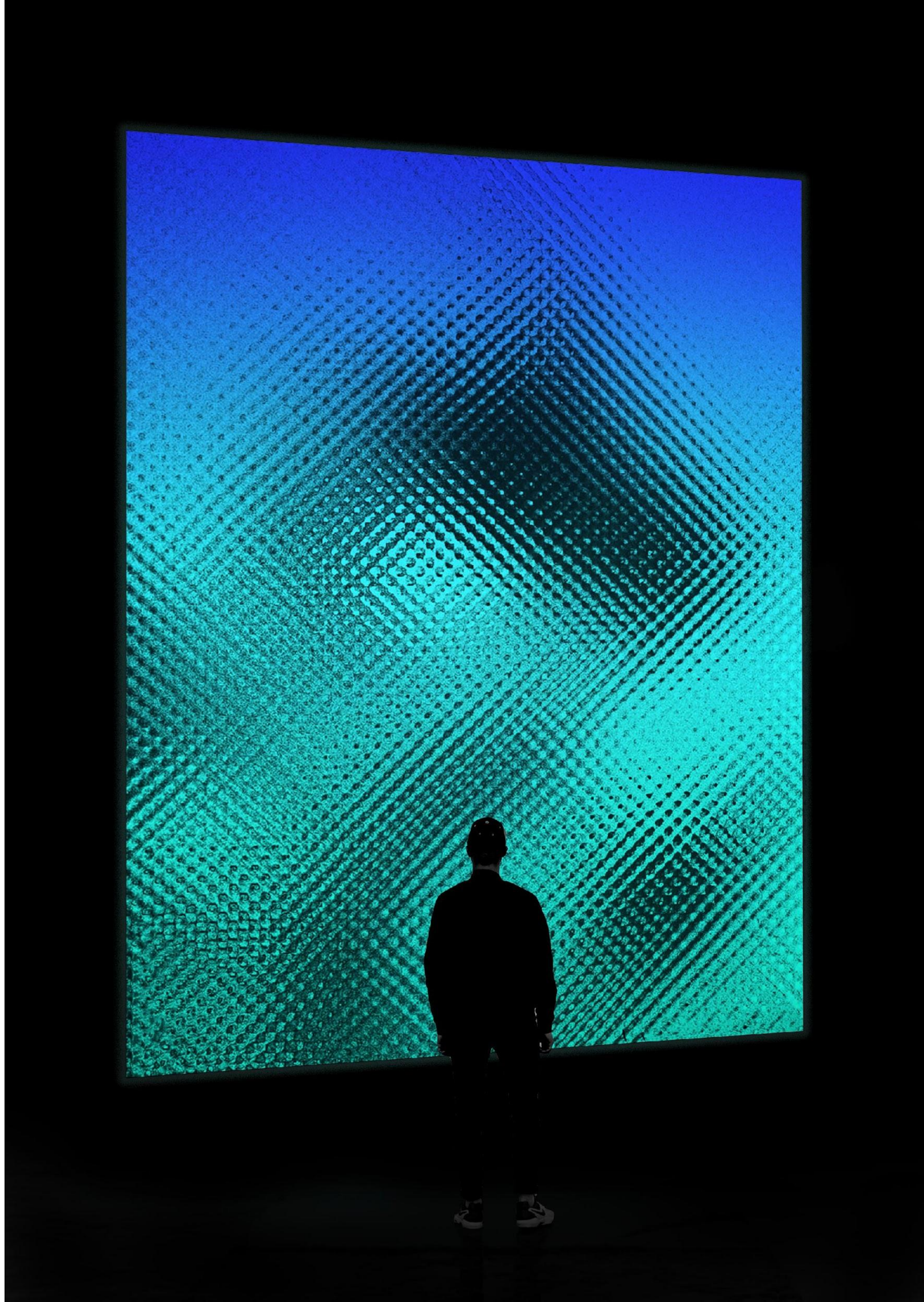
HACKEN

BINANCE HACK

from a blockchain analysis perspective

Prepared by Hacken & CER
Using Crystal Analytics Tool



THE KEY MESSAGE IS

ALL EXCHANGES SHOULD IMMEDIATELY BLACKLIST THE FOLLOWING BTC ADDRESSES

- bc1qtpdptcf4ngfkwq6dr36kqaeh2n5h00rx5unkgc 670.9965
- bc1q8m9h3atn4cqeqhu3ekswdqxchp3g7d4v3qv3wm 567.997
- bc1qp6k6tux6g3gr3sxw94g9tx4l0cjtu2pt65r6xp 555.997
- bc1qld27dqu6wrl4tmjdr8tl55qavmghwrr4ldh7qn 473.9975
- bc1qesy52g7ndy652qudr2awuk57mcaxgmn9qsmpzk 469.9975
- bc1q7p6edvd4zvtya8uj366c23dan8pvlp503spucu 468.9975
- bc1qqp8pwq277d30cy7fjpvhcvhgztvs7v0nudgul5 463.9975
- bc1qecs672j9dpvwr56zeldgf3swtlv3dad52wzuta 463.9975
- bc1ql0wlnu80l8kctjzkzlzd72sdjqwuvruvgepceq 383.998
- bc1qyv4zv0wjn299kx4yz6g7v6g6400wqgzcqgw9vx 383.998
- bc1qvr2jxlmvckap7cg2l6mdgh5fa8glkhe4s88sax 377.998
- bc1q6fejm4r866tmt8ptf42juedv5gevlv2qt72agq 371.998
- bc1qhqap39mpkldjzvqdf3204p732krtnf56mm9aj3 370.998
- bc1qhlhx6lrnr0jf4zpvm788j7yeezau6s8q557p2z 279.9985
- bc1qvstwzsrfml43jrclsp68220l4lx5lw3kwf7dp0 193.999
- bc1q9svj9wp68zftgejjgk6f96ukuyx8c5urkqsv69 193.999
- bc1q3ldtrr6xtpx8jam5gw68aaexz2wtluj0qullvr 189.999
- bc1qshkncv7tkpye7z0z4a3k9yw2e73whha9gjs88z 97.9995
- bc1qanrl8n3flz4jftkscljx2hwuc3h50f9ynp2nyn 89.9995

Blacklisting these addresses will make it more difficult for the hacker to offload BTC on other exchanges

No one is 100% protected from hacker attacks. This is our opportunity to unify efforts to become stronger against such hacks

Hacken and CER are monitoring all movements associated with wallets cited to the left and will share updates as we receive them

HACKEN

WHAT HAPPENED?

INPUT ANALYSIS

E8b406091959700dbffcff30a60b190133721e5c39e89bb5fe23c5a554ab05ea

2 Input Addresses:

1NDyJtNTjmwk5xPNhjgAMu4HDHigtobu1s - main Binance hot wallet

