

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



UC San Diego



NYU



CHAINALYSIS



Ransomware causes financial damages



The image is a screenshot of an Ars Technica article. At the top is a black navigation bar with the 'ars TECHNICA' logo on the left, a search icon, a menu icon, and a 'SIGN IN' link with a dropdown arrow on the right. Below the navigation bar, the article is categorized under 'RISK ASSESSMENT' in green text. The main headline reads 'Two more healthcare networks caught up in outbreak of hospital ransomware'. Below the headline is a sub-headline: 'New server-targeting malware hitting healthcare targets with unpatched websites.' At the bottom left of the article preview, the author 'SEAN GALLAGHER' is listed with the date and time '3/29/2016, 4:11 PM'.

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

ars TECHNICA 🔍 ≡ SIGN IN ▾

RISK ASSESSMENT —

Two more healthcare networks hit by ransomware in outbreak of hospital attacks

New server-targeting malware hitting healthcare websites.

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

BBC Sign in News Sport Weather Shop Earth Tra

NEWS

Home Video World US & Canada UK Business Tech Science Magazine

Technology

University pays \$20,000 to ransomware hackers

🕒 8 June 2016 | Technology



Ransomware causes financial damages

The image is a screenshot of a web browser displaying an NPR news article. At the top, there is a navigation bar with the 'ars TECHNICA' logo on the left, a search icon, a menu icon, and a 'SIGN IN' link. Below this is another navigation bar with the 'npr' logo and links for 'set station', 'news', 'arts & life', 'music', 'programs', 'shop', and a user profile icon. The main content area features the word 'AMERICA' in a small font, followed by a large headline: 'Time Is Running Out For Atlanta In Ransomware Attack'. To the left of the headline are social media sharing icons for Facebook, Twitter, and Email. Below the headline is the date and time: 'March 28, 2018 · 6:14 PM ET'. At the bottom of the article preview, there is a sub-headline: 'University pays \$20,000 to ransomware hackers' and a timestamp '8 June 2016' followed by the category 'Technology'. On the right side of the page, there is a vertical sidebar with a red box labeled 'Magazin' and some partially visible text 'earth' and 'Tra'.

ars TECHNICA

RISK ASSES

Two r
in ou

New serve
websites.

SEAN GALLAGH

npr

set station news arts & life music programs

shop

AMERICA

Time Is Running Out For Atlanta
In Ransomware Attack

March 28, 2018 · 6:14 PM ET

University pays \$20,000 to ransomware
hackers

8 June 2016 | Technology

earth Tra

Magazin

Ransomware causes financial damages

ars TECHNICA

RISK ASSESS

n p r

set station news arts & life music programs

shop

Two more he
in outbreak

New server-targeting m
websites.

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

How much ransomware revenue?

How to shut down ransomware?

