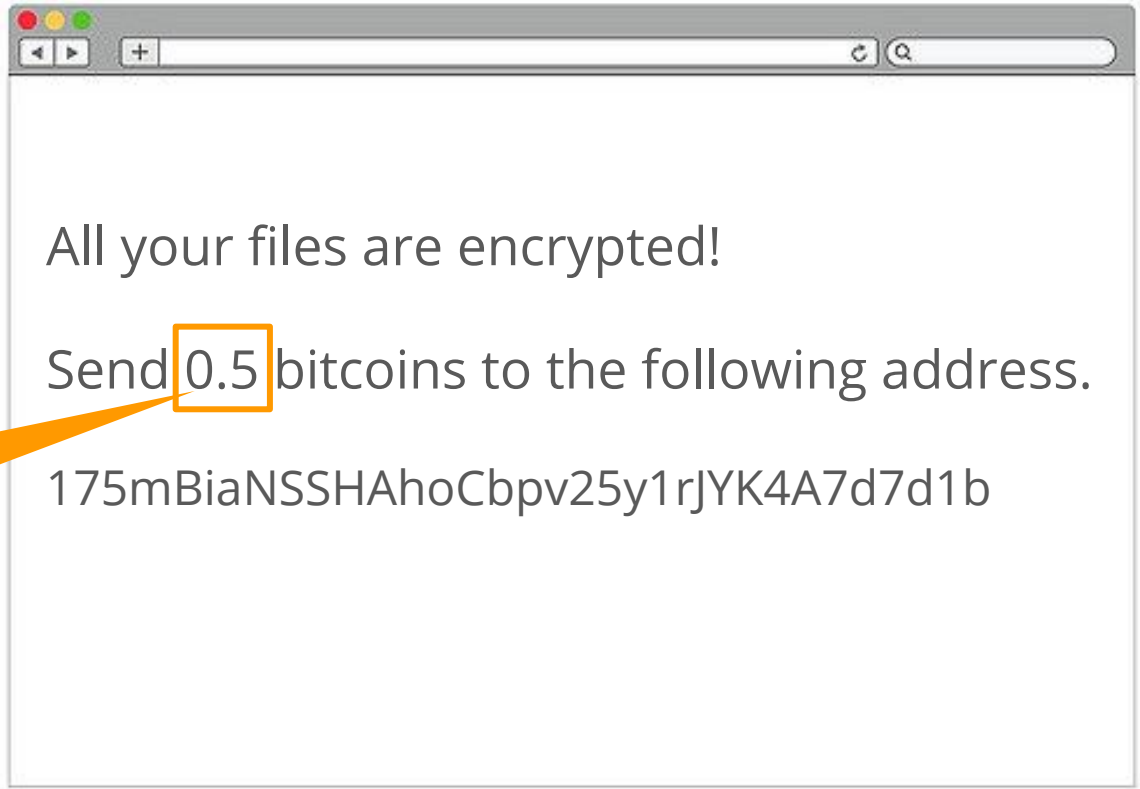


How typical ransomware works

1. Distribution
2. Infection

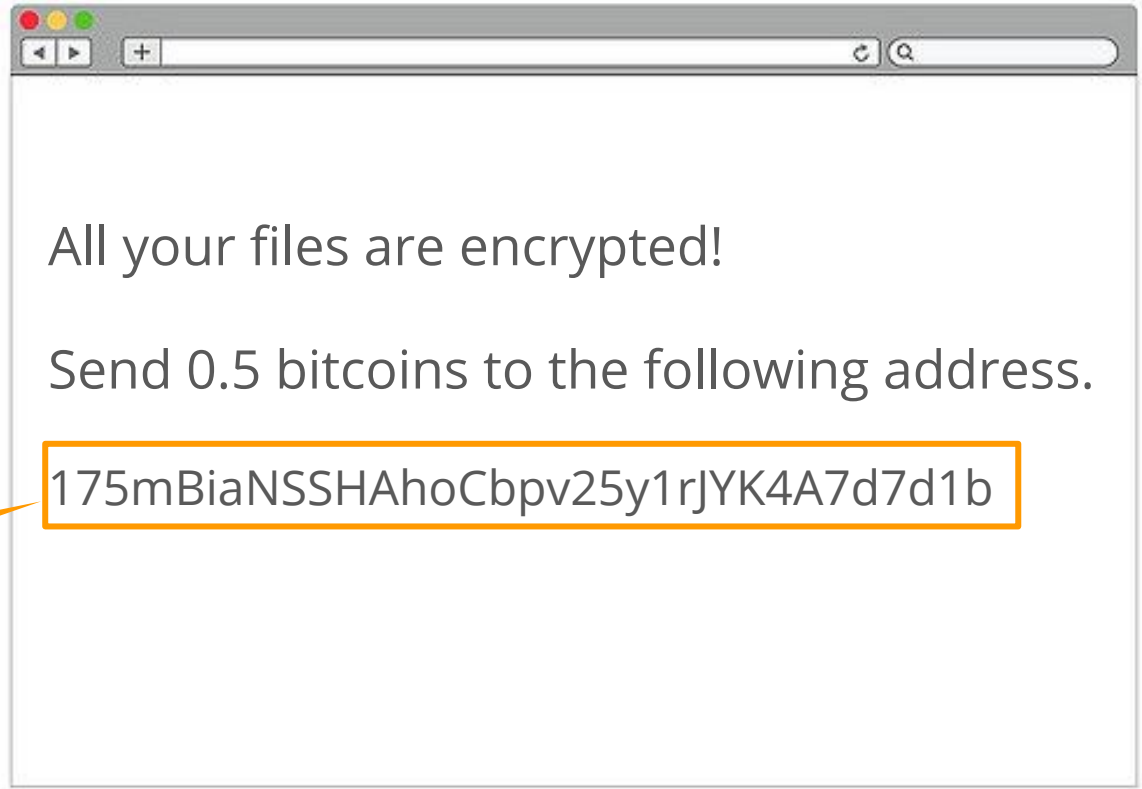
Cerber: median ~$1,000

Locky: median ~$1,800



How typical ransomware works

1. Distribution
2. Infection



How typical ransomware works

Victim’s money

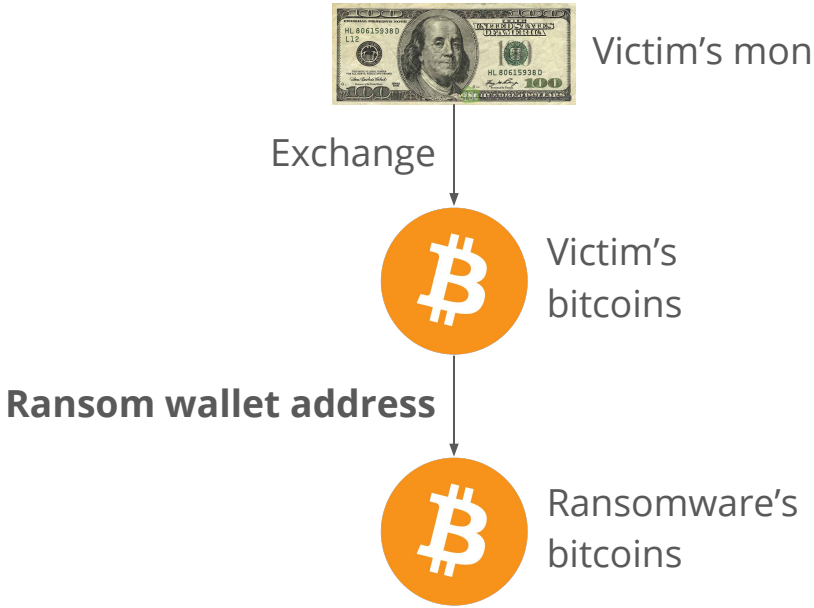
1. Distribution
2. Infection
3. Victim pays bitcoins

