ZERO FRICTION

How Colonial Pipeline and JBS Ransomware Hackers Made their Getaway

Tuan Phan, CISSP, PMP, CCI, CTCE, CBSP, SSBB

www.zerofriction.io

Learning Objectives

1. Learn how to conduct on-chain analysis using OSINT blockchain solutions and tools.
2. Learn how to interpret and build transaction flow diagrams to perform follow-the-money analysis.
3. Pick up advanced forensic techniques such as on-chain queries and IP deanonymization.

Case Studies

Meat giant JBS pays $11m in ransom to resolve cyber-attack

10 June

Menu Search **Bloomberg** Sign In **Subscribe**

Photographer: Samuel Corum/Bloomberg

Cybersecurity

Hackers Breached Colonial Pipeline Using Compromised Password

By William Turton and Kartikay Mehrotra
June 4, 2021, 3:58 PM EDT

- Investigators suspect hackers got password from dark web leak
- Colonial CEO hopes U.S. goes after criminal hackers abroad

LIVE ON BLOOMBERG
Watch Live TV
Listen to Live Radio

ZERO FRICTION

Case #1: Colonial Pipeline Timeline

- May 7, the company reported a ransomware incident demanding $5M in payment. The company halted pipeline operations to minimize any additional damages.
- May 8, the company paid 75 BTC in ransom.
- May 9, the company commenced the phased restart of pipeline assets.
- May 12, pipeline assets returned to full operational state.
- June 7, FBI announced the recovery of $2.3M in Bitcoin from the incident.

Case #2: JBS Timeline

- May 30, the company discovered the attack.
- May 31, the threat actors, later identified as REvil, encrypted the environment.
- June 1, JBS paid the 301 BTC in ransom.

ZERO FRICTION

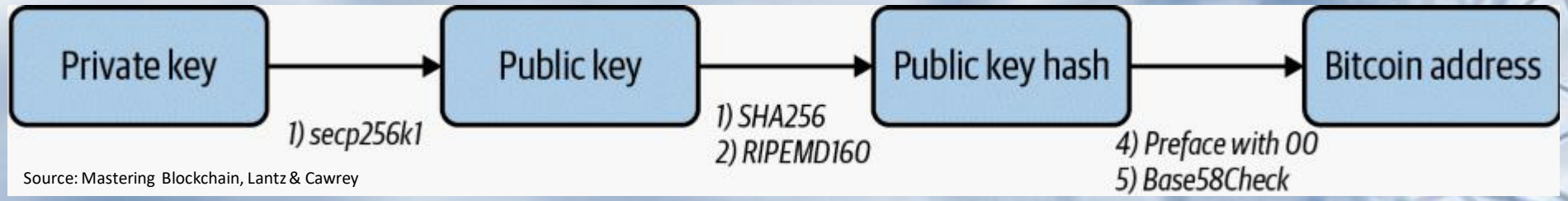
Identity Management of *Typical* Cryptocurrencies

- Employs asymmetric cryptography and cryptographic hash function
- Participant identity = blockchain address
- Public key → hash function → blockchain address

BTC: 1GK67bPQuCErckdhmCABg8esmHfqc32cih
ETH: 0x71ffddd44c3a1d68ed129aa6ef7fd6f55d7f8804

} pseudo-anonymous

- Process to generate Bitcoin address:

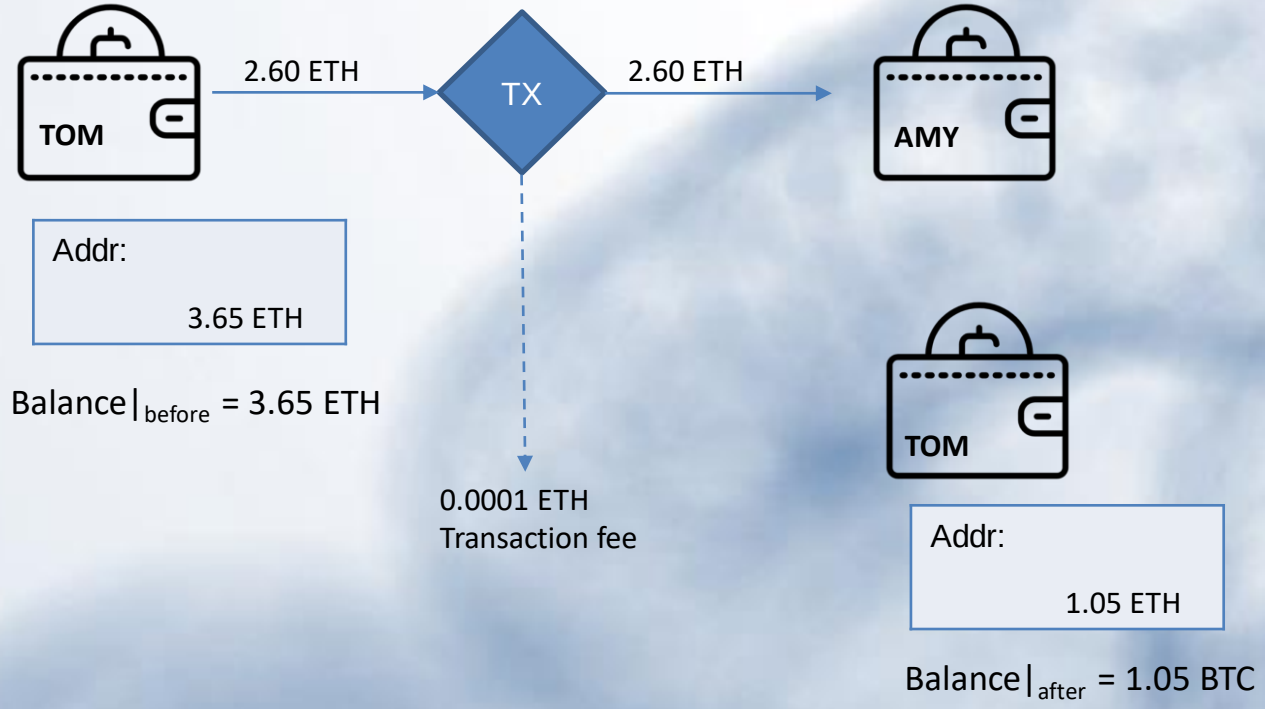


Source: Mastering Blockchain, Lantz & Cawrey

ZERO FRICTION

Accounting Models

Account-Balance Model



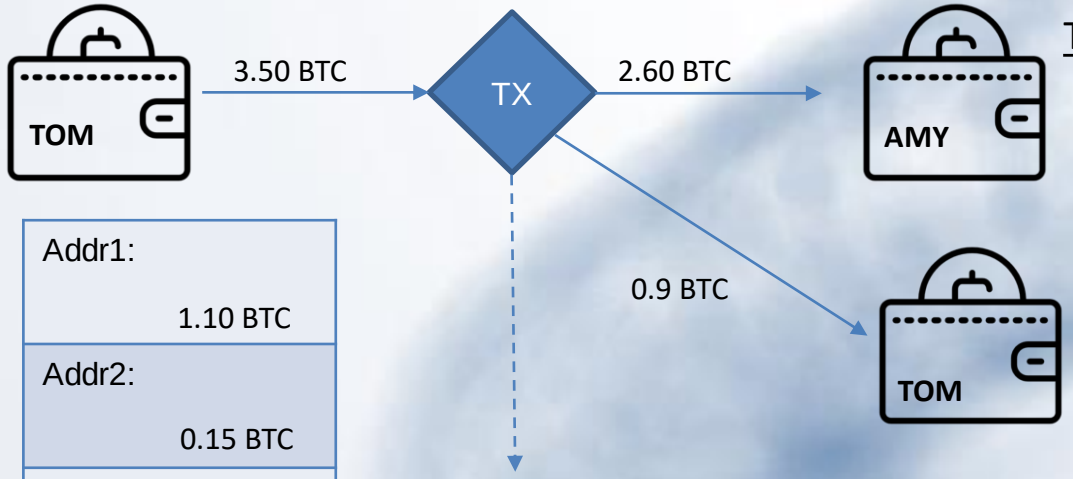
A single address is used for both sending and receiving cryptocurrencies and tokens.

Easiest to track and identify user or account holder.

ZERO FRICTION

Accounting Models

Unspent Transaction Output (UTXO) Model



Tom's Balance

$\text{Balance}|_{\text{before}} = 1.10 + 0.15 + 2.40 = 3.65$ BTC

$\text{Balance}|_{\text{after}} = 0 + 0.15 + 0 + 0.9 = 1.05$ BTC

Addr1:	1.10 BTC
Addr2:	0.15 BTC
Addr3:	2.40 BTC
Addr4:	Unused
Addr5:	Unused

Change Address →

Addr1:	0 BTC
Addr2:	0.15 BTC
Addr3:	0 BTC
Addr4:	0.9 BTC
Addr5:	Unused

Change address adds additional complexity into the tracing of the flow of money.

In addition to liquidity, this is one key driver why BTC is a prefer ransomware crypto payment!

ZERO FRICTION

Let Deconstructing the Incident

- Trace addresses with the largest received values starting from address of interest to point(s) of exit:
  - VASP exit points
  - Holding addresses (unspent addresses)
  - Mixers
  - Decentralized services (DeFi and related swap services)

- Use one or more of the following techniques:
  - Transaction graph analysis
  - Sankey diagram
  - Investigation tool to trace transactions

ZERO FRICTION

How do we get Addresses?

1

28. On or about May 8, 2021, Victim X advised the FBI that it was instructed to send a ransom payment of approximately 75 BTC, calculated to be worth approximately $4.3 million on that date, to cryptocurrency address XXXXXXXXXXXXXL6qeMLgX5VEAFCbRXjc9fr.

