FRAUD

IN THE CRYPTOCURRENCY SPHERE &

METHODS TO COMBAT IT

AMLCrypto.io

PKIA 2024 Conference, India

AMLCrypto.io

CRYPTO INVESTIGATIONS

BLOCKCHAIN ANALYTICS TOOLS

Market capitalization*

$2.4 T

Cryptocurrency owners **

560+ M
worldwide

116+ M
India

Daily turnover of cryptocurrency*

$20-90 B

* According to coinmarketcap.com

** According to Triple A triple-a.io/crypto-ownership-data

0.34%

of transactions are related to **illegal** activities*

* According to Chanalysis Crypto Crime report
go.chainalysis.com/crypto-crime-2024.html

Let's look
at the situation

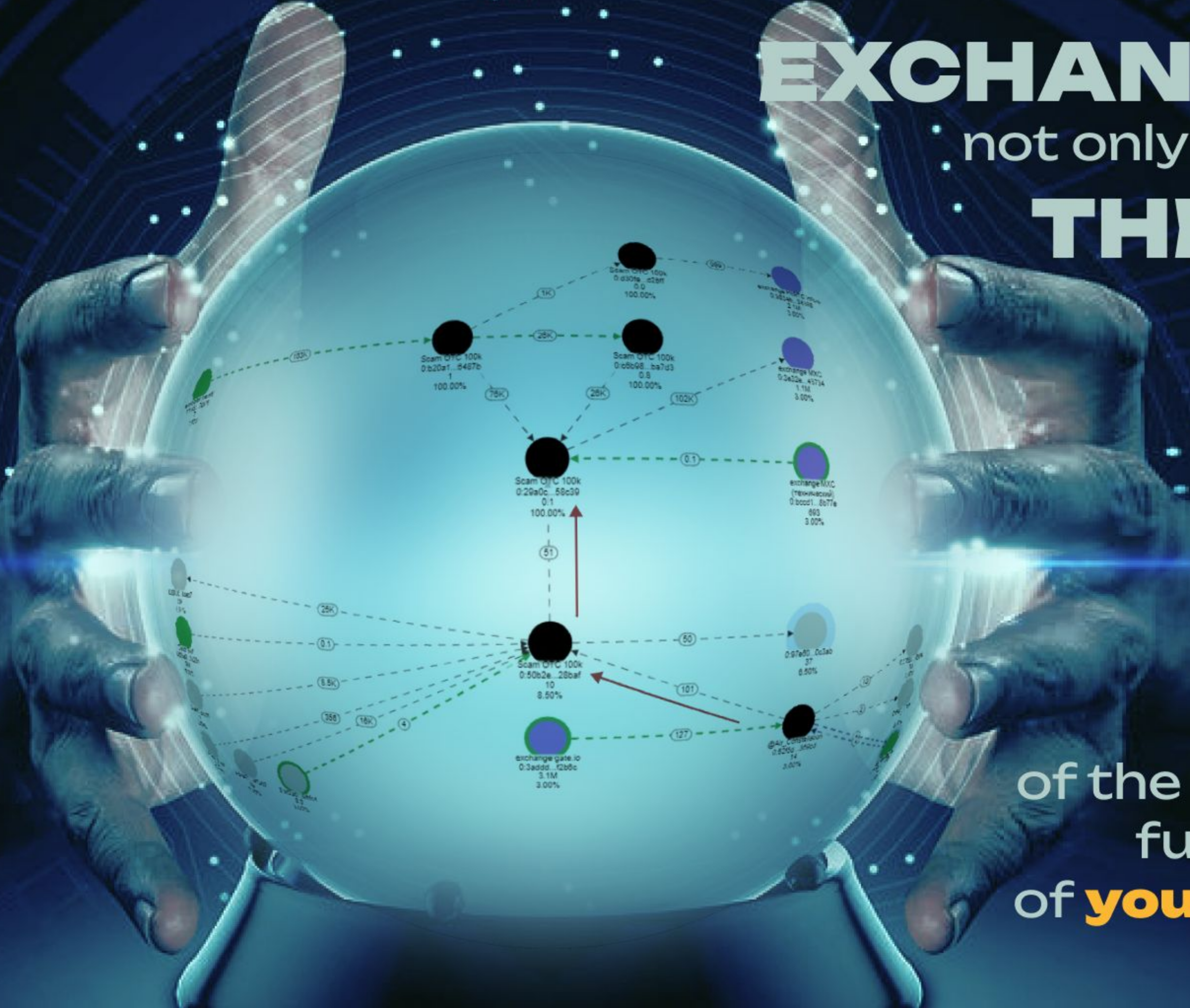
1

You bought **10k USDT**
through a crypto exchanger
at **a favorable rate**

When trying to exchange crypto on the exchange, your funds are...

