
Ethereum

There really aren't any open questions on the Ethereum side. The attack was funded with 10 ETH through Tornado (dead end) and then exited to BTC via renBTC (see below).

There are 3 addresses involved in the attack:
https://etherscan.io/address/0xf224ab004461540778a914ea397c589b677e27bb
(Mastermind address who creates and calls the attacker contract to orchestrate the economic attack)
https://etherscan.io/address/0xc6028a9fa486f52efd2b95b949ac630d287ce0af
(Attacker contract with the steps to execute the attack)
https://etherscan.io/address/0x3811765a53c3188c24d412daec3f60faad5f119b
(Accomplice address who exits with RenBTC)

Transactions that funding the attacking address:
10 ETH from Tornado to Mastermind
https://etherscan.io/tx/0x4b7b9e387a79289720a0226f695913d1d11dbdc681b7218a432136cc089363c4
1 ETH sent form Mastermind to Accomplice
https://etherscan.io/tx/0x87a7a3e0ef64692c964fafa110a04077597cb1410ac126851f68f5e5441ea169

There were two renBTC exit transactions. In the exit transactions, choose 'View Input As…' and select UTF-8 to see the bitcoin address that the renBTC was cashed out too:
https://etherscan.io/address/0x3811765a53c3188c24d412daec3f60faad5f119b#tokentxns
44.66054934 renBTC exit cashed out to 1Paykw4s2WX4SaVjDrQkwSiJr16AiANhiM
eth: https://etherscan.io/tx/0xef20b8f793dc06d23a146e20a7afd54f44d4b00972e7dc750644f236f6c633da
250.73813119 renBTC exit cashed out to 1Paykw4s2WX4SaVjDrQkwSiJr16AiANhiM
eth: https://etherscan.io/tx/0xb39030ee60ce984e96c0201b771927571c3ff3d64af692f93728553ec3914f3a
Transaction into BTC:
https://blockstream.info/address/1Paykw4s2WX4SaVjDrQkwSiJr16AiANhiM

Bitcoin

Much of the bitcoin exited from renBTC remains at rest on the chain. If we can generate a list of the main addresses involved, these can be passed to exchanges to blacklist.

Transaction into BTC:
https://blockstream.info/address/1Paykw4s2WX4SaVjDrQkwSiJr16AiANhiM

A lot of this bitcoin is very transparently just sitting on-chain where it was left:

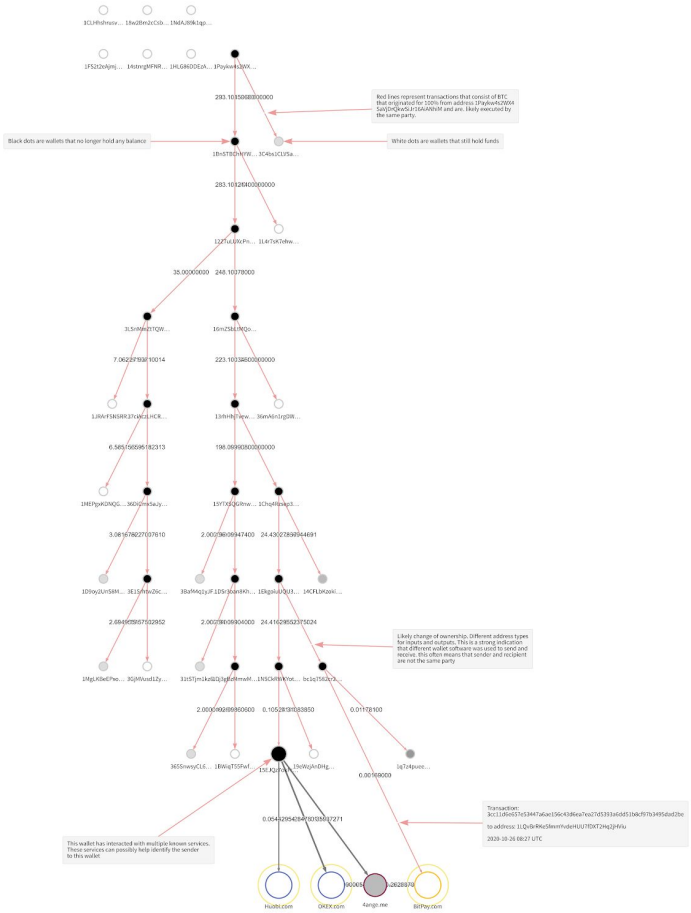
big chunks:
25 BTC https://blockstream.info/address/36mA6n1rgDWmTFY2hQdyim1PmHHMNyRzT2
7.1 BTC https://blockstream.info/address/1JRArFSNSRRhHnX7ywfwcGxX8y5WrJDJiB
6.5 BTC https://blockstream.info/address/1MEPgxKDNQG5opaFrbPdwdso5dsTFYQ69G
3.1 BTC https://blockstream.info/address/1D9oy2UnS8M3PsbMrCstgxytFMrT9ZNyxW
2.7 BTC https://blockstream.info/address/1MgLKBeEPxow7XZxXM7VfMoEd5yrL3epSD
2.7 BTC https://blockstream.info/address/1FA5tP51BGwAwo6A8zAPfgf98Kq32ne1HT
7.0 BTC https://blockstream.info/address/1DSAZNnYNRNjeszpbhQmqvg1zPR6iPJ6BX
2.4 BTC https://blockstream.info/address/14Fip8EBsV6C7QDJkqn62j4oTxEuU3BiiM
2.9 BTC https://blockstream.info/address/1DEdKUVQHM2bYprWVfRpdfcSaBHt9KiAew
6.7 BTC https://blockstream.info/address/1GGGkHehARTgsBsqcRYpMdyggevv1sVHrf
1.5 BTC https://blockstream.info/address/1EAP2ip3HpnYWWqD7k1NUxu18KgN8hmNUp
1.2 BTC https://blockstream.info/address/1PF3oauH2tt6FHG4HpM8jBYeHtGNKy8CCK
1.5 BTC https://blockstream.info/address/198pbLQgPf5HcivTG4Q8jyv6JuWbDoGvX6
1.6 BTC https://blockstream.info/address/1NmMe7xZtw2xQVJLUzcXrFa613VDMWNVod
1.3 BTC https://blockstream.info/address/1FVbZVroscVpmdpoD6N7U44wGthCmiQApc
0.7 BTC https://blockstream.info/address/1CzGfZndYtEusrbsPBpTBjMSJBYPqJDpgh
0.9 BTC https://blockstream.info/address/16griZtBaLPMxAA4MhCJF38Coq12Zoysz2

Transactions that look like they could be mixing-related:
https://blockstream.info/address/1HXPK3k2AAsc2srFAvBnanJVsf6JRUxFSo
it has thousands of transactions
https://blockstream.info/address/34P6x79vDAzNThCpZc4gmUPd92qVRjAoVu
this was reused from a tx in September

---

this address 1NSCkRWKYot7MyZdWZc9EZFxbWMDCXa2Sj
is a few hops down the chain from https://blockstream.info/address/1Chq4Rzsep3GiifdsRjt4SuXujWMfV7Cvp
which is one hop from https://blockstream.info/address/13rhHhjTvewuXduHtpR4qbMiQNdaUPfbwX
which is a few hops down the chain from
https://blockstream.info/address/1Paykw4s2WX4SaVjDrQkwSiJr16AiANhiM

A graphic of the hops to 1NSCkRWKYot7MyZdWZc9EZFxbWMDCXa2Sj:



15EJQz7okFrF1qUTXC4uJC7aaYSHMfr5Xr is the recipient of a small amount (0.10520144 BTC) from 1NSCkRWKYot7MyZdWZc9EZFxbWMDCXa2Sj; this address then interacted with some known services.

A spreadsheet of a cluster of transfers involving a related address:

Cluster_transfers_of_15EJQz7okFrF1qUTXC4uJC7aaYSHMfr5Xr
Description: This is a csv of the transactions that wallet cluster 15EJQz7okFrF1qUTXC4uJC7aaYSHMfr5Xr executed. The services that interacted with this service may be able to identify the sender that sent funds from 1NSCkRWKYot7MyZdWZc9EZFxbWMDCXa2Sj.

Through:
- Flugsvamp 3.0
- wm_cash
- coins.ph
- treddr

kraken
- 84a1c7b16838d695a1ffca1a03762a57a8251ee752302ba831017fac556cc86a
binance
- 7777569f003193ae59dbc5afbbf8bfbf3ac6c8ce8a8ec2b8707de14ddc3329a6
- 9fcc273f2d50fc5824b8fd0bbe832831d02e7fe04bcc09d143e787455c602195
huobi
- 37887243f8a30071b12fe4831e7a01e64a1667ddced6445282f62eece571d871
- a4cb40e5e6d58e8c5a463fc9df49fd506820686bea63b71cfd0ac6490182ba22