# WANNACRY 2.0

*WannaShift to Monero*

powered by NEUTRINO

## Intro

In March and May 2017 thousands of PC worldwide were infected by the ransomware known as Wannacry. In particular the second wave, known as Wannacry 2.0, infected thousands of machines worldwide including hospitals and enterprises. A bitcoin payment was asked to decrypt the files: on August 3rd, the Wannacry group started moving the funds.

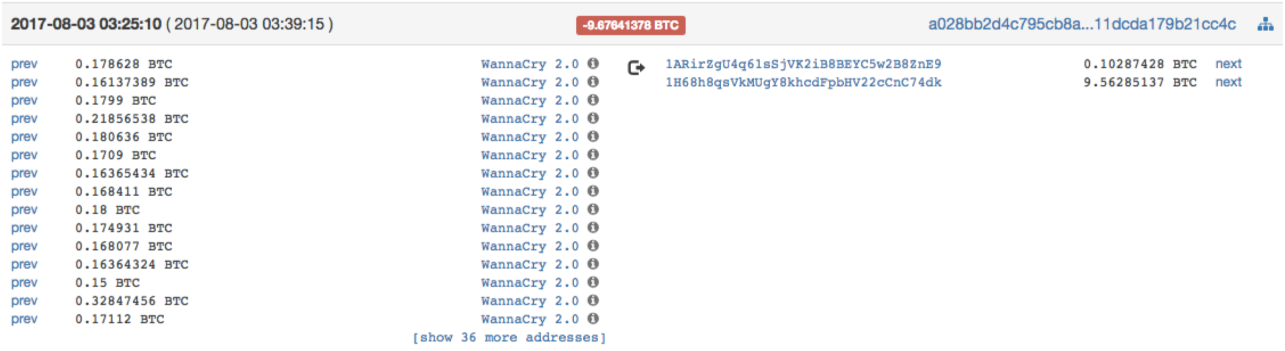
## Analysis

Three bitcoin addresses were identified as belonging to the Wannacry 2.0 used to receive the ransom payments:

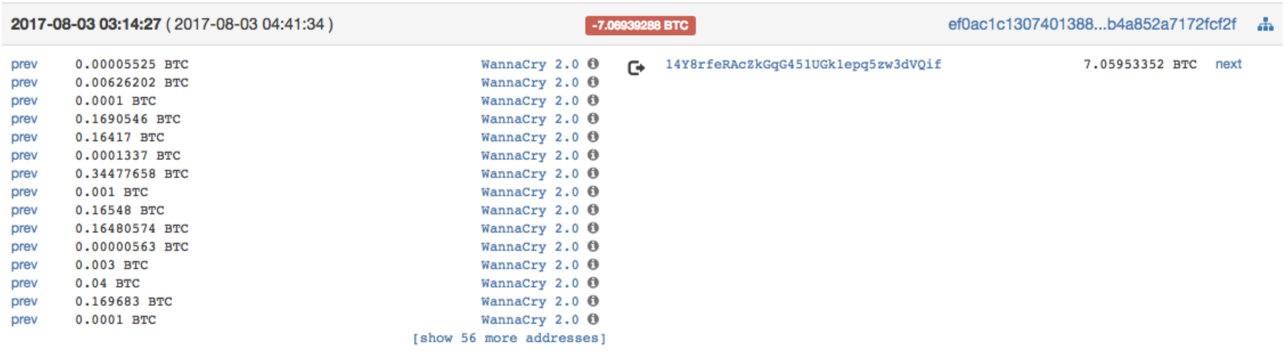
- 13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94
- 115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn
- 12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

A total of 333 incoming transactions for a total of almost 51.93 BTC was collected.

