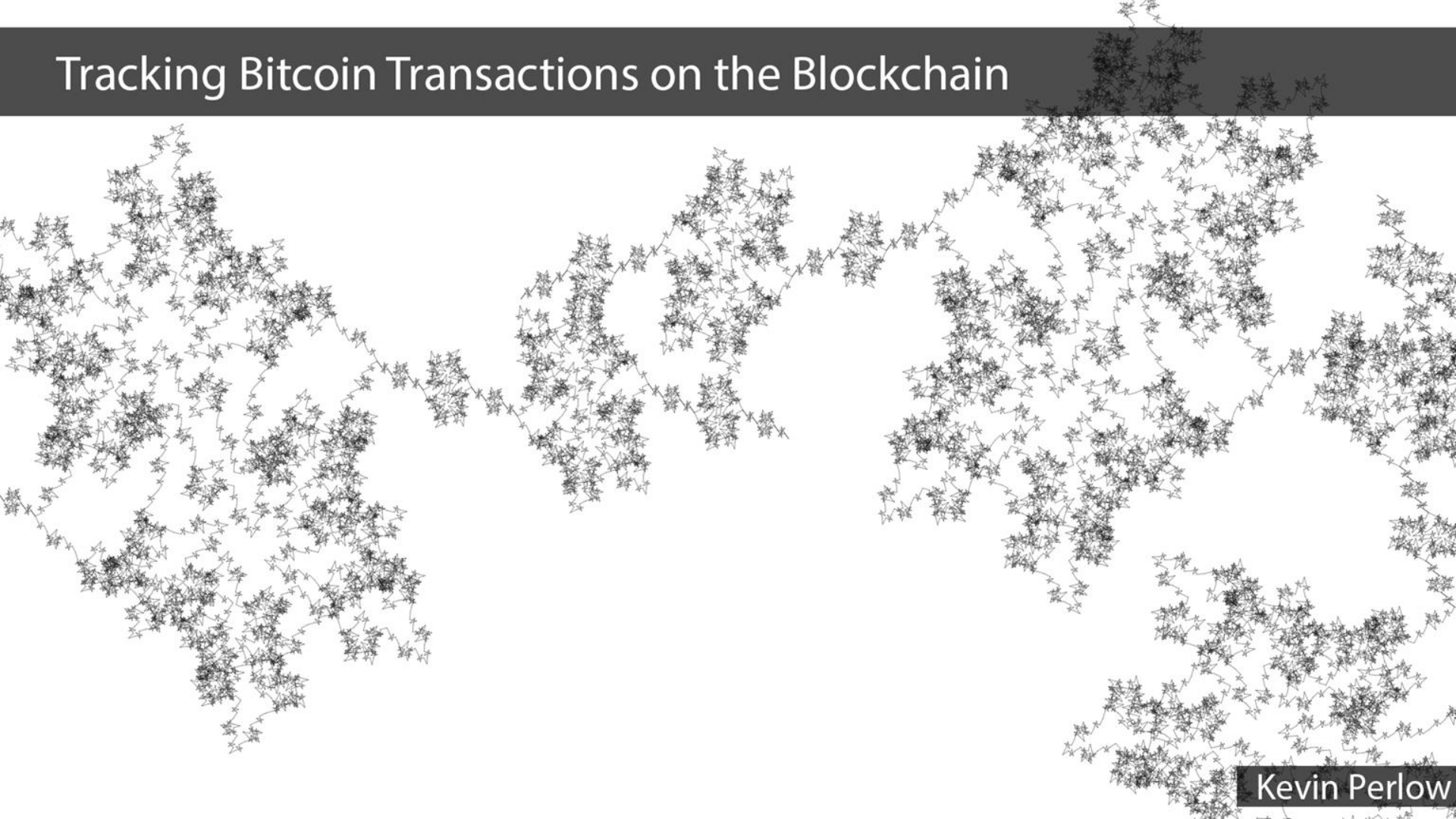
Tracking Bitcoin Transactions on the Blockchain



Kevin Perlow

About Me

- **Booz Allen Hamilton (2015- Present)**
  - Cyber4Sight- TechINT Lead
  - Malware analysis
  - Threat Hunting and Network Forensics

- **Georgetown University**
  - McDonough School of Business (2013)

- DFIR Netwars Champion (SANS CDI 2016)
- Spoke at SANS DFIR in 2016 on YARA rules/VT
  - https://www.youtube.com/watch?v=DdkLY99HgAA

Setting the Stage

What is ~~the~~ a blockchain?

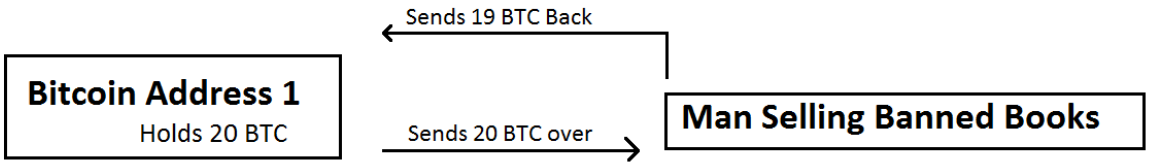
- Public, decentralized ledger
- Consists of a “block” holding transaction batches
  - Hashed and timestamped
  - New transactions broadcast to and collected by nodes in a block, each block holds a hash of the previous block
  - Uses include medical records, currency, DNS

Bitcoins and *the* Blockchain

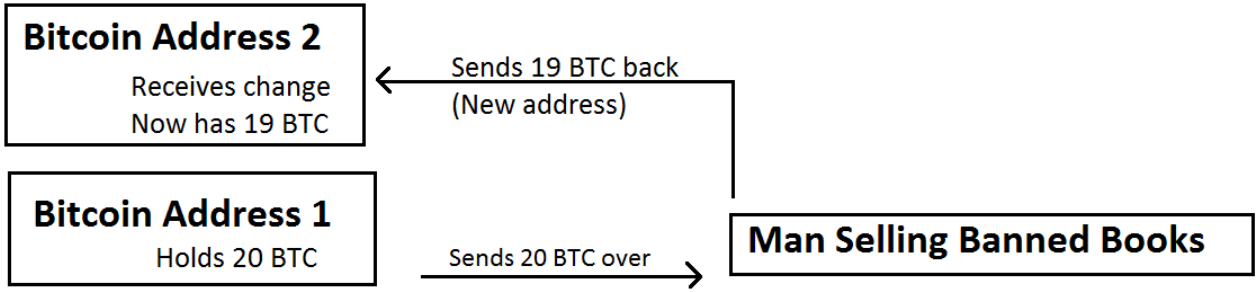
- Released in 2009
- **Wallet** contains **Addresses**
  - Receive money, **change** via address
  - Entire address spent on transaction
  - Wallet configuration determines **change** address
    - *"We automatically generate a new address for you after every transaction you make … so that a third-party can not view all other transactions associated with your account simply by using a blockchain explorer to look-up an address they know to be yours."* - Coinbase

Bitcoin Transaction (With Change)

Option 1



Option 2



Tracking Bitcoin Transactions

Resources Needed

- `Blockchain.info`- record of all bitcoin transactions (bottom)
  - API
  - Search by address or by transaction ID
- `Wallet Explorer` (top right)
  - Collects transactions
  - With enough data, can associate addresses with wallets

Wallet [0008d526bc] (show wallet addresses)

Displaying wallet [0008d526bc], of which part is address 12p2CcaDixL2FCMBzxzfMhPwufMohDbTmH. Show only address 12p2CcaDixL2FCMBzxzfMhPwufMohDbTmH

Page 1 / 80 Next... Last (total transactions: 7,956) Download as CSV

date	received/sent	balance	transaction
2016-10-24 09:34:51	-100. [4b1f425079] -0.01148369 [19d4b3a5e2] (-0.00360753) fee	0.	4ff8eec8157c1d47e6f1…
2016-10-24 07:47:39	[13435fbea3] +4.	100.01509122	3066094fda5409e9ab3c…
2016-10-22 08:52:09	-1.949935 [00003c94f6] -0.01004696 [10e97bc5ca] (-0.00061065) fee	96.01509122	fc779ed6f0db7b85cc04…
2016-10-22 06:45:23	[814919cd41] +0.00030031	97.97568383	6af5af38513eee73b26d…
2016-10-22 03:24:07	[1d3f1ed903] +2.5	97.97538352	0b391530030aa8da5bd7…
2016-10-22 01:04:35	[a3ffc1d7b9] +3.	95.47538352	8b5efa576fb5cf4a355c…
2016-10-21 21:27:14	[00306639fa] +1.	92.47538352	253d5a96f91a01131996…
2016-10-21 18:59:07	[002161f3b9] +3.	91.47538352	a4aed6820d807df27545…
2016-10-21 16:23:24	[853cc010cd] +0.0003	88.47538352	ae5f59bdb8834b0e9009…
2016-10-21 15:58:40	[83e61330d3] +0.00002449	88.47508352	d60e26942fad45d85c3e…
2016-10-21 15:58:40	[853cc010cd] +1.99972691	88.47505903	3bdc8c55986e98165376…
2016-10-21 12:24:54	[01745246b0] +0.01542552	86.47533212	5eb9260fc2504ed29924…
2016-10-21 08:51:56	[3573ac0620] +0.75	86.4599066	a44481eccc3e436d9c25e…
2016-10-21 02:53:59	[002161f3b9] +3.	85.7099066	4a11345f10b02fb847c6…
2016-10-20 17:34:46	[ea32f72c60] +3.	82.7099066	f57b37c01ed915a9b9f5…

69affd84d73a7bbf644fe9defa18bab740b76487c07b636a6bb4a50689d8e8e3 **2016-09-06 06:32:03**

1Q1ifiCyTtoYsrq2MQjZqpHSFREDTteE8E → 17JuZi7GfqPdARPL341WUuy1gqqkLzy5AX 12.9992882 BTC
16YhEbMcksa6zgf2rjcAUWy7fZ9TkgFNXF 500 BTC

-80 BTC

Start Simple- Globe Ransomware

GLOBE

Your files are encrypted!