University pays \$20,000 to ransomware
hackers

8 June 2016 | Technology

How typical ransomware works

1. Distribution

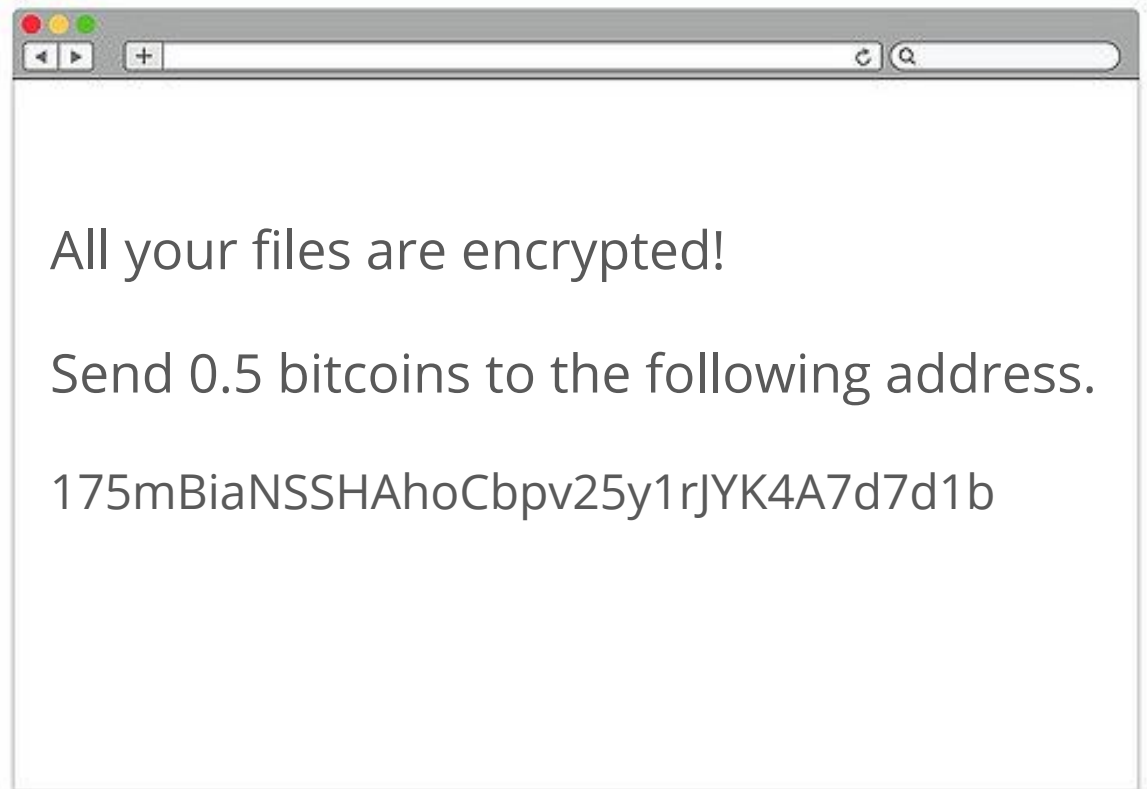
Spam, compromised websites, etc

How typical ransomware works

1. Distribution
2. Infection

How typical ransomware works

1. Distribution
2. Infection

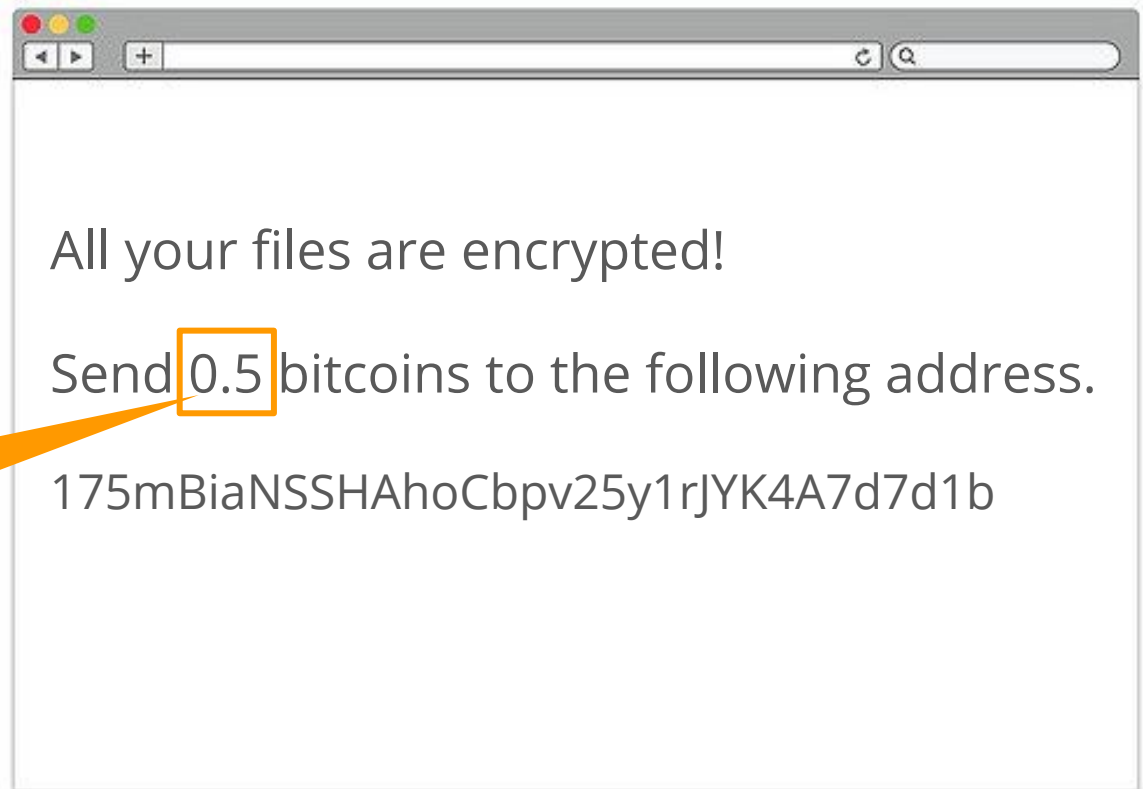


How typical ransomware works

1. Distribution
2. Infection

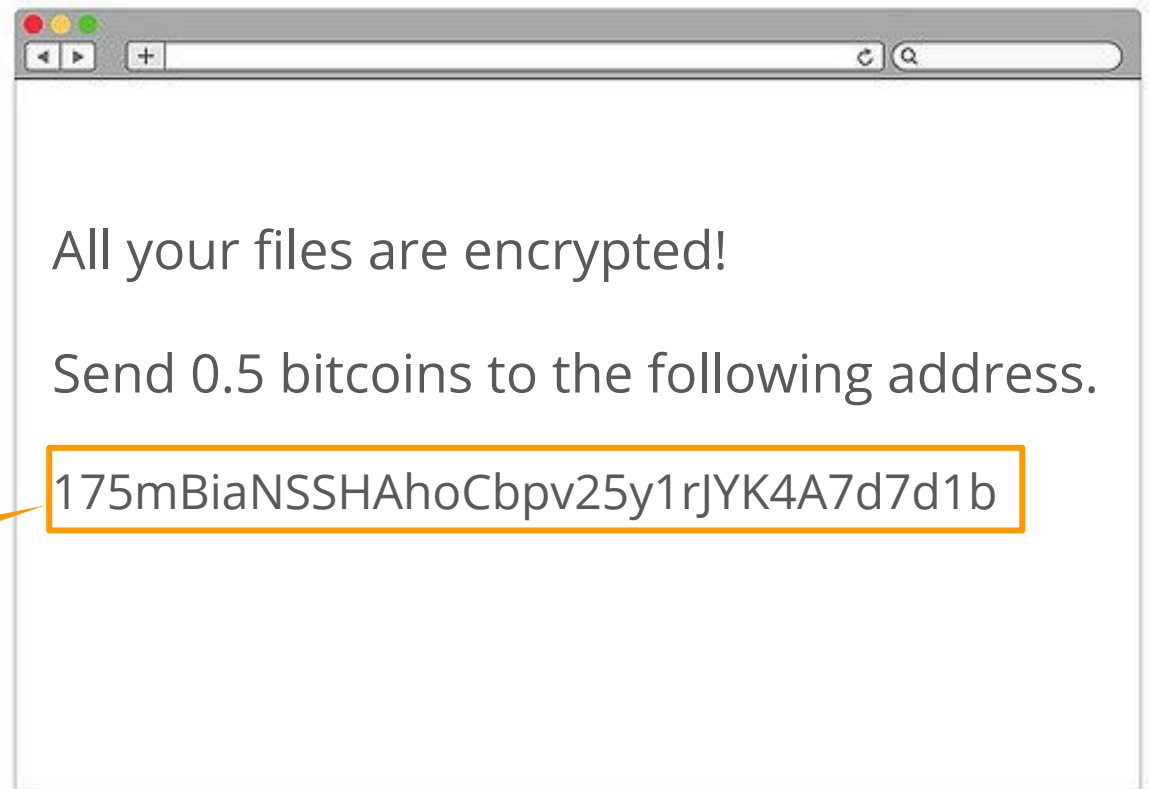
Cerber: median ~\$1,000

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



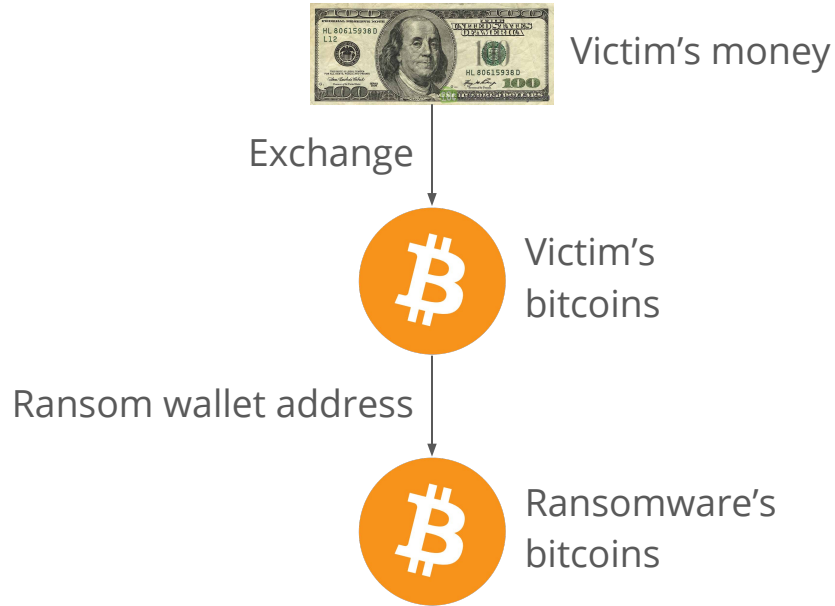
How typical ransomware works

1. Distribution
2. Infection
3. Victim pays bitcoins



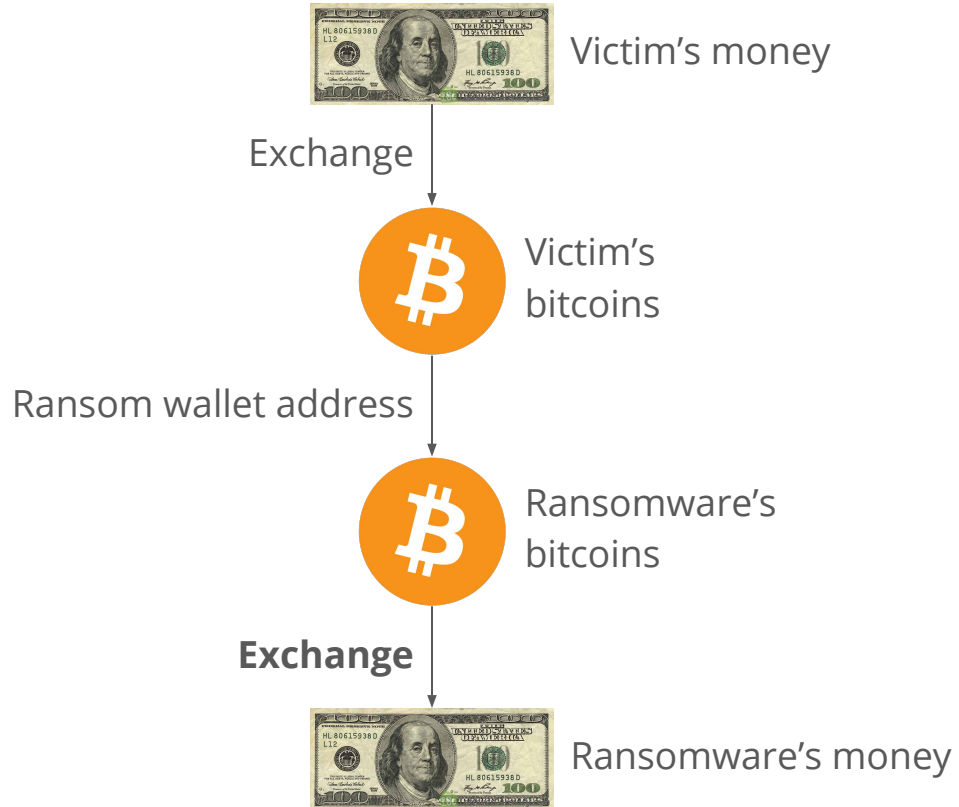
How typical ransomware works

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, \geq \$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, \geq \$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, \geq \$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, \geq \$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, \geq \$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