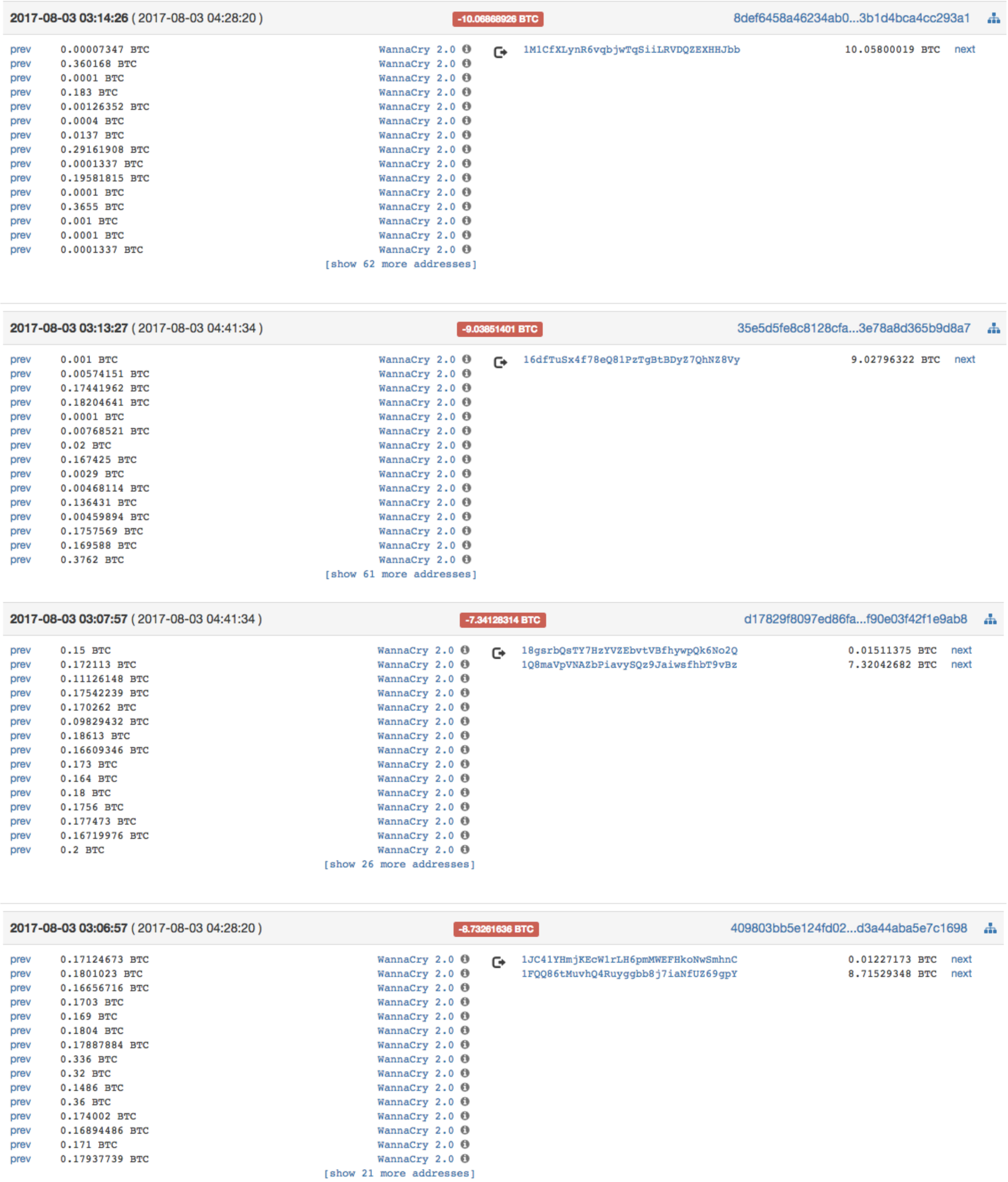
On 03/08, h. 3:06 UCT, a first outgoing transaction was registered on the blockchain. The transaction moved 8.73 BTC; the wallet was emptied in a few hours in five additional transactions.



```
2017-08-03 03:25:10 ( 2017-08-03 03:39:15 )          -9.67641378 BTC          a028bb2d4c795cb8a...11dcda179b21cc4c

prev   0.178628 BTC                WannaCry 2.0   1ARirZgU4q61sSjVK2iB8BEYC5w2B8ZnE9   0.10287428 BTC   next
prev   0.16137389 BTC              WannaCry 2.0   1H68h8qsVkMUgY8khcdFpbHV22cCnC74dk   9.56285137 BTC   next
prev   0.1799 BTC                  WannaCry 2.0
prev   0.21856538 BTC              WannaCry 2.0
prev   0.180636 BTC                WannaCry 2.0
prev   0.1709 BTC                  WannaCry 2.0
prev   0.16365434 BTC              WannaCry 2.0
prev   0.168411 BTC                WannaCry 2.0
prev   0.18 BTC                    WannaCry 2.0
prev   0.174931 BTC                WannaCry 2.0
prev   0.168077 BTC                WannaCry 2.0
prev   0.16364324 BTC              WannaCry 2.0
prev   0.15 BTC                    WannaCry 2.0
prev   0.32847456 BTC              WannaCry 2.0
prev   0.17112 BTC                 WannaCry 2.0
                           [show 36 more addresses]
```



```
2017-08-03 03:14:27 ( 2017-08-03 04:41:34 )          -7.06939288 BTC          ef0ac1c1307401388...b4a852a7172fcf2f

prev   0.00005525 BTC              WannaCry 2.0   14Y8rfeRAcZkGqG451UGk1epq5zw3dVQif   7.05953352 BTC   next
prev   0.00626202 BTC              WannaCry 2.0
prev   0.0001 BTC                  WannaCry 2.0
prev   0.1690546 BTC               WannaCry 2.0
prev   0.16417 BTC                 WannaCry 2.0
prev   0.0001337 BTC               WannaCry 2.0
prev   0.34477658 BTC              WannaCry 2.0
prev   0.001 BTC                   WannaCry 2.0
prev   0.16548 BTC                 WannaCry 2.0
prev   0.16480574 BTC              WannaCry 2.0
prev   0.00000563 BTC              WannaCry 2.0
prev   0.003 BTC                   WannaCry 2.0