BLOCKED

EXCHANGES LOOK
not only at you, but also at
THE HISTORY



of the formation of **your**
funds and the funds
of **your counterparties**

To get **blocked**,

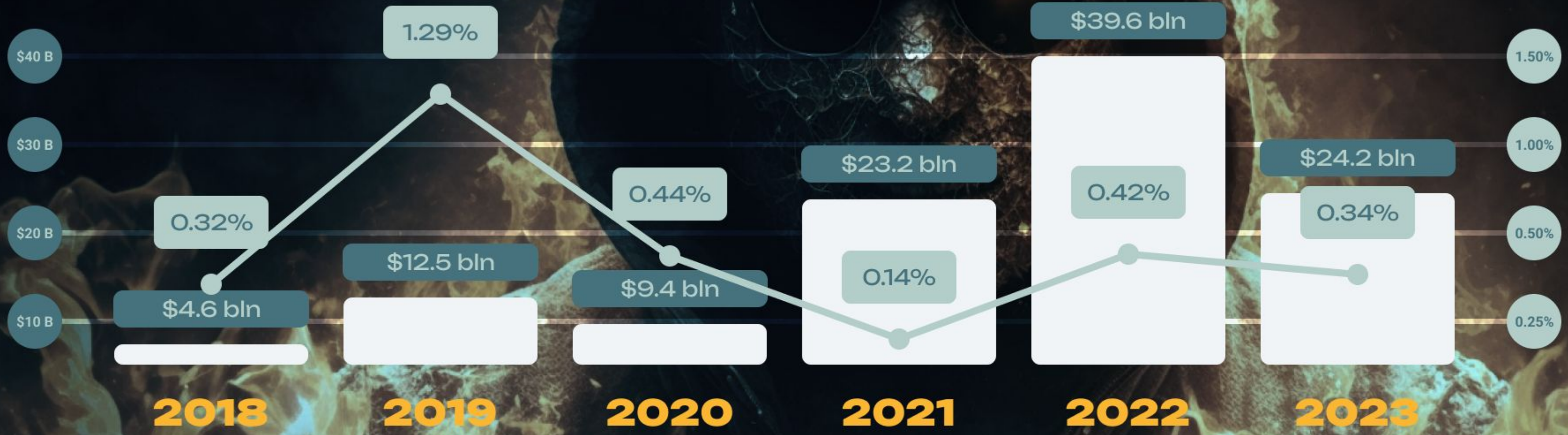
YOU DON’T NECESSARILY HAVE TO DO SOMETHING BAD...

you just have to **be careless**
and **not understand** the history
of the origin of the funds!

The Scale of Crypto Crime in 2023

$24.2 billion came through criminals' blockchain addresses, which is **0.34%** of the total transaction volume

* According to Chanalysis "The 2024 Crypto Crime report" chainalysis.com/wp-content/uploads/2024/06/the-2024-crypto-crime-report-release.pdf



CRYPTO USER FOR AN ATTACKER -

is a **source** of income

is a laundering/masking **tool**

CRYPTO CURRENCY SCAMS

AMLCrypto.io

THE MAGIC OF SOCIAL ENGINEERING

“HELPERS” IN CREATING A CRYPTO WALLET

I just wrote down your recovery phrase here. Make sure no one except you will know about your recovery phrase. Just make sure to transfer all your funds here.

PHISHING WEBSITE:

LIKE STEALING CANDY FROM A CHILD

FAKE EXCHANGE/EXCHANGER

Of course it will go #tothemoon, idiot. I draw the graphics for you in Paint myself...
Successful Investment MentoR
Will it go #TOTHEMOON?
I am your mentor, trust me.