2

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

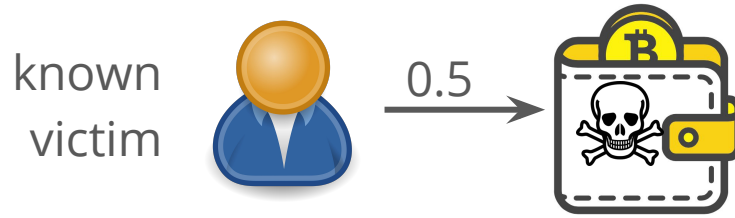
1. Identify known victims
2. Infer unknown victims
3. Estimate total ransom
4. Identify exchanges

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



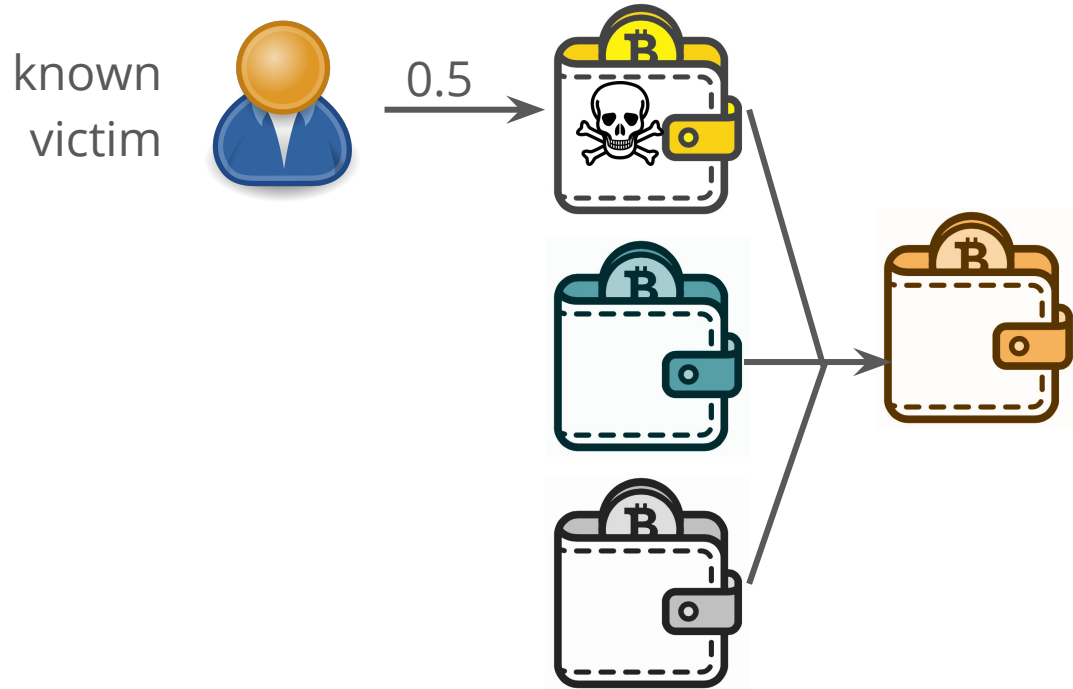
2. Infer unknown victims

3. Estimate total ransom

4. Identify exchanges

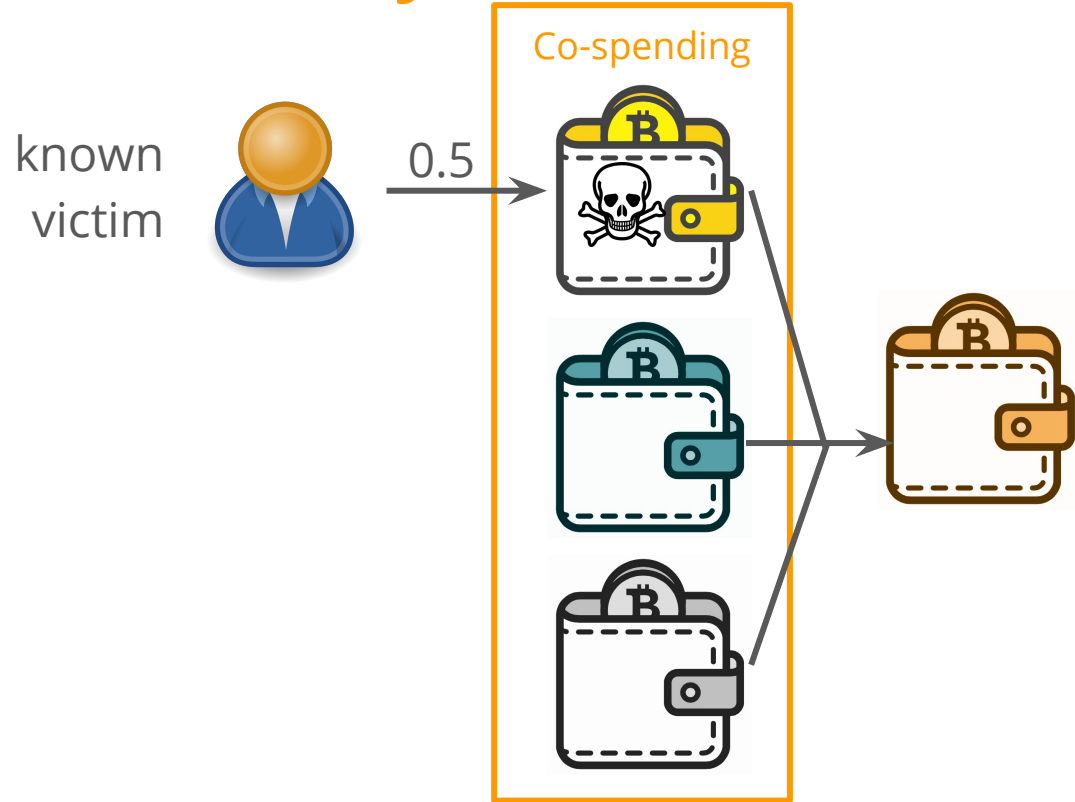
Methodology: Follow the money