How typical ransomware works

1. Distribution
2. Infection
3. Victim pays bitcoins

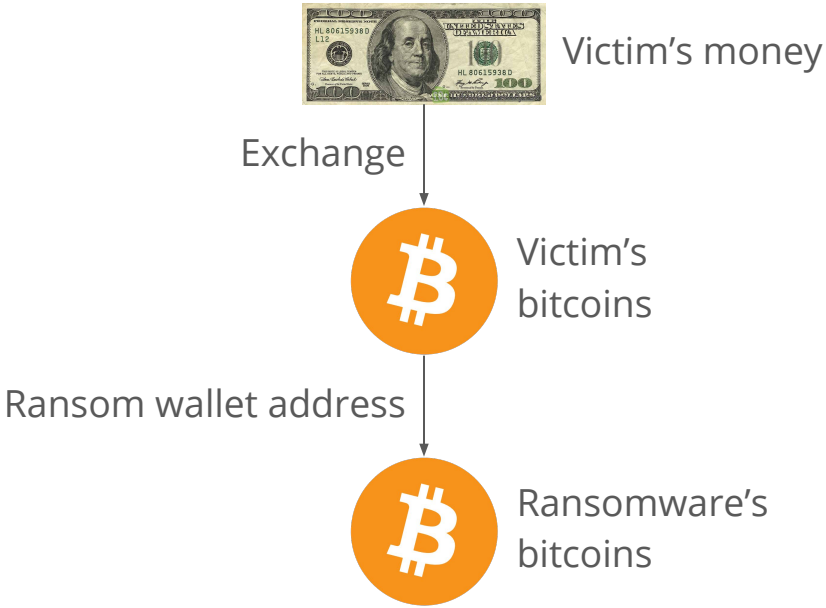
How typical ransomware works

1. Distribution
2. Infection
3. Victim pays bitcoins



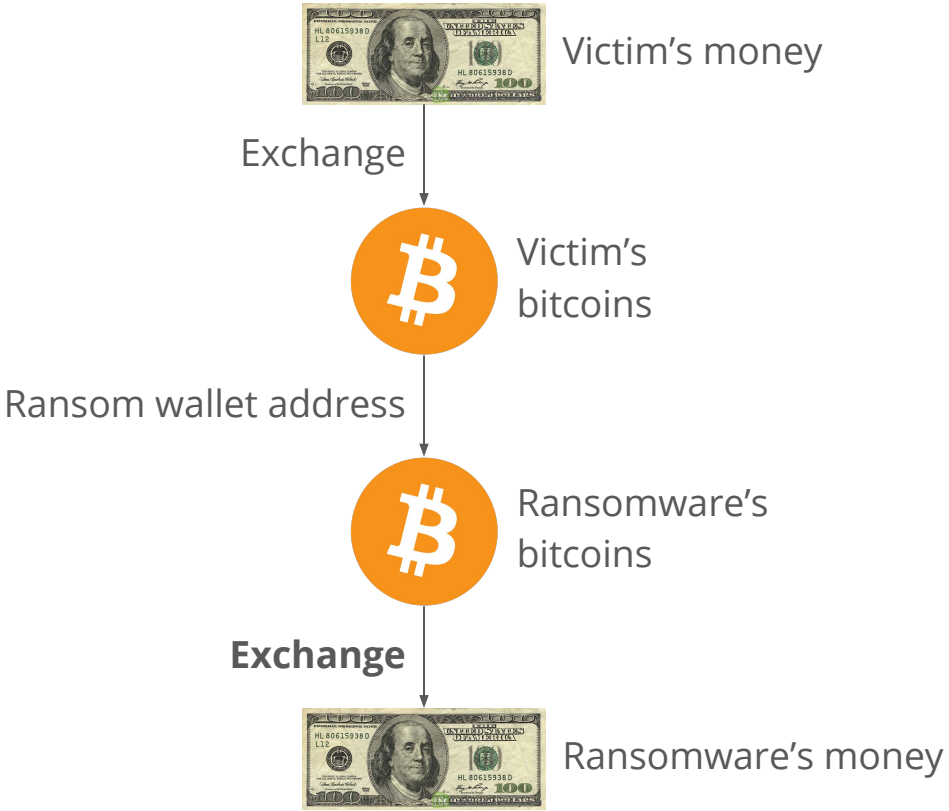
How typical ransomware works

1. Distribution
2. Infection
3. Victim pays bitcoins
4. Decryption



How typical ransomware works

1. Distribution
2. Infection
3. Victim pays bitcoins
4. Decryption
5. Criminal liquidates bitcoins



Research questions

How to estimate the total ransom paid (or revenue)?

Research questions

How to estimate the total ransom paid (or revenue)?

How to identify chokepoints?

Overview of results

How to estimate the total ransom paid (or revenue)?

- 10 families, ≥$16 million over two years; 90% made by two families

How to identify chokepoints?

Overview of results

How to estimate the total ransom paid (or revenue)?

- 10 families, ≥$16 million over two years; 90% made by two families

How to identify chokepoints?

- 40% revenue of one ransomware sent to BTC-e

Overview of results

How to estimate the total ransom paid (or revenue)?

- 10 families, ≥$16 million over two years; 90% made by two families

How to identify chokepoints?

- 40% revenue of one ransomware sent to BTC-e
- 3% affiliates of one ransomware caused 50% infections

Overview of results

How to estimate the total ransom paid (or revenue)?

- 10 families, ≥$16 million over two years; 90% made by two families

How to identify chokepoints?

- 40% revenue of one ransomware sent to BTC-e
- 3% affiliates of one ransomware caused 50% infections

1

Overview of results

How to estimate the total ransom paid (or revenue)?

- 10 families, ≥$16 million over two years; 90% made by two families

How to identify chokepoints?

- 40% revenue of one ransomware sent to BTC-e
- 3% affiliates of one ransomware caused 50% infections

1 Blockchain Analysis

Methodology: Follow the money

1. Identify known victims

Methodology: Follow the money

1. Identify known victims
2. Infer unknown victims

Methodology: Follow the money

1. Identify known victims
2. Infer unknown victims
3. Estimate total ransom

Methodology: Follow the money

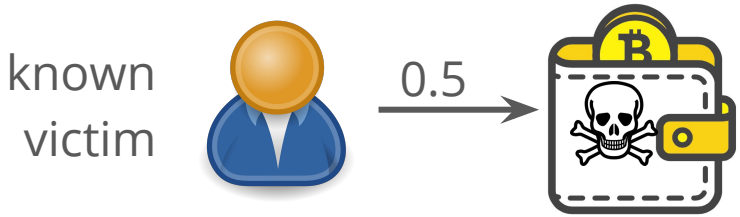
1. Identify known victims
2. Infer unknown victims
3. Estimate total ransom
4. Identify exchanges