prev   0.04 BTC                    WannaCry 2.0
prev   0.169683 BTC                WannaCry 2.0
prev   0.0001 BTC                  WannaCry 2.0
                           [show 56 more addresses]
```



```
2017-08-03 03:14:26 ( 2017-08-03 04:28:20 )          -10.06868926 BTC        8def6458a46234ab0...3b1d4bca4cc293a1

prev   0.00007347 BTC          WannaCry 2.0   1M1CfXLynR6vqbjwTqSiiLRVDQZEXHHJbb   10.05800019 BTC   next
prev   0.360168 BTC            WannaCry 2.0
prev   0.0001 BTC              WannaCry 2.0
prev   0.183 BTC               WannaCry 2.0
prev   0.00126352 BTC          WannaCry 2.0
prev   0.0004 BTC              WannaCry 2.0
prev   0.0137 BTC              WannaCry 2.0
prev   0.29161908 BTC          WannaCry 2.0
prev   0.0001337 BTC           WannaCry 2.0
prev   0.19581815 BTC          WannaCry 2.0
prev   0.0001 BTC              WannaCry 2.0
prev   0.3655 BTC              WannaCry 2.0
prev   0.001 BTC               WannaCry 2.0
prev   0.0001 BTC              WannaCry 2.0
prev   0.0001337 BTC           WannaCry 2.0
                      [show 62 more addresses]
```

```
2017-08-03 03:13:27 ( 2017-08-03 04:41:34 )          -9.03851401 BTC         35e5d5fe8c8128cfa...3e78a8d365b9d8a7

prev   0.001 BTC               WannaCry 2.0   16dfTuSx4f78eQ81PzTgBtBDyZ7QhNZ8Vy   9.02796322 BTC   next
prev   0.00574151 BTC          WannaCry 2.0
prev   0.17441962 BTC          WannaCry 2.0
prev   0.18204641 BTC          WannaCry 2.0
prev   0.0001 BTC              WannaCry 2.0
prev   0.00768521 BTC          WannaCry 2.0
prev   0.02 BTC                WannaCry 2.0
prev   0.167425 BTC            WannaCry 2.0
prev   0.0029 BTC              WannaCry 2.0
prev   0.00468114 BTC          WannaCry 2.0
prev   0.136431 BTC            WannaCry 2.0
prev   0.00459894 BTC          WannaCry 2.0
prev   0.1757569 BTC           WannaCry 2.0
prev   0.169588 BTC            WannaCry 2.0
prev   0.3762 BTC              WannaCry 2.0
                      [show 61 more addresses]
```