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



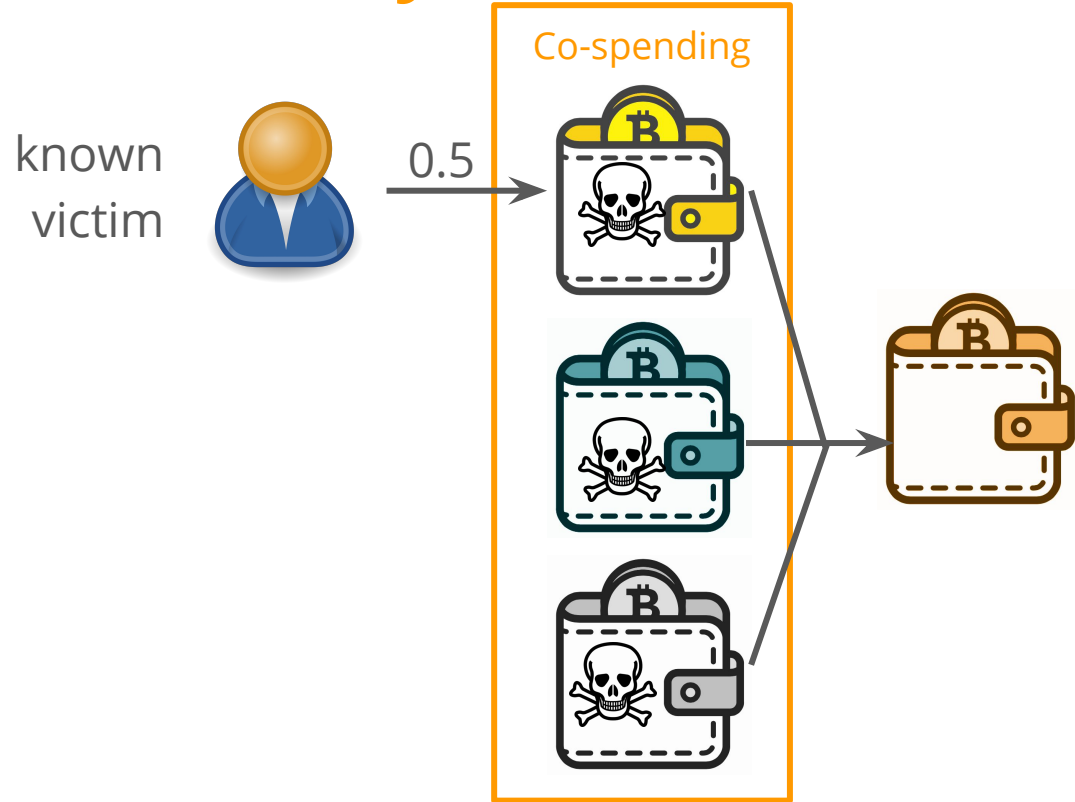
Methodology: Follow the money

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



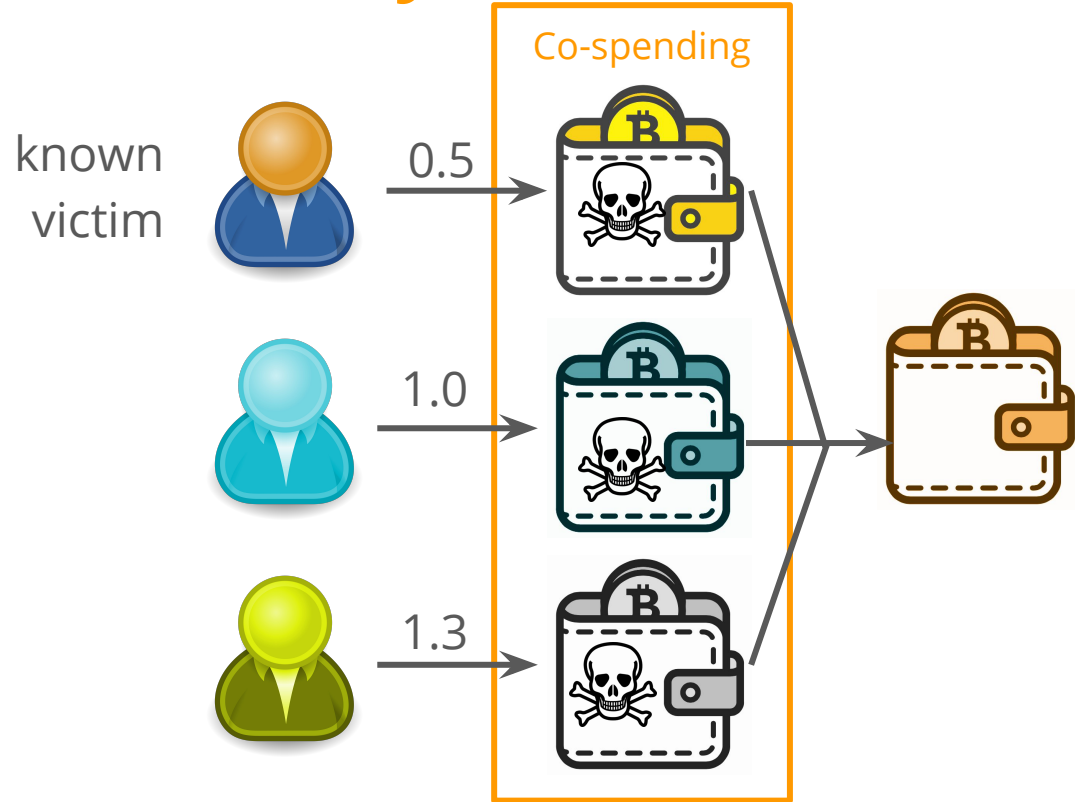
Methodology: Follow the money

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



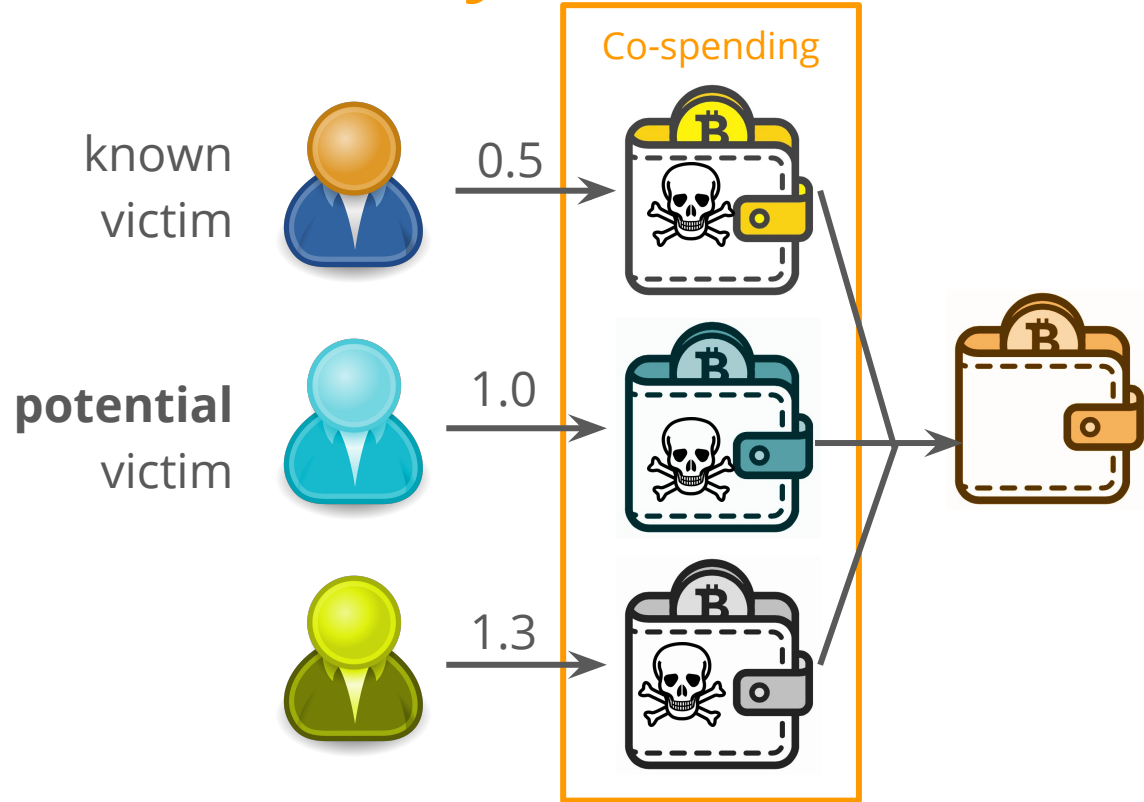
Methodology: Follow the money

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"