ROMATIC BAIT
DECEPTIVE MATE
ROBBERY DATE

💅🌹🥰✅

Wazzap, homie!
It’s J Lo, send me 100 ETH pls,I’m broke 💋

LET'S MEET THE CHARACTERS

Victim

Attacker

Dirty crypto

Law enforcement agencies

Exchanges & exchangers

THE VICTIM

- Inexperience
- Greed
- Ignorance
- Lack of critical thinking
- Lack of technical literacy
- Impulsiveness

THE ATTACKER

- Technical savvy in anonymization tools: VPN, virtual machines, fake numbers, IP telephony, drops
- Cynical and unscrupulous

DIRTY CRYPTO

- Seeks fiat (via exchanges, crypto exchangers, ATM, P2P exchange)
- Laundered (via transit addresses, mixers, anonymous tokens, collateral smart contracts)

LAW ENFORCEMENT AGENCIES

- They don't like such cases, because the statistics of detection are poor
- They become more literate in matters of modern technologies, including cryptocurrencies and blockchain
- There are still not enough specialists

(!) But without them, in many countries it is impossible to obtain data from exchanges and crypto exchangers

EXCHANGES & EXCHANGERS

- Most have formal AML - they perform the minimum level sufficient to avoid liability
- They do not like law enforcement agencies, blockchain investigators and lawyers - audience data does not bring money, but only burdens the system

(!) You have to find a common language with exchanges, since exchanges are often the link to the fiat world

WHERE DOES A CRYPTO INCIDENT INVESTIGATION BEGIN?

DETAILED INTERVIEWING

1

Allows you to verify facts, structure the client's thoughts, and find out significant details

OSINT:
ANALYSIS OF DIGITAL TRACES OF INTRUDERS

2

Allows you to identify potential attackers and provide digital clues for law enforcement

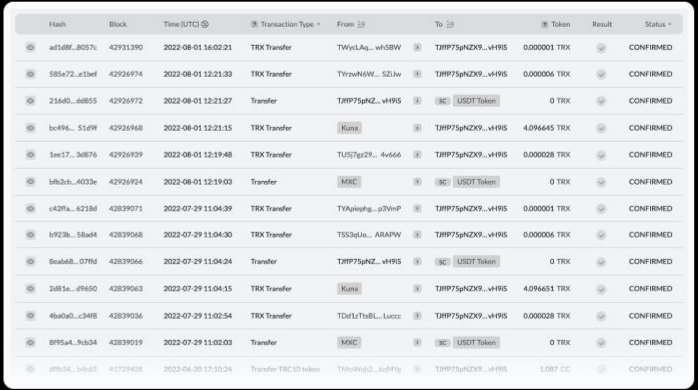
BLOCKCHAIN ANALYSIS OF THE MOVEMENT OF STOLEN FUNDS

3

Allows you to understand where the stolen crypto went

HOW ORDINARY USERS SEE BLOCKCHAIN:

through **blockchain explorer**

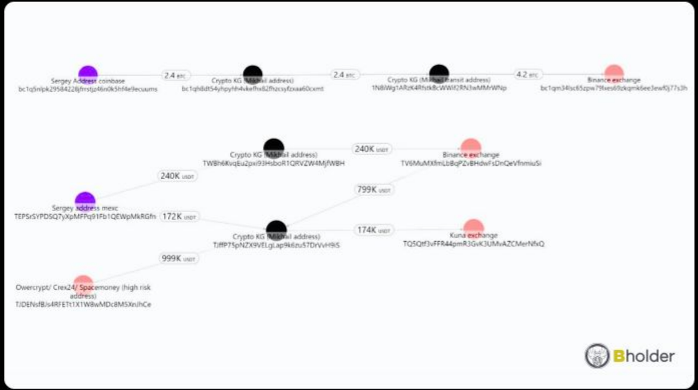


Hash	Block	Time (UTC)	Transaction Type	From	To	Token	Result	Status
ad1d8f...8057c	42931390	2022-08-01 16:02:21	TRX Transfer	TWycLAq... wh5BW	TJffP75pNZX9...vH9iS	0.000001 TRX	✓	CONFIRMED
585e72...e1bef	42926974	2022-08-01 12:21:33	TRX Transfer	TYrzwN6W... SZiJw	TJffP75pNZX9...vH9iS	0.000006 TRX	✓	CONFIRMED
216d0... dd855	42926972	2022-08-01 12:21:27	Transfer	TJffP75pNZ... vH9iS	SC USDT Token	0 TRX	✓	CONFIRMED
bc496... 51d9f	42926968	2022-08-01 12:21:15	TRX Transfer	Kuna	TJffP75pNZX9...vH9iS	4.096645 TRX	✓	CONFIRMED
1ee17... 3d876	42926939	2022-08-01 12:19:48	TRX Transfer	TU5j7gz29... 4v666	TJffP75pNZX9...vH9iS	0.000028 TRX	✓	CONFIRMED
bfb2cb...4033e	42926924	2022-08-01 12:19:03	Transfer	MXC	SC USDT Token	0 TRX	✓	CONFIRMED
c42ffa... 6218d	42839071	2022-07-29 11:04:39	TRX Transfer	TYApiephg... p3VmP	TJffP75pNZX9...vH9iS	0.000001 TRX	✓	CONFIRMED
b923b... 58ad4	42839068	2022-07-29 11:04:30	TRX Transfer	TSS3qUo... ARAPW	TJffP75pNZX9...vH9iS	0.000006 TRX	✓	CONFIRMED
8eab68... 07ffd	42839066	2022-07-29 11:04:24	Transfer	TJffP75pNZ... vH9iS	SC USDT Token	0 TRX	✓	CONFIRMED
2d81e... d9650	42839063	2022-07-29 11:04:15	TRX Transfer	Kuna	TJffP75pNZX9...vH9iS	4.096651 TRX	✓	CONFIRMED
4ba0a0...c34f8	42839036	2022-07-29 11:02:54	TRX Transfer	TDd1zTtsBL... Luccc	TJffP75pNZX9...vH9iS	0.000028 TRX	✓	CONFIRMED
8f95a4...9cb34	42839019	2022-07-29 11:02:03	Transfer	MXC	SC USDT Token	0 TRX	✓	CONFIRMED
dffb34... b4c65	41729428	2022-06-20 17:10:24	Transfer TRC10 token	TNtoWqh2... 6qMYg	TJffP75pNZX9...vH9iS	1,087 CC	✓	CONFIRMED

- 👎 Tabular, non-visual form
- 👎 Faceless addresses
- 👎 Excessive transaction detail

VS

through **Bholder**



Sergey Address coinbase
bc1q5nlpk2958422Bjfrrstjz46n0k5hf4e9ecuums
2.4 BTC
Crypto KG (Mikhail address)
bc1qh8dt54yhpyhh4vkefhx82fhzcsyfzxaa60cxmt
2.4 BTC
Crypto KG (Mikhail transit address)
1N8Wg1ARzK4RfstkBcWWif2RN3wMMrWNp
4.2 BTC
Binance exchange
bc1qm34lsc65zpw79lxes69zkqmk6ee3ewf0j77s3h
Crypto KG (Mikhail address)
TWBh6KvqEu2pxi93HsboR1QRVZW4MjfWBH
240K USDT
Binance exchange
TV6MuMXfmLbBqPZvBHdwFsDnQeVfnmiuSi
240K USDT
799K USDT
Sergey address mexc
TEPSrSYPDSQ7yXpMFPq91Fb1QEWpMkRGfn
172K USDT
Crypto KG (Mikhail address)
TJffP75pNZX9VELgLap9k6zu57DrVvH9iS
174K USDT
Kuna exchange
TQ5Qtf3vFFR44pmR3GvK3UMvAZCMerNfxQ
999K USDT
Owercrypt/ Crex24/ Spacemoney (high risk address)
TJDENsfBJs4RFETt1X1W8wMDc8M5XnJhCe
Bholder

- 👍 Visual graph of connections
- 👍 Known names and address types
- 👍 Sun of all transactions between counterparties

RECOMMENDATIONS FOR FURTHER ACTIONS

4

Allows actions to be broken down into a simple and understandable plan for law enforcement agencies