Your personal ID

Redacted

Your documents, photos, databases, important data were encrypted.
Data recovery is required decipherer.
To get the interpreter should send an email to frogobigens@india.com .
Next, you need to pay for the interpreter. In a response letter you will receive the address of Bitcoin-wallet to which you want perform the transfer of funds in the amount of 1.5 Bitcoin .

MalwareHunterTeam
@malwrhunterteam
Follow

Replying to @struppigel

Maybe this is the new version?
Also, the email frogobigens@india.com was used in Xorist before.
@BleepinComputer @demonslay335

суббота, 8 октября 2016 г.

Globe, Globe2

Globe2 Ransomware
(шифровальщик-вымогатель)

Как удалить? Как расшифровать? Как вернуть данные?
По ссылке выберите Управление "К" МВД России и подайте онлайн-заявление.
См. также статьи УК РФ:
ст. 272 "Неправомерный доступ к компьютерной информации"
ст. 273 "Создание, использование и распространение вредоносных компьютерных программ"

`frogobigens@india[.]com`- Has been used in newer campaigns

Tracking Globe Instance

1HyasSC2VifTZo7YkUNn33udnWXw3Ffq7T

Summary	
Address	1HyasSC2VifTZo7YkUNn33udnWXw3Ffq7T
Hash 160	ba35944be5af594c9b2b07c37e789fa16063e3ef
Tools	Related Tags - Unspent Outputs

Transactions		
No. Transactions	434	
Total Received	67.41793 BTC	
Final Balance	0.00011356 BTC	

Possible Ransom Payments (Not full list):

883e0925ae31b7aef0fbd790501fa825ef5dd2f1351306af31fcb69f01f191a0 — 2016-12-01 17:54:35

1Hb1iKSw1ycazDVokPxemmxgjUMdesjttL → 1HyasSC2VifTZo7YkUNn33udnWXw3Ffq7T — 1.5 BTC

1.5 BTC

c4312ae1428a4d707209a7f305165d4f4668994c388c896a67f1f55f0cfbf2a6 — 2016-12-07 10:20:18

1CskWraRF2yBfD7rt3YFLjk3EKoHcqf8Gm → 1HyasSC2VifTZo7YkUNn33udnWXw3Ffq7T — 1.5 BTC

1.5 BTC

Tracking Globe (2)

Wallet [2b875a1640] (show wallet addresses)

First Previous... Page 3 / 5 Next... Last (total transactions: 430)

date	received/sent		bal
2016-10-30 11:52:50	[3a44188852]	+0.01700375	0.018
2016-10-28 06:13:00		-0.0279 (-0.0002057) [1d7b9c6187] fee	0.00
2016-10-28 06:13:00	[48ef654a1c]	+0.00005087	0.02
2016-10-28 06:06:27	[fbfdf0837b]	+0.00600681	0.02
2016-10-27 10:12:11	[8476e2d2ee]	+0.02230006	0.02
2016-10-25 05:56:41		-0.0356 (-0.0002871) [000001e522] fee	0.00
2016-10-25 05:08:27	[000126aaca]	+0.02206479	0.03
2016-10-23 09:08:14	[48ef654a1c]	+0.00026679	0.01
2016-10-23 08:27:44	[4bca1e64cb]	+0.01264446	0.01
2016-10-22 23:30:15	[00022feb0d]	+0.00135507	0.00
2016-10-22 06:52:00		-0.03617 (-0.0005313) [000001e522] fee	0.00
2016-10-22 06:52:00	[606a1a4b86]	+0.01221423	0.03
2016-10-21 05:46:33	[6998801c98]	+0.01335392	0.02
2016-10-20 11:57:12		-1.0357 (-0.0002057) [e8c064bf99] fee	0.01
2016-10-20 11:57:12	[46486591ca]	+1.	1.04
2016-10-20 06:05:18	[9717b82649]	+0.04614472	0.04

A	B	C
date	received from	received amount
5/26/2017 22:54	d1186b405e50afff	1
5/5/2017 20:19	9190bec89d842e7e	0.8
4/23/2017 19:54	224071e0986144a1	2
4/20/2017 17:12	0630c746c4e64d7b	0.59
4/19/2017 20:52	008e41ad8a8678fe	1.5
4/18/2017 15:20	20199cd4ebe81bb1	1.5
4/18/2017 9:47	000001e522b362b7	0.75
4/12/2017 19:59	7543255a634e11d0	0.4
3/25/2017 0:15	a0fdf9be68e86b22	0.5
3/16/2017 2:26	000157508216dee7	1
3/14/2017 7:44	d746e04cce1a1c1d	2
2/21/2017 20:47	0437a4ebe5055c1d	1.2
2/21/2017 6:17	4a34875678e7433a	1.5
2/9/2017 15:17	ab19978551549617	0.4
2/7/2017 22:41	8d1e9d54fe571569	1.5
1/30/2017 12:46	02615d4725b5585c	1
1/12/2017 2:11	af91bf4ea04f29d5	1.5
1/3/2017 14:00	1833da3fe89b2a71	1.5
12/29/2016 17:01	0a64e72cae98bcfc	1.5
12/28/2016 16:57	3ced56c5201ff754	1.5
12/13/2016 23:25	1e84f976e5fe01e1	1.5
12/7/2016 17:37	32f1d5d3779c3ea9	1.5
12/7/2016 10:21	82c89645ac90e0d9	1.5
12/1/2016 18:08	d06ae32a21a1d091	1.5
11/29/2016 18:24	fdbbee718a00661e	1.5
11/15/2016 21:20	897bf15b82b15760	1.5
10/20/2016 11:57	46486591cabfc1ae	1
10/17/2016 21:19	f04ed191f21deba0	1.5
10/11/2016 17:20	0965a6f25e56fe0a	1
10/10/2016 11:39	676695cbb78064cf	0.25
9/3/2016 7:51	31725ad7f995d90a	1.5
9/2/2016 15:17	0001d2e72691ea9d	1
8/30/2016 11:58	0d25bb944a45662a	1
8/27/2016 17:57	4bf8e5bc9dde6a10	1
8/21/2016 13:47	e52da7215bd36ae1	1
8/21/2016 10:11	6f688ad3a78157ff	1
8/4/2016 18:34	25223bdc09a91dde	1

Total "Possible" Ransom Income
43.89

Total "Probable" Ransom Income
24

- Identify Wallet
- Export Data
- Identify Payments
- Cash outs?

Globe- Takeaways

- Actor provided BTC address via email
- Actor used same BTC address for personal transactions
  - Somewhat atypical
  - Cash-outs not immediately obvious

Example 2- Locky [Scale]

Transactions (Oldest First) Filter

275937c2c30fbdf778390cb33a1ca1236c824c26a0a89af34e540c18d692d648 2016-08-29 11:38:30

178HGmCfR26dSSiFxJQah1U588p2CjgX7f → 1Q1ifiCyTtoYsrq2MQjZqpHSFREDTteE8E 80 BTC
12p2CcaDixL2FCMBzxzfMhPwufMohDbTmH 0.01000307 BTC

-3 BTC

d873345c1aecbaee3333fbab8a03ad0900cd37bbc0fca1884e211de85f970db9 2016-08-29 05:49:32

33Ypk7PMwf7pJzTQ4wzgaN27MwHDqMWSpC
37iBN9HDzzU2xcoq8ajLjFostAuDzLY2Ec
33BJxctd6xKj39BHPztyESuexRSKyesY7X

Locky "victim"

178HGmCfR26dSSiFxJQah1U588p2CjgX7f 3 BTC

Payment address, per Locky ransom .onion page

3 BTC

-Money Sent to a Locky address (`178HGmCfR26dSSiFxJQah1U588p2CjgX7f`)
-Locky address then moves that money to “1Q1” and “12p2” addresses
-Bigger Wallet? Let’s “map out” an address

