THREAT INTELLIGENCE REPORT

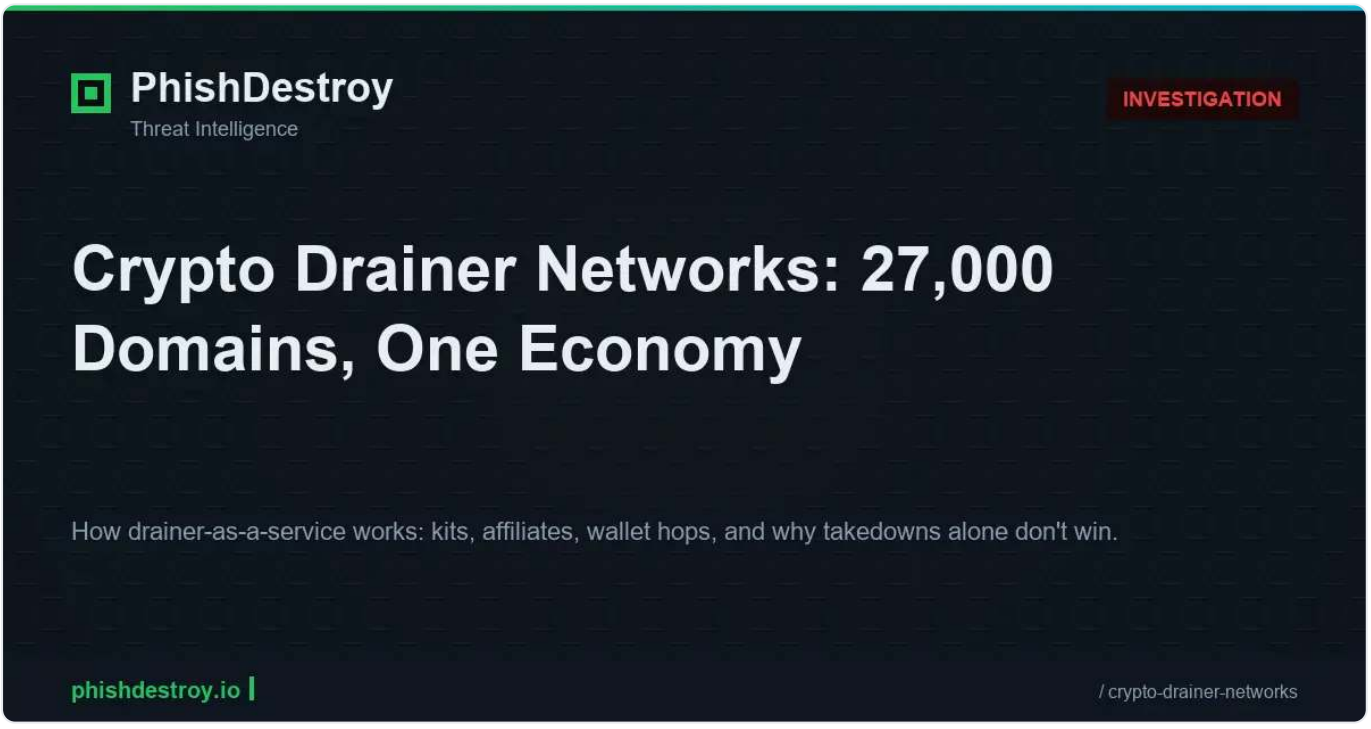
Crypto Drainer Toolkit: Inside the Angel Drainer Resellers Targeting Your Wallet

Ref. **PD-TI-2026-98009** Published **10 July 2026** Source **phishdestroy.io/crypto-drainer-networks**

ScamIntelLogs Investigation

Three drainer-as-a-service operations dissected at the code level. AI-generated phishing kits with debug statements still in production. An 80%-commission affiliate model fueling rapid expansion. And one archived network proving that coordinated disruption works. This is the infrastructure behind the next wallet you almost connected to.

~10 min read · Updated **March 2026** · PhishDestroy Intelligence
3 Active Drainer Networks 15+ Phishing Domains 80% Affiliate Commission 1 Network Archived



0
Phishing Domains
0
Drainer Operations
0
Members Tracked
0
Wallets Identified
0

Forced Sign Retries

0

% Affiliate Commission

The 9-Step Attack Chain: From Fake Airdrop to Empty Wallet

Every crypto drainer follows a predictable sequence. What makes drainer-as-a-service operations dangerous is not innovation -- it is scale. The same attack chain gets replicated across dozens of domains, each one a fresh trap for unsuspecting victims. Here is the exact sequence extracted from TRXDrop's source code, step by step.