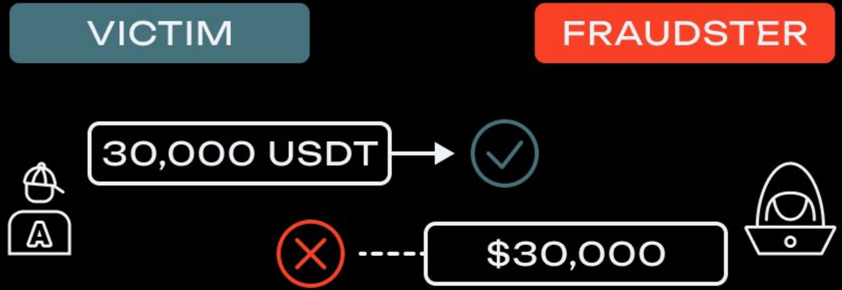
AML CRYPTO WILL BUY YOUR BICYCLE

Very interesting, just tell me the details where to deposit the money

FRAUDULENT CASE

P2P CRYPTO EXCHANGE VIA TELEGRAM

The fraudster poses as the guarantor of the transaction and the buyer of the cryptocurrency, receives funds from the victim



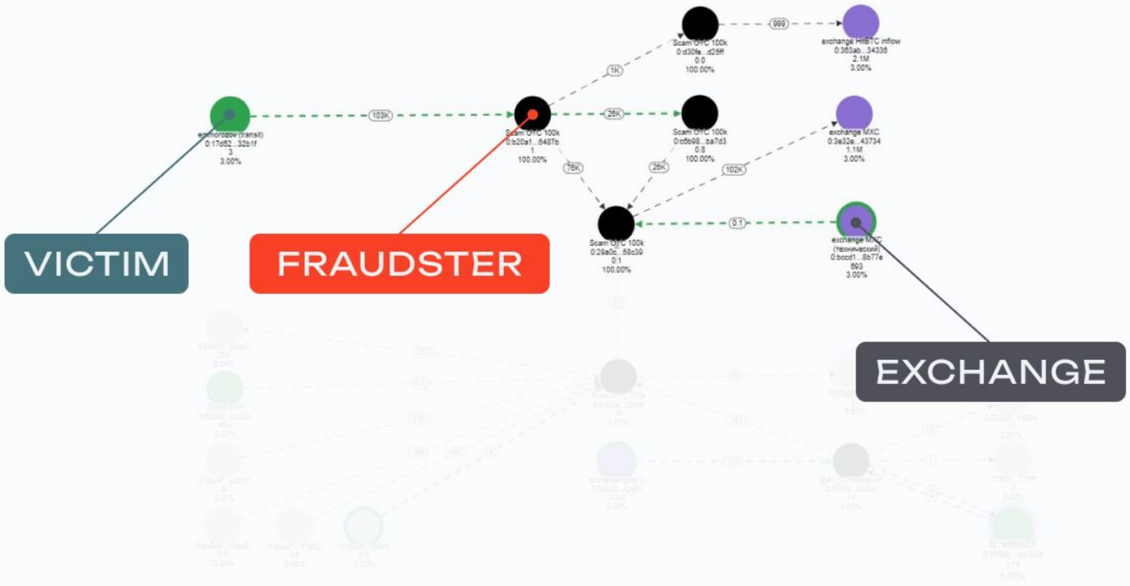
VICTIM

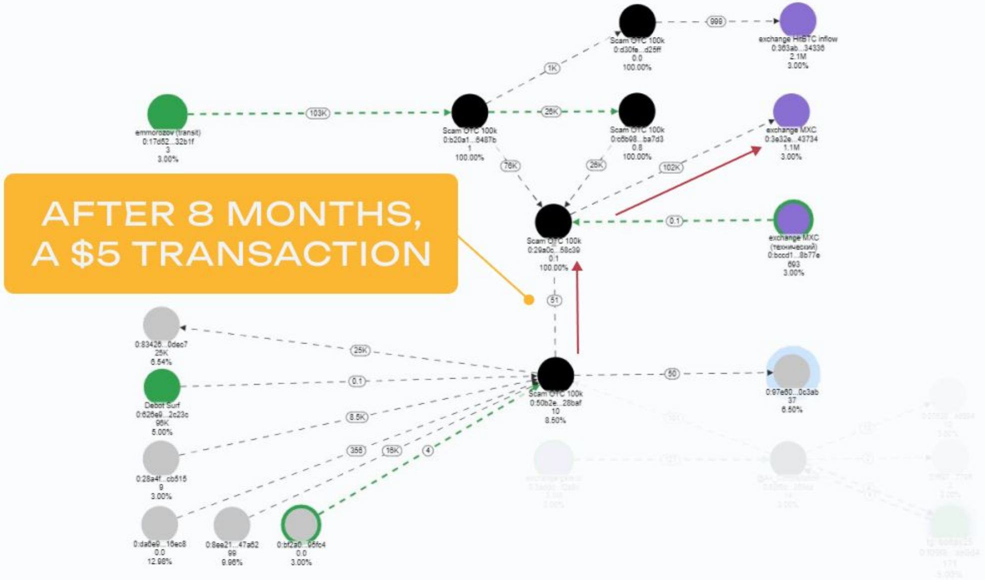
FRAUDSTER

30,000 USDT → ✓

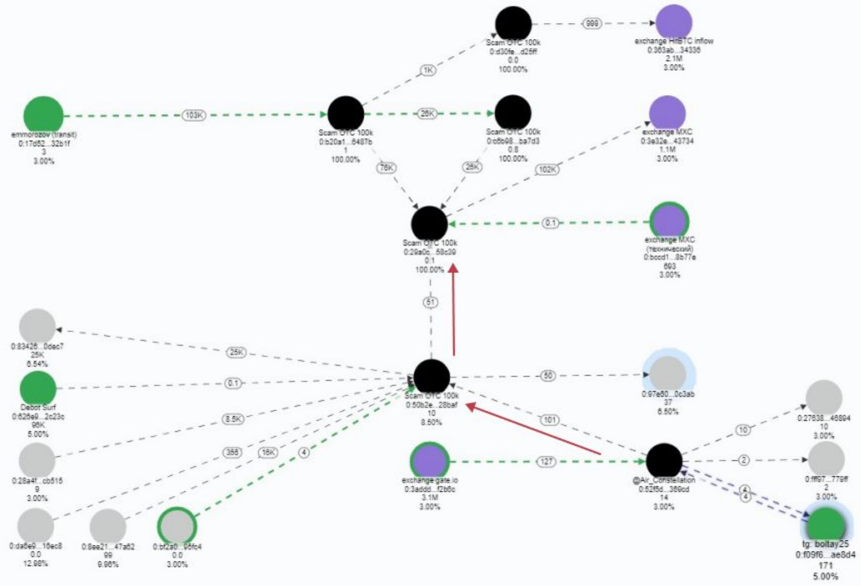
☒ ---- $30,000