Methodology: Follow the money

1. Identify known victims
2. Infer unknown victims
3. Estimate total ransom
4. Identify exchanges

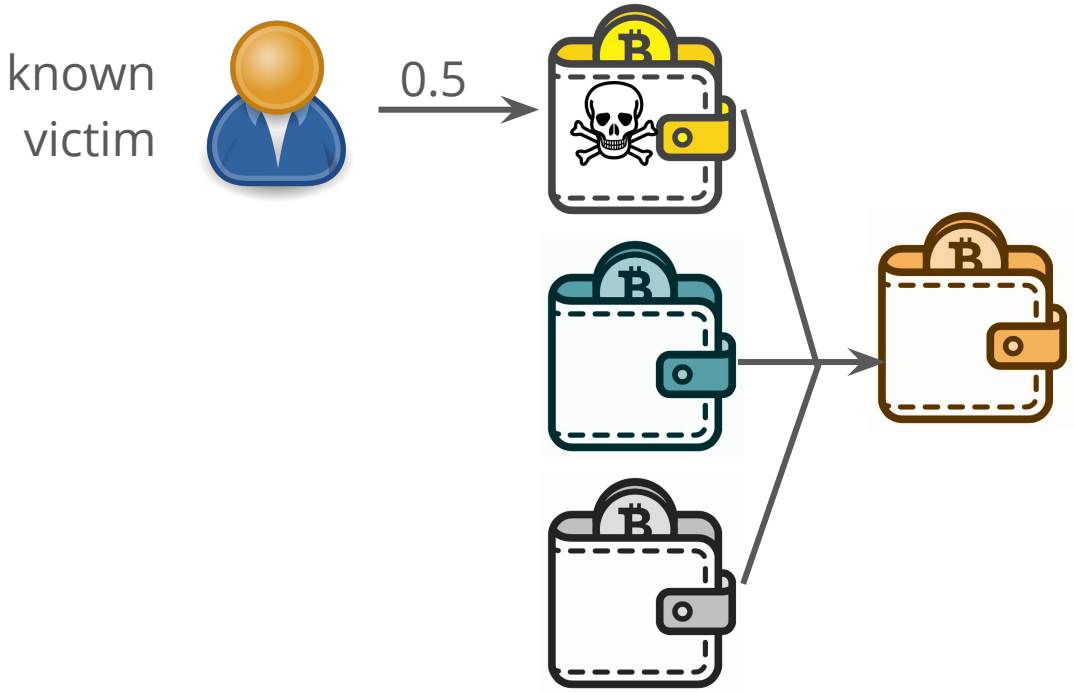
Methodology: Follow the money

1. Identify known victims
2. Infer unknown victims
3. Estimate total ransom
4. Identify exchanges



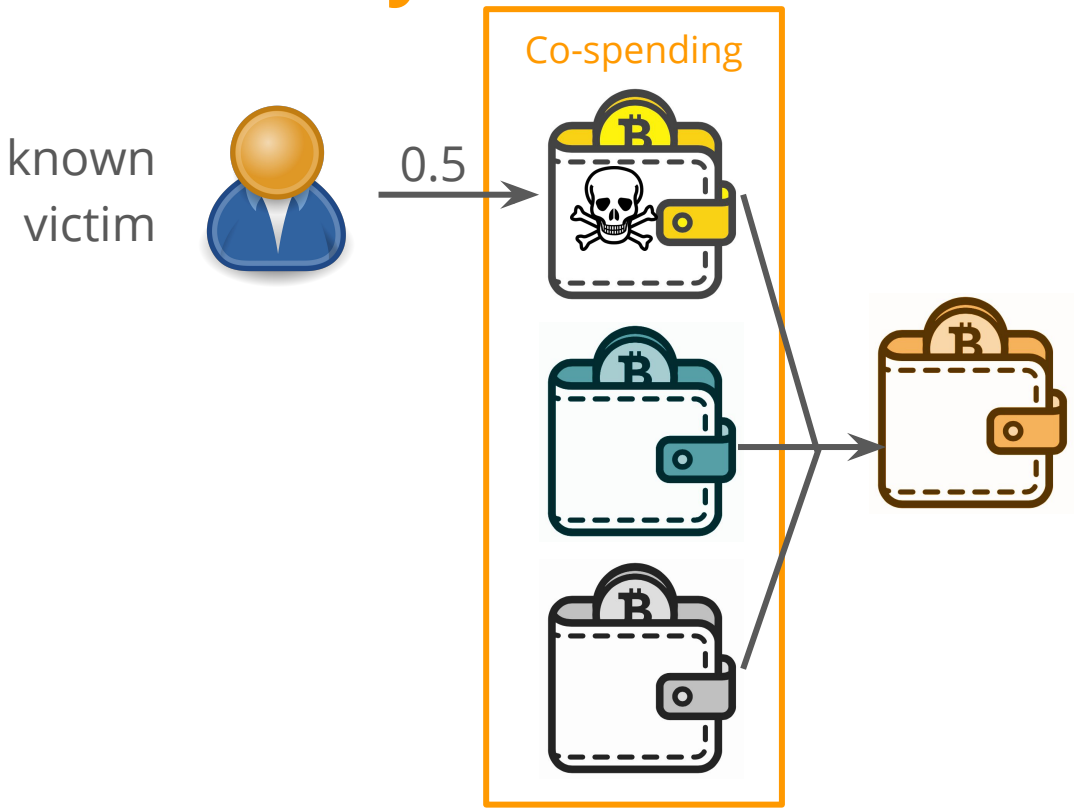
Methodology: Follow the money

1. Identify known victims
2. Infer unknown victims
3. Estimate total ransom
4. Identify exchanges



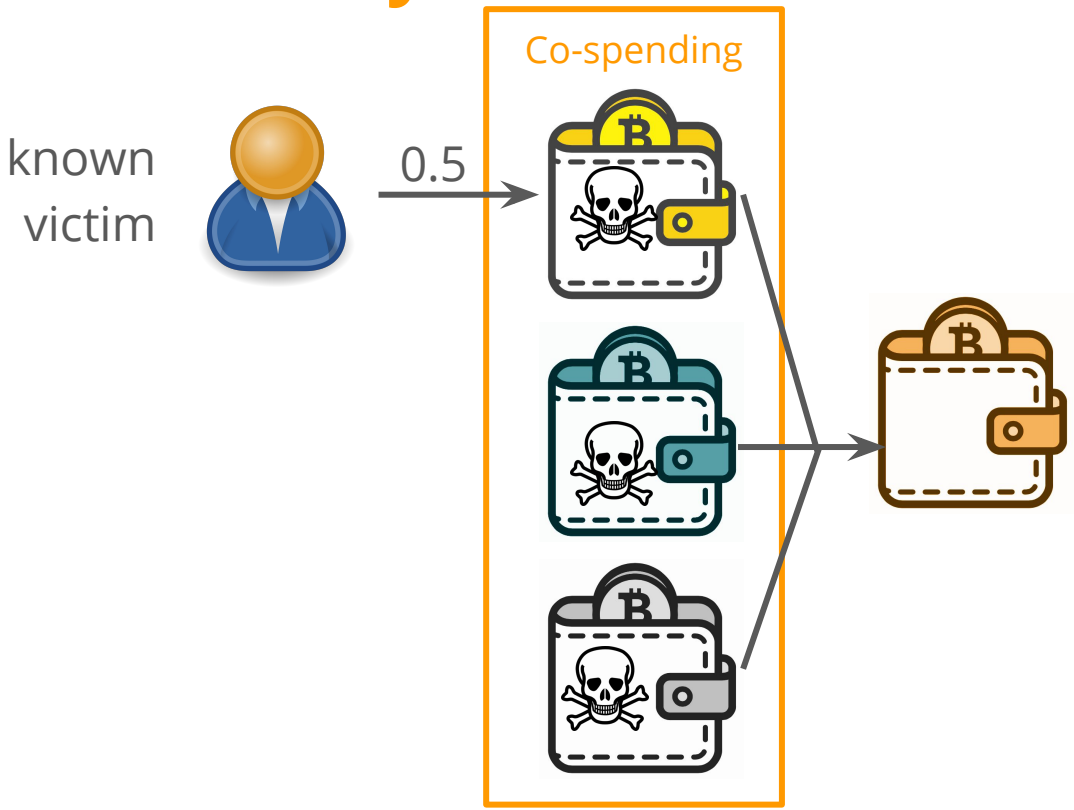
Methodology: Follow the money

1. Identify known victims
2. Infer unknown victims
3. Estimate total ransom
4. Identify exchanges



