metalicjames / **vtc-attack.md**

Last active 20 days ago

vtc-attack.md

Vertcoin (VTC) was 51% attacked

Preamble

Vertcoin is a Bitcoin clone that aims to be ASIC-resistant by hard forking to new mining algorithms whenever ASICs are deployed on the network. Vertcoin was previously 51% attacked in Dec 2018 and has since changed its proof-of-work algorithm to Lyra2REv3. On Nov 30th 2019, a Vertcoin miner noticed a large upswing in hashrate rental prices for Lyra2REv3 on Nicehash. This was combined with workers connected to Nicehash's stratum server being sent work for unknown (non-public) Vertcoin blocks. I contacted Bittrex, Vertcoin's most prominent exchange, to recommend they disable the Vertcoin wallet on their platform once it became clear an attack was in progress, which they subsequently did.

The Attack

On Sunday, 1 December 2019 15:19:47 GMT 603 blocks were removed from the VTC main chain and replaced by 553 attacker blocks. We note that 600 blocks is the current confirmation requirement for VTC on Bittrex. There were 5 double-spent outputs in which ~ 125 VTC (~$29) was redirected. Each of the double-spent outputs are coinbase outputs owned by the attacker and it is unknown to whom the coins were originally sent before being swept to an attacker address after the reorg.

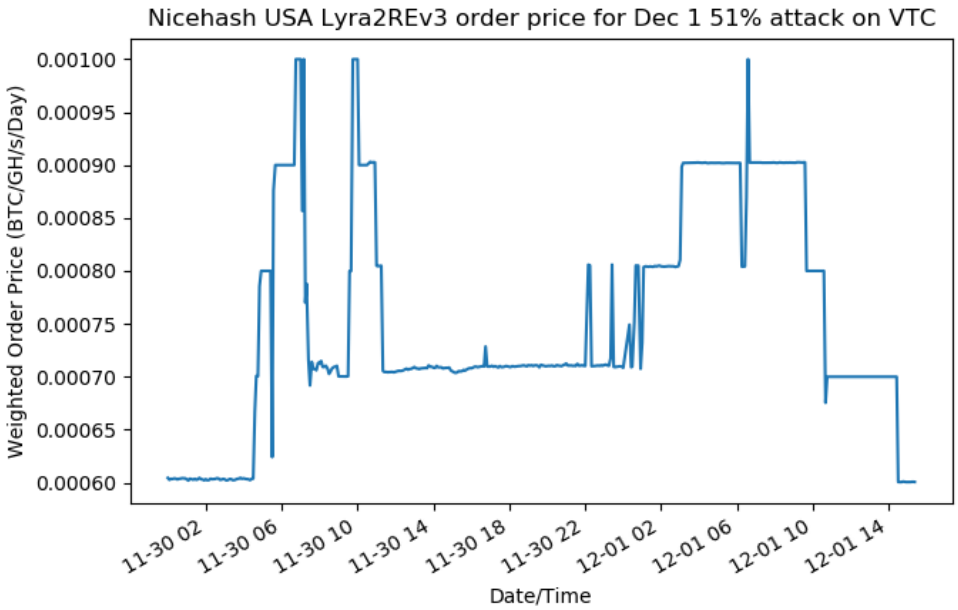
- 18.33311434 VTC originally sent to vtc1qwnatpej2z5gm6qlhlvg90cpr8ly78hpf045lah and 6.66666666 VTC originally sent to vtc1qmvf89czpsee63xeghwk6469se8lng05ck7th4r in transaction 4ca37b55adf49d85f9c5a7f797f27703e1bd7246ae40d879b4af717abee09dd2
- 18.33311434 VTC originally sent to vtc1qeu5la72vcw4qf7ml3e7z7tnja6gdt7yl86z00u and 6.66666666 VTC originally sent to vtc1qwvj5ama3zqclm0h2dry9ltug392wup0ylsujp6 in transaction f4cb9e1b84f175ec6a41d316be0454837810d70d33669528ce2b87e1082c90d4
- 18.33337473 VTC originally sent to vtc1qz03flmgkjzd7jgwx3ul0c7fftclgfz5da63dtq and 6.66666666 VTC originally sent to vtc1q5306cezk7cls0lh29l2tfh07gnz0kkqf776aye in transaction a6e56ea963d1f29ed1cb44a17e24f77e6b6d0a8f945667c7fb88f11391c48ecb
- 23.999779 VTC originally sent to 3981xNMVBzfbXMoPCr3EojpbQXfpCdvLYV and 1 VTC originally sent to 3HeLfVTCjBRHtTp1s1Sra5peg58HMCR6kp in transaction 4522207fd077a05787cc74e8eb579922701dbf82e5da12c94f4dcece3d976b07
- 18.33311434 VTC originally sent to vtc1qw933nxhazxps5lfgqvc5mummcsya9688mek7f3 and 6.66666666 VTC originally sent to vtc1quhhqsexsf7x4pakf4a4jlypvzyqezgydh3wvk5 in transaction e7ae030fac290fe03fbfacaeb5f24a11114eeffdd8fb2b7e32543faea25eb708

Each of the above transactions were invalidated by a single transaction on the attacker's fork 77864705e247a9df8a427598b874afffc57469f5a79e06215b3d08e3d8c8df61 that sent 11000 VTC to VqqBJ8BLW2q4dpiBTbCSC4PN3DHSKbFUCK and 24.93491439 VTC to 3KFkRwvBbZtgBMpm8rPgc5Y545PiesMrdk. This transaction swept the coinbase outputs from the attacker's blocks as well as double-spending the aforementioned outputs. The attacker mined with the address VmoGb9SRaeTeVYGeoZxWAq71FHSCyPAPbm.

