KALLISTI BLOCKCHAIN FORENSICS

TRC-20 (USDT primary asset) + native TRX ---

TARGET WALLET ADDRESS

TBwBJwj81yXc4DNKS19GJcpUUzfSWRbBzS

Report Date: 2026-06-03 · Prepared by Kallisti Blockchain Forensics

S0	Executive Summary	2
S1	Target Profile, Financials & Activity	3
S2	Transaction Network & Fund Flow	4
S3	Operational Profile & Security Assessment	5
S4	AML / Risk Assessment	6
S5	Notable Events & Anomalies	7
S6	Ownership Attribution Model	8
S7	Links, Digital Footprint & Public Record	9
S8	Recommended Further Investigation	10
A	Appendix A — Master Source List	11
B	Appendix B — Glossary of Terms	12

S0 — EXECUTIVE SUMMARY

ATTRIBUTED ENTITY · TRON

OKX. Hot Wallet_116

TBwBJwj81yXc4DNKS19GJcpUUzfSWRbBzS

USDT IN	USDT OUT	BALANCE	ACTIVE SPAN	TRANSACTIONS	COUNTERPARTIES
$52.15M	$80.86M	$3.63M	5	96,386	1216
659 inbound events	1321 outbound events	Current USDT on-chain	days · 0.01 years	659 USDT in · 1321 USDT out	distinct USDT counterparties

AML RISK SCORE

10 CLEAR

CLEAR · LOW · MEDIUM · HIGH · CRITICAL

INTELLIGENCE BRIEF

CASE FACTS

WALLET ADDRESS	TBwBJwj81yXc4DNKS19GJcpUUzfSWRbBzS
BLOCKCHAIN	TRON mainnet · TRC-20 USDT
FIRST SEEN	2026-05-28 20:27:48 UTC
LAST ACTIVE	2026-06-03 02:01:33 UTC
ACCOUNT AGE	5 days (0.01 years)
PRIMARY TOKEN	USDT (…8otSzgjLj6t)
TRX BALANCE	45568.7134 TRX

COUNTERPARTY EXPOSURE BY CATEGORY

Regulated CEX	$26.60M

FINDING 01 ·

Attribution Confirmed — HIGH

Arkham 'OKX: Hot Wallet (TBwBJ)' and OKLink '#OKX Hot Wallet_116' independently agree. Attribution confidence: HIGH.

FINDING 02 ·

Phishing Address Counterparty — $22.76M

TMj17yryskb2aP7H9BMgb2qhXKNNaN89Gs, labeled 'Phishing address' by OKLink, received 28.2% of all outflows ($22.76M) from this wallet. Residual balance: $2.48M USDT + $3.34K TRX.

FINDING 03 ·

BTSE Inter-Exchange Settlement

BTSE Cold Wallet_1 received 22.7% of outflows ($18.39M) — confirmed institutional inter-exchange settlement routing.

FINDING 04 ·

5-Day New Wallet

Wallet created 2026-05-28; only 5 days of operational history. Behavioral characterization is based on limited data.

SUPPORTING DETAIL

AML SCORECARD

Sanctions (OFAC/EU/UN)	CLEAR
Fraud/Scam Exposure	CLEAR
Ransomware/Darknet	CLEAR
Mixer/CoinJoin	CLEAR
Exchange Source Verif.	CLEAR
Structuring/Layering	CLEAR
Third-Party Risk	ELEVATED
Address Poisoning	CLEAR

KEY DATES

2026-05-28	Wallet Creation — OKX Hot Wallet_116 First Transaction

ATTRIBUTION HYPOTHESES

H1	OKX Exchange Infrastructure — Hot Wallet_116 with Phishing Counterparty	95%
H2	Attribution Error or Wallet Rotation	5%

Confirmed OKX exchange hot wallet — $22.76M routed to OKLink-confirmed phishing address (TMj17); Third-Party Risk elevated