Complete Drainer Attack Flow

This 9-step chain was reconstructed from decompiled TRXDrop source code. Every step is documented with corresponding code references in the ScamIntelLogs repository.

9-step crypto phishing attack chain — from fake airdrop ad through wallet drain to laundering.

1

Fake Airdrop Ad

Victim sees a promoted post or Telegram message advertising a TRX/SOL airdrop. Domain examples: trx-drop.com, tronrefund.com, trxairdrop.io.

2

Landing Page

Professional-looking page mimics a legitimate TRON Foundation airdrop. Countdown timers and fake claim counters create urgency.

3

WalletConnect Prompt

Site initiates WalletConnect using stolen Project ID `fbf5b42d9006502246e73447f5d50e33` . Victim

connects their wallet believing it is required to claim.

4

Permission Request

Drainer requests broad token permissions. The signing prompt is intentionally vague to obscure what is being approved.

5

Token Approval

Victim signs an `approve()` transaction granting the drainer contract unlimited spend authority over specific tokens.

6

setApprovalForAll

A second transaction calls `setApprovalForAll()` , granting the attacker control over NFTs and all token types in the wallet.

7

Transfer Tokens

Drainer contract immediately calls `transferFrom()` to move all approved tokens to the attacker's collection wallet.

8

Drain Wallet

Native chain tokens (TRX, SOL) are transferred last. The wallet is emptied completely. If the victim rejects, the drainer retries up to **50 times** before allowing escape.