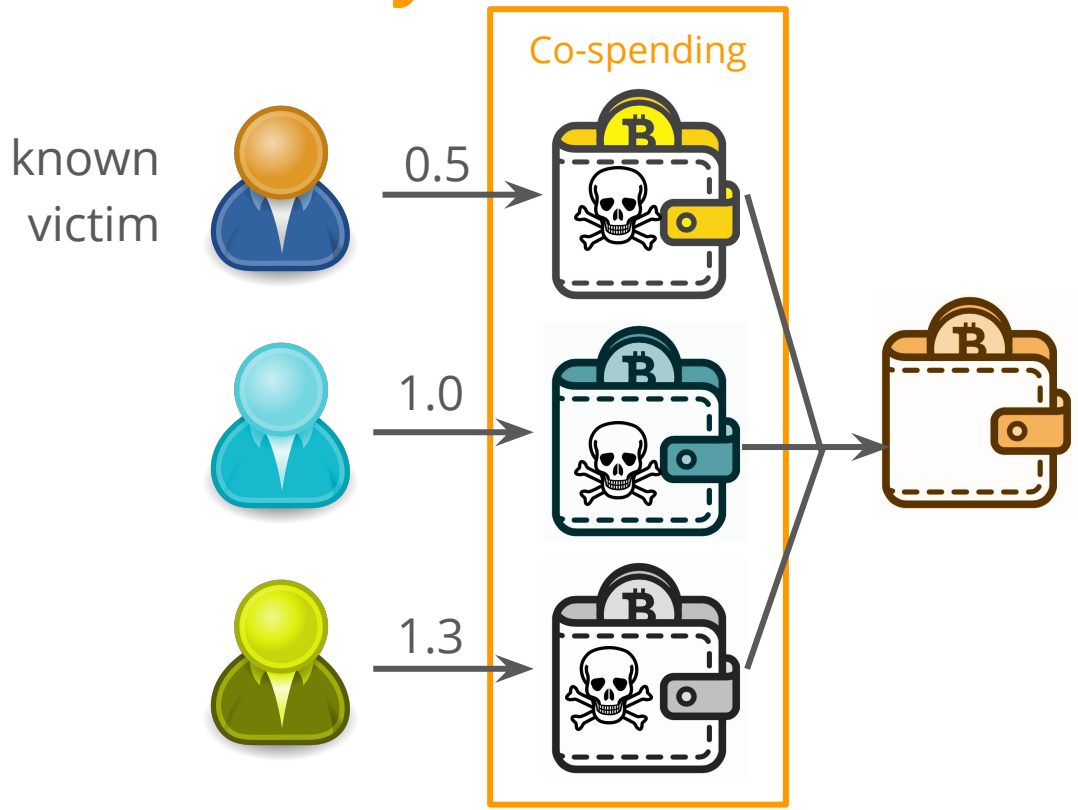
Methodology: Follow the money

1. Identify known victims
2. Infer unknown victims
3. Estimate total ransom
4. Identify exchanges



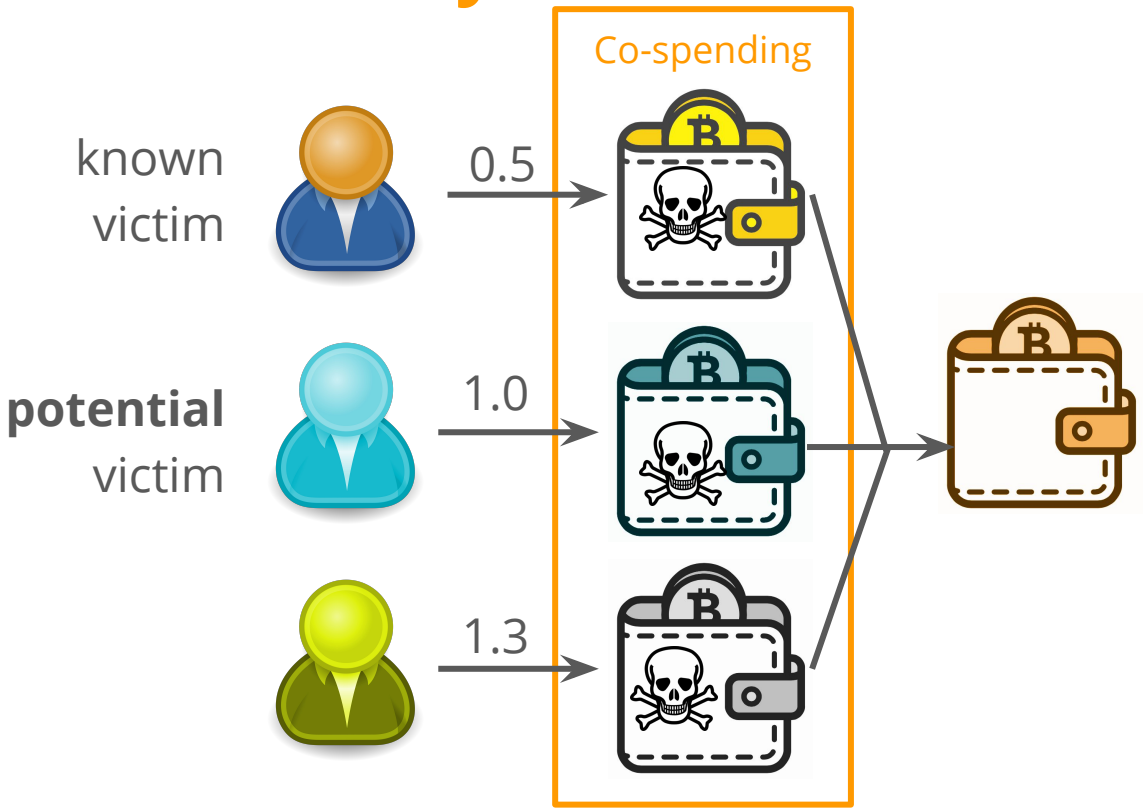
Methodology: Follow the money

1. Identify known victims
2. Infer unknown victims
3. Estimate total ransom
4. Identify exchanges



Methodology: Follow the money

1. Identify known victims
2. Infer unknown victims
3. Estimate total ransom
4. Identify exchanges



Methodology: Follow the money

1. Identify known victims
2. Infer unknown victims
3. Estimate total ransom
4. Identify exchanges

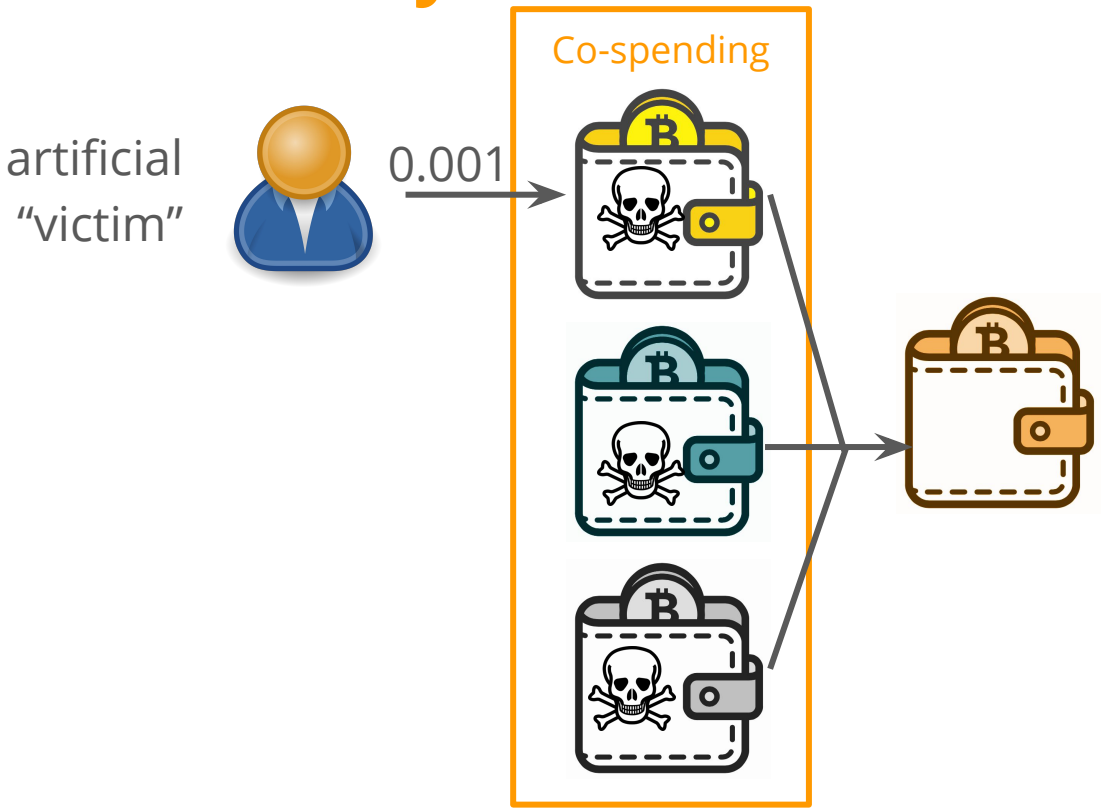
artificial "victim"