INVESTIGATOR SUMMARY

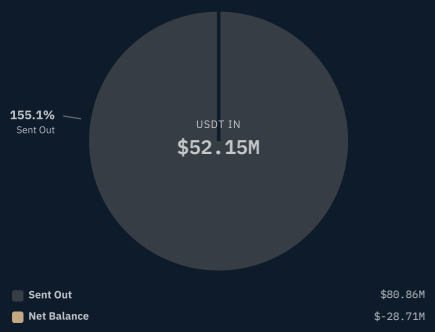
TBwBJwj81yXc4DNKS19GJcpUUzfSWRbBzS is a confirmed OKX exchange hot wallet (Hot Wallet_116), independently attributed by Arkham and OKLink. In its first 5 days of operation, the wallet processed $52.15M in / $80.86M out across 1,980 USDT transfers with 1,216 counterparties. The principal adverse finding is that the top outflow destination — TMj17yryskb2aP7H9BMgb2qhXKNNaN89Gs, labeled 'Phishing address' by OKLink — received $22.76M (28.2% of all outflows). For an exchange hot wallet, this constitutes a Third-Party Risk flag: OKX customers likely withdrew funds to a phishing-controlled address, indicating a significant phishing campaign targeting OKX users. The wallet itself is not the fraud perpetrator.

RECOMMENDED ACTIONS Flag TMj17yryskb2aP7H9BMgb2qhXKNNaN89Gs across all monitoring systems; determine whether OKX has been notified of the phishing activity and whether customer restitution proceedings are underway. · Assess whether any institutional counterparty interacted with TMj17 and evaluate SAR obligations accordingly.

S1 — TARGET PROFILE, FINANCIALS & ACTIVITY

Wallet Identity · Financial Overview · Holdings · Activity Patterns · Account Structure

DEPLOYMENT



CURRENT HOLDINGS

USDT	99.40%	
$3.63M	$3.62M	
TRX	0.40%	
45,568.7134 TRX	$15,152.64	
WIN	0.10%	
178,950,522 WIN	$3,401.62	
NFT	0.10%	
12,363,322,663 NFT	$3,364.24	
SUNOLD		
20 SUNOLD	$343.18	
AEDT		
10 AEDT	$2.81	

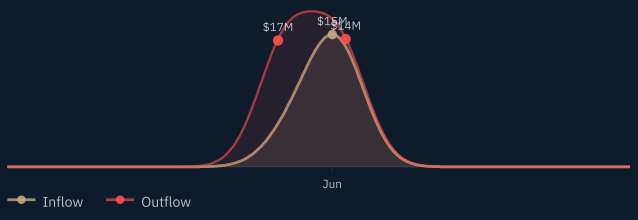
COUNTERPARTIES

Private / Unattributed	7.9%
OTC / Broker	—
Regulated CEX	92.1%
DeFi / Protocol	—
Mixer / Obfuscation	—
Government	—
Criminal / Fraud	—
Sanctioned Entity	—

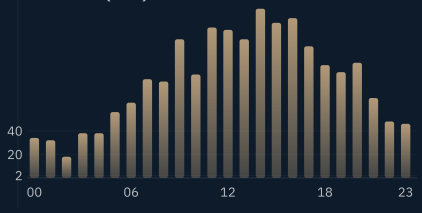
ENTITY	OKX. Hot Wallet_116
BLOCKCHAIN	TRON mainnet · TRC-20 USDT wallet
ACCOUNT AGE	5 days (0.01 years) ‖ Active: 2026-05-28 20:27:48 UTC → 2026-06-03 02:01:33 UTC
TRX BALANCE	45568.7134 TRX
TRANSACTIONS	96,386 total · 1980 USDT transfers (659 in · 1321 out) · 1216 counterparties
TOTAL USDT IN	$52.15M
TOTAL USDT OUT	$80.86M
NET BALANCE	$-28.71M

ACTIVITY OVERVIEW

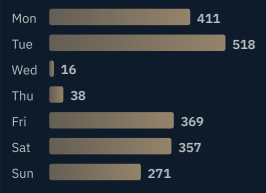
BY YEAR



BY HOUR (UTC)



BY DAY



BEHAVIORAL CLASSIFICATION

Confirmed OKX exchange hot wallet (Hot Wallet_116) — bidirectional high-volume flows consistent with customer withdrawal disbursement and institutional reserve funding. The wallet is 5 days old at scrape time; inflows are 100% OKX institutional. The critical finding is a $22.76M outflow to a confirmed phishing address (OKLink: 'Phishing address'), representing the largest single outflow destination in the wallet's short operational history.