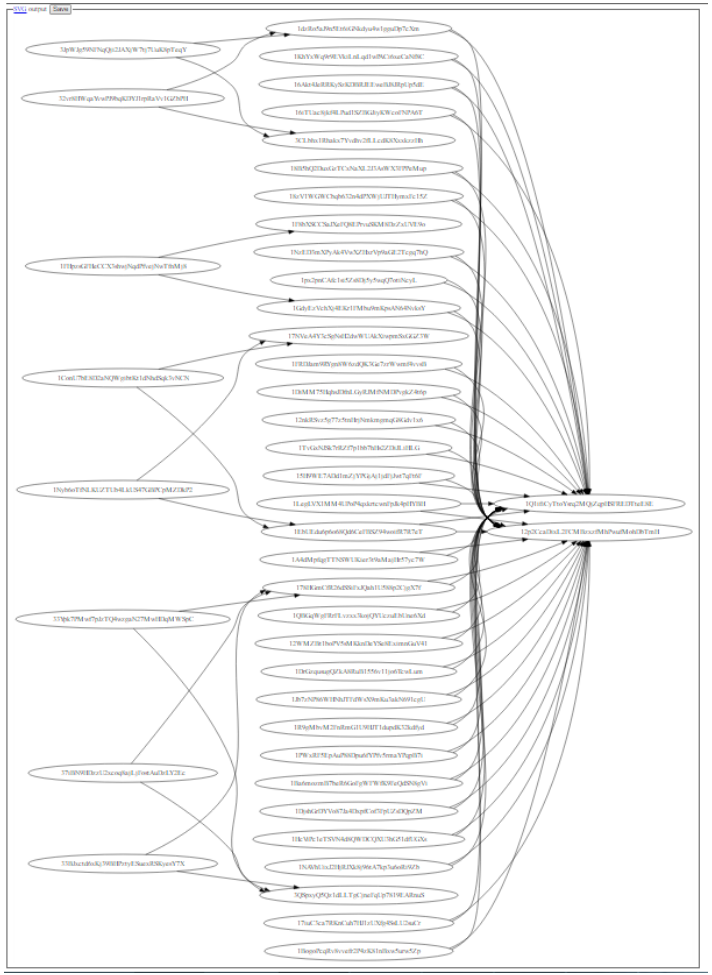
Example 2- Locky (2)

bitcoinmapping.py -

File Edit Format Run Options Window Help

```python
import json
import requests

z = 0
i = 0
firstpart = "https://blockchain.info/rawaddr/"
initialinput = input("please type the 'seed' address: ")
initialreq = firstpart + initialinput

firstjson = (requests.get(initialreq)).json()
graphvizlines = []

addresslist = []
usedaddresslist = []

addresslist.append(initialinput)
usedaddresslist.append(initialinput)

while i < 4:
    if z is 1:
        initialreq = firstpart + addresslist[i]
        firstjson = (requests.get(initialreq)).json()

    for transaction in firstjson["txs"]:
        payerlist = []
        recipientlist = []

        print("\n" + transaction["hash"])

        for item in transaction["inputs"]:
            payerlist.append(item["prev_out"]["addr"])
            if item["prev_out"]["addr"] not in addresslist:
                addresslist.append(item["prev_out"]["addr"])

        for target in transaction["out"]:
            recipientlist.append(target["addr"])
            if target["addr"] not in addresslist:
                addresslist.append(target["addr"])

        for payer in payerlist:
```

Ln: 12 Col: 0



https://github.com/kevinperlow/SANS-DFIR-2017

Example 2- Locky (3)

275937c2c30fbdf778390cb33a1ca1236c824c26a0a89af34e540c18d692d648 — **2016-08-29 11:38:30**

1GdyEzVchXj4EKr1FMbu9mKpsAN64NvksY	→	1Q1ifiCyTtoYsrq2MQjZqpHSFREDTteE8E — 80 BTC 12p2CcaDixL2FCMBzxzfMhPwufMohDbTmH — 0.01000307 BTC

-2 BTC

d528122807fd91e3b7250c8dd14641c5a61d60165ea50f70e566fbfa0142f4ee — **2016-08-22 17:52:33**

1FHpzsGFHeCCX3shwjNqdPfvejNwTfnMj8	→	1GdyEzVchXj4EKr1FMbu9mKpsAN64NvksY — 2 BTC

2 BTC

Example 2 - Locky (4)

Wallet [0008d526bc] (show wallet addresses)

Displaying wallet [0008d526bc], of which part is address 12p2CcaDixL2FCMBzxzfMhPwufMohDbTmH.

Page 1 / 81 Next... Last (total transactions: 8,021) Download as CSV

2017-01-26 19:08:08	[22e1162f9a]	+5.	88.48189315	75eaa4b6848821feb9c8...
2017-01-26 18:47:08	[935606826f]	+2.9995	83.48189315	fa88ea2459987e94f650...
2017-01-26 08:25:48	[cf1b316015]	+0.42954172	80.48239315	7463ff0313556d2389b4...
2017-01-26 03:00:01	[365a6c478e]	+4.	80.05285143	604f5ff51911e229e8fa...
2017-01-25 21:51:10	[e38599edd2]	+0.0001469	76.05285143	ba4e5c4184b628a41697...
2017-01-25 21:17:51	[e38599edd2]	+3.9998531	76.05270453	5b3dd39e0d014043500e...
2017-01-25 15:59:24	[52c616dcdb]	+3.	72.05285143	d559daa854fb45838a43...
2017-01-25 13:15:59	[2a4a6ed6eb]	+3.	69.05285143	403c9f3bd4e543d7331e...
2017-01-25 03:47:32	[c4ea0c0b39]	+4.	66.05285143	49f82f6df6e18e4a6654...

-Large number of “whole number” or “half” number transactions

-Activity started in February 2016, when Locky first gained steam

-!!!! There are 81 pages of this!!!!

Example 2 - Locky (5)

- Exported all 80 pages in October 2016
- **ONLY BTC input transactions divisible by .25** - 11,295.75 BTC (5410 victims)
- **Take BTC input transactions < 4 characters in length** - 13,677.22 BTC (6136 victims)
- **Take ALL received (they've never received > 10 BTC)** - 15,229.78 BTC (8313 victims)
- ***Somewhere between 11,000 BTC and 15,000 BTC from February 2016 through October 2016***

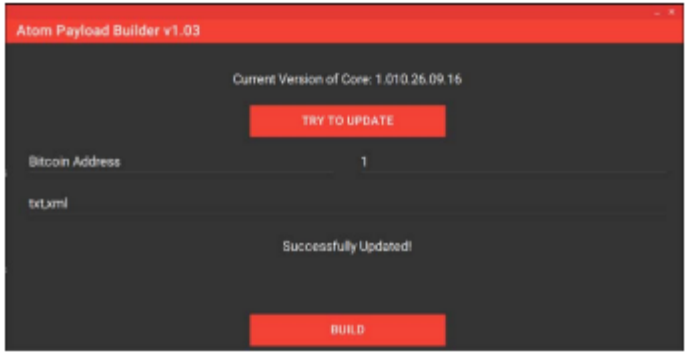
Example 2- Locky (6)

Cash-outs:

date	received from	received a	sent amount	sent to	balance
3/30/2016 7:38			220.01	BTC-e.con	146.1594
3/21/2016 8:18			213.29	BTC-e.con	84.05528
3/25/2016 9:05			207.2	BTC-e.con	147.9155
3/24/2016 8:09			203.7	BTC-e.con	239.4734
10/7/2016 18:19			200	ff96ddc43	20.60924
10/7/2016 18:19			200	ff96ddc43	20.60924
9/10/2016 14:45			200	a290ef9d9	56.03713
3/28/2016 8:16			179.2	BTC-e.con	143.9319
9/29/2016 15:35			170	3d635df25	27.88771
3/31/2016 8:16			156.1	BTC-e.con	179.8066
9/26/2016 4:39			150	63c6e86f3	121.6684
9/16/2016 19:10			150	a290ef9d9	57.19603
8/10/2016 13:48			150	17d3b063(	41.89273
4/29/2016 8:38			150	d0995a01c	86.56104
4/7/2016 11:18			150	9d996cace	48.54091
3/31/2016 8:58			150	002452c11	52.50276
3/10/2016 15:44			150	BTC-e.con	303.5281
4/4/2016 8:04			147	BTC-e.con	138.1819
4/1/2016 10:00			144.69	BTC-e.con	137.4983

Example 3- Shark/Atom [Attribution]

- Ransomware as a Service (RaaS)
  - 20% of collected ransom went to authors
  - Advertised on Russian website
  - Major OPSEC failure



Example 3- Shark/Atom (2)

BTC payment automatically split between the author and the “renter”

Transactions (Oldest First) Filter

83d4af3042bdaeb4632726b072009a25f235552b1afb9aa5d1bbe17fec2df339 2016-09-26 19:23:19

1J5FX1p6XFCenNyPkdt5NvJXcX3aWXXESB → 1D8gLLcPUENoVC6zoFuTsNpv1rEfrqCnqX 0.0798 BTC
1FzWxf1Ay6DYbJC6hY63CLiBtYpCZQFMf6 0.02 BTC

80/20 Split

20%, owned by authors

-0.1 BTC

e824089b79ffd3a74d3378fc2fce054151078df150488d57184ceb73f28e0784 2016-09-26 18:59:09