Methodology: Follow the money

1. Identify known victims
2. Infer unknown victims
3. Estimate total ransom
4. Identify exchanges

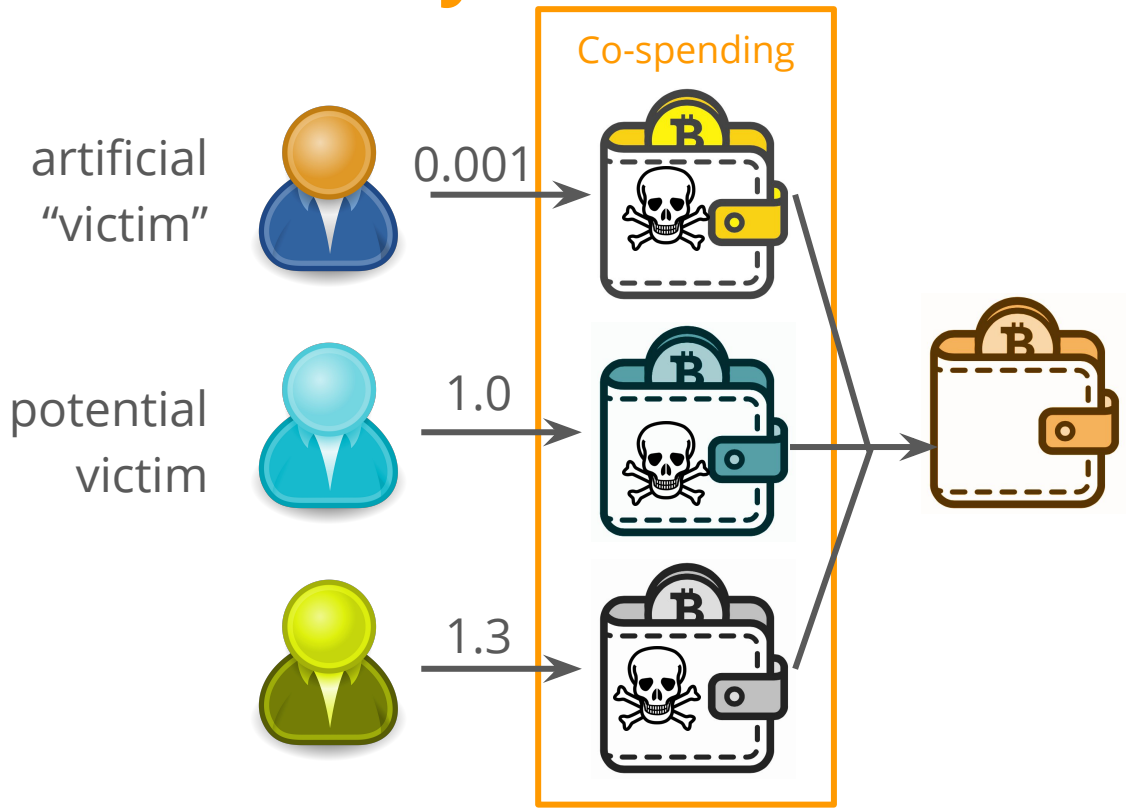
Methodology: Follow the money

1. Identify known victims
2. Infer unknown victims