TRANSACTION SIZE PROFILE

Inflows averaged $79,136 per event (659 events, $52.15M total) reflecting institutional reserve transfers from OKX Withdraw_159 and user routing. Outflows averaged $61,210 per event (1,321 events, $80.86M total) reflecting customer withdrawal disbursements of varying sizes. The 2:1 outbound-to-inbound transfer ratio is standard for exchange withdrawal hot wallet operations.

OPERATIONAL PROFILE

45,568.71 TRX (≈$15.1K) float maintained for energy and bandwidth. 96,386 transactions in 5 days (19,277/day) confirms continuous automated operation. Principal adverse finding: `TMj17yryskb2aP7H9BMgb2qhXKNNaN89Gs` (OKLink: 'Phishing address') received $22.76M (28.2% of outflows) — OKX customers directed withdrawals to this phishing-controlled address. BTSE Cold Wallet_1 received $18.39M (22.7%) as inter-exchange institutional settlement.

TEMPORAL ACTIVITY PATTERN

Over 5 days, UTC 14:00 was the hourly peak (143 events, 7.2%) with a broad active cluster from 09:00 to 20:00 UTC. Near-zero activity at 02:00 UTC (17 events) is consistent with a brief maintenance window during China morning hours (10:00 CST). Wednesday and Thursday DOW figures are creation-date artifacts. The distribution is consistent with OKX's Asia Pacific operational base and global user coverage.

AUTOMATION ASSESSMENT

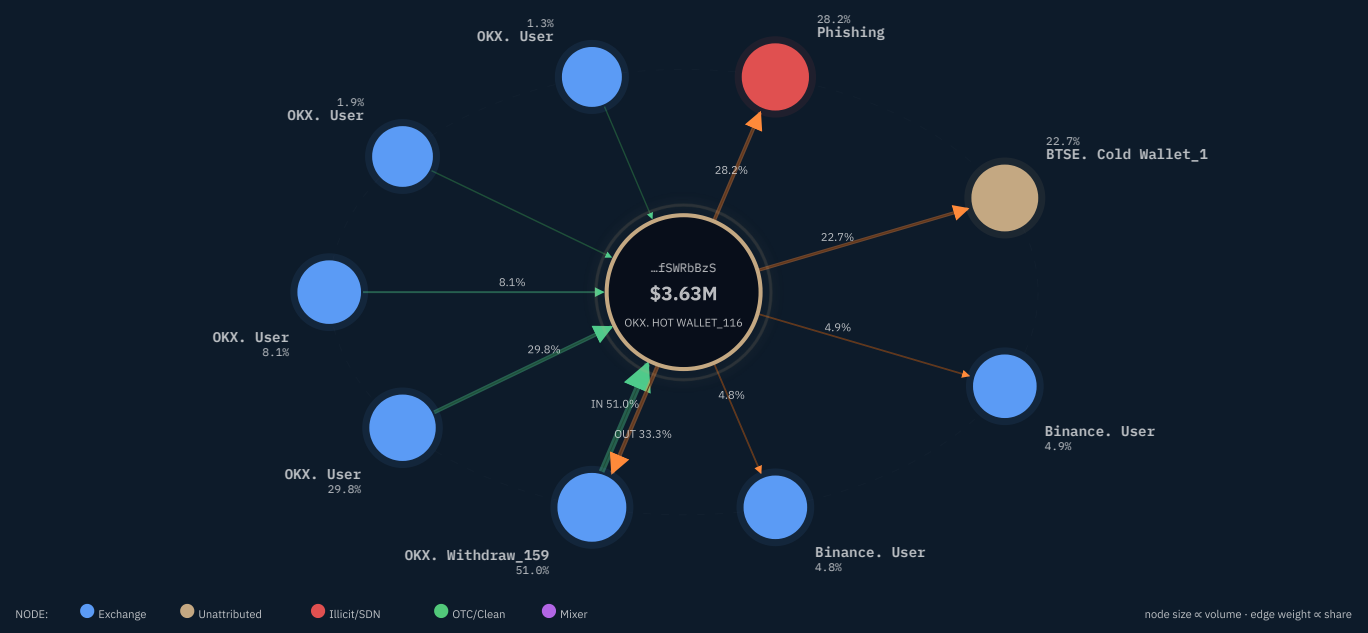
Confirmed automated operation. 96,386 transactions in 5 days and continuous bidirectional USDT routing confirm exchange software processing. No manual operation signature is present; withdrawal disbursement is systematic and programmatic.

