THREAT INTELLIGENCE REPORT

Trust Wallet Phishing Panel Exposed: $239K Stolen, 6 Operators Identified

Ref. **PD-TI-2026-86459** Published **10 July 2026** Source **phishdestroy.io/trustwallet-panel-exposed**

ACTIVE THREAT INVESTIGATION
tttadmin.com · Live Chat Scam · IDOR · 14 Months Active · March 2026

9 min read · Updated **March 2026** · PhishDestroy Intelligence

1,900
Victim Chat Sessions
$239K+
Confirmed Stolen (USDT/ETH/BTC)
21
Scammer Wallets Identified
6
Named Operators

Executive Summary

This investigation documents **TrustWalletPanel** — a sophisticated phishing operation impersonating Trust Wallet through the backend domain `tttadmin.com` . Running for **14 months** (January 2025 –

February 2026), the operation targeted crypto users via fake support chat, extracting seed phrases and demanding deposits under false pretenses of “OFAC compliance” and “asset replacement.” All 1,900 victim conversations were extracted through a critical IDOR vulnerability. The primary operator has been deanonymized.

How the Scam Works: Attack Flow

The operation follows a carefully designed 5-stage pipeline to extract maximum value from each victim:

Stage 1
Discovery — Victims find phishing domain via Telegram groups, romance scam lures (persona “Sofia”), or search engine results
Stage 2
Fake Wallet — Phishing site mimics Trust Wallet interface; captures mnemonic seed phrase and password on “wallet creation”
Stage 3
Live Chat Trigger — Withdrawal attempts deliberately fail; chat operator appears as “Trust Wallet Support”
Stage 4
Social Engineering — Operators claim assets frozen due to OFAC/AML violations, demand cryptocurrency deposits for “replacement” or “verification”
Stage 5
Repeat Extraction — Continuous demands for additional payments with urgency tactics and deadline pressure

Financial Damage: Top Confirmed Losses

Chat ID	Amount	Asset	Context
#1795	197,000 USDT	TRON (TRC-20)	Borrowed from ex-wife
#481	~45.77 ETH	Ethereum	Multiple deposits
#965	~16,000 USDT	USDT	Sequential deposits
#720	8,000 USDT	TRC-20	Single day transfer
#1090	5,839 USDT	USDT	Single mother, confirmed loss
#1430	~3,686 USDT	USDT	Two separate deposits
#92	3,340.23 USDT	USDT	Confirmed exact amount
#1089	0.3201 BTC	Bitcoin	From Ledger hardware wallet

Actual Damage Likely Much Higher

These are unverified self-reports from chat logs. Many victims never reported amounts. Wallet rotation makes on-chain totals impossible to calculate without full blockchain tracing.

Operator Identification

Primary Operator: Vasiliy Navrotsky

Parameter	Value
Full Name	**Vasiliy Navrotsky** (Василий Навроцкий)
Telegram ID	`6005741623`
Current Handle	`@Addmeks`
Username History	`@Slo221` , `@Li_Sin_main` , `@Handert` , `@Surr2201` , `@surr2204`
Active Period	July 2023 – May 2025
Messages Tracked	249 across 61 Telegram groups
Key Groups	Binance RU (34), P2P LAB (9), Trust Wallet RU (6)

Team Members Identified in Chat Logs

👤
Lyokha / Alexey
Primary chat operator

👤
Dima
Operator (Chat #92)

👤
Maksim
Operator (Chat #446, 201 msgs)

👤
Andrey
Operator (Chat #579)

👤
Aleksander
Telegram recruiter

👤
Sofia
Romance scam lure persona

Social Engineering Tactics

Tactic	Messages	Description
Trust Wallet Impersonation	1,905	Posing as official Trust Wallet support
Wallet Freeze/Block Claims	360	Claiming wallet frozen due to “suspicious activity”
Asset Replacement Offers	305	Promising to “replace” frozen assets after deposit
OFAC Sanctions Threats	210	False claims of US Treasury sanctions on wallet

Deposit-for-Unlock Demands	185	Requiring cryptocurrency deposit to “unlock” wallet
Fake Staking Offers	161	Custom APY staking pools in admin panel
AML/CTF Accusations	66	Accusing victims of money laundering

The Irony

Russian-speaking scammers targeting Russian-speaking victims (51% of chats in Russian) with threats of **US Treasury OFAC sanctions** — a regulatory mechanism geographically irrelevant to their victim base. Template-based social engineering, not contextual understanding.