33. An online public blockchain explorer identified at least 23 other addresses collected together with address XXXXXXXXXXXXuRTnHQA8tNuG7S2pKcdNxB in one wallet. [redacted] on May 27, 2021, funds from the collection of addresses, totaling 69.60422177 BTC, including 63.70000000 BTC accessible from address XXXXXXXXXXXXuRTnHQA8tNuG7S2pKcdNxB was transferred to address XXXXXXXXXXXX950klpjcawuy4uj39ym43hs6cfsegq (the "Subject Address"), and it has not moved since.

34. The private key for the Subject Address is in the possession of the FBI in the Northern District of California.

Source: FBI's Seizure Warrant for Colonial Pipeline Hack

2

Obtained from screenshot of the ransom screen:

sophos_READ[redacted].TXT - Notepad

File Edit Format View Help

```
---------- [ Welcome to DarkSide ] ------------->

What happend?
---------------------------------------------
Your computers and servers are encrypted, backups are deleted. We use strong encryption algorithms, so you cannot decrypt your data.
But you can restore everything by purchasing a special program from us - universal decryptor. This program will restore all your network.
Follow our instructions below and you will recover all your data.

Data leak
---------------------------------------------
First of all we have uploaded more then 140GB data.

These files include:
 - Accounting
 - Research & Development

Your personal leak page: http://darkside[redacted]
On the page you will find examples of files that have been stolen.
The data is preloaded and will be automatically published if you do not pay.
After publication, your data will be available for at least 6 months on our tor cdn servers.

We are ready:
- To provide you the evidence of stolen data
- To delete all the stolen data.


What guarantees?
---------------------------------------------
We value our reputation. If we do not do our work and liabilities, nobody will pay us. This is not in our interests.
All our decryption software is perfectly tested and will decrypt your data. We will also provide support in case of problems.
We guarantee to decrypt one file for free. Go to the site and contact us.

How to get access on website?
---------------------------------------------
Using a TOR browser:
1) Download and install TOR browser from this site: https://torproject.org/
2) Open our website: http://darksid[redacted]

When you open our website, put the following data in the input form:
Key:
```

SOPHOS labs

ZERO FRICTION

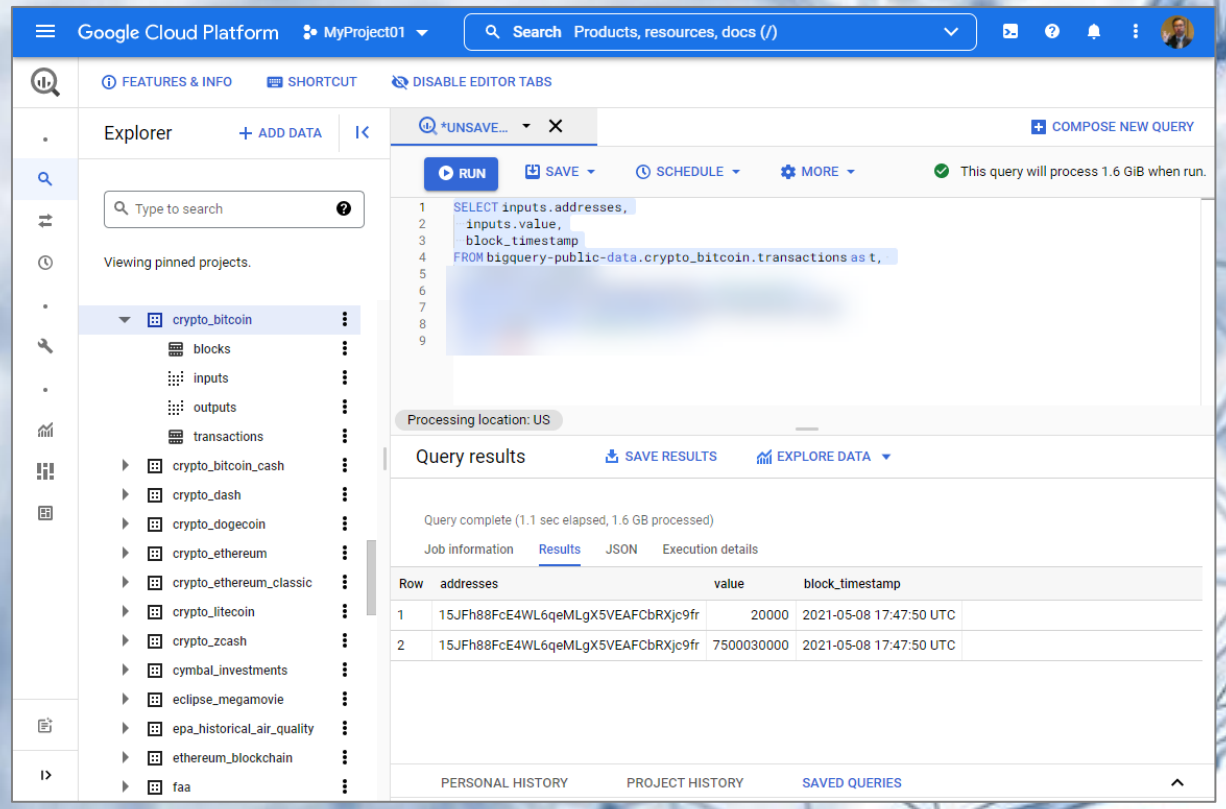
Colonial Pipeline - Address Hunting using Partial Addresses

28. On or about May 8, 2021, Victim X advised the FBI that it was instructed to send a ransom payment of approximately 75 BTC, calculated to be worth approximately $4.3 million on that date, to cryptocurrency address XXXXXXXXXXXXXL6qeMLgX5VEAFCbRXjc9fr.