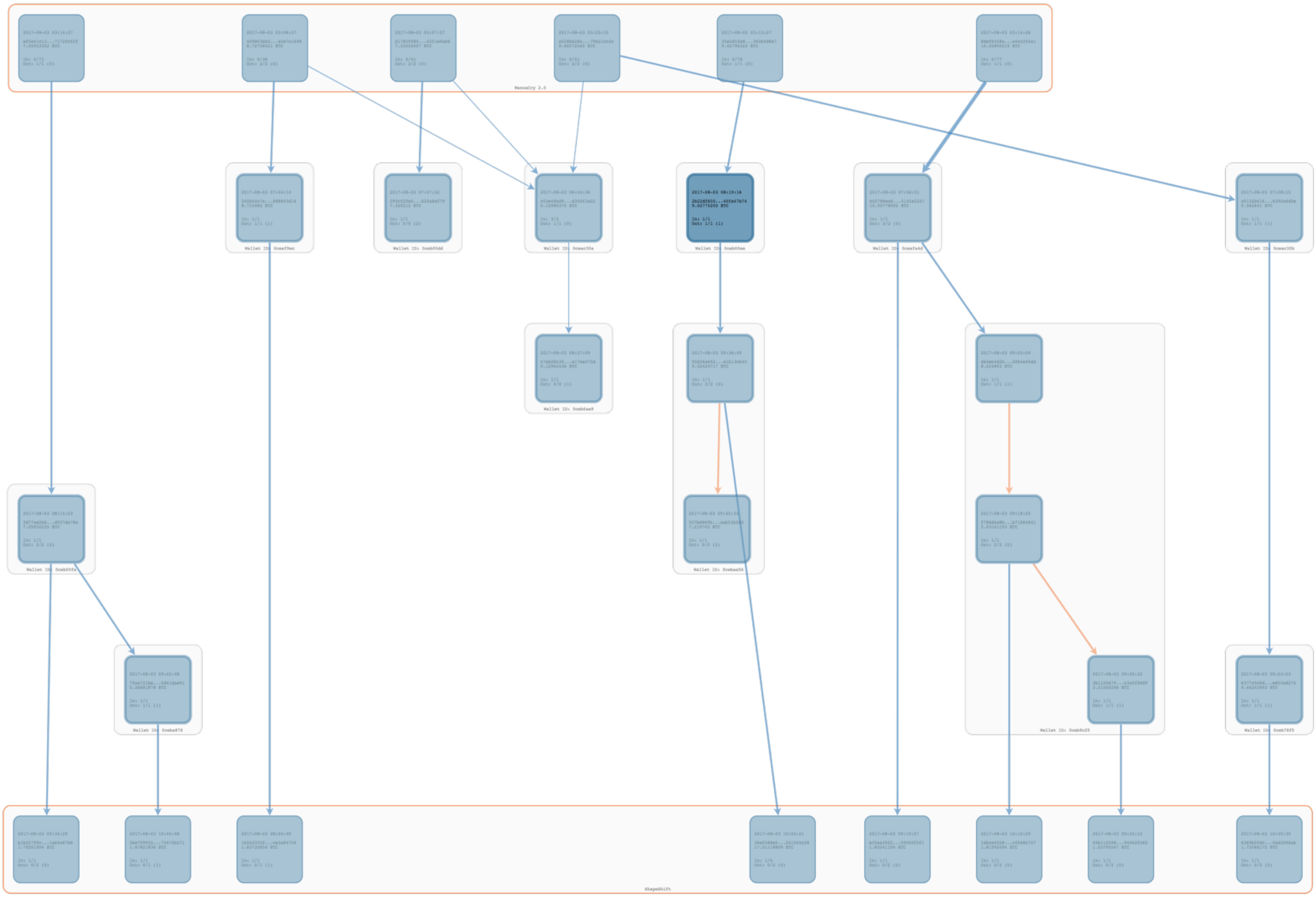
```
2017-08-03 03:07:57 ( 2017-08-03 04:41:34 )          -7.34128314 BTC         d17829f8097ed86fa...f90e03f42f1e9ab8

prev   0.15 BTC                WannaCry 2.0   18gsrbQsTY7HzYVZEbvtVBfhywpQk6No2Q   0.01511375 BTC   next
prev   0.172113 BTC            WannaCry 2.0   1Q8maVpVNAZbPiavySQz9JaiwsfhbT9vBz   7.32042682 BTC   next
prev   0.11126148 BTC          WannaCry 2.0
prev   0.17542239 BTC          WannaCry 2.0
prev   0.170262 BTC            WannaCry 2.0
prev   0.09829432 BTC          WannaCry 2.0
prev   0.18613 BTC             WannaCry 2.0
prev   0.16609346 BTC          WannaCry 2.0
prev   0.173 BTC               WannaCry 2.0
prev   0.164 BTC               WannaCry 2.0
prev   0.18 BTC                WannaCry 2.0
prev   0.1756 BTC              WannaCry 2.0
prev   0.177473 BTC            WannaCry 2.0
prev   0.16719976 BTC          WannaCry 2.0
prev   0.2 BTC                 WannaCry 2.0
                      [show 26 more addresses]
```

```
2017-08-03 03:06:57 ( 2017-08-03 04:28:20 )          -8.73261636 BTC         409803bb5e124fd02...d3a44aba5e7c1698

prev   0.17124673 BTC          WannaCry 2.0   1JC41YHmjKEcW1rLH6pmMWEFHkoNwSmhnC   0.01227173 BTC   next
prev   0.1801023 BTC           WannaCry 2.0   1FQQ86tMuvhQ4Ruyggbb8j7iaNfUZ69gpY   8.71529348 BTC   next
prev   0.16656716 BTC          WannaCry 2.0
prev   0.1703 BTC              WannaCry 2.0
prev   0.169 BTC               WannaCry 2.0
prev   0.1804 BTC              WannaCry 2.0
prev   0.17887884 BTC          WannaCry 2.0
prev   0.336 BTC               WannaCry 2.0
prev   0.32 BTC                WannaCry 2.0
prev   0.1486 BTC              WannaCry 2.0
prev   0.36 BTC                WannaCry 2.0
prev   0.174002 BTC            WannaCry 2.0
prev   0.16894486 BTC          WannaCry 2.0
prev   0.171 BTC               WannaCry 2.0
prev   0.17937739 BTC          WannaCry 2.0
                      [show 21 more addresses]
```