137yLAXkgXikiJbamGZRhKtC6h3KuL8N9d → 1J5FX1p6XFCenNyPkdt5NvJXcX3aWXXESB 0.1 BTC

Victim

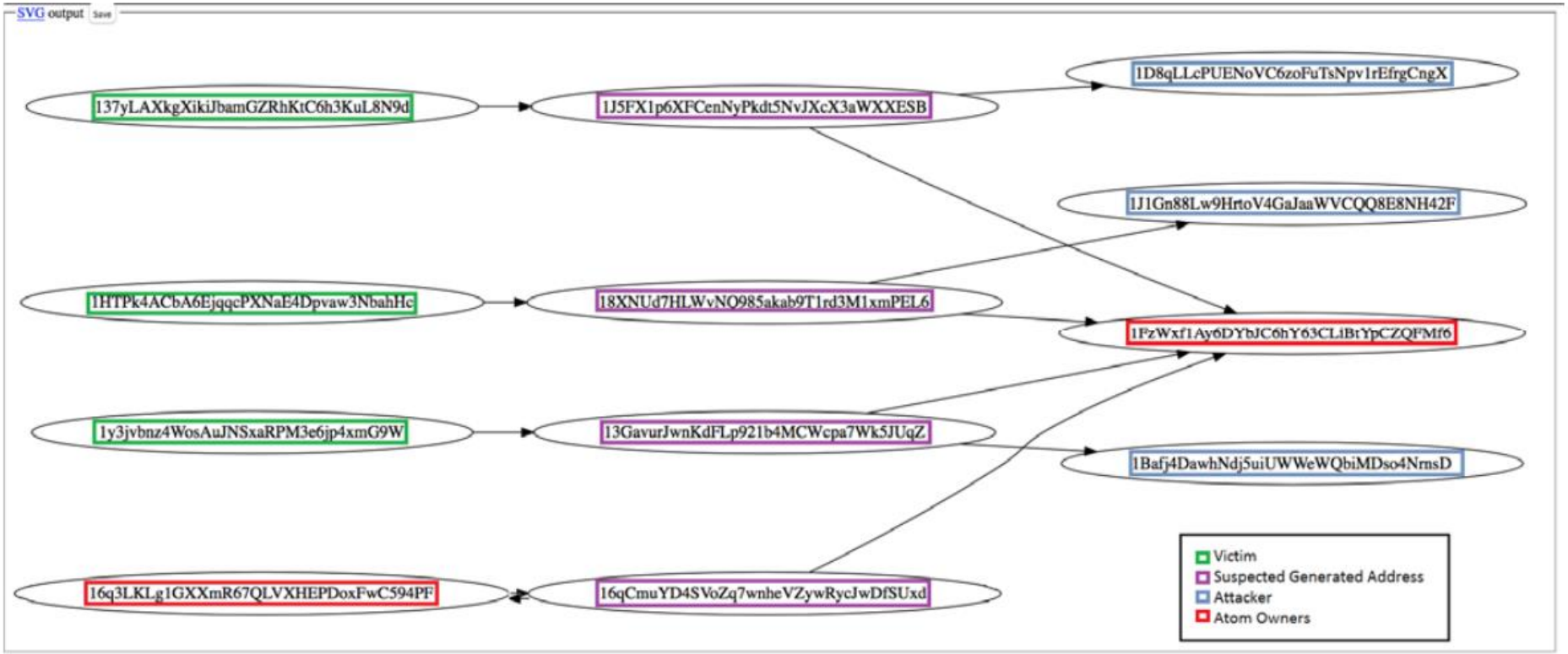
Payment Address

0.1 BTC

Author’s share went to `1FzWxf1Ay6DYbJC6hY63CLiBtYpCZQFMf6`

Example 3- Shark/Atom (2)

Other addresses sent the “cut” to the same “author” address



Example 3- Shark/Atom (3)

- What other addresses are associated with 1FzW?

Wallet [43ffccaec2] (show transactions)

Page 1 / 1 (total addresses: 2)

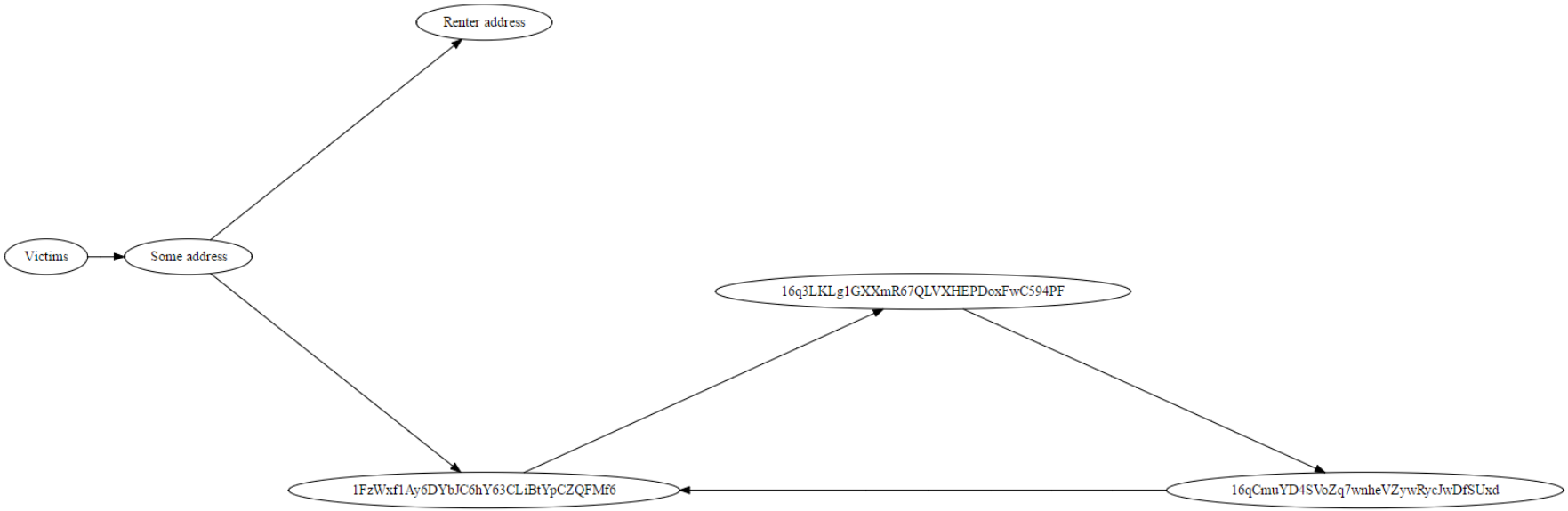
address	balance	incoming txs	last used in block
16q3LKLg1GXXmR67QLVXHEPDoxFwC594PF	0.010682	7	457787
1FzWxf1Ay6DYbJC6hY63CLiBtYpCZQFMf6	0.0028	6	453602

Page 1 / 1 (total addresses: 2)

Example 3- Shark/Atom (3)

- Another method using newer data (this is going to get tricky…)
  - We know who "owns" `1FzWxf1Ay6DYbJC6hY63CLiBtYpCZQFMf6`
  - First address ever to put money in `1FzW`: `16qCmuYD4SVoZq7wnheVZywRycJwDfSUxd`
  - First address ever to put money in `16qC`: `16q3LKLg1GXXmR67QLVXHEPDoxFwC594PF`
    - Which has also been paid by `1FzW`

Example 3- Shark/Atom (4)

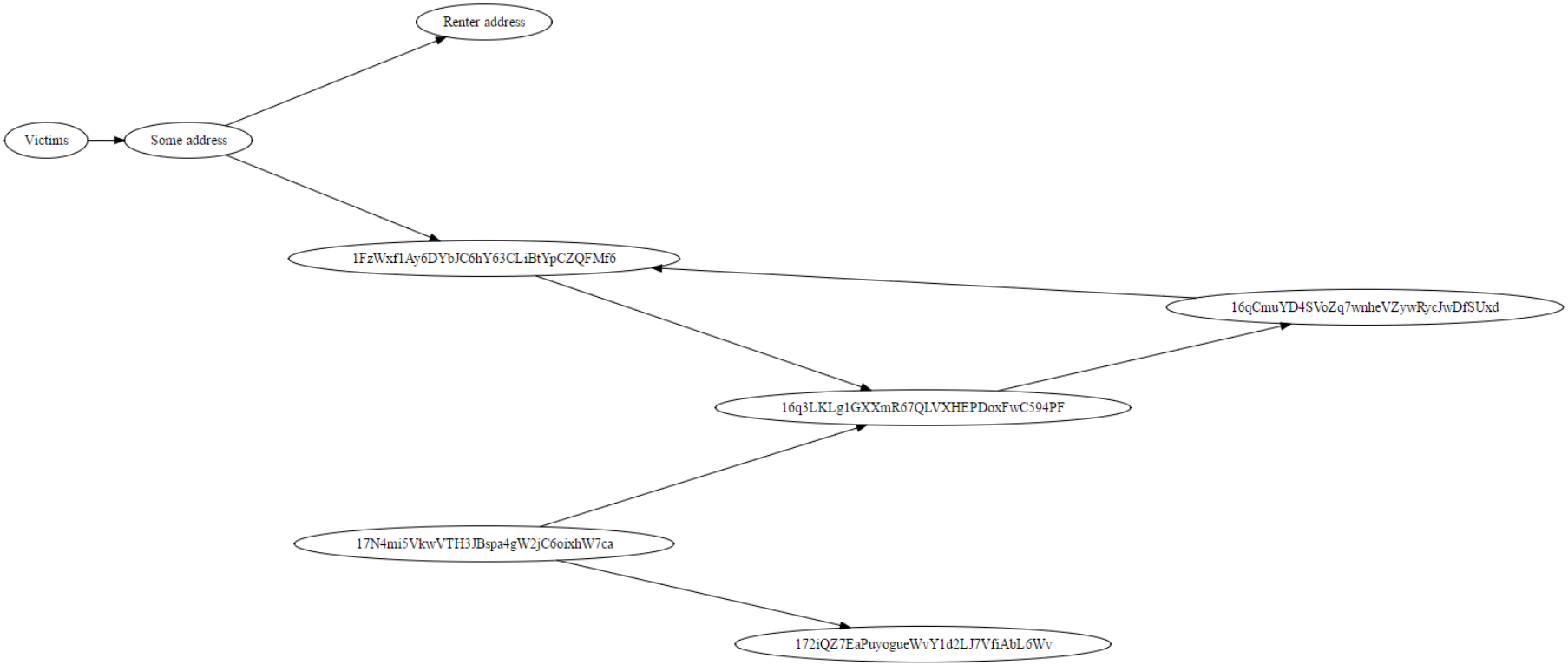


The same person who controls `1FzW` likely controls the other two addresses.