Source: FBI's Seizure Warrant for Colonial Pipeline Hack

Leverage Google's Bigquery for real-time search against public crypto datasets.

https://cloud.google.com/bigquery



Result: 15JFh88FcE4WL6qeMLgX5VEAFCbRXjc9fr

ZERO FRICTION

JBS – Address Hunting for Specific Conditions

Meat giant JBS pays $11m in ransom to resolve cyber-attack

10 June

The world's largest meat processing company has paid the equivalent of $11m (£7.8m) in ransom to put an end to a major cyber-attack.

Computer networks at JBS were hacked last week, temporarily shutting down some operations in Australia, Canada and the US.

The payment was reportedly made using Bitcoin after plants had come back online.

We look for addresses with specific combination of amount and timeframe.

Google Cloud Platform | MyProject01 | Search products and resc

FEATURES & INFO | SHORTCUT | DISABLE EDITOR TABS

Explorer | + ADD DATA

Type to search

Viewing pinned projects.

- crypto_bitcoin
  - blocks
  - inputs
  - outputs
  - transactions
- crypto_bitcoin_cash
- crypto_dash
- crypto_dogecoin
- crypto_ethereum
- crypto_ethereum_classic
- crypto_litecoin
- crypto_zcash
- cymbal_investments

*UNSAVE...

RUN | SAVE | SCHEDULE | MORE

```
SELECT outputs.addresses,
    outputs.value,
    block_timestamp
FROM bigquery-public-data.crypto_bitcoin.transactions as t,

limit 1000;
```

Query results | SAVE RESULTS | EXPLORE DATA

Query complete (1.3 sec elapsed, 1.2 GB processed)

Job information | Results | JSON | Execution details

Row	addresses	value	block_timestamp
1	1NmcvEH2rMeXaw3C9mkLhc3QkjV2AyNbLg	30100000000	2021-06-01 23:20:00 UTC
2	3L7ECcRBCypxrS5U9Kw9WexcsHmX4wKYz6	30100000000	2021-06-01 23:25:38 UTC
3	1PdGND2KXZprBxoH5fs3yEp8gWzNLToGBB	30100000000	2021-06-30 18:47:53 UTC
4	38Vkp5DM9gTeWWZrrAo3e92oPK98yrHXaG	30100000000	2021-06-25 05:11:31 UTC

ZERO FRICTION

JBS – Address Hunting for Specific Conditions

Row	addresses	value	block_timestamp
1	1NmcvEH2rMeXaw3C9mkLhc3QkjV2AyNbLg	30100000000	2021-06-01 23:20:00 UTC
2	3L7ECcRBCypxrS5U9Kw9WexcsHmX4wKYz6	30100000000	2021-06-01 23:25:38 UTC
3	1PdGND2KXZprBxoH5fs3yEp8gWzNLToGBB	30100000000	2021-06-30 18:47:53 UTC
4	38Vkp5DM9gTeWWZrrAo3e92oPK98yrHXaG	30100000000	2021-06-25 05:11:31 UTC

#1

1NmcvEH2rMeXaw3C9mkLhc3QkjV2AyNbLg

Address | Inflow | Outflow | Money Flow

Address Statistics

Metric	Value
Inputs in Transactions	1
Outputs in Transactions	1
First transaction date	2021-06-01
Last transaction date	2021-06-01
Received in Outputs	301 BTC
Spent to Inputs	301 BTC
Balance (unspent outputs)	0 BTC

Total 7 rows

#2

3L7ECcRBCypxrS5U9Kw9WexcsHmX4wKYz6

Address | Inflow | Outflow | Money Flow

Address Statistics

Metric	Value
Inputs in Transactions	1
Outputs in Transactions	1
First transaction date	2021-06-01
Last transaction date	2021-06-01
Received in Outputs	301 BTC
Spent to Inputs	301 BTC
Balance (unspent outputs)	0 BTC

Total 7 rows

#3

1PdGND2KXZprBxoH5fs3yEp8gWzNLToGBB

Address | Inflow | Outflow | Money Flow

Address Statistics

Metric	Value
Inputs in Transactions	723
Outputs in Transactions	723
First transaction date	2019-09-11
Last transaction date	2021-07-26
Received in Outputs	114739.89793502 BTC
Spent to Inputs	114739.89793502 BTC
Balance (unspent outputs)	0 BTC