Analyzing the chain, we identified the destination of part of this funds as Shapeshift, the same service provider the author of Wannacry 1.0 used to move those bitcoins.

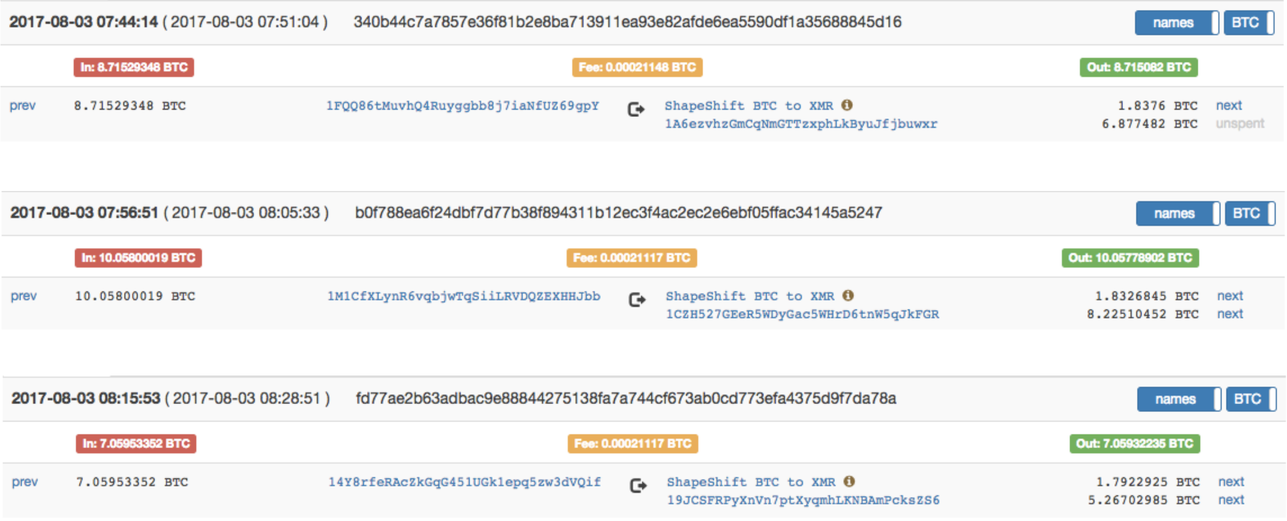
Shown below the graphical representation of the transaction scheme.