9

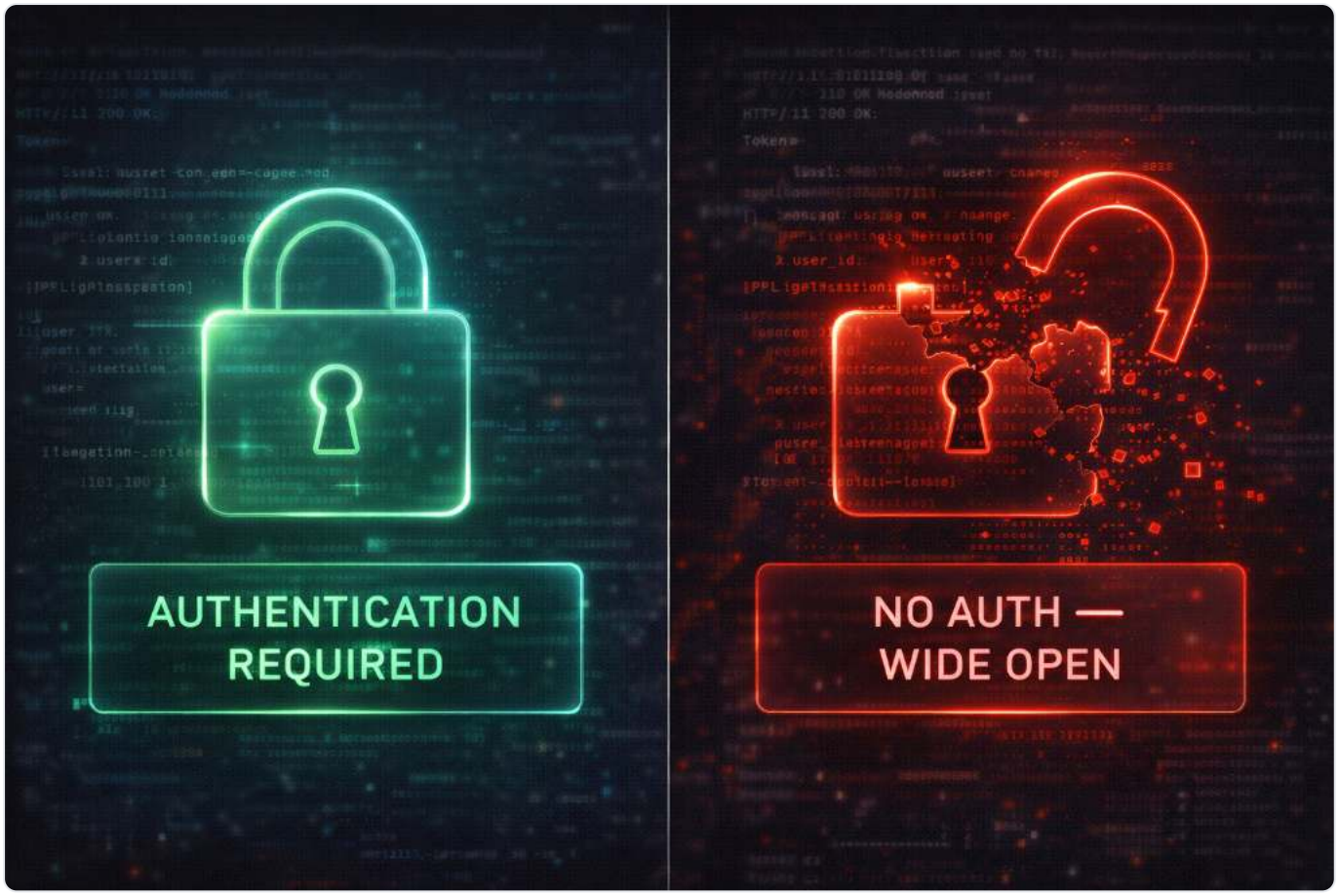
Funds to Operator

Stolen funds are routed to the operator's wallet. TRXDrop charges a 30 TRX commission per drain. The rest goes to the affiliate who deployed the phishing page.

50 Forced Retries

If a victim clicks "Reject" on the signing prompt, the TRXDrop code immediately re-triggers the request. This loop repeats **50 times** before the victim is allowed to close the modal. Most users give up and sign after 3-5 attempts, believing the site is glitched rather than malicious. This is not a bug. It is by design.

TRXDrop Deep Dive: AI-Generated Code with 30+ Debug Statements in Production



TRXDrop API exposed without authentication — anyone with the URL can read wallet logs, payment data, and operator IDs.

TRXDrop is an Angel Drainer reseller targeting TRON and Solana wallets. What sets this operation apart is not sophistication -- it is the opposite. The source code reveals unmistakable markers of AI-assisted development: repetitive structure, verbose commenting, and most tellingly, over 30 `console.log` debug statements left in production code.

These are not the marks of an experienced developer. They are the marks of someone who prompted an LLM to write a drainer and deployed the output without review.

AI-Generated Code Markers

The TRXDrop codebase contains 30+ `console.log` debug statements in the production build. Messages like `console.log("Attempting wallet connection...")` and `console.log("Approval transaction sent")` appear throughout. No professional developer -- and no experienced criminal -- ships debug logging to production. This is raw LLM output, deployed as-is.

XOR Encryption Key

All communication between the drainer frontend and backend panel is encrypted with a hardcoded XOR key: `TRX_SECURE_2024_PANEL_KEY` . XOR with a static key is trivially reversible -- another indicator of copy-paste development.

Crypto drainer admin panel v1.2 showing 1,337 victims, $12,450 stolen, connected wallets and real-time drain log - EXPOSED

WalletConnect Abuse

WalletConnect Project ID `fbf5b42d9006502246e73447f5d50e33` is embedded in all 15+ domains. A single revocation of this project ID would disable wallet connectivity across the entire TRXDrop network simultaneously.

50 Forced Retries

The signing prompt loop retries 50 times before allowing the victim to exit. This psychological pressure tactic is hardcoded, not configurable by affiliates -- it is a core feature of the Angel Drainer kit.

30 TRX Commission

Each successful drain sends a 30 TRX commission to the operator wallet. At current rates, this is approximately $7-8 USD per victim -- a low margin suggesting the operation depends on volume over value.