3. Estimate total ransom
4. Identify exchanges

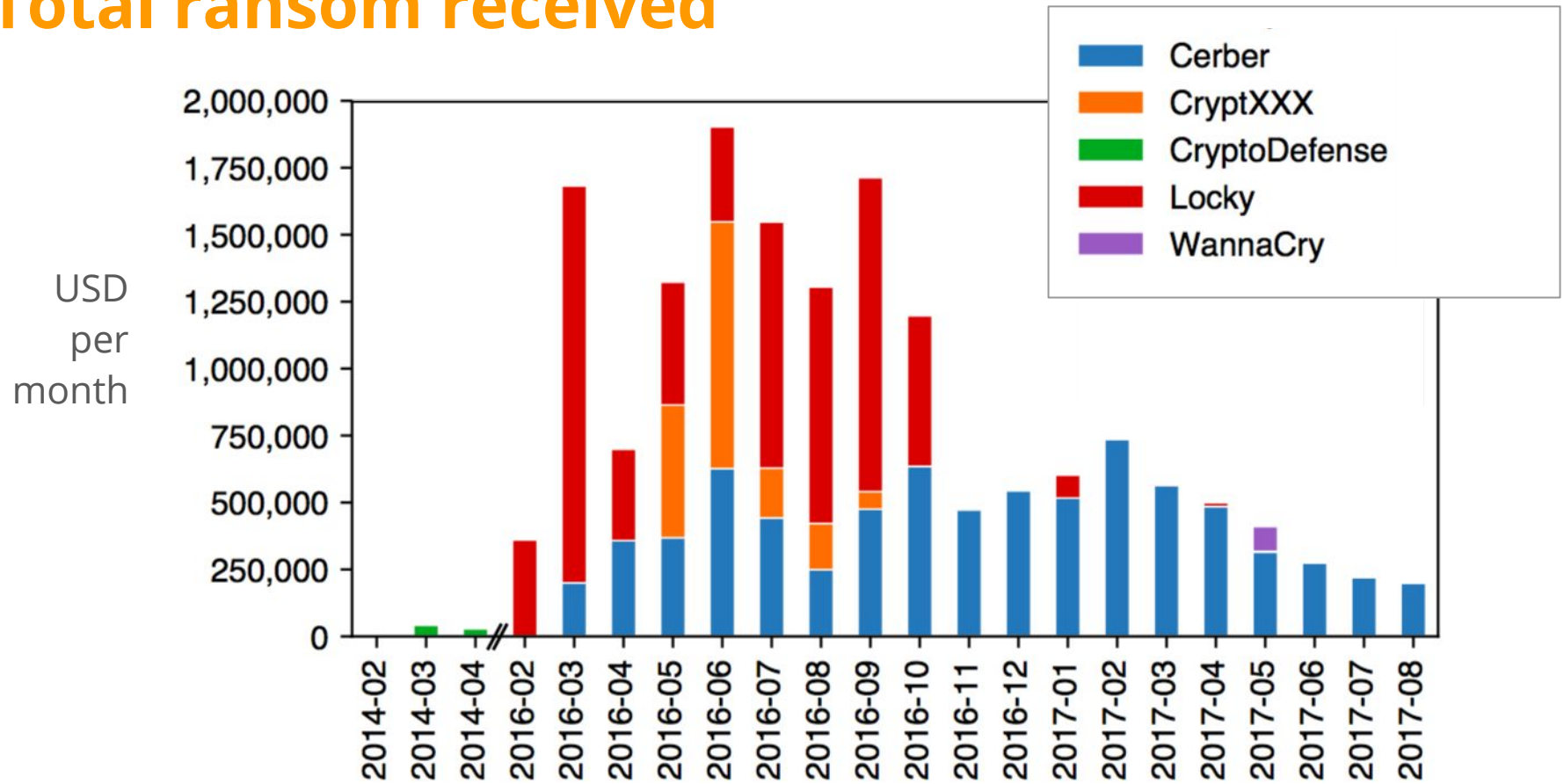


Methodology: Follow the money

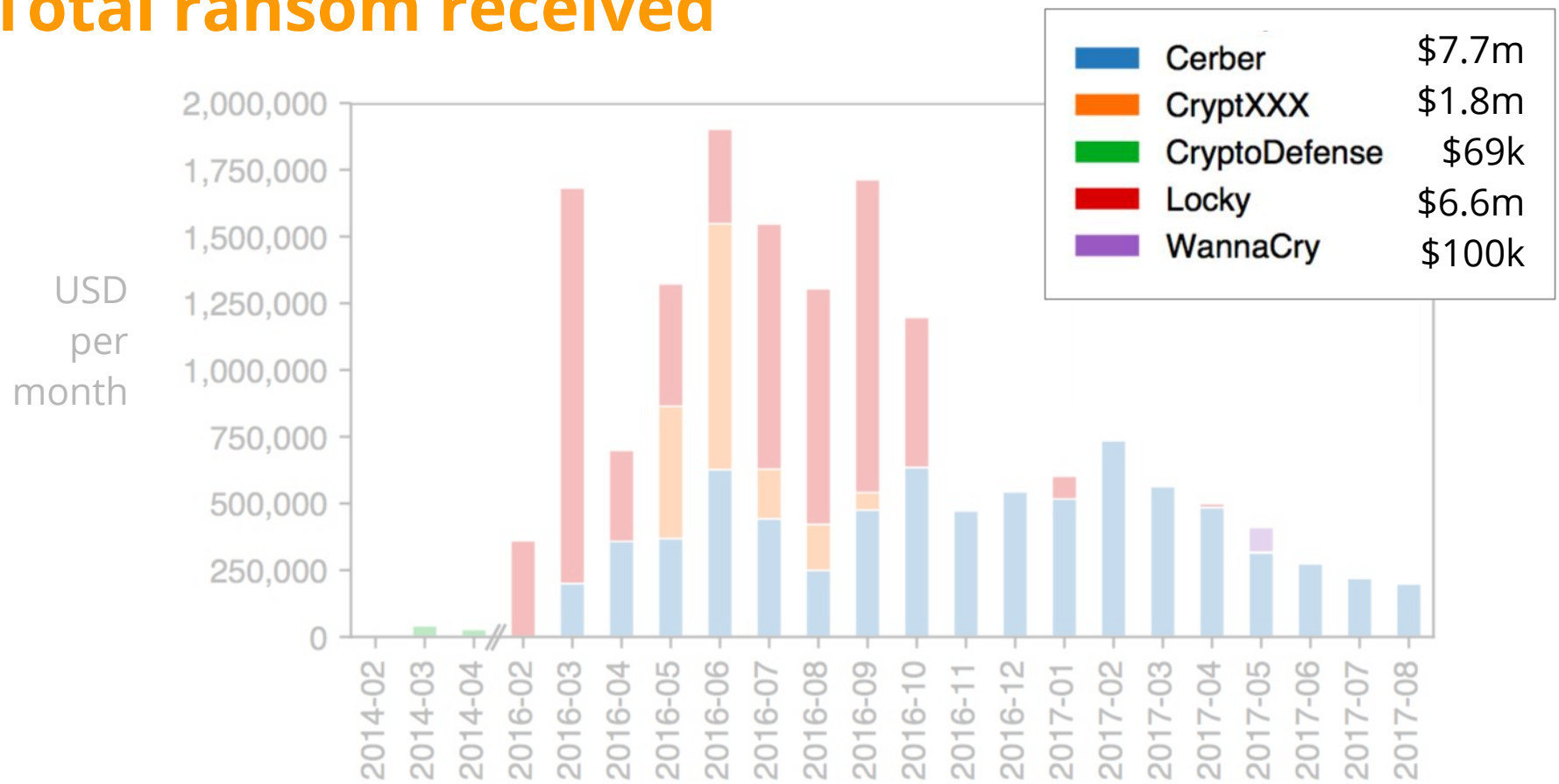
1. Identify known victims
2. Infer unknown victims
3. Estimate total ransom
4. Identify exchanges