### Graphical representation of the Wannacry 2.0 transactions[1]



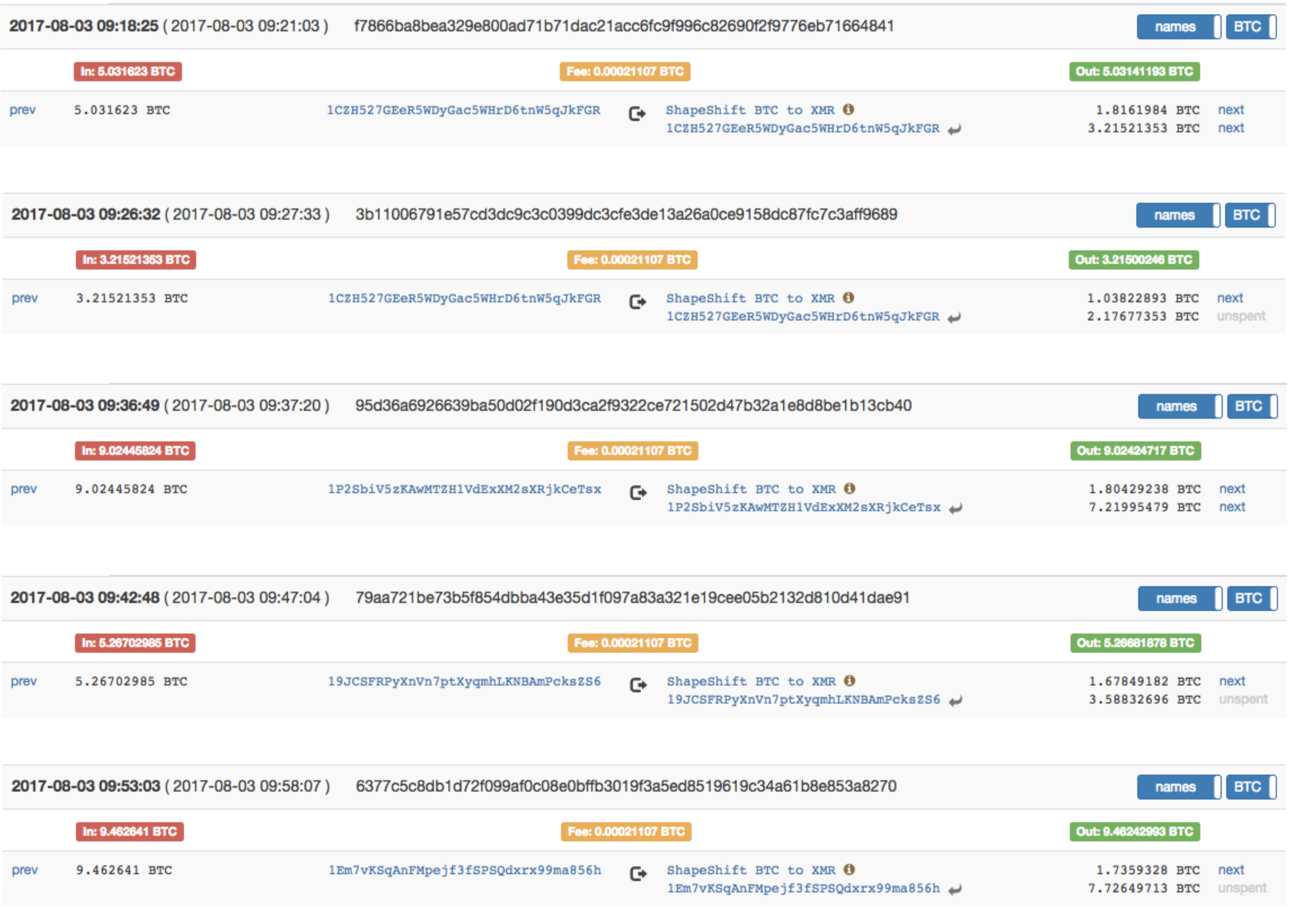
As we can see in the graph, so far there are eight transactions that move funds to Shapeshift.