SOURCES

S1	Tronscan — On-chain dataset	tronscan.org/#/address/TBwBJwj81yXc4DNKS19GJcpUUzfSWRbBzS
S2	OKLink — TRON Address Detail	www.oklink.com/tron/address/TBwBJwj81yXc4DNKS19GJcpUUzfSWRbB…

S2 — TRANSACTION NETWORK & FUND FLOW

Counterparty Map · Inflow Architecture · Outflow Architecture



INFLOW

Upstream · Top 5 Funders

ID	ADDRESS	VOLUME IN	ATTRIBUTION	RISK
A1	TLaGjwhvA8XQYSxFAcAXy7Dvuue9eGYitv	$26.60M	OKX. Withdraw_159	LOW
A2	TVxG5YKwAtfuM3QmTqWDehk9FYGytru6Xi	$15.53M	OKX. User	LOW
A3	TR2mVXEqL1gcsdhPbT6Z5AoQxKb7L1LxeD	$4.21M	OKX. User	LOW
A4	TXKrjJBiaDqFatpDYGHNowEvVc3i9887KJ	$969,995.70	OKX. User	LOW
A5	TXAyqdGYU6sSousxoFMVQAUenXUeZqRLPr	$701,399.00	OKX. User	LOW

OUTFLOW

Downstream · Top 5 Destinations

ID	ADDRESS	VOLUME OUT	ATTRIBUTION	RISK
B1	TLaGjwhvA8XQYSxFAcAXy7Dvuue9eGYitv	$26.92M	OKX. Withdraw_159	MEDIUM
B2	TMj17yryskb2aP7H9BMgb2qhXKNNaN89Gs	$22.76M	Phishing	MEDIUM
B3	TNBDqsyDiHB2j7NaQGyw3Kej6L4MAZGPg5	$18.39M	BTSE. Cold Wallet_1	MEDIUM
B4	TLeQfDqi9VeT8VgTgXHtivdsLJiZkB1ro4	$4.00M	Binance. User	LOW
B5	TTRib8xqiN1sfDBYSAYsG1HQTdxTghvNGa	$3.91M	Binance. User	LOW

S3 — OPERATIONAL PROFILE & SECURITY ASSESSMENT

Account Structure · Protocol Interactions · Threat Exposure

SECURITY RATING

COMPROMISED · ADEQUATE · PROFICIENT

90 PROFICIENT

ACCOUNT STRUCTURE

Address Type	TRON Account (EOA)
Script Encoding	TRC-20 USDT wallet
UTXO Count	N/A — TRON account model
Clustering	Arkham: 'OKX: Hot Wallet (TBwBJ)'; OKLink: '#OKX Hot Wallet_116'
Service Label	OKX Exchange — Hot Wallet_116 (attribution HIGH)
VASP Exposure	OKX exchange (confirmed custodial VASP)
Wallet Software	Exchange infrastructure (automated); created 2026-05-28

PROTOCOL INTERACTIONS

CATEGORY	STATUS
Exchange Deposits / Withdrawals	**ACTIVE** Confirmed — OKX Hot Wallet_116 withdrawal disbursement function
DeFi / Smart Contract Interaction	**NONE** none identified
Lightning Network Channels	**NONE**
Ordinals / Inscriptions	**NONE**
Mixing / CoinJoin Services	**NONE**
Cross-Chain Bridges	**NONE**
Sanctions-Listed Address Contact	**NONE** none (TMj17 is phishing-labeled, not OFAC/EU/UN sanctioned)