Sum of loss: **$30,000** Token: **USDT / EVER**

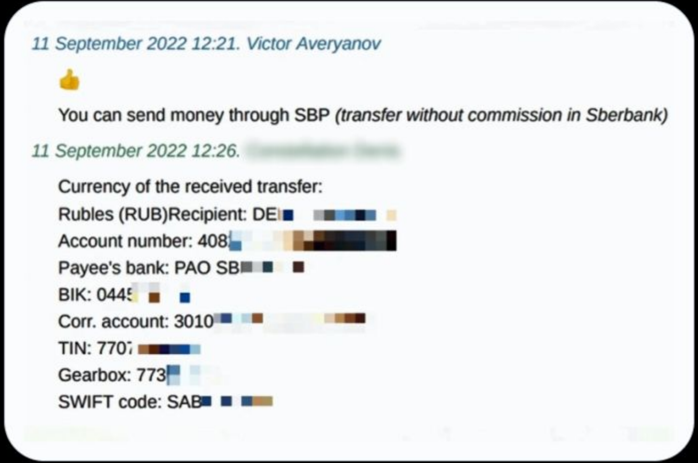

exmorozov (transit)
0:17d52...32b1f
3
3.00%
103K
Scam OTC 100k
0:b20a1...6487b
1
100.00%
1K
Scam OTC 100k
0:d30fe...d25ff
0.0
100.00%
999
exchange HitBTC inflow
0:363ab...34336
2.1M
3.00%
26K
Scam OTC 100k
0:c6b98...ba7d3
0.8
100.00%
exchange MXC
0:3e32e...43734
1.1M
3.00%
76K
26K
102K
Scam OTC 100k
0:29a0c...58c39
0.1
100.00%
0.1
exchange MXC
(технический)
0:bccd1...8b77e
693
3.00%
VICTIM
FRAUDSTER
EXCHANGE