### Transactions to the ShapeShift wallet in chronological order



```
2017-08-03 07:44:14 ( 2017-08-03 07:51:04 )   340b44c7a7857e36f81b2e8ba713911ea93e82afde6ea5590df1a35688845d16   names  BTC

     In: 8.71529348 BTC                         Fee: 0.00021148 BTC                         Out: 8.715082 BTC

prev   8.71529348 BTC         1FQQ86tMuvhQ4Ruyggbb8j7iaNfUZ69gpY   ShapeShift BTC to XMR              1.8376 BTC   next
                                                                    1A6ezvhzGmCqNmGTTzxphLkByuJfjbuwxr 6.877482 BTC   unspent

2017-08-03 07:56:51 ( 2017-08-03 08:05:33 )   b0f788ea6f24dbf7d77b38f894311b12ec3f4ac2ec2e6ebf05ffac34145a5247   names  BTC

     In: 10.05800019 BTC                        Fee: 0.00021117 BTC                         Out: 10.05778902 BTC

prev   10.05800019 BTC        1M1CfXLynR6vqbjwTqSiiLRVDQZEXHHJbb   ShapeShift BTC to XMR              1.8326845 BTC   next
                                                                    1CZH527GEeR5WDyGac5WHrD6tnW5qJkFGR 8.22510452 BTC  next

2017-08-03 08:15:53 ( 2017-08-03 08:28:51 )   fd77ae2b63adbac9e88844275138fa7a744cf673ab0cd773efa4375d9f7da78a   names  BTC

     In: 7.05953352 BTC                         Fee: 0.00021117 BTC                         Out: 7.05932235 BTC

prev   7.05953352 BTC         14Y8rfeRAcZkGqG451UGk1epq5zw3dVQif   ShapeShift BTC to XMR              1.7922925 BTC   next
                                                                    19JCSFRPyXnVn7ptXyqmhLKNBAmPcksZS6 5.26702985 BTC  next
```