There is strong evidence this attack was performed using rented hashrate from Nicehash. The attack was originally discovered by inspecting the work being sent from Nicehash's stratum servers, which were sending work for non-public blocks. Below is a screenshot of a Nicehash miner's mining software console output showing work given for VTC block 1253804 when at the time the public block height of VTC was 1253800.

```
[2019-11-30 12:30:56] lyra2rev3.eu.nicehash.com:3373 asks job 638995845 for block 1253804
[2019-11-30 12:31:06] DEBUG: job_id=de2a759 00000000261664ba xnonce2=000000 time=12:31:05
[2019-11-30 12:31:06] lyra2rev3.eu.nicehash.com:3373 asks job 639001786 for block 1253804
[2019-11-30 12:31:16] DEBUG: job_id=de2a763 00000000261677d6 xnonce2=000000 time=12:31:15
[2019-11-30 12:31:16] lyra2rev3.eu.nicehash.com:3373 asks job 639006678 for block 1253804
[2019-11-30 12:31:26] DEBUG: job_id=de2a76d 00000000261695e7 xnonce2=000000 time=12:31:25
[2019-11-30 12:31:26] lyra2rev3.eu.nicehash.com:3373 asks job 639014375 for block 1253804
[2019-11-30 12:31:36] DEBUG: job_id=de2a777 000000002616a906 xnonce2=000000 time=12:31:35
[2019-11-30 12:31:36] lyra2rev3.eu.nicehash.com:3373 asks job 639019270 for block 1253804
[2019-11-30 12:31:43] GPU #0: 1670 MHz 75C FAN 0%
[2019-11-30 12:31:46] DEBUG: job_id=de2a781 000000002616c4b5 xnonce2=000000 time=12:31:45
[2019-11-30 12:31:46] lyra2rev3.eu.nicehash.com:3373 asks job 639026357 for block 1253804
[2019-11-30 12:31:50] GPU #0: GeForce GTX 1050 Ti, 11.54 MH/s
[2019-11-30 12:31:50] GPU #0: start=00000000 end=2941dc7c range=2941dc7c
[2019-11-30 12:31:50] CTRL_C_EVENT received, exiting
[2019-11-30 12:31:50] restart_threads
```

Post-attack analysis of the Nicehash orderbook during the attack's preparation shows a large upswing in hashrate rental price from the market equilibrium on both their EU and USA markets. Now that the attack is over, the rental price has returned to the baseline market equilibrium.



Based on the market prices during the attack's preparation and the difficulty of the blocks the attacker produced, we estimate the attacker spent between 0.5-1 BTC to perform the attack. The total value of the block rewards the attack received is 13825 VTC (~0.44 BTC). Given the attack was likely not profitable to perform based solely on block rewards, the motivation for the attack is not certain. Given the reorg was just deeper than 600 blocks (Bittrex's confirmation requirement for VTC), it is possible that Bittrex was the original target, but the double-spend portion attack was aborted due to Bittrex disabling their wallet before the fork could be released. It is also possible that no double-spend was ever intended, and the attack was a proof of concept or sabotage attack.

soldat13 commented on 2 Dec 2019

The dPoW security can save you for the next attack

zawy12 commented on 2 Dec 2019

How did 553 blocks have more chain work than 603? Fewer blocks implies slow solvetime, but slower solvetimes should have resulted in lower chain work. The difficulty chart fell off a cliff at midnight, 15 hours before the blocks were submitted. Might be DA problem.

metalicjames commented on 2 Dec 2019 — Author — Owner

@zawy12 Vertcoin's difficulty adjusts every block, so a miner producing blocks at a faster rate would experience a higher difficulty per block, meaning you can have fewer blocks with a higher chainwork. The drop in difficulty on the main chain would likely be caused by rented hashrate that is normally used by honest miners being outbid by the attacker.

zawy12 commented on 2 Dec 2019 • edited

What you're saying seems to apply only if the attacker starts with a high hashrate and then drops back some, or the algorithm overshoots the difficulty, or he had bad luck compared to the public chain in addition to a higher difficulty. OK, now I see the chart above is the original chain, not the attacker's chain which is the final chain.

tromp commented on 2 Dec 2019 • edited

> Fewer blocks implies slow solvetime,

Not necessarily. You can have 553 fast blocks, the last of which ended a while ago, so that the next block will be VERY slow.
That will accumulate more work than 603 slow ones.

zawy12 commented on 2 Dec 2019 • edited

Yes, but only under certain circumstances that I described above. Another possibility is that the lower hashrate attacked more hashrate from other sources after it dropped a lot, and they got a lot of blocks before the algorithm had time to respond. I am guessing that what happened here is that the attacker used a higher hashrate than he should have which triggered KGW's shorter SMA averaging window which resulted in him getting an unlucky higher difficulty because SMA overshoots difficulty with small N, especially when it first starts (such as suddenly going to a shorter window).

lookfirst commented on 3 Dec 2019

Interesting that one of the addresses ends with FUCK.

zawy12 commented on 3 Dec 2019 • edited

If out of sequence timestamps are not disallowed by the protocol or otherwise limited in how "negative" solvetimes can be, this method of dealing with out of sequence timestamps may allow a >50% selfish miner to get an unlimited number of blocks in less than 2x the difficulty window. See timespan limit attack here. Perhaps most coins are vulnerable to this attack and all devs so far are ignoring it. For example, the BTC/LTC code has the same vulnerability due to the 1/4 and 4x limits. DGW has 1/3 and 3x limits, and BCH has 1/2 and 2x limits.