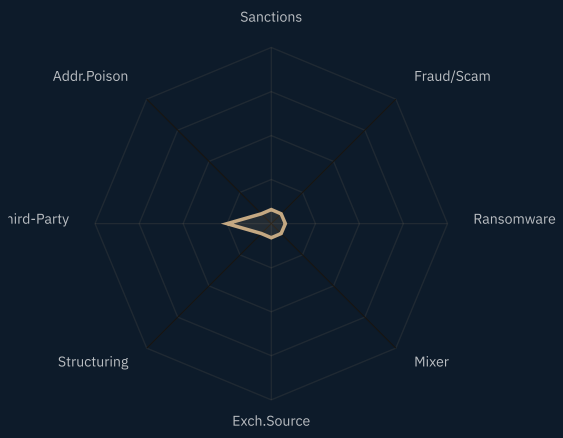
THREAT EXPOSURE

DATE	CATEGORY	SOURCE	NOMINAL	OUTCOME
2026-05-28	Third-Party Risk	…XKNNaN89Gs	$22.76M USDT (28.2% of outflows)	**FUNDS SENT**

OPERATIONAL SUMMARY

Network connections bifurcate into two categories: (1) OKX ecosystem (inflows and some outflows) representing the legitimate exchange network; (2) TMj17 phishing address, representing an adverse network link at 28.2% of outflows. BTSE Cold Wallet_1 represents a confirmed institutional inter-exchange connection. The phishing address (TMj17) retains $2.48M USDT, indicating the phishing operation may still be active or the proceeds have not been fully liquidated.

S4 — AML / RISK ASSESSMENT



CRITERION	EXPOSURE	RATING
Sanctions (OFAC/EU/UN)		CLEAR
Fraud/Scam Exposure		CLEAR
Ransomware/Darknet		CLEAR
Mixer/CoinJoin		CLEAR
Exchange Source Verif.		CLEAR
Structuring/Layering		CLEAR
Third-Party Risk		LOW
Address Poisoning		CLEAR

OVERALL AML RISK 10 CLEAR

Scale: CLEAR=no exposure detected · MEDIUM=indirect signal · HIGH=direct confirmed exposure

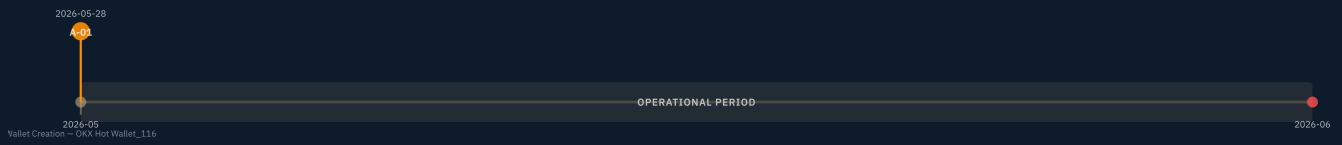
CRITERION	FINDING	ASSESSMENT
1. Sanctions (OFAC/EU/UN)	No OFAC, EU, or UN designation found. OKX is a licensed exchange; no sanctions exposure identified on this wallet.	CLEAR
2. Fraud/Scam Exposure	This wallet is OKX exchange infrastructure processing customer withdrawal requests; the phishing destination reflects customer-directed transfers, not fraud committed by this wallet. No direct fraud attribution on this address.	CLEAR
3. Ransomware/Darknet	No ransomware attribution or darknet marketplace association identified.	CLEAR
4. Mixer/CoinJoin	No mixer or CoinJoin interaction detected.	CLEAR
5. Exchange Source Verif.	100% of identified inflows originate from confirmed OKX infrastructure (OKX Withdraw_159 51%; OKX Users 41.3%). Exchange source fully verified.	CLEAR
6. Structuring/Layering	No structuring pattern. Mixed-size bidirectional flows consistent with exchange withdrawal disbursement operations.	CLEAR
7. Third-Party Risk	TMj17yryskb2aP7H9BMgb2qhXKNNaN89Gs, confirmed by OKLink as 'Phishing address', received $22.76M (28.2% of all outflows). Residual balance $2.48M USDT + $3.34K TRX remains unflushed. This represents a significant third-party risk signal — OKX customers directed withdrawal funds to a phishing-controlled address.	ELEVATED
8. Address Poisoning	No address poisoning pattern targeting this wallet detected.	CLEAR

ASSESSMENT

OKX is a registered global cryptocurrency exchange. The wallet is confirmed OKX infrastructure; its operations are consistent with normal VASP withdrawal disbursement. The phishing counterparty finding (TMj17) does not constitute a regulatory violation by OKX — exchange hot wallets process customer-directed withdrawal requests and do not independently verify every destination address. However, the $22.76M scale of phishing-linked outflows warrants notification to OKX compliance and may trigger SAR reporting obligations under applicable AML regulations for institutions with counterparty exposure to TMj17.