[1] The wallet at the top is the Wannacry 2.0 one, the one at the bottom is belonging to Shapeshift. The blue arrows are representing the outgoing transactions, the orange ones the transactions change.



```
2017-08-03 09:18:25 ( 2017-08-03 09:21:03 )   f7866ba8bea329e800ad71b71dac21acc6fc9f996c82690f2f9776eb71664841   names  BTC
        In: 5.031623 BTC                       Fee: 0.00021107 BTC                                   Out: 5.03141193 BTC
prev    5.031623 BTC        1CZH527GEeR5WDyGac5WHrD6tnW5qJkFGR     ShapeShift BTC to XMR                 1.8161984 BTC   next
                                                                   1CZH527GEeR5WDyGac5WHrD6tnW5qJkFGR    3.21521353 BTC  next

2017-08-03 09:26:32 ( 2017-08-03 09:27:33 )   3b11006791e57cd3dc9c3c0399dc3cfe3de13a26a0ce9158dc87fc7c3aff9689   names  BTC
        In: 3.21521353 BTC                     Fee: 0.00021107 BTC                                   Out: 3.21500246 BTC
prev    3.21521353 BTC      1CZH527GEeR5WDyGac5WHrD6tnW5qJkFGR     ShapeShift BTC to XMR                 1.03822893 BTC  next
                                                                   1CZH527GEeR5WDyGac5WHrD6tnW5qJkFGR    2.17677353 BTC  unspent

2017-08-03 09:36:49 ( 2017-08-03 09:37:20 )   95d36a6926639ba50d02f190d3ca2f9322ce721502d47b32a1e8d8be1b13cb40   names  BTC
        In: 9.02445824 BTC                     Fee: 0.00021107 BTC                                   Out: 9.02424717 BTC
prev    9.02445824 BTC      1P2SbiV5zKAwMTZH1VdExXM2sXRjkCeTsx     ShapeShift BTC to XMR                 1.80429238 BTC  next
                                                                   1P2SbiV5zKAwMTZH1VdExXM2sXRjkCeTsx    7.21995479 BTC  next

2017-08-03 09:42:48 ( 2017-08-03 09:47:04 )   79aa721be73b5f854dbba43e35d1f097a83a321e19cee05b2132d810d41dae91   names  BTC
        In: 5.26702985 BTC                     Fee: 0.00021107 BTC                                   Out: 5.26681878 BTC
prev    5.26702985 BTC      19JCSFRPyXnVn7ptXyqmhLKNBAmPcksZS6     ShapeShift BTC to XMR                 1.67849182 BTC  next
                                                                   19JCSFRPyXnVn7ptXyqmhLKNBAmPcksZS6    3.58832696 BTC  unspent

2017-08-03 09:53:03 ( 2017-08-03 09:58:07 )   6377c5c8db1d72f099af0c08e0bffb3019f3a5ed8519619c34a61b8e853a8270   names  BTC
        In: 9.462641 BTC                       Fee: 0.00021107 BTC                                   Out: 9.46242993 BTC
prev    9.462641 BTC        1Em7vKSqAnFMpejf3fSPSQdxrx99ma856h     ShapeShift BTC to XMR                 1.7359328 BTC   next
                                                                   1Em7vKSqAnFMpejf3fSPSQdxrx99ma856h    7.72649713 BTC  unspent
```

There are similarities between these cryptocurrency swap activities and the one we observed for Wannacry 1.0:

- In both cases the authors used Shapeshift to swap Bitcoins into Monero, XRM;

- Wannacry 1.0 swapped bitcoin sending them to one single Monero address in 4 different transactions, the same is true for Wannacry 2.0: the 8 transactions registered so far were sending the total amount of 13.53 bitcoins, about 820,8 XMR, to the following Monero address:

*46jECbnrkJTUks7Fg5YtwShdUCiwUwEEZJtJBhKLK4GBWfBX7PLrYBuWR9zhzos5uQ1u XGUgFpGCSBR5o651pL5ERxmwqHu*

- According to the behavior of the two cases, we consider plausible that the same group of people is laundering the bitcoins collected with the two Wannacry campaign.

**Neutrino S.r.l.** An innovative startup founded in 2016 by a team with over ten years' experience in cyber security: a cyberlab dedicated to the research of innovative solutions to the new and complex challenges facing the security sector.

**P-Flow**, the first project developed by Neutrino, provides actionable insight on the blockchain and bitcoin network, offering to all of those interested in virtual currency, information which would otherwise not be accessible.

DISCLAIMER:
Please consider that the information contained into this report are confidential and are not intended for public disclosure, unless authorized or on a specific act from Neutrino representative.

Neutrino does not represent the information as being all-inclusive or to contain all information that may be desirable and **Neutrino is making no representations or warranties, express or implied, as to the accuracy or completeness of the information, and that Neutrino will have no liability with respect to any use or reliance upon any of the information.**

For more information: info@neutrino.nu