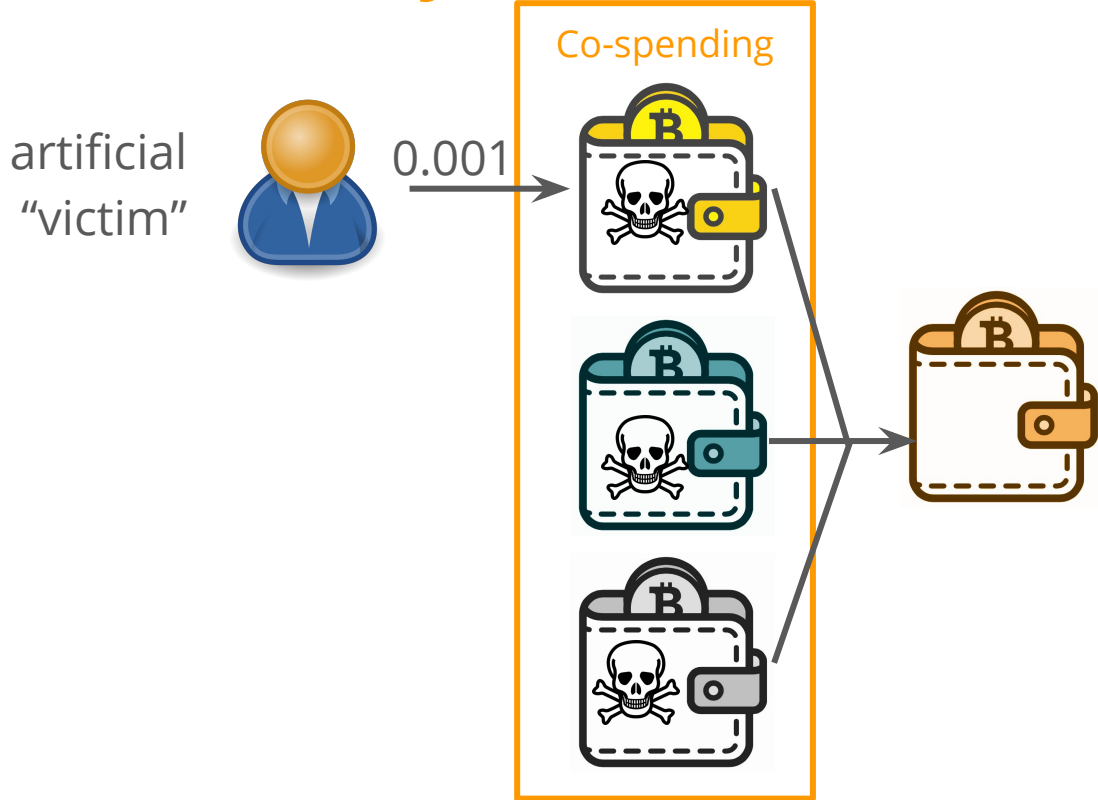
Methodology: Follow the money

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



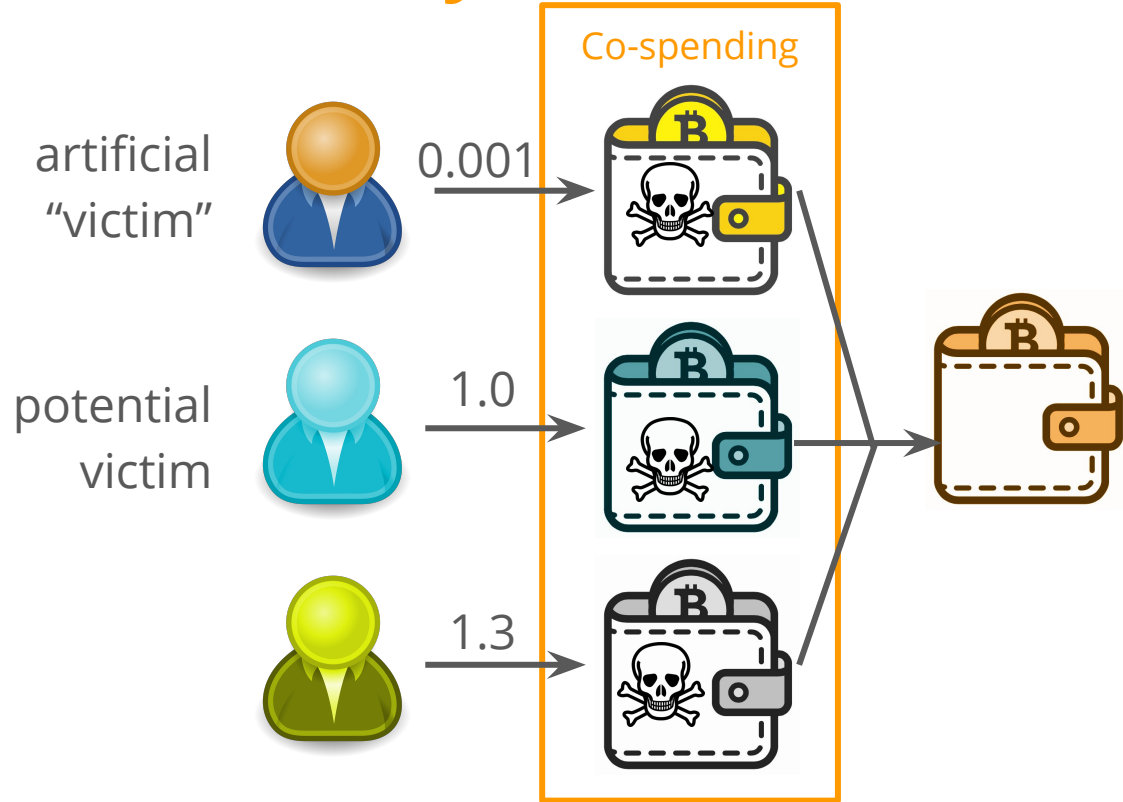
Methodology: Follow the money

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