3CTPRyUbCKkByGmAVvDV6ReZXT1WfV3UPd - vehicle address for Binance hot wallet

71 Inputs:

70 inputs 100 BTC each from 1NDyJtNTjmwk5xPNhjgAMu4HDHigtobu1s

1 input 74.19 BTC from 3CTPRyUbCKkByGmAVvDV6ReZXT1WfV3UPd

Conclusion: The analysis above indicates the max amount of 100 BTC was withdrawn from 70 “2nd Verification Level” accounts.

WHAT HAPPENED?

OUTPUT ANALYSIS

E8b406091959700dbffcff30a60b190133721e5c39e89bb5fe23c5a554ab05ea

44 Output Addresses:

20 new wallets were created containing 7,070.96 BTC

24 existing wallets containing 3.22 BTC

HISTORICAL OUTPUT ANALYSIS

WHAT ARE HOT & COLD WALLETS POLICIES?

- **For the last 6 months the biggest common output was 2,000 BTC which occurred 57 times. All withdrawals were conducted to Binance's cold wallet.**

- **On March 28th, 2019, a withdrawal of 6,020 BTC was conducted in 4 batches, each batch not exceeding the 2,000 BTC withdrawal limit. Such grouping may indicate the existence of a hot wallet output transfer policy - no output can be above 2,000 BTC:**
  07cfcb4eda27e58a3ca5408302fa8e590e98040cfdb0729424a3e597e8811519
  B032d5fa88a2cfb442afe2a746b60ece4fa745ee056a3b0d3738d5d57d084664
  A7640e5476cbb0068281f0a068acdc10b1bca61906f2cb4145f86e7561d9855a
  143afacd01ebd7a870afe68ae969b3f2991a20c0a066b84350db9872335e6476

- **The latest largest withdrawal was for the amount of 2,091 BTC where BTC was sent from a Binance hot wallet to the following accounts:**
  Hot wallet address: 4d058fe942e068682e2b7faa43877ac95ecffe4ac9ecf863eea5a1c9f51dbc9b
  999.99 BTC to Coinbase
  999.99 BTC to Bitstamp
  91 BTC other various external trx combined in one

- **Conclusion: Based on the pattern of large withdrawals Binance has conducted, we believe they have a 2,000 BTC withdrawal limit policy in place.**

HISTORICAL OUTPUT ANALYSIS

WHAT ARE HOT & COLD WALLETS POLICIES?