Example 3- Shark/Atom (5)

- First address to “fund” `16q3`?
  - `17N4mi5VkwVTH3JBspa4gW2jC6oixhW7ca`
  - Likely also owned by Atom author
- `17N5mi` also sent money to `172iQZ7EaPuyogueWvY1d2LJ7VfiAbL6Wv` in same transaction

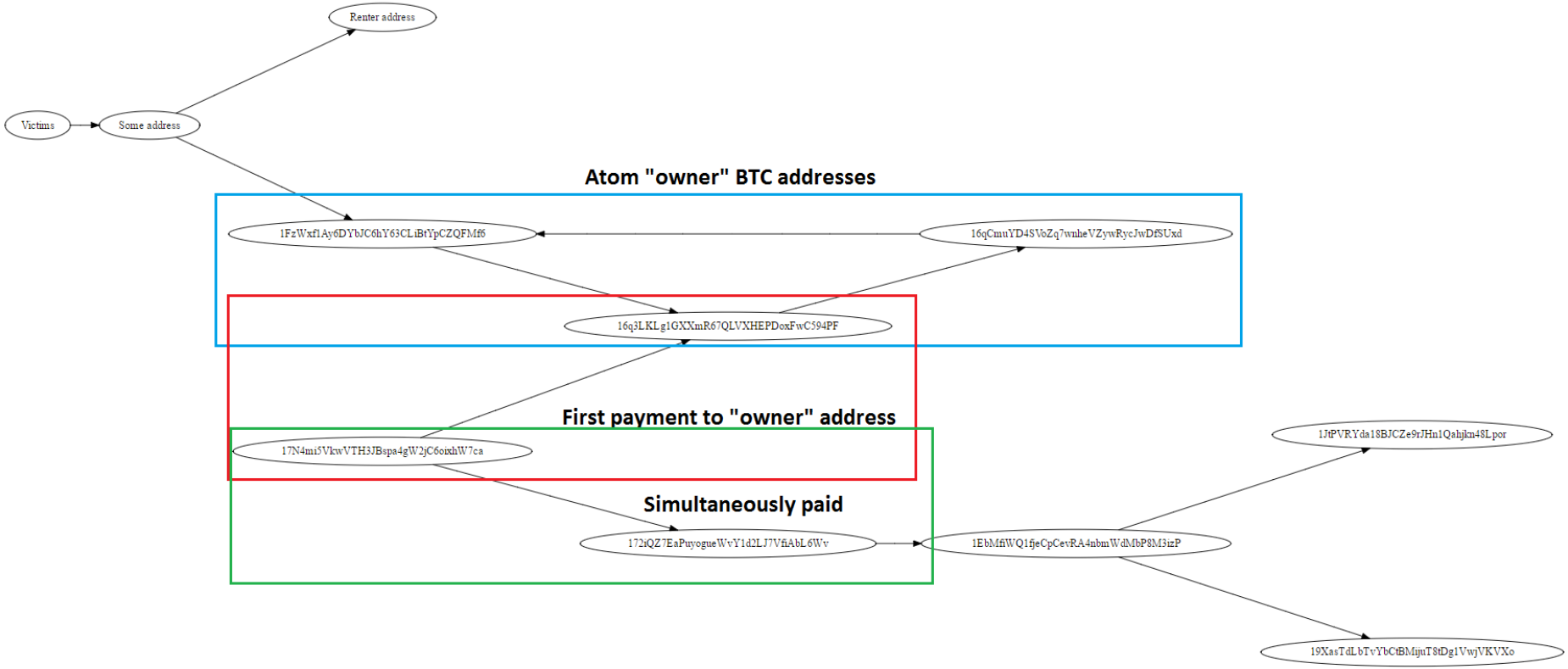
Example 3- Shark/Atom (6)



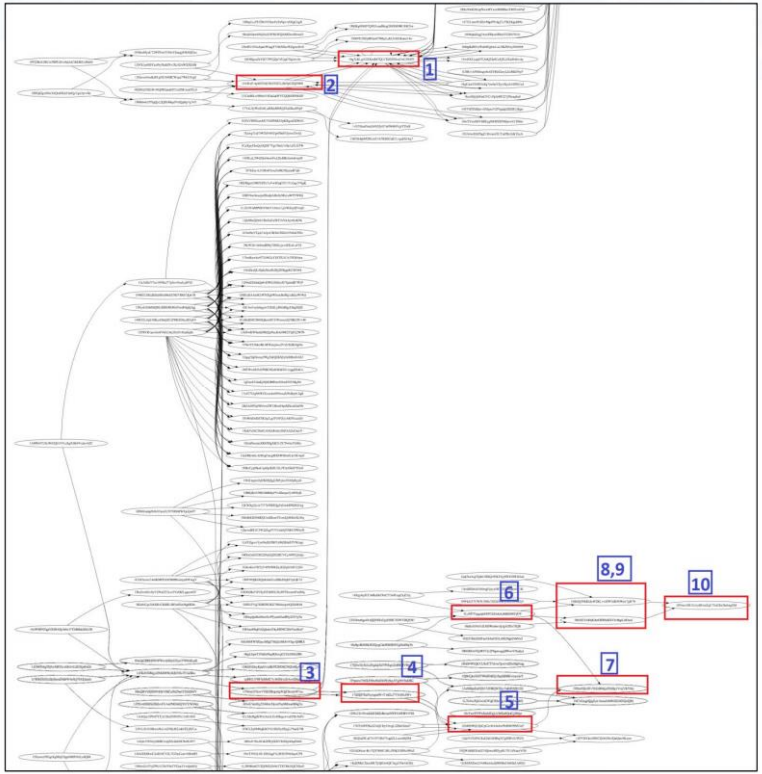
Example 3- Shark/Atom (7)

- *172iQZ7EaPuyogueWvY1d2LJ7VfiAbL6Wv* sends money to *1EbMfiWQ1fjeCpCevRA4nbmWdMbP8M3izP*, only transaction ever conducted.
- 1EbM's only "output" transactions at the time were to *1JtPVRYda18BJCZe9rJHn1Qahjkn48Lpor* and *19XasTdLbTvYbCtBMijuT8tDg1VwjVKVXo*

Example 3- Shark/Atom (8)



Example 3- Shark/Atom (9)

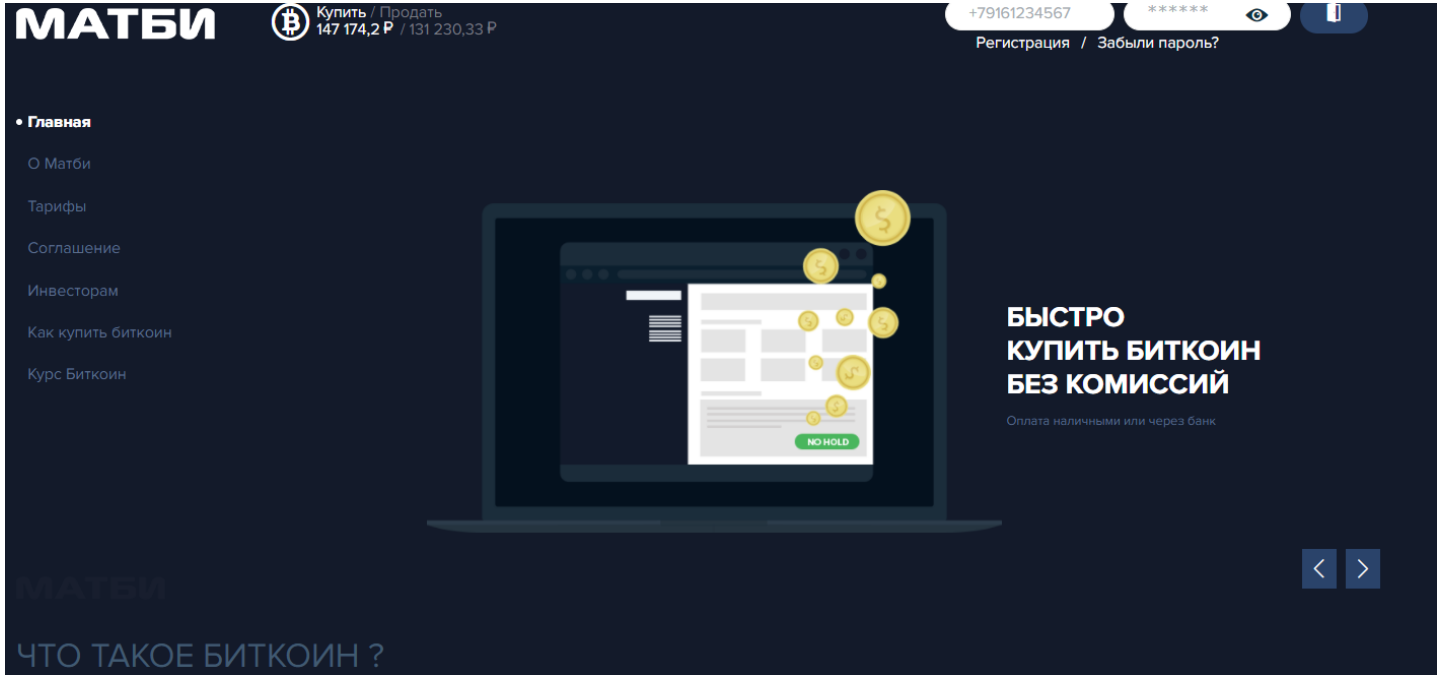


- Automatically generated graph of above
- Bottom right (7-10) are Matbea addresses
- Not enough to generate “answer” on its own, but saves time