Victim Engagement Funnel

Initial Sessions
1,900
100%
Responded to Chat
679
35.7%
Deep Engagement (10+ msgs)
175
9.2%
Confirmed Fund Transfers
~20
1%

Languages: Russian 51% (3,013 msgs) · English 40% (2,995 msgs) · Other 9% (365 msgs)

Peak Activity: November 2025 (959 messages). Working hours 10:00–13:00 UTC, weekends 40% lower.

Infrastructure Analysis

Core Domain Architecture: tttadmin.com

IDOR NO AUTH SOURCE MAPS EXPOSED CORS MISCONFIGURED

Component	Details
Victim API	`appp.tttadmin.com`
Admin Backend	`core.tttadmin.com` / `app.tttadmin.com`
Static CDN	`static.tttadmin.com`
Backend Stack	Java Spring Boot + Spring Security, JWT RS256
Database	PostgreSQL (JPA/Hibernate)
Frontend	React CRA + Material UI (339 source files recovered)
Web Server	nginx/1.18.0 (Ubuntu)

Hosting Infrastructure

IP	Location	Provider	Role
`45.144.30.6`	Moscow, RU	UFO Hosting (AS33993)	Primary victim-facing
`2.56.178.117`	Moscow, RU	UFO Hosting (AS33993)	Early-stage (Jan-Feb 2025)
`185.170.198.121`	Vilnius, LT	Hostinger (AS47583)	Phishing frontend
`69.10.62.71`	New York, US	Interserver (AS19318)	Victim-facing
`69.49.231.166`	Atlanta, GA	Network Solutions	Current primary — all *.tttadmin.com
`94.131.121.154`	Moscow, RU	UFO Hosting (AS33993)	Phishing
`146.185.239.62`	Madrid, ES	GTHost (AS63023)	Secondary (casino + Next.js)

Phishing Domains (Rotated)

ALIVE (Cloudflare)
wallet-premium.com
PARKED (Epik)
trustarter.io
DEACTIVATED
trust-multi-chain.com
trust-multichain.com
trust-multi.online
coinbridge.online
premium-trust.com
ROMANCE SCAM FEEDER
rynova-qw.shop

Critical Security Vulnerabilities

The scam panel's infrastructure was riddled with vulnerabilities that made complete data extraction trivial:

11 Unauthenticated API Endpoints

IDOR - enumerate all 1,900 chats by sequential ID POST /chat/get → Full chat transcript, no auth # Returns latest victim session data POST /session/get → Mnemonic + password leaked # Inject messages into any victim chat POST /message/save → No auth required # Create fake victim sessions POST /session/init → Captures seed phrases # Full system config POST /system/get → swap_percent, status_support # All token/network config (174KB) POST /network/get → Full network data POST /token/info/get/all → Live CoinMarketCap prices POST /stake/get/all → Staking pool configs # Admin login - no rate limiting POST /admin/sign-in → Unlimited brute-force
IDOR on /chat/get
All 1,900 chats enumerable without auth
Source Maps Exposed
339 source files (3.4MB) recovered

CORS Misconfigured
Reflects any Origin with credentials
No Rate Limiting
Unlimited brute-force on admin login

Admin Panel Capabilities (Source Code Analysis)

339 source files were recovered from exposed production source maps (`main.3924229a.js.map`). The panel features:

Wallet Manager
View/edit all victim wallets with mnemonics
Live Chat (1s poll)
Real-time victim chat as “Trust Wallet Support”
Transaction Control
Edit status, inject fake transactions
Staking Pools
Custom APY rates, lock periods, fake yields

Third-Party Research Activity Detected

Reverse Shell Payload Found in Chat #1

A base64-encoded reverse shell payload was found injected via the unauthenticated `/message/save` endpoint on **May 6, 2025** — approximately 10 months before this investigation. This indicates the vulnerabilities were publicly exploitable for an extended period, and another researcher discovered them long before us.

Operation Timeline

Jan 2025
First victim sessions appear (845 messages). Infrastructure on Moscow IPs.
May 2025
Third-party researcher discovers IDOR, injects reverse shell payload
Nov 2025
Peak activity: 959 messages in single month. SSL certificates renewed.
Feb 2026
Latest certificate issued. Operation still active, new sessions created.
Mar 1, 2026
PhishDestroy investigation published. All 1,900 chats extracted and analyzed.