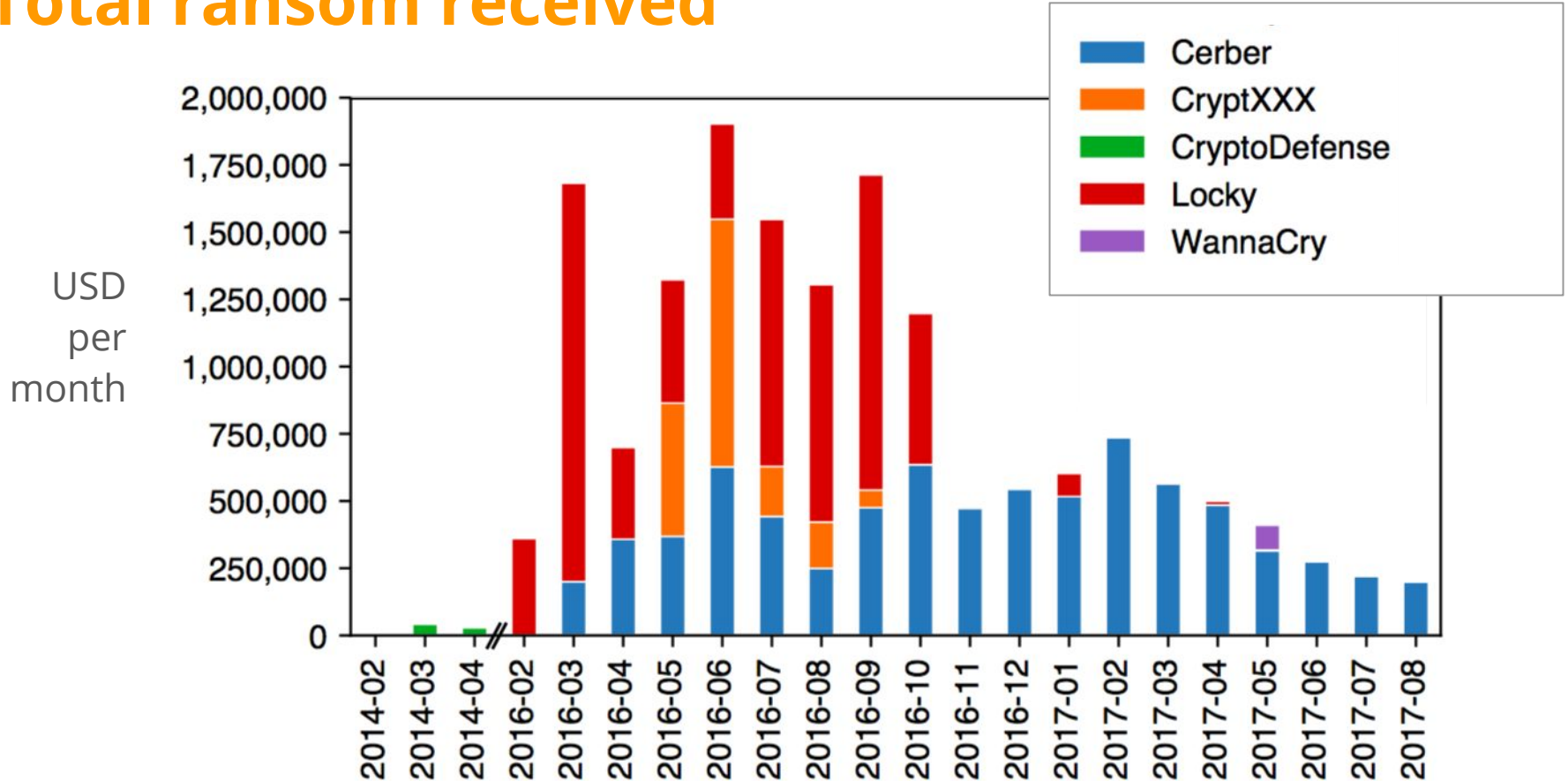


Methodology: Follow the money

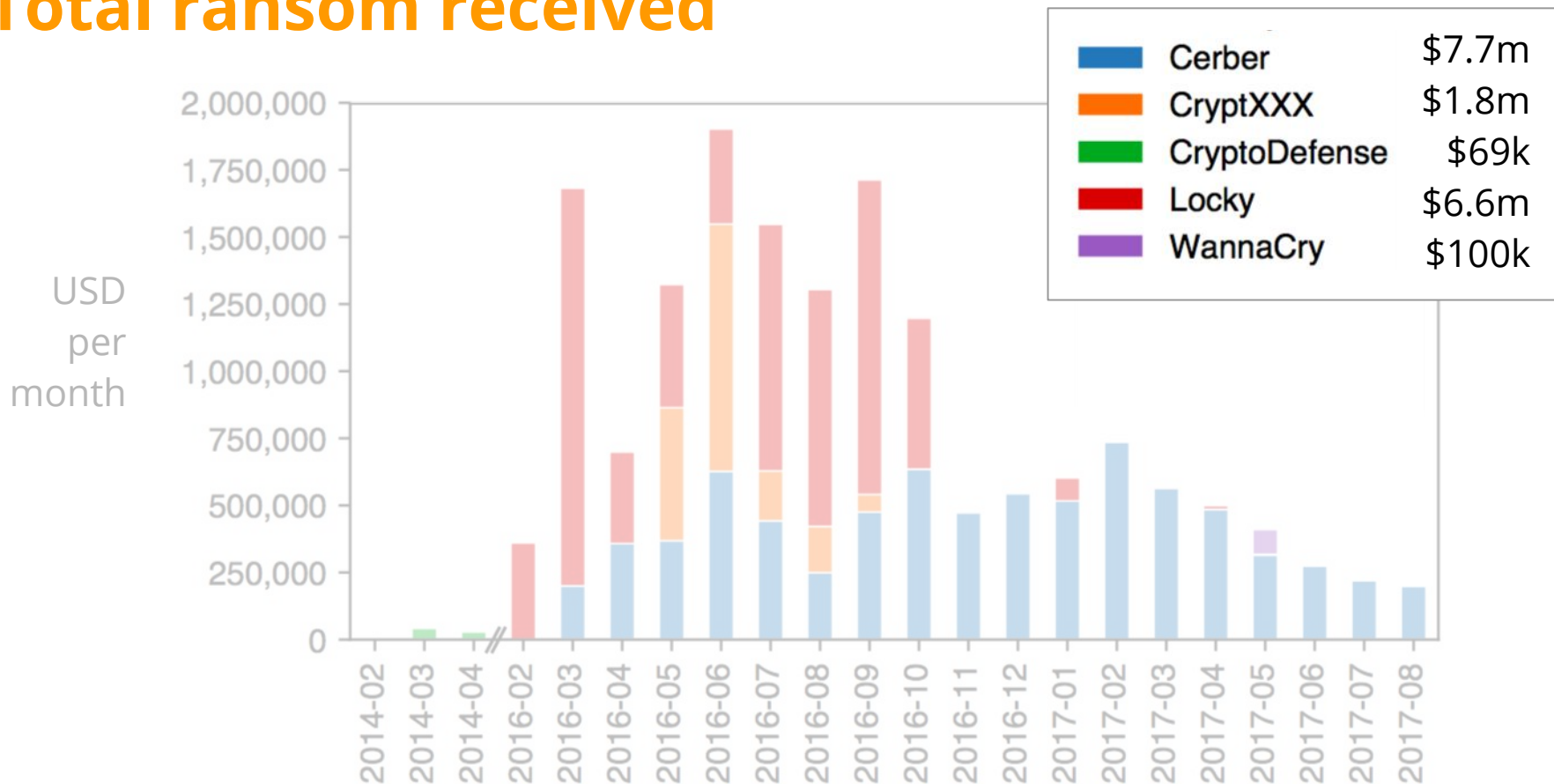
1. Identify known victims
2. Infer unknown victims
3. Estimate total ransom
4. Identify exchanges



