BSVCloud.com Investigation Report: Exchange Exit Points Analysis

Executive Summary

This updated investigation into bsvcloud.com has uncovered critical evidence regarding the movement of stolen cryptocurrency. Most significantly, we have confirmed that funds were moved to an OKX exchange hot wallet, providing a direct connection to a major cryptocurrency exchange where the operators may be attempting to cash out stolen funds. This report details our findings on exchange exit points, transaction patterns, and recommendations for potential recovery options.

1. Key Exchange Exit Points

Confirmed OKX Exchange Connection

- **Address**: bc1quhruqrghgcca950rvhtrg7cpd7u8k6svpzgzmrjy8xyukacl5lkq0r8l2d
- **Status**: Confirmed as OKX Exchange Hot Wallet
- **Evidence**: Labeled as "Exchange: OKX, Hot Wallet" in the OKX blockchain explorer
- **Significance**: This address was previously identified in the investigation as potentially containing a significant amount of funds (possibly up to $250 million)

Transaction Flow to Exchange

The investigation has traced a clear pattern of fund movement from victim deposits to exchange wallets:

1. **Initial Collection Points**:
   - 3LXZ5o9DRHWRMhLXxyXqXidcj3A1F5JCjN (received user's 0.05355071 BTC)
   - MVWSK6wHvYQvQcfvYQuLgd8J8MhCbMtQJe (received user's 48.5000076 LTC)
   - Multiple other addresses across different cryptocurrencies
2. **Intermediate Addresses**:
   - 3LaRfQs5611ChaDdmY5B7QPCVHdjk4qnz5 (high volume address with 173 transactions)
   - bc1q4ud9tc7mmv0t6c2ssgunk22sdj3m0m8qs2s287 (33 transactions)
   - Various other addresses used to move funds between collection points and final destinations
3. **Final Destination**:
   - bc1quhruqrghgcca950rvhtrg7cpd7u8k6svpzgzmrjy8xyukacl5lkq0r8l2d (OKX Exchange Hot Wallet)

2. Fund Movement Analysis

Transaction Characteristics

1. **Multi-Step Transfers**:
   - Funds typically move through multiple addresses before reaching exchange wallets
   - This "layering" technique is commonly used to obscure the trail of funds
2. **Multi-Currency Operations**:
   - The scam operates across multiple cryptocurrencies (BTC, LTC, ETH, BNB, BCH, DOGE)
   - This diversification makes tracing more difficult by spreading transactions across different blockchains
3. **Exchange Deposits**:
   - The final step in the pattern involves transferring funds to exchange wallets
   - OKX has been confirmed as one of the exchanges used

Volume Analysis

3LXZ5o9DRHWRMhLXxyXqXidcj3A1F5JCjN

- Total transactions: 67
- Total volume: 1.48706712 BTC (approximately $122,227)
- Current balance: 0 BTC

3LaRfQs5611ChaDdmY5B7QPCVHdjk4qnz5

- Total transactions: 173
- Total volume: 37.39446108 BTC (approximately $3,076,849)
- Current balance: 0.00000600 BTC ($0.49)

bc1q4ud9tc7mmv0t6c2ssgunk22sdj3m0m8qs2s287

- Total transactions: 33
- Transaction fees: 0.0080087 BTC
- Current balance: 0 BTC

bc1quhruqrghgcca950rvhtrg7cpd7u8k6svpzgzmrjy8xyukacl5lkq0r8l2d

- Confirmed as OKX Exchange Hot Wallet
- Reportedly contains significant funds (possibly up to $250 million)

Timing Patterns

The transaction history shows a systematic approach to moving funds:

1. **Collection Phase**:

- Victim deposits are collected in initial addresses
- These addresses show incoming transactions from multiple sources

2. **Consolidation Phase**:
   - Funds are moved to intermediate addresses
   - These addresses show both incoming and outgoing transactions
3. **Exchange Deposit Phase**:
   - Funds are ultimately transferred to exchange wallets
   - This enables conversion to other cryptocurrencies or fiat

3. Recovery Recommendations

OKX Cooperation Potential

The identification of OKX as an exit point creates a potential recovery avenue:

1. **Exchange Notification**: OKX can be notified about the fraudulent activity with specific transaction details
2. **Account Identification**: OKX has the ability to identify which user account(s) received funds from the identified addresses
3. **Potential Fund Freezing**: If notified promptly, OKX may be able to freeze accounts associated with the scam
4. **Law Enforcement Cooperation**: OKX typically cooperates with law enforcement agencies in cases of fraud

Recommended Actions

1. **File a report with OKX**:
   - Submit detailed information about the scam
   - Provide all transaction IDs and addresses
   - Include evidence of the fraudulent nature of BSVCloud
2. **Law Enforcement Report**:
   - File a report with relevant authorities
   - Emphasize the connection to OKX exchange
   - Request assistance in contacting OKX through official channels
3. **Blockchain Forensics**:
   - Consider engaging a professional blockchain forensics service
   - They can provide more detailed analysis of fund movements
   - May have established relationships with exchanges for recovery

4. Website and Domain Analysis (From Previous Investigation)

False Company Claims

- **Establishment Date Discrepancy**: Claims to be "Established in 2017" but domain was only registered in December 2018
- **Anniversary Contradiction**: Running an "8 YEARS Anniversary SALE" which contradicts their own founding date claim

- **No Official Registration**: No company registered as "BSVCloud" or "BSV Cloud" exists in the UK Companies House database
- **False Regulatory Claims**: Claims to be "registered and operating under UK regulations" but has no regulatory authorization

Domain Registration Details

- **Registrar**: NameCheap, Inc.
- **Domain Created**: 2018-12-21 (contradicting their claim of being established in 2017)
- **Domain Updated**: 2025-04-03
- **Domain Expires**: 2026-12-21
- **Status**: clientTransferProhibited

Privacy Protection Service

- **Service Provider**: Withheld for Privacy ehf
- **Address**: Kalkofnsvegur 2, Reykjavik, Capital Region, 101, Iceland
- **Phone**: +354.4212434

5. Conclusion

The investigation has uncovered critical evidence linking BSVCloud's fraudulent operation to the OKX cryptocurrency exchange. The confirmation that funds were moved to an OKX exchange hot wallet provides a significant lead for potential recovery efforts. This finding supports the theory that the BSVCloud operators are using established cryptocurrency exchanges to cash out stolen funds.

The fund movement analysis reveals a sophisticated operation designed to obscure the trail of stolen cryptocurrency. The operators of BSVCloud have implemented a multi-step, multi-currency approach to laundering the funds, with the final destination being cryptocurrency exchanges, particularly OKX.

By focusing recovery efforts on working with OKX, there may be a possibility of identifying the perpetrators or freezing their assets. This represents the most promising avenue for potential recovery of the stolen funds.

6. Additional Resources

A comprehensive investigation website documenting findings about the BSVCloud.com scam has been created at: https://fuimqbjo.manus.space