Operator Intelligence

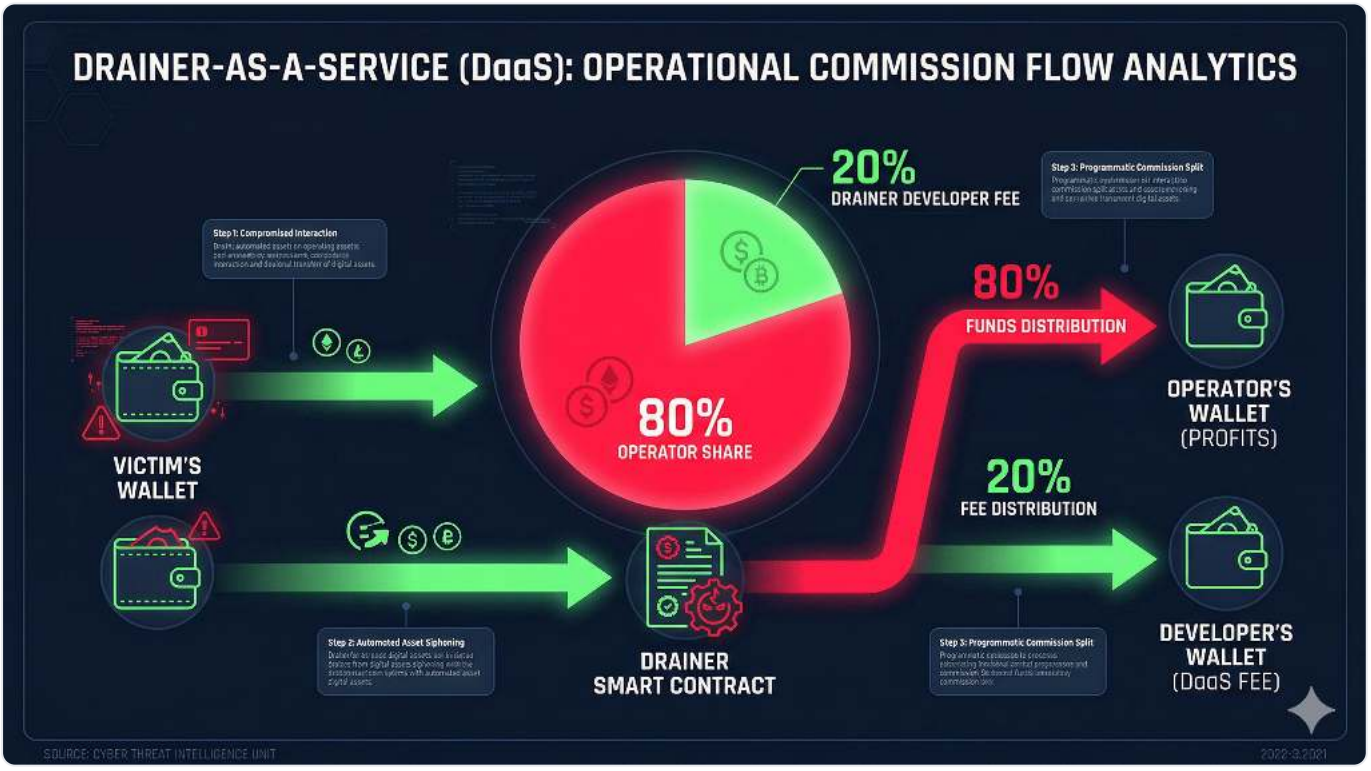
Telegram: `@STNlRAWbIaFLiH` (User ID: `6823931109`)
Collection Wallet: `TRAGn9E6hbTiQrYG5V4sk1gNv3JaWHSxak`
Chains Targeted: TRON, Solana
Drainer Kit: Angel Drainer (resold/customized)

TRXDrop Domain Infrastructure (15+ Domains)

Domain	Type	Status
`trx-drop.com`	Primary landing	Active
`tronrefund.com`	Refund lure	Active

Domain	Type	Status
`tronfund.net`	Fund lure	Active
`trxfund.pro`	Fund lure	Active
`trxairdrop.io`	Airdrop lure	Active
`trondrop.org`	Airdrop lure	Active
`tronreward.com`	Reward lure	Active
`tronreward.net`	Reward lure	Active
`tronrefund.net`	Refund lure	Active
`trxfund.org`	Fund lure	Active
`trxdrop.com`	Airdrop lure	Active
`trxdrop.org`	Airdrop lure	Active
`trongiving.com`	Giveaway lure	Active
`tronclaims.com`	Claims lure	Active
`trondrop.pro`	Airdrop lure	Active

NiceCrypto: The 80% Commission Machine



Drainer-as-a-Service commission flow: 80% to affiliate operator, 20% developer fee — from victim wallet through smart contract to laundering.

NiceCrypto operates on a simple proposition: give affiliates the highest payout in the drainer market, and they will bring the victims. At 80% commission, NiceCrypto offers the most generous affiliate split

we have documented in any drainer-as-a-service operation. The operator keeps just 20% -- a razor-thin margin that only works at scale.

The math is straightforward. If an affiliate drains a wallet containing $1,000 in tokens, they keep $800. NiceCrypto takes $200. With $8,454+ in documented affiliate payments, the operation has processed a minimum of $42,270 in stolen funds -- and that figure only accounts for payments we can directly observe on-chain.

Revenue Model: 80/20 Split

$8,454+ in documented payments to affiliates represents the floor, not the ceiling. At an 80% affiliate rate, total stolen funds processed by NiceCrypto exceed **$42,000** minimum. The true figure is likely significantly higher, as not all transactions are captured in our monitoring window.