Total 7 rows

#4

38Vkp5DM9gTeWWZrrAo3e92oPK98yrHXaG

Address | Inflow | Outflow | Money Flow

Address Statistics

Metric	Value
Inputs in Transactions	292
Outputs in Transactions	294
First transaction date	2020-10-01
Last transaction date	2021-07-26
Received in Outputs	92533.82467882 BTC
Spent to Inputs	92533.82466788 BTC
Balance (unspent outputs)	0.00001094 BTC

Total 7 rows

CSV JS GraphQL

ZERO FRICTION

The Colonial Pipeline Story in Three Episodes

The Heist

1

The Seizure

2

On the Lam

3

ZERO FRICTION

Episode #1 “The Heist”

We will transition to Breadcrumbs when I will walk you thru the tracing process. To do that we will need the result of the query as our starting point.

15JFh88FcE4WL6qeMLgX5VEAFCbRXjc9fr (Ransom Address)
bc1qq2euq8pw950klpjcawuy4uj39ym43hs6cfsegq (Subject Address)

https://www.breadcrumbs.app

ZERO FRICTION

Summary of Episode #1

1. Ransom address was paid possibly from Coinbase (attribution)
2. 75 BTC was transferred to bc1q7eqww9dmm9p48hx5yz5gcvmncu65w43wfytpsf
3. 11.2 BTC was sent to the DarkSide Developer address
4. 63.7 BTC was sent to bc1qxu83k5qkj8kcqdqqenwzn7khcw4llfykeqwg45
5. bc1qxu83k5qkj8kcqdqqenwzn7khcw4llfykeqwg45 is also a collector address for other payments (which implies there were other victims).
6. 63.7 BTC was sent to 3EYkxQSUv2KcuRTnHQA8tNuG7S2pKcdNxB and then onto a Darkside Affiliate (bc1qq2euq8pw950klpjcawuy4uj39ym43hs6cfsegq) as payment for the successful campaign.

Episode #2 “The Seizure”

June 7, FBI announced the recovery of $2.3M or 63.7 BTC from the incident by seizing funds from bc1qq2euq8pw950klpjcawuy4uj39ym43hs6cfsegq.

Let take a look at that.

https://www.breadcrumbs.app

ZERO FRICTION

Summary of Episode #2

1. FBI seized 63.7 BTC to their address bc1qpx7vyv5tp7dm0g475ev527krg764t73dh77gls on June 7 @1:45 PM UTC via TX 943f2d576ed8d9f388ba75eb82fe35cce29479b84121827ac368a5a94f44cf7a
2. 8 minutes after the seizure, remaining balance of 5.9 BTC was moved to bc1qvjh9cq6qlj4f4q5vxnkgt25mc6qld04vv20fhe via TX bc1qvjh9cq6qlj4f4q5vxnkgt25mc6qld04vv20fhe. Most likely by the Affiliate.
3. By Aug 18, the FBI has prepped the address to return the funds to Colonial Pipeline into 1Eq1WadiQw5PWr78waw8pt3rdU6KFMVqRc and back to centralized service address 1L21V6B31zYcChfwDQjCaLoCwEGg6UQApV.

ZERO FRICTION

Episode #3 “On the Lam”

Back in June 2021, address bc1q2sewgrnau4e4gvceh8ykzf8lqxawpluu0k0607 (Darkside Developer) has 107 BTC within it.

With so much unwanted publicity, the developer starts to run using several peel chains.

Let look at that.

https://oxt.me/transaction/0ff023e3193272e4188c763e86e92526abcf5cd945f84c17bce0497e155f0c46