AFTER 8 MONTHS, A $5 TRANSACTION


Scam OTC 100k
0:d30fe...d25ff
0.0
100.00%
999
exchange HitBTC inflow
0:363ab...34336
2.1M
3.00%
1K
emmorozov (transit)
0:17d52...32b1f
3
3.00%
103K
Scam OTC 100k
0:b20a1...6487b
1
100.00%
26K
Scam OTC 100k
0:c6b98...ba7d3
0.8
100.00%
exchange MXC
0:3e32e...43734
1.1M
3.00%
76K
26K
102K
Scam OTC 100k
0:29a0c...58c39
0.1
100.00%
0.1
exchange MXC
(технический)
0:bccd1...8b77e
693
3.00%
51
0:83426...0dec7
25K
6.54%
25K
Debot Surf
0:626e9...2c23c
96K
5.00%
0.1
8.5K
0:28a4f...cb515
9
3.00%
358
16K
4
0:da6e9...16ec8
0.0
12.98%
0:8ee21...47a62
99
9.96%
0:bf2a0...96fc4
0.0
3.00%
Scam OTC 100k
0:50b2e...28baf
10
8.50%
50
0:97e60...0c3ab
37
6.50%
101
exchange gate.io
0:3addd...f2b6c
3.1M
3.00%
127
@Air_Constellation
0:52f5d...369cd
14
3.00%
10
0:27638...46894
10
3.00%
2
0:fff97...779ff
2
3.00%
4
4
tg: boltay25
0:f09f6...ae8d4
171
5.00%

ANALYZING DIGITAL FOOTPRINTS AND TRANSACTIONS VIA Bholder



11 September 2022 12:21. Victor Averyanov

👍

You can send money through SBP *(transfer without commission in Sberbank)*

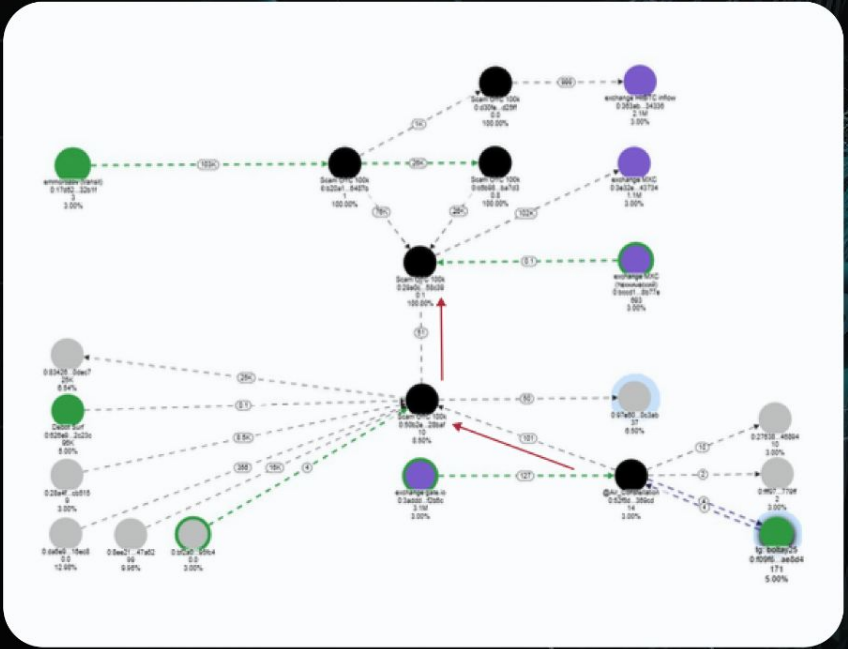
11 September 2022 12:26. [redacted]