Example 3- Shark/Atom (10)

Wallet Matbea.com (show wallet addresses)

Displaying wallet Matbea.com, of which part is address 19XasTdLbTvYbCtBMijuT8tDg1VwjVKVXo.



Bonus Example- Spora

```
push    offset aBeginRsaPrivat ; "-----BEGIN RSA PRIVATE KEY-----\r\n"
push    edi             ; lpString1
call    lstrcpyA
push    [ebp+hMem]      ; lpString2
mov     esi, lstrcatA
push    edi             ; lpString1
call    esi ; lstrcatA
push    offset aEndRsaPrivateK ; "-----END RSA PRIVATE KEY-----\r\n"
push    edi             ; lpString1
call    esi ; lstrcatA
mov     ebx, lstrlenA
push    edi             ; lpString
call    ebx ; lstrlenA
mov     edi, eax
add     edi, [ebp+var_10]
lea     eax, [ebp+SystemTime]
push    eax             ; lpSystemTime
call    GetLocalTime
movzx   eax, [ebp+SystemTime.wYear]
push    eax
movzx   eax, [ebp+SystemTime.wMonth]
push    eax
movzx   eax, [ebp+SystemTime.wDay]
push    eax
push    offset a02hu_02hu_04hu ; "%02hu.%02hu.%04hu|"
push    edi             ; LPSTR
call    wsprintfA
add     edi, eax
add     esp, 14h
lea     eax, [ebp+nSize]
push    eax             ; nSize
push    edi             ; lpBuffer
mov     [ebp+nSize], 101h
call    GetUserNameA
push    offset asc_403300 ; "|"
push    edi             ; lpString1
call    esi ; lstrcatA
push    edi             ; lpString
call    ebx ; lstrlenA
push    9               ; cchData
add     edi, eax
push    edi             ; lpLCData
push    7               ; LCType
push    400h            ; Locale
call    GetLocaleInfoA
push    offset asc_403300 ; "|"
push    edi             ; lpString1
call    esi ; lstrcatA
push    edi             ; lpString
call    ebx ; lstrlenA
add     edi, eax
push    offset aFdUtLs  ; "S$\bót\a{+=+%T"
push    edi             ; lpString1
call    esi ; lstrcatA
push    offset asc_403300 ; "|"
push    edi             ; lpString1
call    esi ; lstrcatA
push    edi             ; lpString
call    ebx ; lstrlenA
push    dword_405EA4
add     edi, eax
push    dword_405EA0
push    dword_405E9C
push    dword_405E98
push    dword_405E94
push    dword_405E90
push    offset aUUUUUU  ; "%u|%u|%u|%u|%u|%u"
push    edi             ; LPSTR
call    wsprintfA
add     esp, 20h
```

```
-----BEGIN RSA PRIVATE
KEY-----BwIAAACkAABSU0EyAAQAAAEAAQAr8ah5lDiqWZMdVRlf7+zS92vtQ97FZcHtRh/rJ
tEH6LaStR9yRityBr1MFBHBemtMeiCmqyLSrtByj9moO+jS59hNC69wa580MqZPsVxRftkPrJ
hwjcARf/bX0aGks3CBmJhQ7iVFmQyag2J50eKZgdL6yNxLbJkIHRSfhU4FqzXCrA2lIxOY3m2
ywSASOmpI3sryeeVo86r+VzDCmDafNjboUqlCXfTAz/f2nfsMSBKS7kvFO+lAtJgJ9z09leXf
UfUiFYwzgBiOHjQaxaMAAfU0eNAeN7dqXAcXPsKvOgbjZwlUEGPR8K5sNkRFEur7c9qPGgrf0
GCEmlQlBLO+NSa+ES1maMGytiZPGlFx7yYwmxm5210XTaO5hIlZD0qX8ru1ruWQR2qCDoFoHp
lBpKsYecTFYg7JfaPCdz61NjfZdGEZKqqyC10AWRDss0IE11/GdmjAhoBaKN7f6Qb58Nq3uYd
W3IN2trUCGZ51yGypBr1kjOrAFIuJTs03A74aIC1elbd7HO34xlNwC889hHgNvjUvqTeW+nO8
6vKv4YhXJRSGdW4PiS8rz0KjyKjgDQ7A40S2GS9Zljnui6Vu4RTE39SCOsv2ddF66VZaval9L
rmdCc1SeSa/98wpa522Zxv01pZrtYb2YNO3S6l6iNYz7oIULKaMmk8a2ytJG31ZFdikaU/cDc
aRLsWMKVZeyFPkn/LpqZdvB7ru9PZjdi2TQeFEobQmkHyM8y+gLJE2IeMZM7YOS1+nMZVVjSg
-----END RSA PRIVATE KEY-----12.01.2017|MAL|USA|D283C31972|0|0|0|2|9|61
```

```
push    edi             ; cchData
lea     eax, [ebp+LCData]
push    eax             ; lpLCData
push    7               ; LCType
push    400h            ; Locale
call    GetLocaleInfoW
movzx   ecx, byte ptr [ebp+var_18+2]
xor     eax, eax
mov     [ebp+var_34], ax
movzx   eax, byte ptr [ebp+var_18+1]
shr     ecx, 4
push    ecx
mov     ecx, eax
and     ecx, 0Fh
push    ecx
shr     eax, 4
push    eax
movzx   eax, byte ptr [ebp+var_18]
push    eax
lea     eax, [ebp+LCData]
push    eax
push    offset aS02x01x01x01x ; "%s%02X%01X-%01X%01X"
```

> AppData > Roaming

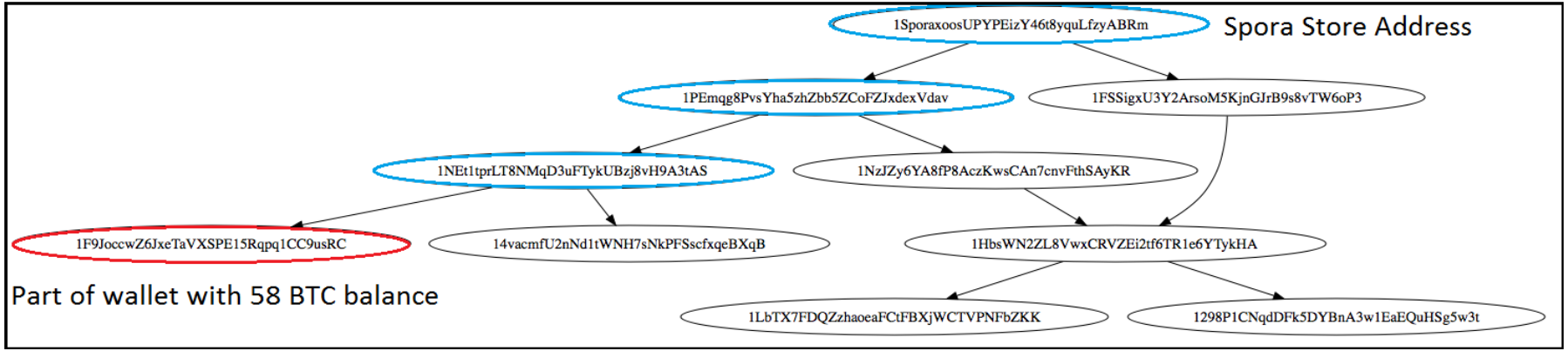
Name	Date modified	Type
Microsoft	12/23/2015 6:35 AM	File folder
4208964771	1/12/2017 5:21 AM	File
US0D0-CDZTZ-TZTRT-KTFXY.KEY	1/12/2017 7:28 AM	KEY File
winscp.rnd	12/22/2015 6:59 PM	RND File

Spora Store

- Initial version: needed to upload key file to Spora[.]biz
- Store is digitally signed with BTC address
- Store contains your payment address
- Address: `1SporaxoosUPYPEizY46t8yquLfzyABRm`

Bonus Example- Spora (2)

- Early on: able to show the actor possessed at least 58 BTC
  - Possible startup funding?
  - First ransoms?
- New activity shows a LOT of money moving in and out



Bonus Example- Spora (3)