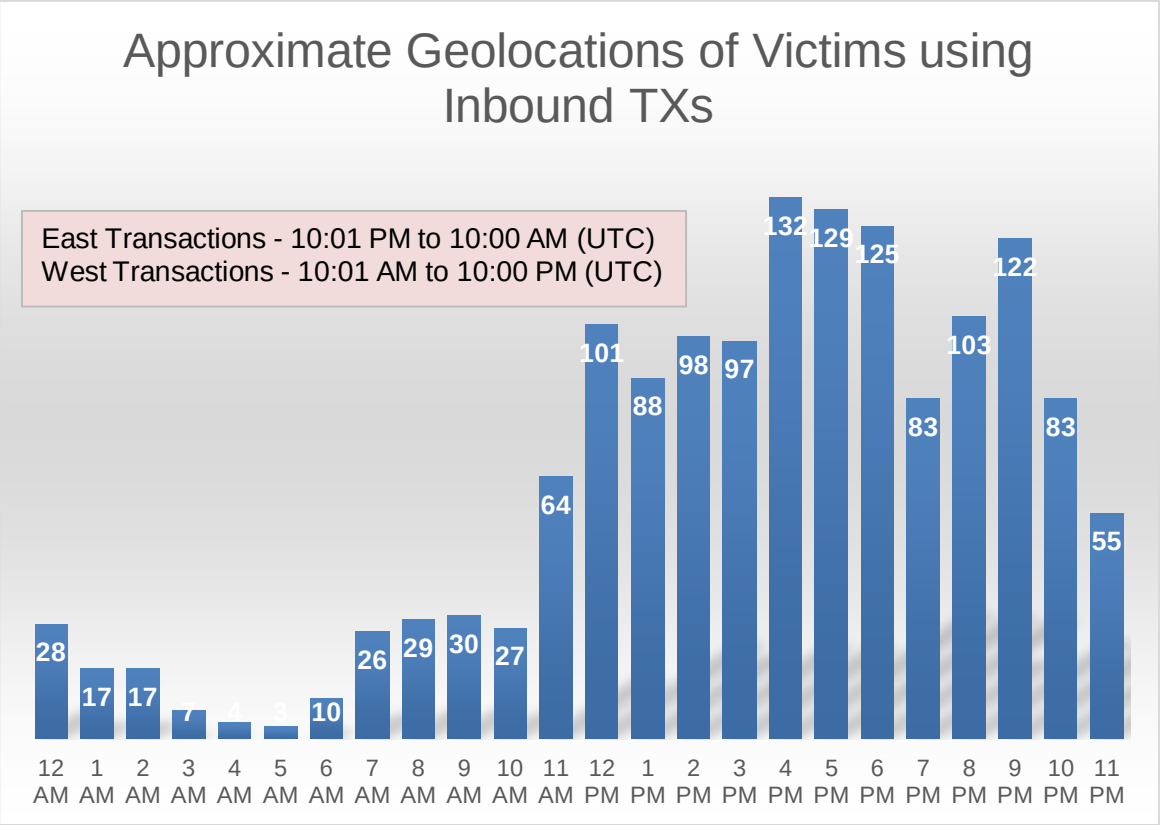
https://www.breadcrumbs.app

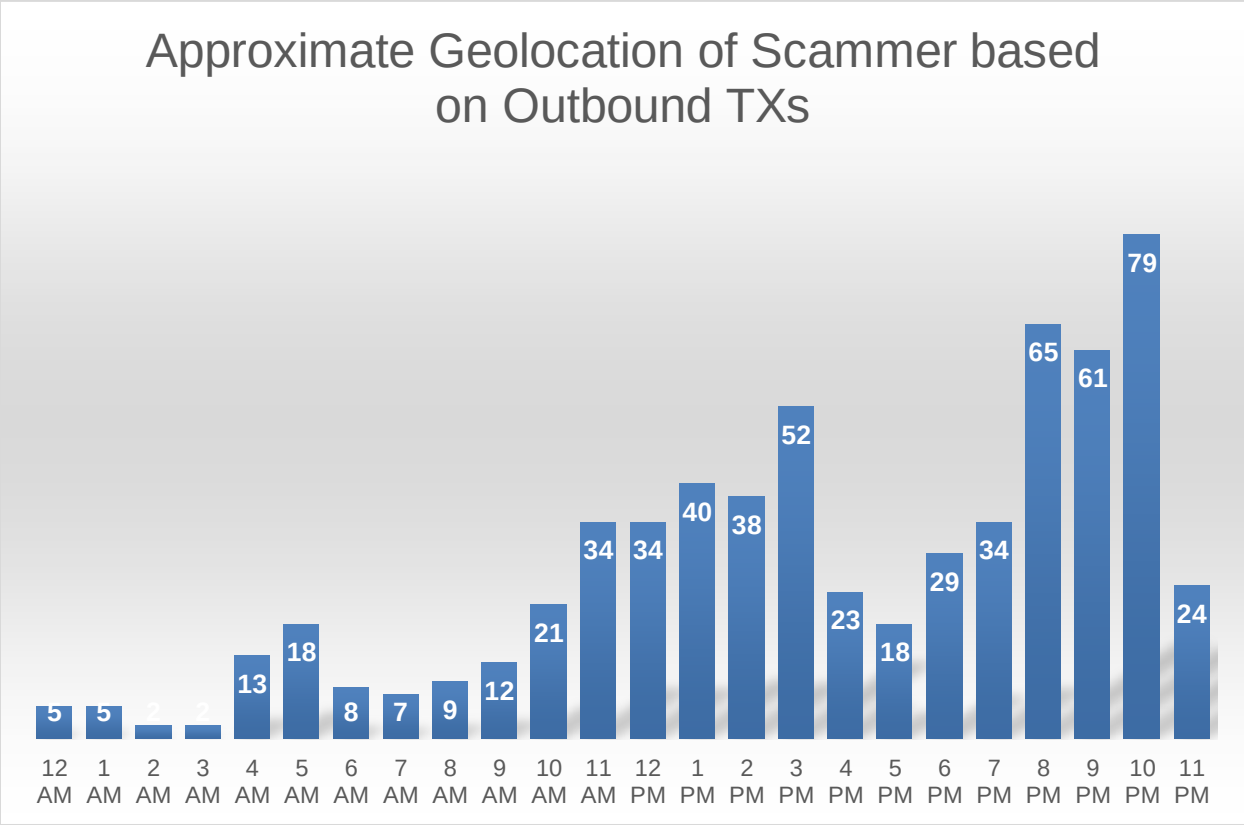
Summary of Episode #3

1. Several peel chains have been initiated to hide funds across multiple addresses.
2. To achieve that the DarkSide developer either switched or added a different software wallet – Evidence in transition from bc1q... into 13Fm...
3. Peel amounts are in small random but nice round integers in attempt to evade detection.
4. Why JBS hacker got away and not Colonial Pipeline hacker?