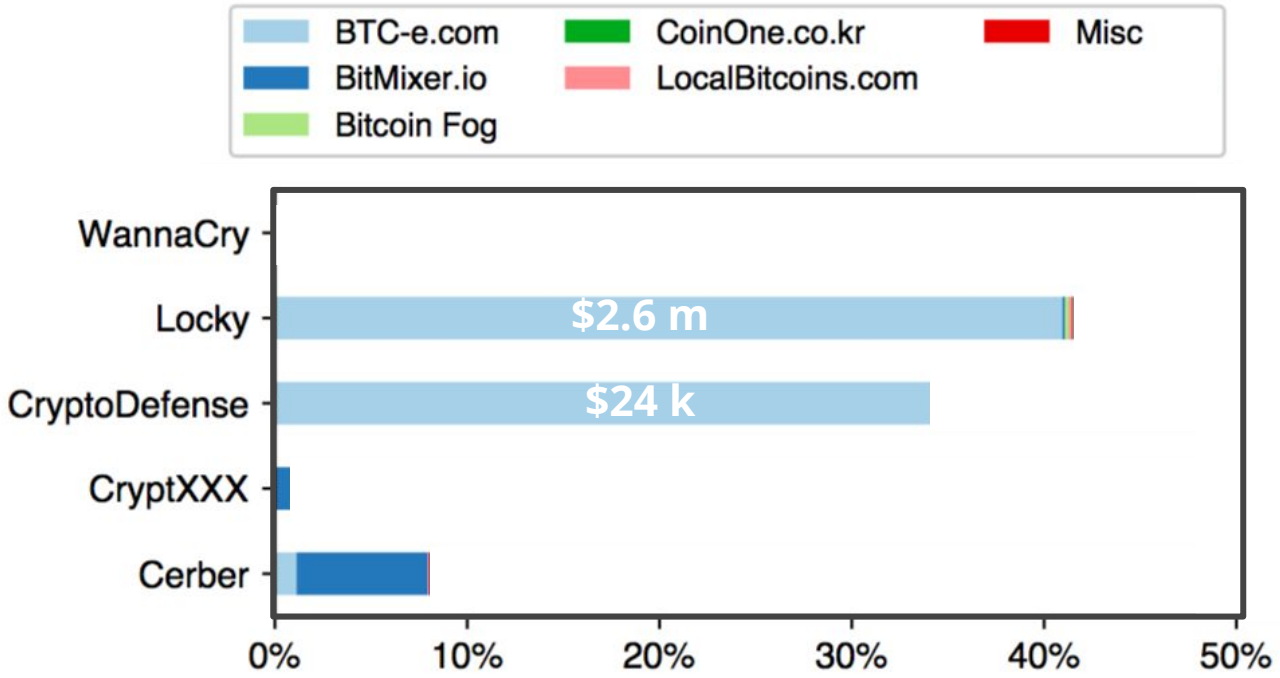
Total ransom received



Total ransom received



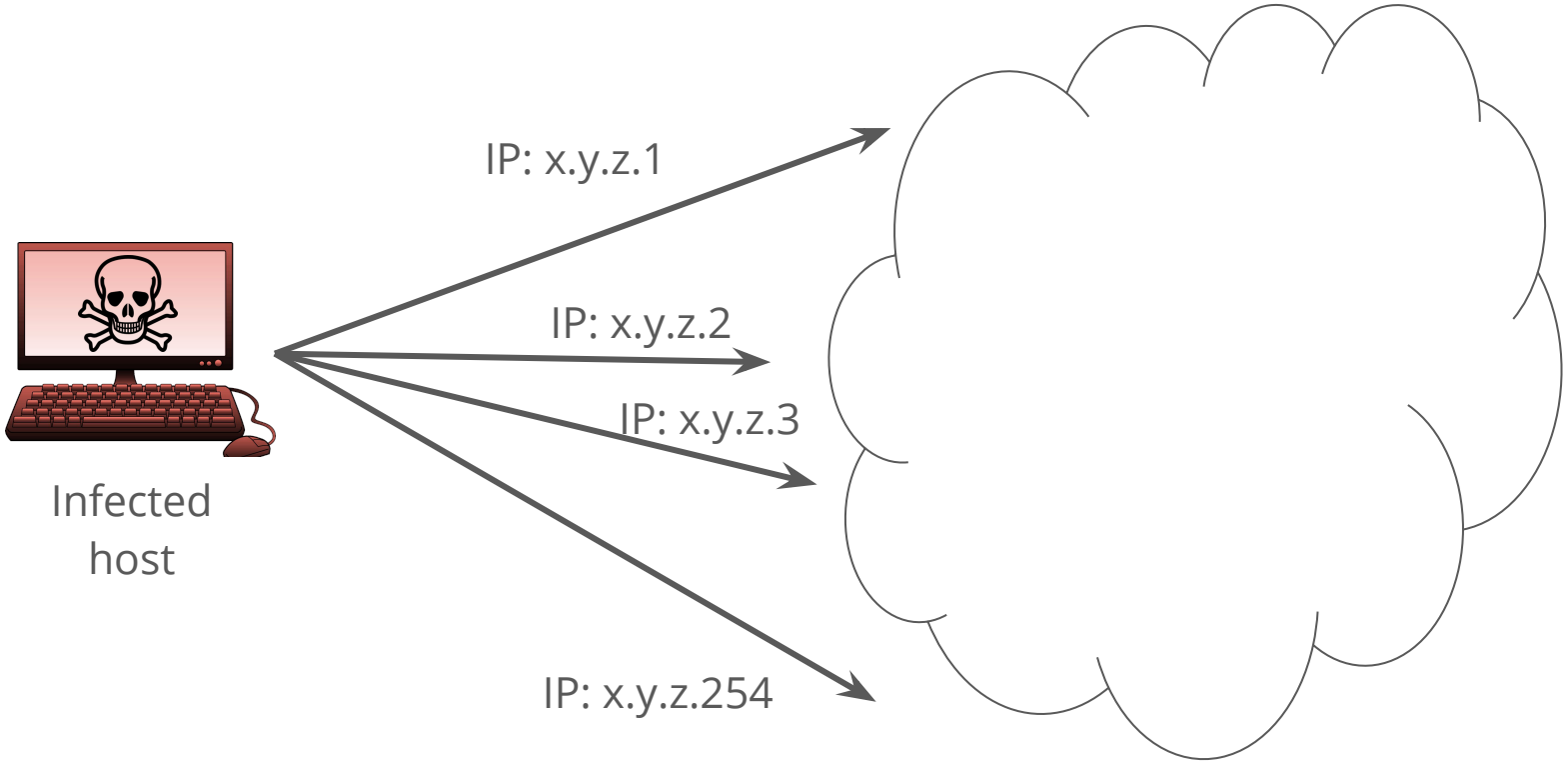
Potential liquidation at exchanges



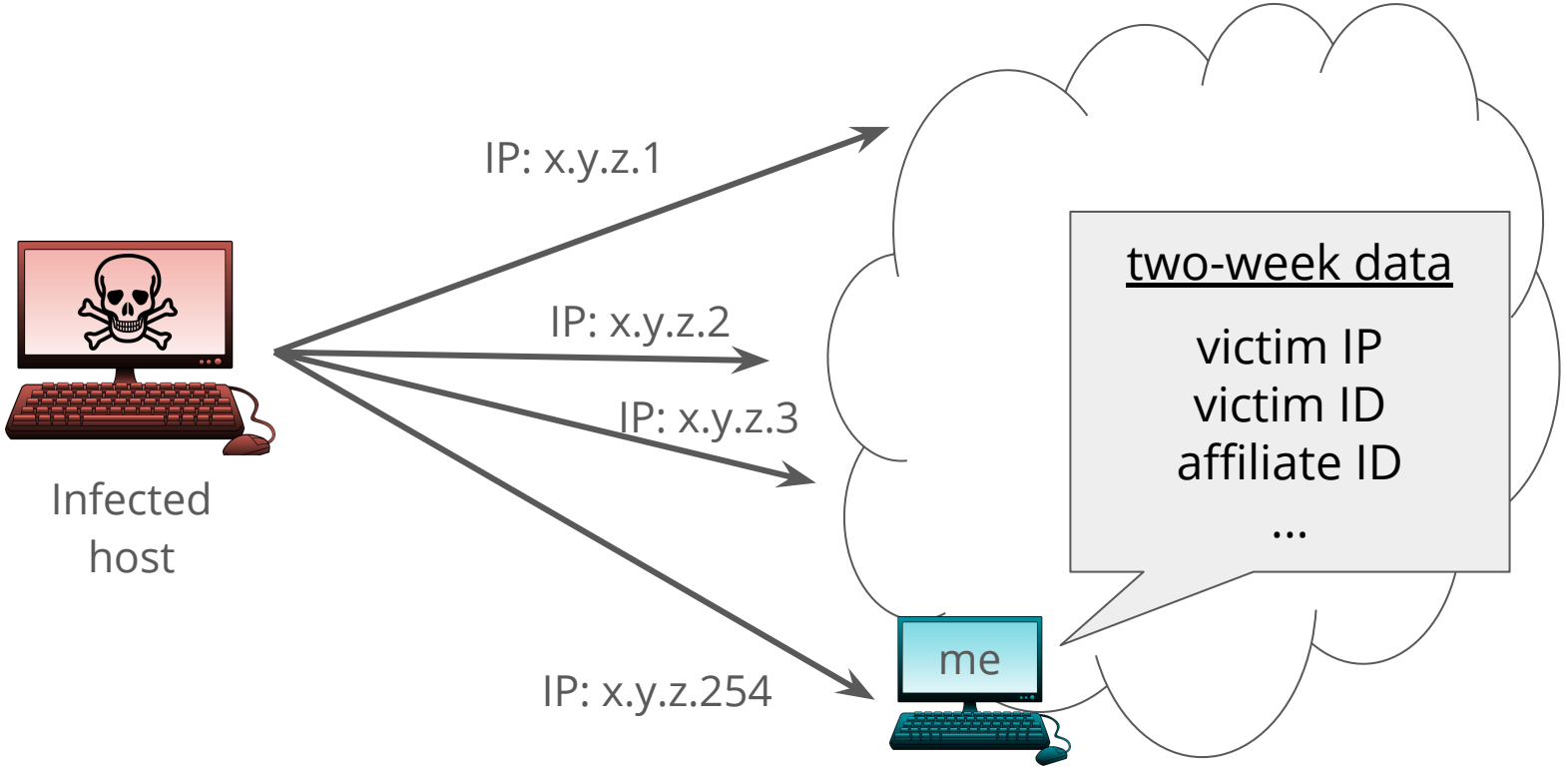
Fraction of revenue sent to exchanges

2 Reverse Engineering Cerber's C&C

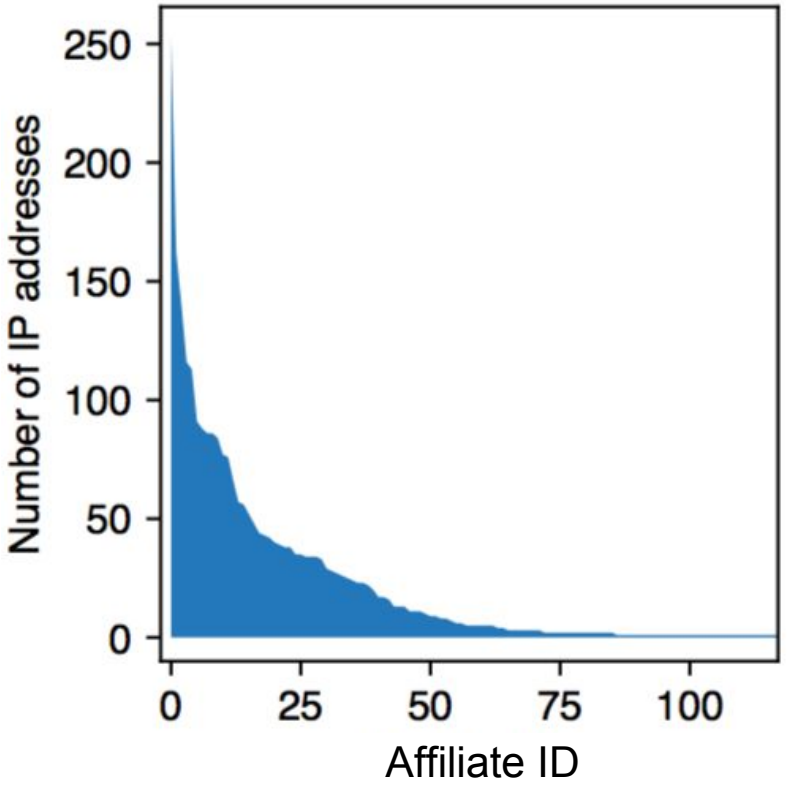
Cerber’s outbound UDP traffic



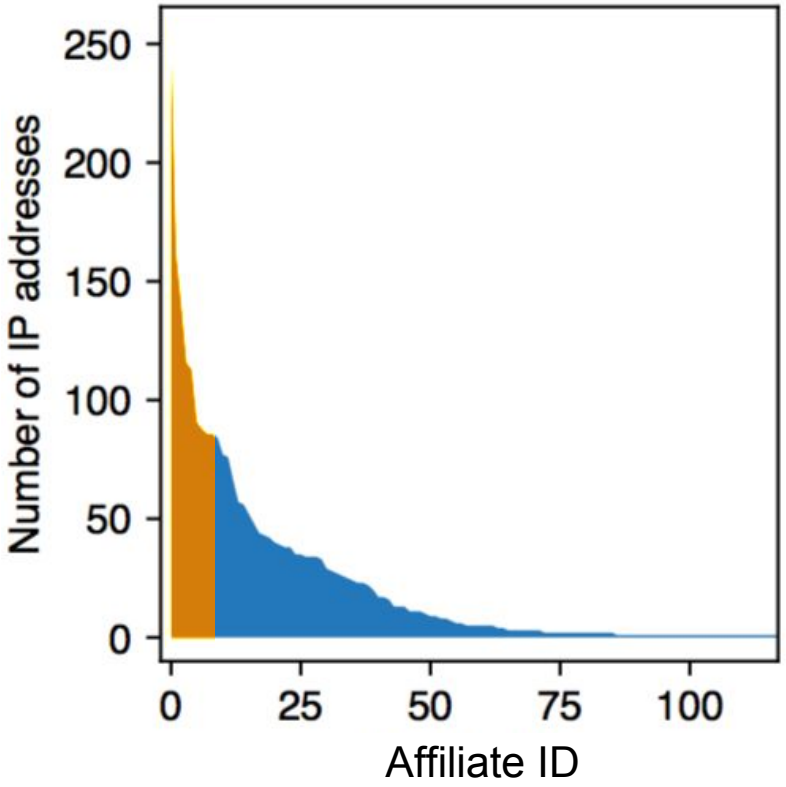
Cerber's outbound UDP traffic



Number of infected IP addr per affiliate



3% of affiliates caused 50% of infected IPs



3 Summary

Summary

Key Methods

Tracked ransom payments for 10 ransomware families using co-spending wallet addr

Summary

Key Methods

Tracked ransom payments for 10 ransomware families using co-spending wallet addr

Reverse engineered C&C protocol for Cerber ransomware