- **During the past 6 months, there were only two withdrawal transactions above 2,100 BTC:**
  19.12.2018 for the amount of 2,400 BTC - 500 BTC to Kraken and 1,706 BTC to 3MmX8JfumgnV7yEPrD4weHZximdQ2ijH5Z
  15.11.2018 for the amount of 10,000 BTC - transfer to cold Binance wallet. 2,000 BTC policy breaker

- **Last transaction above 2,500 BTC from Binance's hot wallet directly to an external address was more than 1 year ago (February 10th, 2018) when 30,000 BTC was moved to a series of undefined external wallets:**
  E5b282a85d9b74cdca48d0323011492c3ef4deba7791e44edeefe96090a7d990

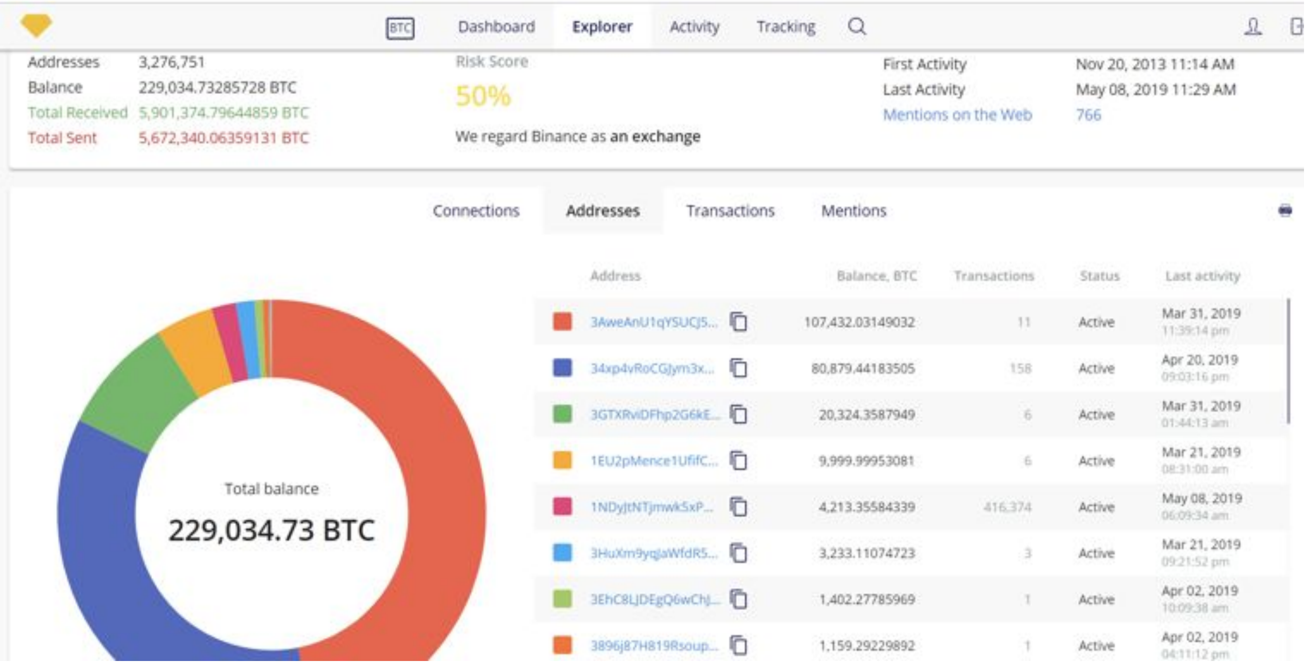
- **The latest biggest external transaction from Binance was on April 2nd, 2019, for the amount of 9,887 BTC. It was done through a series of transactions from Binance's 2nd biggest cold wallet 34xp4vRoCGJym3xR7yCVPFHoCNxv4Twseo:**
  061e9d8dc9baefb5d41aa923526d5df45cbad705a584df38bdc433479499c2cf

- **Conclusion: Transactions above a certain amount are handled manually and are usually withdrawn from cold wallets.**

BINANCE BALANCE OVERVIEW

- According g to official statement, Binance’s biggest and main hot wallet was hacked
- The Hacker knew the approximate inflow/outflow and balance on the day of the hack
- **Conclusion** - The Hacker withdrew the amount that was available in the hot wallet and not the amount accessible to the individuals reach.