318312db6505bb20a028520236ed47fb7676319f3e4a82d87bd20a31637f1adf (Fee: 0.00109986 BTC - 164.9 sat/B - Size: 667 bytes) 2017-02-28 12:29:41

185TLEuGBQiNh9fubeUkqDTotvuMzK36Yd (5 BTC - Output)
19JTkrLvwDmnTdowMekNzX6SHKxybK5CTq (5 BTC - Output)
14L7UxKJYCpTwRgmN4bwNunCGt2cvTqZhm (5 BTC - Output)
137zbLqMQjc96kYcEyPonpT442eWuuvKYK (5 BTC - Output)

1Mksbc9nYE6uXKLhN5J4h7mNZSk7QA1Vvm - (Spent) 0.80059898 BTC
142QvhE8nK4vCP2UsFM4JbR4j1YqnRvBV8 - (Spent) 19.19830116 BTC

-5 BTC

527770af4930cf07fcd7a14db440ce08a0eca0a250b3112bbbc9a6c366ba57cb (Fee: 0.00494499 BTC - 180.8 sat/B - Size: 2735 bytes) 2017-02-26 09:52:09

1AX2yGhcXuptKTQL7EhSEXqrczzo9mdric (0.082 BTC - Output)
1Jwv2HCEYRUPaUJkw89Jw1uVSwJr2p3cCU (0.19098 BTC - Output)
1ExtYUYgqPbNTTbDr3CegF5jw72wk4Vzxs (0.176 BTC - Output)
1MZ1CMrZtawziAtb8hWGT8PnK4xxuWKcDg (0.19 BTC - Output)
17J8rrR18duW3PWzu4oRXgZ4gf3jJ9extC (0.443849 BTC - Output)
1J5XgEcjB7q1B5tnv6WNcBRvCPwKeDwqu1 (0.19 BTC - Output)
1ASSf6B2r5mDcRTgurdghq4WsEUBHpNEnd (0.376 BTC - Output)
1FnKjKwmWwwVDZpmUDyXHTz94qv93zdJZ2 (0.19994621 BTC - Output)
1PWyxDgq7PTEUnzzmvwh1z1RLWb383J3AN (0.1995 BTC - Output)
16mPyh4RHu7NDH7RuPYAkLPK7vU5KsNf2z (0.37895 BTC - Output)
19yY4NvoVZNhVed2V5u8wxmdeDxNts3Qsf (0.2449 BTC - Output)
1HEMpfJ55h1K5YFfurRugvPMS89WZU1eat (0.389897 BTC - Output)
15HLwotXAA48EEbSxUFBrRpAAyuxQQvNJ6 (0.2189775 BTC - Output)
1MYbrUPBxBRRD4MizhZfWYuZyZZRkEoCKu (0.586658 BTC - Output)
1HJ1krFU2XVvJTxpYCiaCwK4AUefJZpoeS (0.19588 BTC - Output)
1NeD6fEmF5ZPqqJvhxkUkFcgqYt3k5a6vR (0.240266 BTC - Output)
1J6NQNzydpxdpTDpJqyPgUctqrsGvmMjCQ (0.51726156 BTC - Output)
1AE2caZoyJbEDVEfPNNyjCSwhvMA5YhaNN (0.19388 BTC - Output)

1ENWiqpCHqSfqikx7draY7uR1bNTGmSZrK - (Spent) 0.01000028 BTC
137zbLqMQjc96kYcEyPonpT442eWuuvKYK - (Spent) 5 BTC

5 BTC

Separately, the ransom payments (bottom left) get sent to addresses in batches (bottom right)

Bonus Example- Spora (4)

- Suspected affiliate program based on its blockchain properties
- Later corroborated by other research
- Follow the money: `137zbLqMQjc96kYcEyPonpT442eWuuvKYK`

Source: https://blog.cyber4sight.com/2017/01/blockchain-analysis-suggests-spora-ransomware-operates-via-affiliate-program/spora/

The Namecoin Bockchain

Namecoin (.Bit) Domains

- Decentralized blockchain for DNS records (Requires special DNS server or OpenNIC)
- Carries DNS records with transaction
  - New (registration fee, destroyed by transaction)
  - First Update
  - Update
- Functions as cryptocurrency
  - Domains get a special coin
  - This “special coin” property “flattens” part of the blockchain
  - Makes it easier to correlate IPs and domains
- Holds historical data- We can use to identify domains, timeline of campaign, other IPs

Shifu Banking Trojan

- Unit42 report- came out 6 January 2017
  - Shifu Banking trojan underwent update in 2016
  - Two domains (klyatiemoskali[.]bit, slavaukraine[.]bit)

Name d/slavaukraine (slavaukraine.bit)

Status	Active
Expires after block	358723 (15159 blocks to go)
Last update	2017-01-12 17:20:10 (block 322723)
Registered since	2016-06-03 20:43:10 (block 288981)

Operations

Date/time	Block	Transaction	Operation	Value
2017-01-12 17:20:10	322723	159c179a81...	OP_NAME_UPDATE	{"ns":["a.dnspod.com","b.dnspod.com","c.dnspod.com"]}
2017-01-11 20:45:33	322585	cc07584366...	OP_NAME_UPDATE	{"ip":["0.0.0.0"]}
2017-01-08 19:37:33	322040	925d5a6d6a...	OP_NAME_UPDATE	{"ip": ["192.52.166.149"]}
2016-11-05 15:29:32	312309	e3848b6d92...	OP_NAME_UPDATE	{"ip": ["103.199.16.106"]}
2016-06-03 20:43:10	288981	5c9adc978a...	OP_NAME_FIRSTUPDATE	{"ip": ["103.199.16.106"]}
2016-06-03 17:51:04	288965	bd78adb5a8...	OP_NAME_NEW	8771927dd4534d09c129605c26ace7b210dd068a

http://researchcenter.paloaltonetworks.com/2017/01/unit42-2016-updates-shifu-banking-trojan/

Shifu Banking Trojan (2)

Transaction

Bottom transaction from previous slide

Change, address used to make second domain (klyatiemoskali)

Transaction	bd78adb5a870bfdf2058556dbef91a330d37b5be029cfb4b9caf65c23ae7cdae		
NFbbTh2tH73pqVBYN3KLpBtJ85ReRuGuFa	24.1950952 NMC	>	N4Yjkm4pbrFS7sGehJG3SRXGGtPnxjQNXH 24.1650952 NMC
			NH9DNuTjddQ28W4X1dZwWSG2KrWimgM2te 0.02 NMC

Initial funding address- can we trace back?

Summary

Size	258 bytes
Block	288965
Total inputs	24.1950952 NMC (1 scripts)
Total outputs	24.1850952 NMC (2 scripts)
Fees	0.01 NMC

Name operation

Operation	OP_NAME_NEW
Name	d/slavaukraine
Hash	8771927dd4534d09c129605c26ace7b210dd068a

An address was used in a transaction that:
-Made d/Slavaukraine
-Made an address that made d/klyatiemoskali

What was this address used for previously?

Address NFbbTh2tH73pqVBYN3KLpBtJ85ReRuGuFa

Date/time	Transaction	Block	Debit	Credit	Balance
2016-06-03 17:51:04	bd78adb5a8...	288965	-24.1950952 NMC		0 NMC
2016-05-29 19:14:04	b0ab8493bd...	288285		24.1950952 NMC	24.1950952 NMC

Shifu Banking Trojan (3)

Transaction

Transaction b0ab8493bdc1b203f4439d1031e4d5b94a8c4a7505c1f85658c4d4f37acf837f

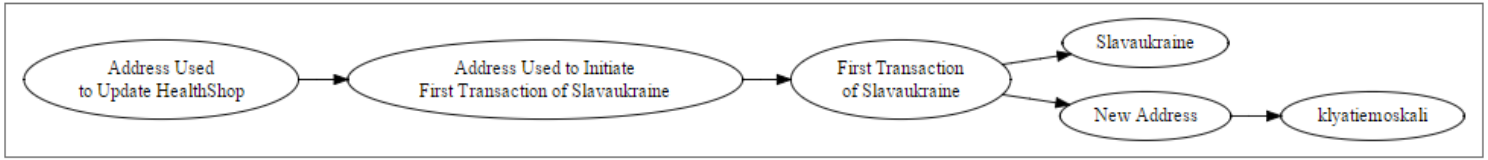
Mxnhkghr8LoAYcLWJt9RZdUbk31VuDhTbT	0.01 NMC	>	NFbbTh2tH73pqVBYN3KLpBtJ85ReRuGuFa	24.1950952 NMC
MwvRdncMBJgDDwv4YtzJ9QnkCtC6pJhcEH	24.2050952 NMC		NBwDuwi6LYV6fjSzm3gvUo64k48BM6RHwa	0.01 NMC

We've identified a new domain associated with addresses used to register and update known malicious domains based on blockchain proximity. Can we demonstate that this domain is likely owned by the same threat actors?