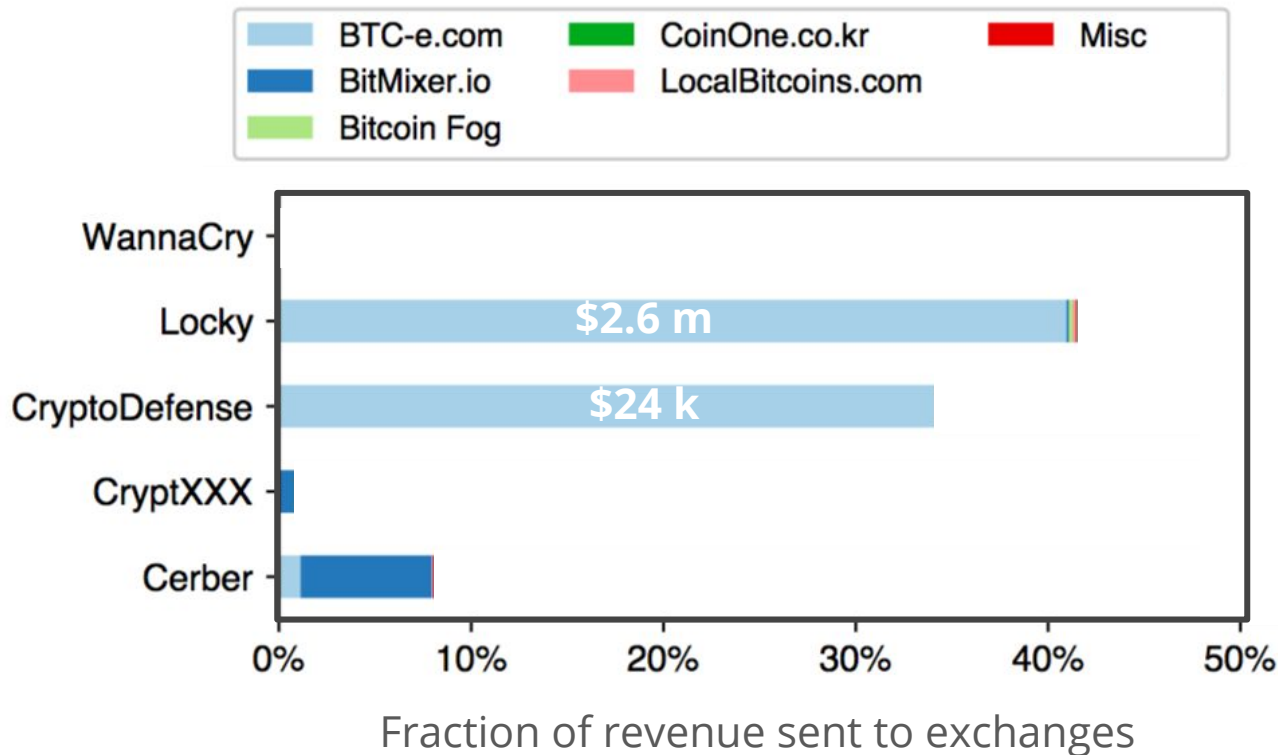
Total ransom received



Total ransom received



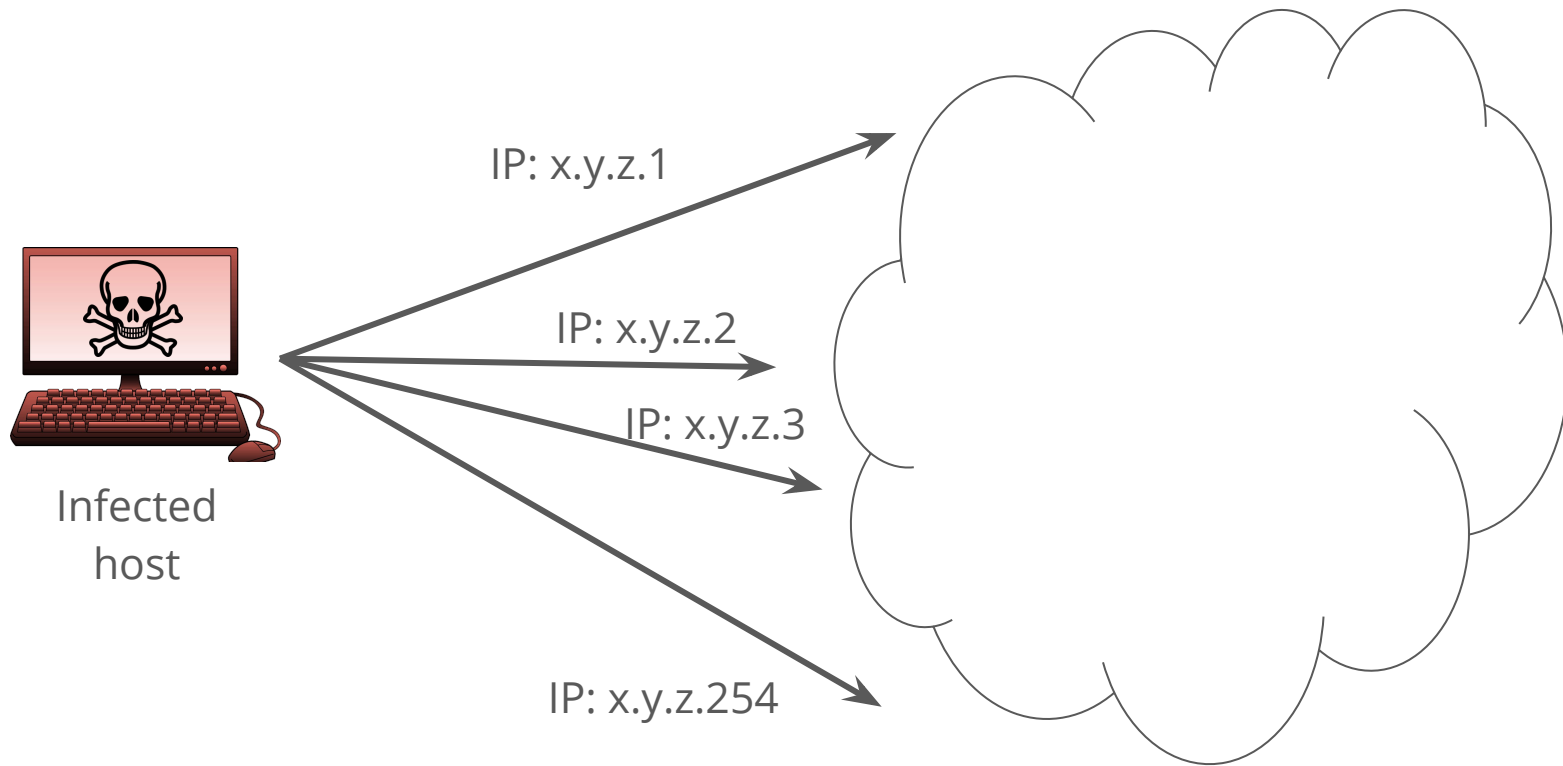
Potential liquidation at exchanges



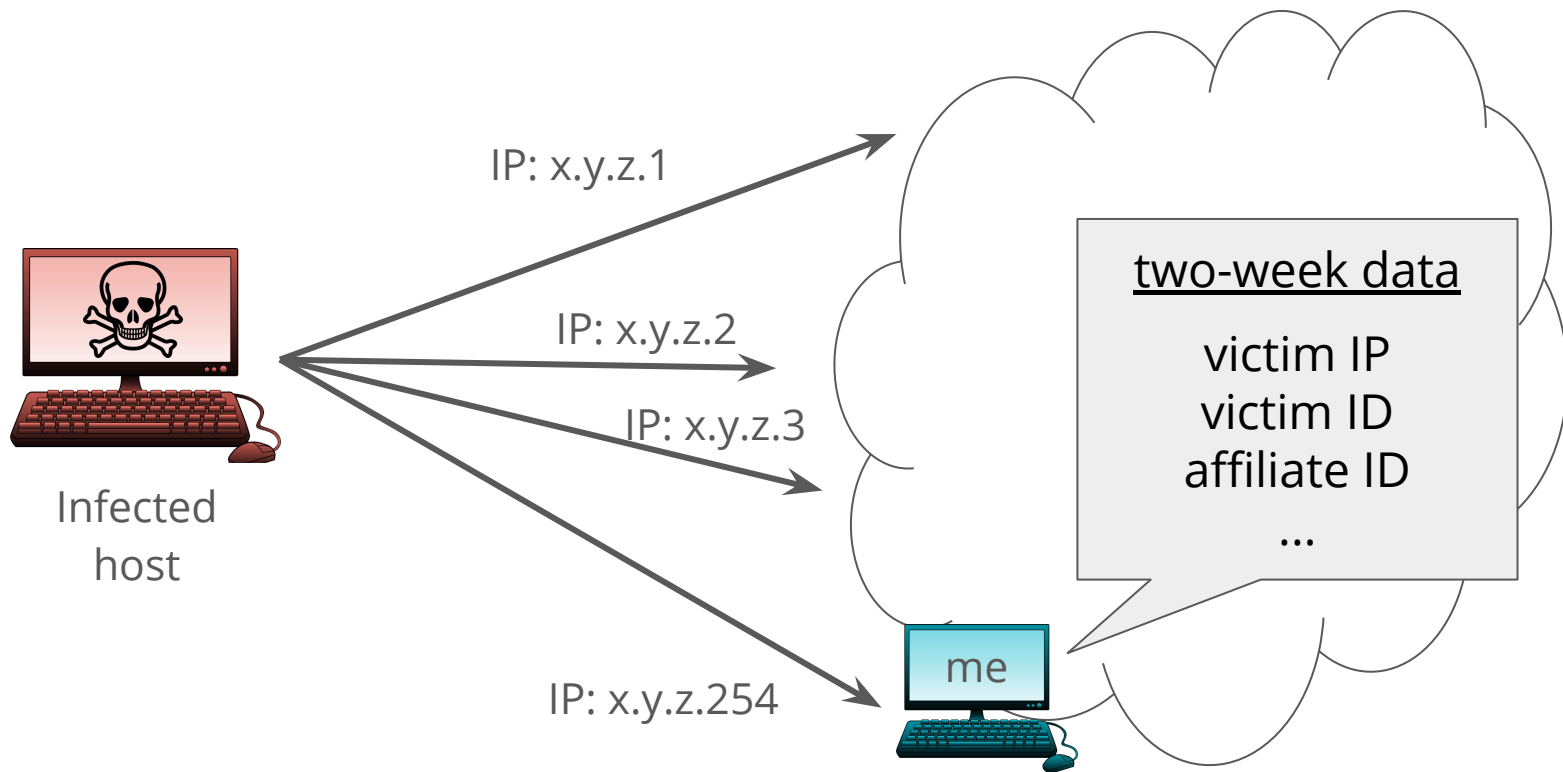
2

Reverse Engineering Cerber's C&C

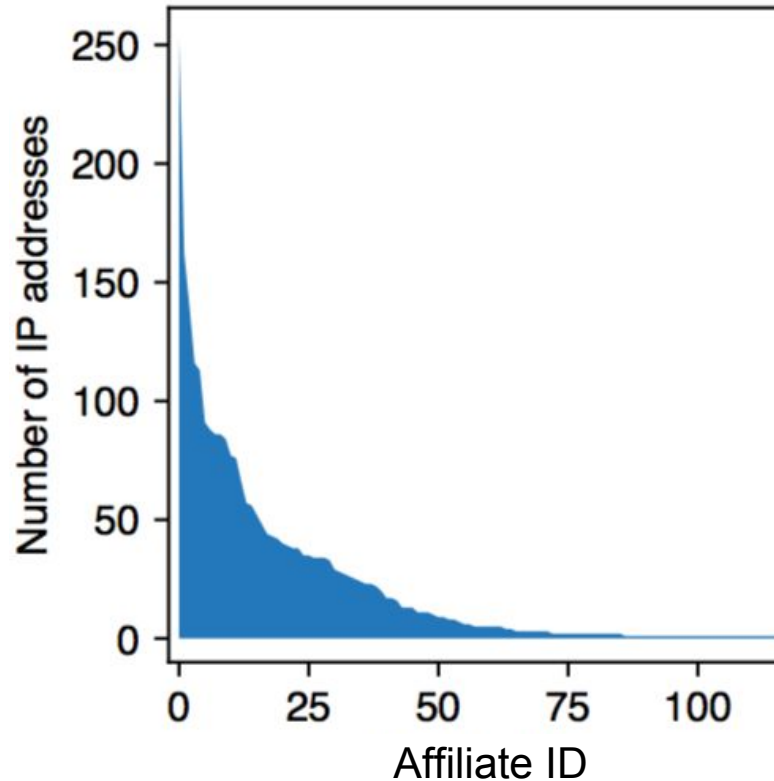
Cerber's outbound UDP traffic



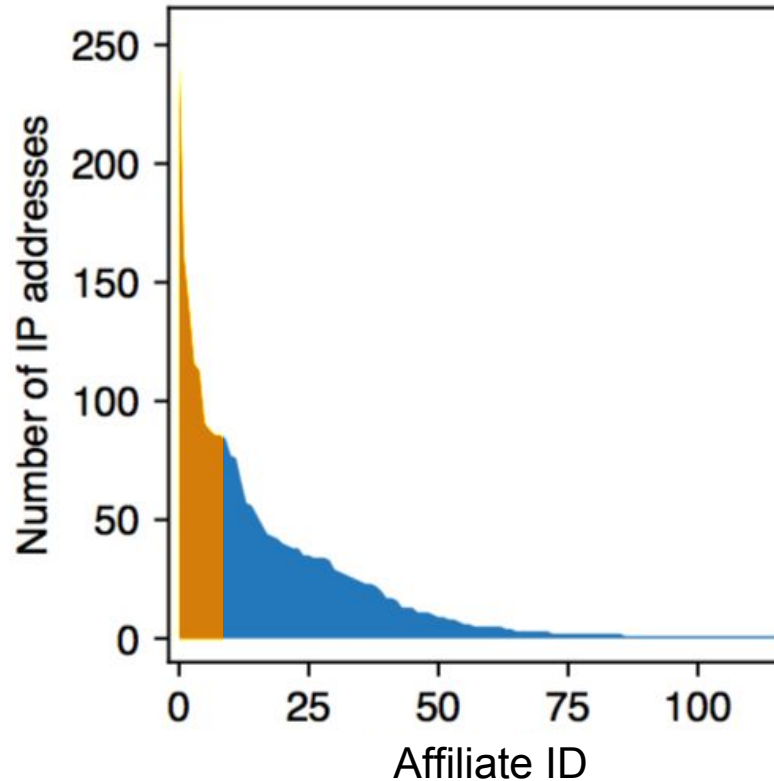
Cerber's outbound UDP traffic