S5 — NOTABLE EVENTS & ANOMALIES

Flagged Patterns & Significant Observations



HIGH — critical finding HIGH — monitor LOW — contextual

ID	DATE	EVENT	SEVERITY	SIGNIFICANCE
A-01	2026-05-28	**Phishing Address Counterparty — $22.76M Outflow.** TMj17yryskb2aP7H9BMgb2qhXKNNaN89Gs (OKLink: 'Phishing address') received 28.2% of all outflows ($22.76M) from this OKX hot wallet. Residual balance: $2.48M USDT + $3.34K TRX.	CRITICAL	Largest single outflow destination is a confirmed phishing address. Indicates a large-scale phishing campaign targeting OKX withdrawal customers. The wallet is not the perpetrator; it processed customer-directed withdrawal requests.

SYNTHESIS

TBwBJwj81yXc4DNKS19GJcpUUzfSWRbBzS is confirmed OKX Hot Wallet_116, independently attributed by Arkham and OKLink. In 5 days: $52.15M in / $80.86M out across 1,980 USDT transfers; 1,216 counterparties. Critical finding: TMj17yryskb2aP7H9BMgb2qhXKNNaN89Gs (OKLink 'Phishing address') received $22.76M (28.2% of outflows) — Third-Party Risk elevated to 0.25. All inflows fully OKX-sourced. AML: LOW. Security: PROFICIENT (90). Attribution: HIGH. Priority action: flag TMj17 and notify OKX compliance.

S6 — OWNERSHIP ATTRIBUTION MODEL

Hypothesis Assessment

OKX Exchange Infrastructure — Hot Wallet_116 with Phishing Counterparty 95%

Attribution Error or Wallet Rotation 5%

Probabilities sum to 100%. Attribution confidence: 95 / 5.

WHAT THIS MEANS FOR YOU

This wallet is confirmed OKX exchange infrastructure. Any counterparty interaction with this address is an interaction with the OKX platform. The phishing address finding (TMj17, $22.76M) indicates a significant phishing campaign targeting OKX customers. If TMj17 appears in your customer's transaction history, enhanced due diligence and SAR assessment are warranted. If you are an OKX customer who withdrew funds to a phishing address during May–June 2026, contact OKX security immediately.

S7 — LINKS, DIGITAL FOOTPRINT & PUBLIC RECORD

Government Records · Press Coverage · Research & Analytics · Blockchain Intelligence

BLOCKCHAIN EXPLORERS

OKLink 2026-06-02

Address tagged '#OKX Hot Wallet_116' by OKLink. Counterparty TMj17yryskb2aP7H9BMgb2qhXKNNaN89Gs labeled 'Phishing address' by OKLink — the critical adverse finding in this case.

https://www.oklink.com/tron/address/TBwBJwj81yXc4DNKS19GJcpUUzfSWRbBzS

Tronscan 2026-06-02

On-chain history retrieved. 96,386 transactions in 5 days. 45,568 TRX operational float confirmed. No Tronscan risk tag on subject address.

https://tronscan.org/#/address/TBwBJwj81yXc4DNKS19GJcpUUzfSWRbBzS

GOVERNMENT & OFFICIAL RECORDS

OFAC SDN List 2026-06-02

NEGATIVE SWEEP: Address not found in OFAC Specially Designated Nationals list as of 2026-06-02.

https://sanctionssearch.ofac.treas.gov/

MEDIA & PRESS

OKX Exchange 2026-06-02

Subject address is confirmed OKX exchange infrastructure. OKX is a global tier-1 centralized cryptocurrency exchange serving 50M+ users in 180+ countries. Exchange entity is the registered operator of this wallet.

https://www.okx.com/

RESEARCH & ANALYTICS

CoinGecko — OKX 2026-06-02

OKX exchange profile on CoinGecko confirms top-5 global CEX by spot volume. TRON/USDT operations active. No adverse regulatory designation listed as of 2026-06-02.