Name operation

Operation	OP_NAME_UPDATE
Name	d/healthshop

```
{
    "ip": [
        "87.120.37.85"
    ]
}
```



Shifu Banking Trojan (4)

Name d/healthshop

Operations

Date/time	Value
2017-01-11 20:45:33	{"ip":["0.0.0.0"]}
2017-01-08 22:08:34	{"ip":["192.52.166.149"]}
2016-12-10 22:20:00	{"ip":["103.199.16.106"]}
2016-12-01 15:35:28	{"ip": ["103.199.16.106"]}
2016-11-05 15:29:32	{"ip":["87.120.37.85"]}
2016-05-29 19:14:04	{"ip":["87.120.37.85"]}
2016-05-23 16:31:08	{"ip":["87.120.37.85"]}
2016-05-22 16:13:59	0c5ebaa3db71c6b83609273267d1facd92309805

Name d/slavaukraine

Operations

Date/time	Value
2017-01-12 17:20:10	{"ns":["a.dnspod.com","b.dnspod.com","c.dnspod.com"]}
2017-01-11 20:45:33	{"ip":["0.0.0.0"]}
2017-01-08 19:37:33	{"ip": ["192.52.166.149"]}
2016-11-05 15:29:32	{"ip": ["103.199.16.106"]}
2016-06-03 20:43:10	{"ip": ["103.199.16.106"]}
2016-06-03 17:51:04	8771927dd4534d09c129605c26ace7b210dd068a

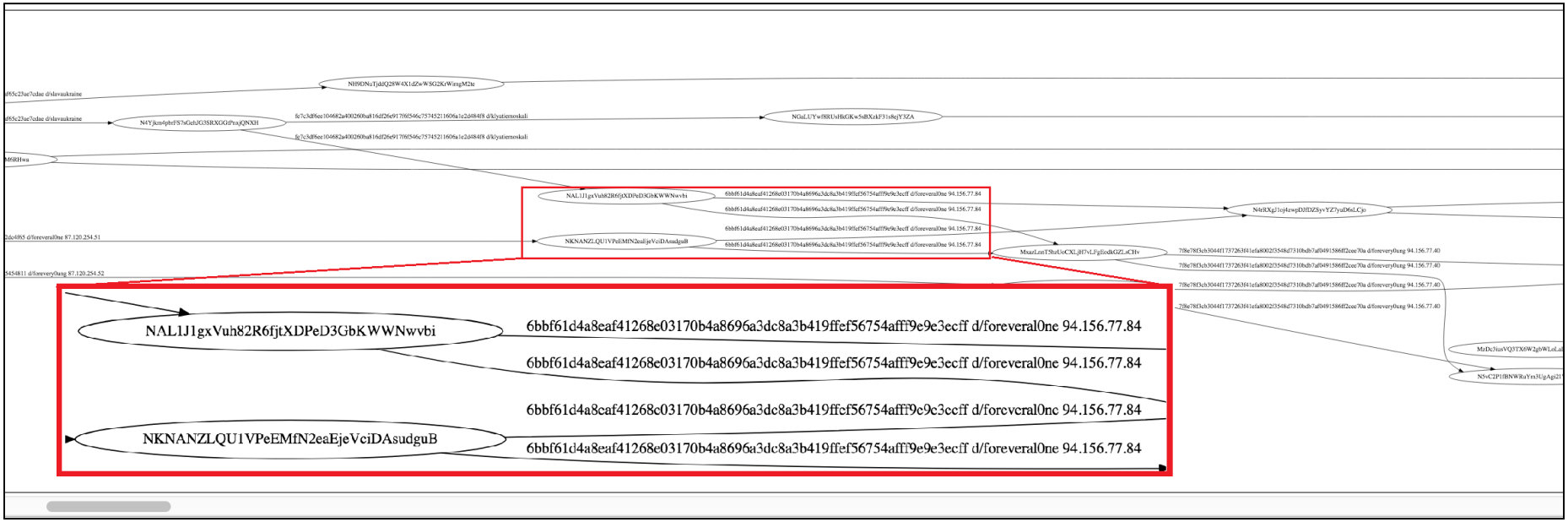
These two .bit domains have shared the same IP, were both updated and zeroed out at the same time, and are associated on the blockchain.

New IOCs! What happens if we map out the rest of the Namecoin chain?

Shifu Banking Trojan (5)

- Namecha.in
  - No API, you're on your own for a script
  - The script should:
    - Capture IP info
    - Capture domain info
    - Associate transactions and addresses
  - Remember, this is a *flatter* blockchain

Shifu Banking Trojan (6)



- Did my best to zoom in, but clearly graphing this isn't *quite* enough
- We need to output some data to CSVs
  - Timeline
  - Infrastructure

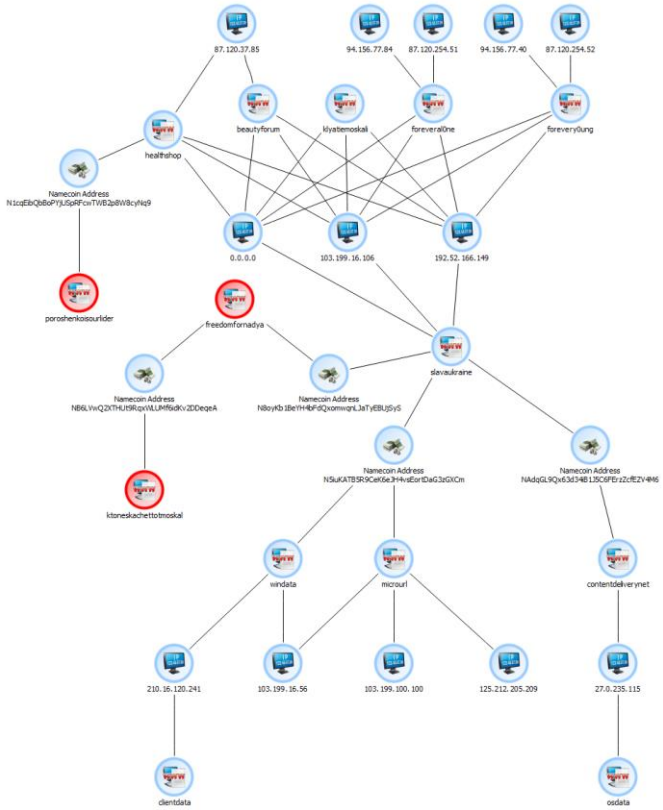
13	d/beautyforum	103.199.16.106
14	d/foreveral0ne	103.199.16.106
15	d/foreveral0ne	103.199.16.106
16	d/forevery0ung	103.199.16.106
17	d/forevery0ung	103.199.16.106
18	d/healthshop	103.199.16.106
19	d/healthshop	103.199.16.106
20	d/klyatiemoskali	103.199.16.106
21	d/klyatiemoskali	103.199.16.106
22	d/slavaukraine	103.199.16.106
23	d/slavaukraine	103.199.16.106
24	d/microurl	103.199.16.56
25	d/microurl	103.199.16.56
26	d/windata	103.199.16.56
27	d/windata	103.199.16.56
28	d/microurl	125.212.205.209
29	d/microurl	127.0.0.1
30	d/microurl	127.0.0.1
31	d/microurl	127.0.0.1
32	d/microurl	127.0.0.1
33	d/windata	127.0.0.1
34	d/windata	127.0.0.1
35	d/windata	127.0.0.1
36	d/windata	127.0.0.1
37	d/clusterdata	127.0.1.1
38	d/clusterdata	127.0.1.1
39	d/beautyforum	192.52.166.149
40	d/foreveral0ne	192.52.166.149
41	d/forevery0ung	192.52.166.149
42	d/healthshop	192.52.166.149

We can now show that different domains on 103.199.16.106 are related to domains on 192.52.166.149, even if they only used one of the two IPs

Similar IP Space

1	d/microurl	3/29/2016
2	d/microurl	3/29/2016
3	d/microurl	3/29/2016
4	d/microurl	5/20/2016
5	d/healthshop	5/22/2016
6	d/beautyforum	5/22/2016
7	d/healthshop	5/23/2016
8	d/healthshop	5/23/2016
9	d/beautyforum	5/23/2016
10	d/beautyforum	5/23/2016
11	d/windata	5/23/2016
12	d/windata	5/23/2016
13	d/windata	5/23/2016
14	d/foreveral0ne	5/28/2016
15	d/forevery0ung	5/28/2016
16	d/healthshop	5/29/2016
17	d/foreveral0ne	5/29/2016
18	d/foreveral0ne	5/29/2016
19	d/forevery0ung	5/29/2016
20	d/forevery0ung	5/29/2016
21	d/slavaukraine	6/3/2016
22	d/slavaukraine	6/3/2016
23	d/slavaukraine	6/3/2016
24	d/klyatiemoskali	6/3/2016
25	d/klyatiemoskali	6/3/2016
26	d/klyatiemoskali	6/3/2016
27	d/foreveral0ne	6/4/2016
28	d/forevery0ung	6/4/2016
29	d/microurl	10/17/2016
30	d/windata	10/17/2016

Shifu Banking Trojan (8)



Identified Domains:

- d/slavaukraine
- d/healthshop
- d/klyatiemoskali
- d/contentdeliverynet
- d/foreveral0ne
- d/clientdata
- d/forevery0ung
- d/beautyforum
- d/freedomfornadya
- d/microurl
- d/windata
- d/osdata
- d/ktoneskachettotmoskal
- d/clusterdata

Quick Recap

- Blockchain technology stores a LOT of data
- We can track and correlate this data
  - Monetary transactions
  - Domains
  - Property??
  - Medical records??
- Questions?