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, \geq \$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, \geq \$16 million over two years

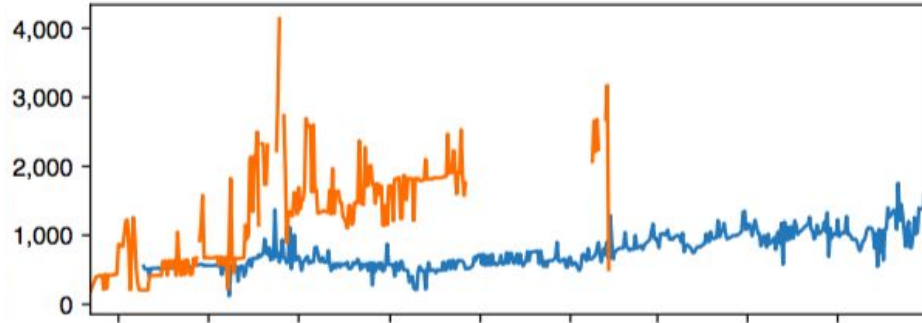
Possible chokepoints: exchanges and affiliates

4

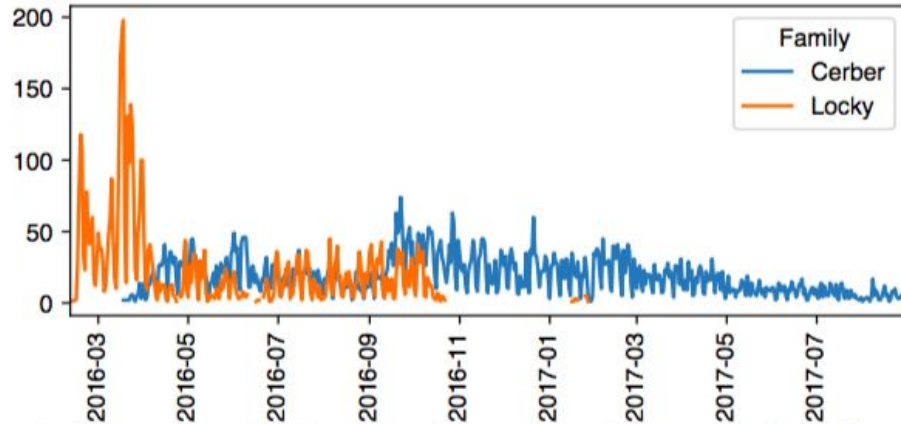
Appendix

Ransom payments over time

Median ransom
amount per day
(USD)



Number of
payments per day



Potentially missing Locky's ransom payments