ZERO FRICTION

Geolocation using Transaction Timestamp





ZERO FRICTION

Identifying the Earliest Broadcast of Specific TX

Propagation of TXs to Peers on Bitcoin

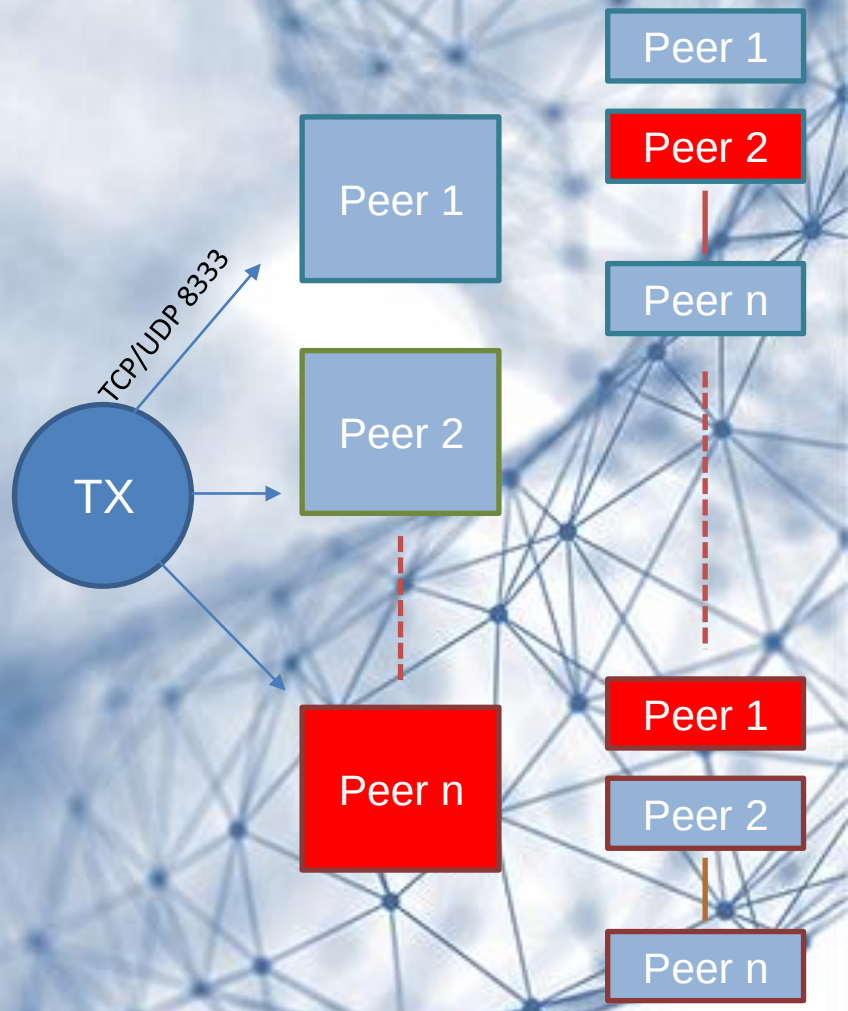
Node window

Information | Console | Network Traffic | Peers

NodeId	Node/Service	Ping	Sent	Received	User Agent
0	↑ 192.69.53.70:8333	64 ms	1 KB	1 MB	/Satoshi:0.21.1/
1	↑ 73.164.232.241:8333	319 ms	1 KB	3 KB	/Satoshi:0.21.1/
3	↑ 62.171.140.140:8333	249 ms	22 KB	185 KB	/Satoshi:0.21.1/
6	↑ 35.236.147.169:8333	389 ms	18 KB	154 KB	/Satoshi:0.20.1/
9	↑ 165.22.233.194:8333	54 ms	12 KB	103 KB	/Satoshi:0.20.1/
13	↑ 194.180.110.10:8333	N/A	6 KB	2 KB	/Satoshi:0.21.0/
14	↑ 35.183.49.55:8333	114 ms	4 KB	42 KB	/Satoshi:0.20.1/
15	↑ 37.97.249.17:8333	104 ms	2 KB	3 KB	/Satoshi:0.21.1/
16	↑ 35.237.109.49:8333	47 ms	2 KB	1 KB	/Satoshi:0.20.1/
17	↑ 47.94.243.77:8333	446 ms	1 KB	30 KB	/Satoshi:0.16.0/