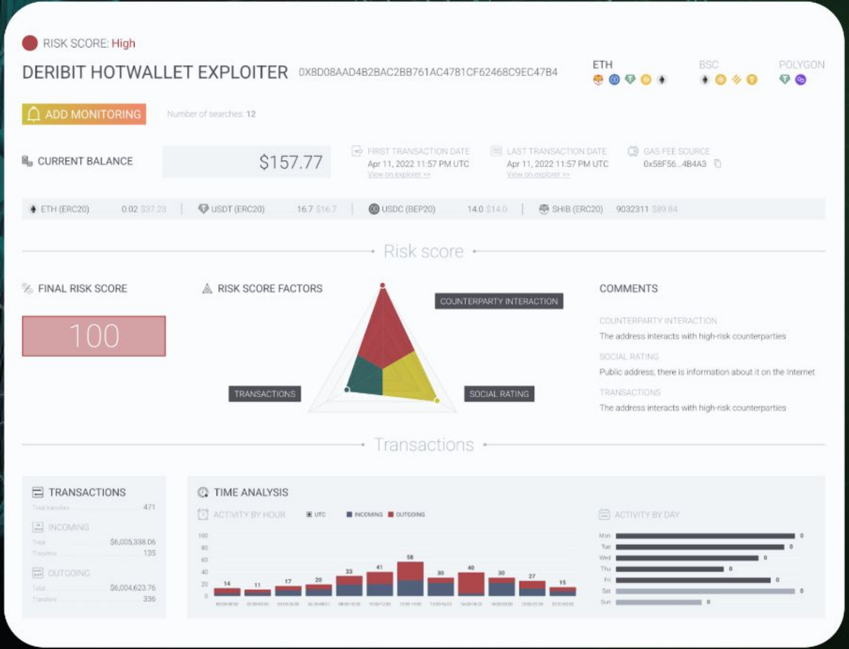
Currency of the received transfer:
Rubles (RUB)Recipient: DE[redacted]
Account number: 408[redacted]
Payee's bank: PAO SB[redacted]
BIK: 044[redacted]
Corr. account: 3010[redacted]
TIN: 770[redacted]
Gearbox: 773[redacted]
SWIFT code: SAB[redacted]

OUR SOLUTIONS

Bholder. Graph of connections

Btrace. Address checking





● RISK SCORE: High

DERIBIT HOTWALLET EXPLOITER 0X8D08AAD4B2BAC2BB761AC4781CF62468C9EC47B4

ETH BSC POLYGON

ADD MONITORING

Number of searches: 12

CURRENT BALANCE $157.77

FIRST TRANSACTION DATE
Apr 11, 2022 11:57 PM UTC
View on explorer >>

LAST TRANSACTION DATE
Apr 11, 2022 11:57 PM UTC
View on explorer >>

GAS FEE SOURCE
0x58F56...4B4A3

ETH (ERC20) 0.02 $37.23 | USDT (ERC20) 16.7 $16.7 | USDC (BEP20) 14.0 $14.0 | SHIB (ERC20) 9032311 $89.84

Risk score

FINAL RISK SCORE

100

RISK SCORE FACTORS

COMMENTS

COUNTERPARTY INTERACTION
The address interacts with high-risk counterparties

SOCIAL RATING
Public address, there is information about it on the Internet

TRANSACTIONS
The address interacts with high-risk counterparties

Transactions

TRANSACTIONS

Total transfers	471

INCOMING

Total	$6,005,338.06
Transfers	135

OUTGOING

Total	$6,004,623.76
Transfers	336

TIME ANALYSIS

ACTIVITY BY HOUR ▣ UTC ■ INCOMING ■ OUTGOING

ACTIVITY BY DAY

AML CRYPTO
BLOCKCHAIN ANALYTICS · CRYPTO INVESTIGATION

MAKE BLOCKCHAIN TRANSPARENT AGAIN IN PARTNERSHIP

Vladimir Lazarev
Ilya Boytsov

✉ Lvv@amlcrypto.io

Telegram @AMLcrypto

amlcrypto.io