https://www.coingecko.com/en/exchanges/okx

Chainabuse 2026-06-02

NEGATIVE SWEEP: No reports filed for this address on Chainabuse as of 2026-06-02. Phishing counterparty TMj17 should be checked as a separate OSINT target.

https://www.chainabuse.com/address/TBwBJwj81yXc4DNKS19GJcpUUzfSWRbBzS

INTELLIGENCE PLATFORMS

Arkham Intelligence 2026-06-02

Address attributed to OKX exchange (Hot Wallet) by Arkham Intelligence cluster. Attribution independently confirmed by OKLink entity tag.

https://intel.arkm.com/explorer/address/TBwBJwj81yXc4DNKS19GJcpUUzfSW…

OSINT SUMMARY

Inbound flows are 100% OKX institutional. Outbound routing contains one critical adverse link: TMj17 phishing address ($22.76M, 28.2%). BTSE institutional settlement and 1,200+ customer withdrawals account for the remainder.

S8 — RECOMMENDED FURTHER INVESTIGATION

Priority Actions & Engagement Opportunities

P1	**Notify OKX Compliance** — Report the phishing counterparty finding (TMj17, $22.76M) to OKX security/compliance team. Request confirmation of the phishing incident and any customer restitution actions. · *Regulatory*
P2	**Flag TMj17 Across All Systems** — Add TMj17yryskb2aP7H9BMgb2qhXKNNaN89Gs to all monitoring systems. Track residual $2.48M USDT balance for movement; any outflow may indicate active liquidation of phishing proceeds. · *On-chain*
P3	**SAR Assessment** — Evaluate SAR obligations for any institution with documented counterparty exposure to TMj17yryskb2aP7H9BMgb2qhXKNNaN89Gs. · *SAR*
P4	**OSINT — Phishing Address Investigation** — Conduct OSINT on TMj17yryskb2aP7H9BMgb2qhXKNNaN89Gs; search for OKX phishing incident reports, security advisories, and any victim disclosures referencing this address or the May–June 2026 period. · *OSINT*

INVESTIGATOR ASSESSMENT

Priority action: flag `TMj17yryskb2aP7H9BMgb2qhXKNNaN89Gs` (phishing address, $22.76M received) across all monitoring systems and notify OKX compliance. The $2.48M residual USDT balance at the phishing address has not been moved — monitoring for outflow will indicate when/if the phishing operator liquidates remaining proceeds.

APPENDIX A — MASTER SOURCE LIST

REF	SOURCE
S1	**On-chain dataset -- TRC-20 Transfers** https://tronscan.org/#/address/TBwBJwj81yXc4DNKS19GJcpUUzfSW... *Full TRC-20 transfer history via Tronscan API. Retrieved 2026-06-03.*
S2	**On-chain dataset -- Raw Transactions** https://tronscan.org/#/address/TBwBJwj81yXc4DNKS19GJcpUUzfSW... *Full transaction log via Tronscan API. Retrieved 2026-06-03.*
S3	**Arkham -- Address Profile** https://intel.arkm.com/explorer/address/TBwBJwj81yXc4DNKS19G... *Screenshot captured 2026-06-03. File: screenshot_arkham.png*
S4	**Tronscan -- Address Profile** https://tronscan.org/#/address/TBwBJwj81yXc4DNKS19GJcpUUzfSW... *Screenshot captured 2026-06-03. File: screenshot_tronscan.png*
S5	**Oklink -- Address Profile** https://www.oklink.com/tron/address/TBwBJwj81yXc4DNKS19GJcpU... *Screenshot captured 2026-06-03. File: screenshot_oklink.png*

APPENDIX B — GLOSSARY OF TERMS

TERM	DEFINITION
Phishing Address	An address flagged by blockchain intelligence platforms as associated with phishing operations — typically used to receive funds from victims deceived into providing fraudulent withdrawal or payment destinations.
Inter-Exchange Settlement	A transfer between two known exchange cold or treasury wallets representing institutional-level liquidity movement, not a customer transaction — standard in exchange treasury management.
Hot Wallet	An exchange-operated online wallet used for processing real-time customer deposits and withdrawals; maintains a working balance of assets for immediate disbursement.