62.171.140.140:8333 (node id: 3)
via 50.206.65.238:56763

Permissions	N/A
Direction	Outbound
Version	70016
User Agent	/Satoshi:0.21.1/
Services	NETWORK & WITNESS & NETWORK_LI
Starting Block	696122
Synced Headers	696122
Synced Blocks	696122
Connection Time	2 m 45 s
Last Send	1 s
Last Receive	0 s
Sent	22 KB
Received	185 KB
Ping Time	249 ms
Ping Wait	N/A
Min Ping	249 ms
Time Offset	-50 s
Mapped AS	N/A



ZERO FRICTION

Identifying the Earliest Broadcast of Specific TX

DATA PROPAGATION

Get inv propagation stats in milliseconds for a block or transaction broadcasted over 8 hours ago. Stats are calculated based on the inv arrival times (UNIX time in milliseconds) from the first 1000 nodes.

```
GET https://bitnodes.io/api/v1/inv/<INV_HASH>/
```

Values in stats represent the following information:

- head - Arrival times for the first 10 nodes in a list of ["<ADDRESS>:<PORT>", <TIMESTAMP>].
- min - Delta for earliest arrival time. Value can be 0 if the delta is less than 1 millisecond.
- max - Delta for latest arrival time.
- mean - Average of deltas.
- std - Standard deviation of deltas.
- 50% - 50th percentile of deltas.
- 90% - 90th percentile of deltas.

Viewer | Text

```
JSON
  inv_hash : "943f2d576ed8d9f388ba75eb82fe35cce29479b84121827ac368a5a94f44cf7a"
  stats
    std : 2428
    head
      0
        0 : "xywyvvvcs5pohots5lelilnigze5ittndtepmyerqzlshf4nom3pyfyd.onion:8333"
        1 : 1623087625504
      1
        0 : "in7r5ieo7ogkxbne.onion:8333"
        1 : 1623087626384
      2
        0 : "cncwik3tnd2ejm5z.onion:8333"
        1 : 1623087626423
      3
        0 : "rk4vbyca7xnn3top.onion:8333"
        1 : 1623087626560
      4
        0 : "pnd6ujrytfwabe4m.onion:8333"
        1 : 1623087626804
      5
        0 : "gkzo2hlkmdkwbj2v.onion:8333"
        1 : 1623087626888
      6
        0 : "52.15.186.116:48333"
        1 : 1623087626920
      7
        0 : "63.32.178.253:8333"
        1 : 1623087626931
      8
        0 : "[2002:d1b1:5615::d1b1:5615]:8333"
        1 : 1623087626934
      9
        0 : "54.185.108.174:8333"
        1 : 1623087626934
    min : 880
    max : 10118
    50% : 5494
    90% : 9077
    mean : 5723
```

Viewer | Text

```
JSON
  inv_hash : "280c5f96397b9502b99703842712b78fda84f1a0faabf826f683448082f46369"
  stats
    std : 1056
    head
      0
        0 : "rk4vbyca7xnn3top.onion:8333"
        1 : 1623088121619
      1
        0 : "xywyvvvcs5pohots5lelilnigze5ittndtepmyerqzlshf4nom3pyfyd.onion:8333"
        1 : 1623088122205
      2
        0 : "yzlai35raddd2kdjnukns7u5t4m4ngi5dfrlq72e6lqf2hp5dzkuszqd.onion:8333"
        1 : 1623088122345
      3
        0 : "v5i7np5tvgqkook2.onion:8333"
        1 : 1623088122352
      4
        0 : "6awaoeg6duhngrvd.onion:8333"
        1 : 1623088122510
      5
        0 : "ndgi74ath5c7j5d2.onion:8333"
        1 : 1623088122569
      6
        0 : "in7r5ieo7ogkxbne.onion:8333"
        1 : 1623088122667
      7
        0 : "hyw3lm5us7fnamyd.onion:8333"
        1 : 1623088122799
      8
        0 : "kgcarpwdts5y5xhu.onion:8333"
        1 : 1623088122896
      9
        0 : "gnwq5b3pvdiymn7d.onion:8333"
        1 : 1623088122931
    min : 586
    max : 5767
    50% : 3962
    90% : 5531
    mean : 4240
```


ZERO FRICTION

Key Takeaways

- How to conduct on-chain analysis for transactions using OSINT blokchain explorers and tools.
- Learn how to interpret and build transaction flow diagrams to perform follow-the-money analysis.
- How address attribution work and how that can support deanonymization of bitcoin addresses.
- Learned some advanced forensic techniques such as on-chain queries and IP deanonymization.

More details at https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2021/did-the-fbi-hack-bitcoin-deconstructing-the-colonial-pipeline-ransom

Contact Information

Tuan Phan, CISSP, PMP, CCI, CTCE, CBSP, SSBB

Zero Friction LLC

+1 202-780-5455

tphan@zerofriction.io

@ChainOpSec

https://www.linkedin.com/in/tuanphan/

ZERO FRICTION