Current balance at 14:12 08 May 2019	4,213
Total input after the Hack	3,834
Total output after the Hack	85
Total amount hacked	7,079
Balance at the moment of Hack	**7,373**



Addresses	3,276,751	Risk Score		First Activity	Nov 20, 2013 11:14 AM
Balance	229,034.73285728 BTC	50%		Last Activity	May 08, 2019 11:29 AM
Total Received	5,901,374.79644859 BTC			Mentions on the Web	766
Total Sent	5,672,340.06359131 BTC	We regard Binance as **an exchange**			

Total balance
229,034.73 BTC

	Address	Balance, BTC	Transactions	Status	Last activity
🟥	3AweAnU1qYSUCJ5...	107,432.03149032	11	Active	Mar 31, 2019 11:39:14 pm
🟦	34xp4vRoCGJym3x...	80,879.44183505	158	Active	Apr 20, 2019 09:03:16 pm
🟩	3GTXRviDFhp2G6kE...	20,324.3587949	6	Active	Mar 31, 2019 01:44:13 am
🟧	1EU2pMence1UfifC...	9,999.99953081	6	Active	Mar 21, 2019 08:31:00 am
🟥	1NDyJtNTjmwk5xP...	4,213.35584339	416,374	Active	May 08, 2019 06:09:34 am
🟦	3HuXm9yqjaWfdR5...	3,233.11074723	3	Active	Mar 21, 2019 09:21:52 pm
🟩	3EhC8LJDEgQ6wChJ...	1,402.27785969	1	Active	Apr 02, 2019 10:09:38 am
🟧	3896j87H819Rsoup...	1,159.29229892	1	Active	Apr 02, 2019 04:11:12 pm

KEY QUESTION. USERS HACK OR BINANCE HACK OR INSIDER JOB?

Attack vector on user:

- **Hacker gained access to Binance’s biggest accounts, login, and password:**

  This can be done through bruteforce techniques if accounts are identified and compromised

  This can be mitigated by adding additional controls for checking new or existing users logins and entered password in leaked databases aggregators like https://haveibeenpwned.com/

- **Hacker bypassed 2FA:**

  2FA bypass methodology - this needs to be done individually for every compromised account. Quite difficult not to be noticed if you need to hack 70 accounts

- **Hacker got access to users email**

  Each Binance withdrawal needs confirmation by email. Hacker needed access to email as well

KEY QUESTION. USERS HACK OR BINANCE HACK OR INSIDER JOB?

Attack vector on Binance servers:

- Hacker got access to Binance’s login & password databases as well as to secret one-time-password (OTP) database.
- Hacker bruteforced the biggest accounts, email, and manually confirmed withdrawals
- Hacker targeted Binance’s executive accounts who had access to hot wallet private keys:
  - Phishing
  - Physical theft
  - Viruses

KEY QUESTION. USERS HACK OR BINANCE HACK OR INSIDER JOB?

WE HOPE NOT

ARGUMENTS

	Binance Hack	Users Hack	Insider Job
+	The amount hacked equates to 95% of the hot wallet balance (as of May 8th, 2019)	Publicity of the announcement. If that was internal leakage, most probably would not be disclosed	Could be a third party insider job
+	Could be relatively easy to exercise if C-level executive access point was compromised	Binance's public statement for attack vector	Unintentional lack of attention from C-level executives
+	No significant withdrawals from hot wallet to external accounts for the past 6 months	Most common hackers technique	
-	Binance public statement	Hot wallets withdrawal policy of 2,000 BTC	Existence of hot wallets policies decreases the number of individuals who can execute the hack
-	Not the best time for attack - two days before the hot wallet balance was over 9k BTC	Complexity of the simultaneous control over compromised accounts	Acknowledgement of complexity for stolen funds usage
-		No significant withdrawals from hot wallet to external accounts for past 6 months	

HACKEN

SUMMARY

- We are sharing results of our blockchain analysis and not pushing any conclusions
- Results of the Binance internal investigation should be made available to the public
- Most of the crypto exchanges funds have to be kept at cold storages
- Hot & cold wallets private key management has to be reviewed by 3rd party digital assets auditor

ABOUT HACKEN AND CER

- **Hacken** is a cybersecurity consulting company with high profile clients that is focusing on the blockchain industry by offering the following services:

  - Cybersecurity Consulting
  - Smart Contract Auditing
  - Penetration Testing
  - Digital assets auditing
  - Crowdsourced Security Management

- **CER** (Cryptocurrency Exchange Ranking) focuses on ranking cryptocurrency exchanges by their Blockchain Balance and CyberSecurity Score. The following certifications are conducted to ensure a cryptocurrency exchange is transparent with its user base:

  - Proof of Funds CERtification
  - Cybersecurity CERtification
  - CryptoCurrency Exchange Due Diligence

SPECIAL THANKS TO

Crystal

The Crystal™ platform is the all-in-one blockchain analytics tool. Designed for financial institutions and law enforcements, Crystal provides a comprehensive view of the public blockchain ecosystem and uses advanced analytics to map suspicious transactions and related entities.

Follow Crystal™ on social media:

- /CrystalBlockchainAnalytics
- @CrystalPlatform

FOLLOW US

Follow Hacken and CER for more blockchain security insights

HACKEN

- /Hacken.io
- @Hacken_io

CER

- /CER.Hacken
- @CER_Hacken

HACKEN