Summary

Key Methods

Tracked ransom payments for 10 ransomware families using co-spending wallet addr

Reverse engineered C&C protocol for Cerber ransomware

Key Results

Estimated revenue:
10 families, ≥$16 million over two years

Summary

Key Methods

Tracked ransom payments for 10 ransomware families using co-spending wallet addr

Reverse engineered C&C protocol for Cerber ransomware

Key Results

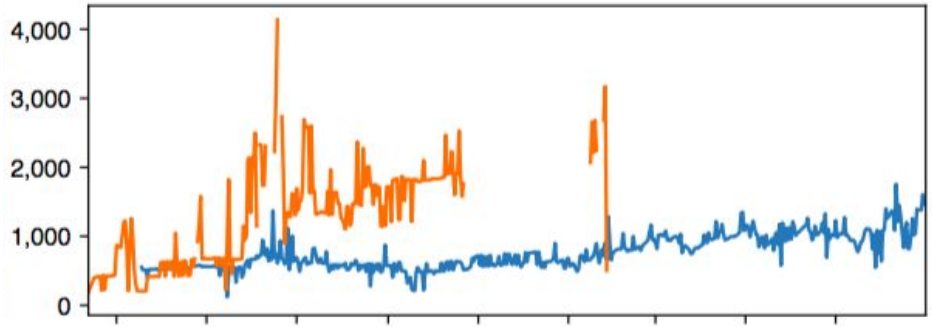
Estimated revenue:
10 families, ≥$16 million over two years

Possible chokepoints:
exchanges and affiliates

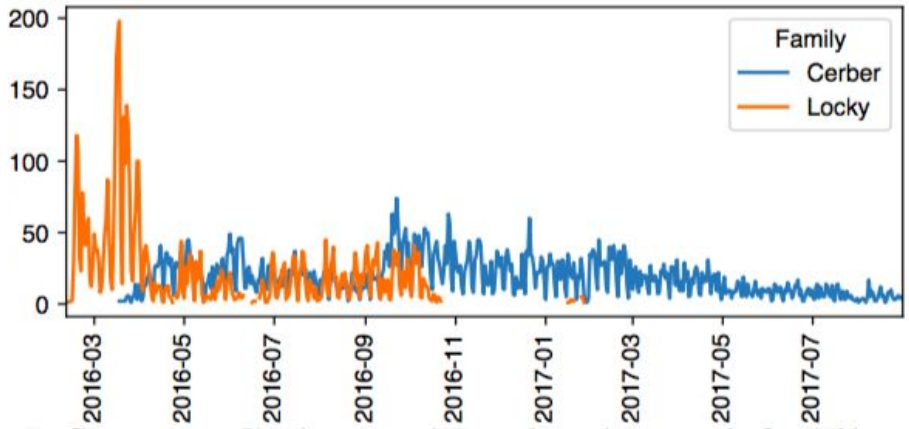
4 Appendix

Ransom payments over time

Median ransom amount per day (USD)



Number of payments per day



Potentially missing Locky's ransom payments

Google results
binaries found
bitcoin payment