Recommendations for Users

- **Never share seed phrases** via chat, email, or any support channel — Trust Wallet will never ask for them
- **Verify support contacts** exclusively through official Trust Wallet channels

- **Recognize OFAC/AML threats** as common scam pretexts — legitimate services do not freeze wallets via chat
- **Report phishing domains** to Trust Wallet security team and PhishDestroy
- **Use hardware wallets** for withdrawal signing to prevent unauthorized transfers
- **Verify wallet status** through blockchain transaction history, not through any “support” interface

Full Technical Report with Chat Logs

Complete investigation data including all chat transcripts, wallet addresses, operator analysis, and interactive visualizations

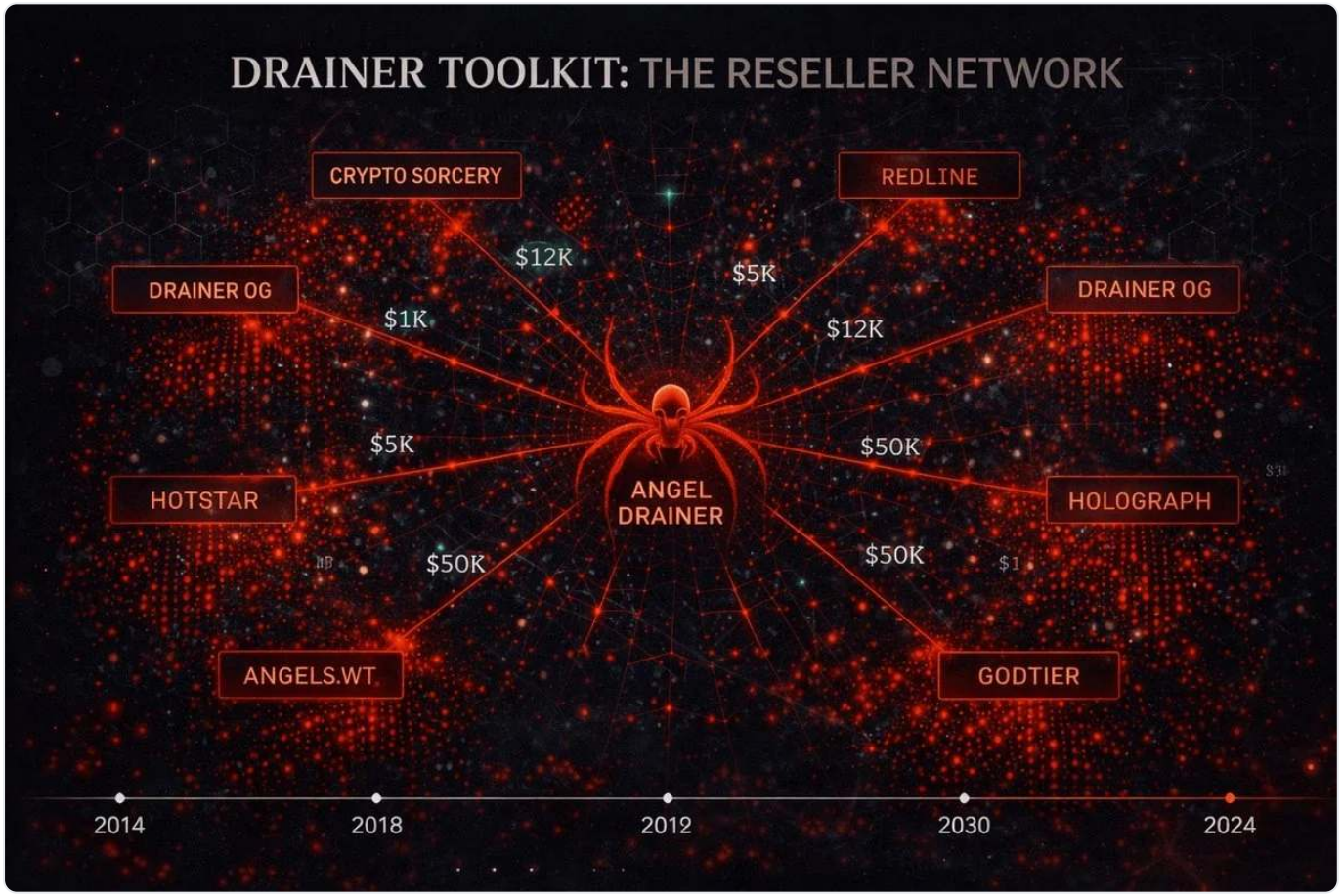
View Full Report on GitHub →

Browse All 1,900 Chat Transcripts →

Share This Investigation

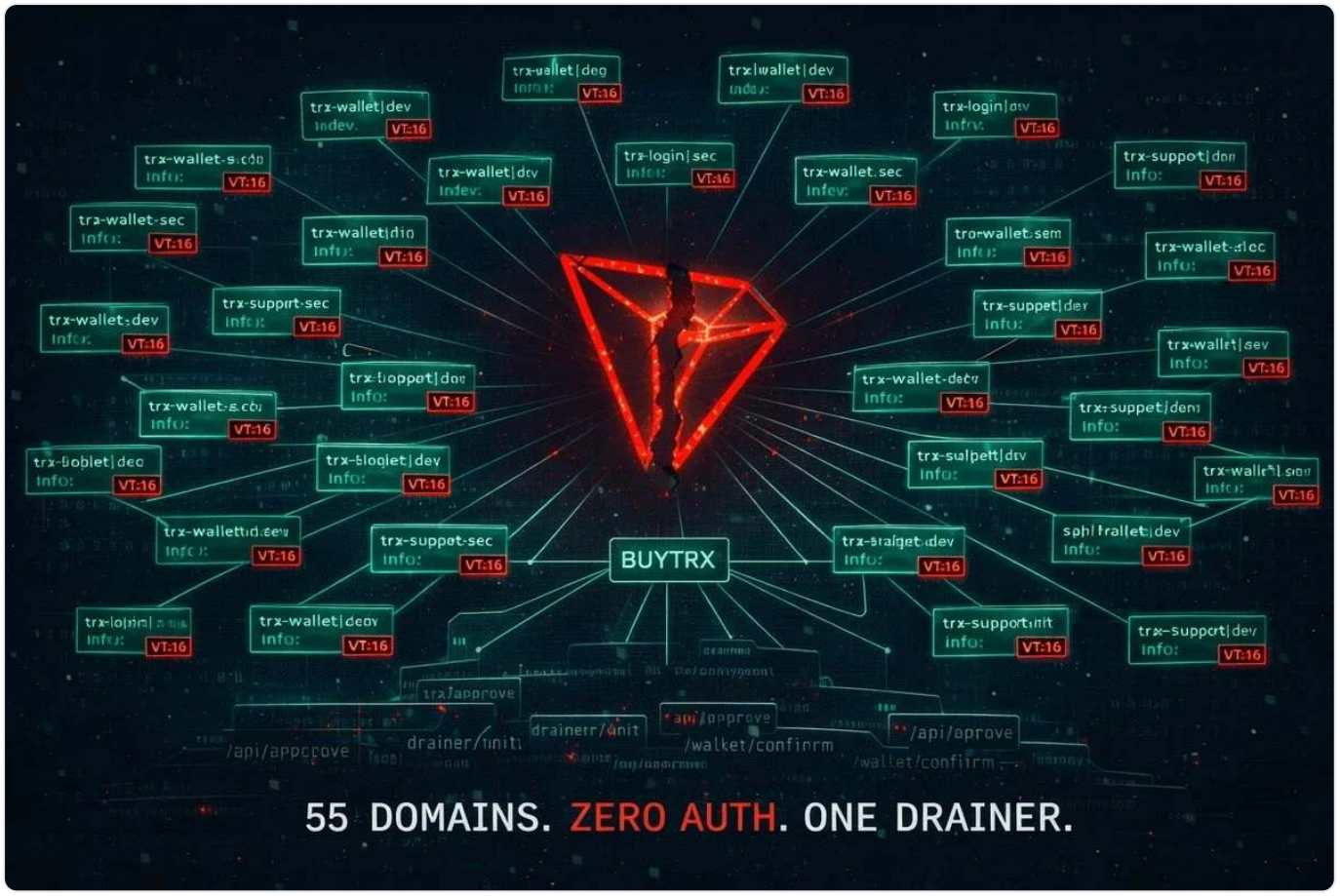
X / Twitter Telegram Reddit LinkedIn

Related Investigations



DEEP INVESTIGATION

Crypto Drainer Toolkit: Angel Drainer Resellers Exposed



INVESTIGATION

BUYTRX Exposed: 55 Domains & TRON Approval Drainer

DEEP INVESTIGATION

Anatomy of Crypto Phishing: 8 Real Seed Phrase Stealers Reverse-Engineered