Multi-Chain Expansion

NiceCrypto started on TRON but configuration files recovered from their infrastructure reveal active expansion to **Solana** , **EVM-compatible chains** (Ethereum, BSC, Polygon), and **TON** . Four blockchain ecosystems under a single drainer panel.

Forum Presence

NiceCrypto recruits affiliates through `wwh2club.to` , a known cybercrime forum. Their Telegram bot `@NCsetup_bot` handles onboarding -- new affiliates receive a configured drainer kit within minutes of contact.

WasabiSquad Connection

NiceCrypto's website domain `wasabihub.one` raises questions about a possible connection to the WasabiSquad operation. Whether this is shared infrastructure, a rebrand, or coincidence requires further investigation.

Telegram Automation

Bot `@NCsetup_bot` automates affiliate management: deployment of drainer kits, commission tracking, and payout distribution. The operator rarely needs to interact with affiliates directly.

NiceCrypto IOCs

Telegram Bot: `@NCsetup_bot`
Website: `wasabihub.one`
Forum: `wwh2club.to`
Affiliate Commission: 80%
Documented Payouts: $8,454+
Chains: TRON (active), Solana (expanding), EVM (expanding), TON (expanding)

80% to affiliates. We keep 20%. You bring the traffic, we handle the code. Setup takes 5 minutes.
-- NiceCrypto advertisement on wwh2club.to

717Team: Archived = Disruption Works

717Team is the proof that these operations can be stopped. With 125 members and 85 tracked wallets, 717Team was a mid-sized drainer operation running 12+ phishing domains. The confirmed drain total of $2,946.25 may seem modest compared to larger operations, but the real story is the outcome: **archived** .

In our tracking system, "archived" means the operation has been disrupted to the point of cessation. Domains taken down. Infrastructure burned. The admin exposed. 717Team did not voluntarily shut down. It was shut down through coordinated reporting, domain takedowns, and intelligence sharing with blockchain security partners.

Disruption Confirmed

717Team's ARCHIVED status is not a label we apply lightly. It means sustained disruption across multiple vectors: domain takedowns, hosting provider reports, wallet flagging, and exposure of admin identity. The operation's cost of continuing exceeded its revenue. That is what successful disruption looks like.

Admin: @imdebank

Admin Telegram handle `@imdebank` (User ID: `7149807602`) has been linked to **RublevkaTeam** , a separate Russian-language scam network previously documented in our TON investigation. Cross-operation admin sharing is a recurring pattern.

Network Scale

125 members tracked across Telegram groups. **85 wallets** identified through on-chain analysis. **$2,946.25** confirmed drained. 717Team recruited through `lolz.live` , a Russian-language cybercrime forum.

Domain Infrastructure

12+ domains including `checkscore.cc` , `cryptomus-payment.com` , `check-score.ru` , and others. Multiple domain registrars used in an attempt to resist coordinated takedowns.

Bot Operations

Telegram bot `@team717_bot` managed affiliate coordination, victim tracking, and payout distribution. The bot was deactivated as part of the disruption effort.

717Team IOCs

Admin: `@imdebank` (ID: `7149807602`)
Linked Group: RublevkaTeam
Bot: `@team717_bot`
Forum: `lolz.live`
Members: 125 tracked
Wallets: 85 identified
Confirmed Drained: $2,946.25
Status: ARCHIVED (Disrupted)

Anti-Analysis: Present but Trivial to Bypass

TRXDrop deploys two anti-analysis techniques that are standard in the drainer toolkit playbook. Both are designed to frustrate casual inspection. Neither poses a meaningful obstacle to a trained analyst.

Debugger Traps

A `setInterval` loop fires every 1,000 milliseconds, executing a `debugger` statement. When DevTools is open, this pauses execution continuously, making it appear the page is frozen. **Bypass:** Disable breakpoints in DevTools (`Ctrl+F8`) or use the "Never pause here" context menu option. Total bypass time: 2 seconds.

Console Hijacking

The code overwrites `console.log` , `console.warn` , and `console.error` with empty functions to suppress output. Ironic, given that the developer left 30+ debug statements that these overrides are designed to hide. **Bypass:** Store a reference to the original console methods before the page loads, or use the browser's native console API. Total bypass time: 5 seconds.

Amateur Hour

The combination of AI-generated code, debug statements in production, static XOR encryption, and trivially bypassable anti-analysis paints a clear picture: TRXDrop's operator is not a skilled developer. They are a scammer who bought a drainer kit and prompted an LLM to customize it. The danger is not sophistication -- it is accessibility. When the barrier to entry is "can you type a prompt," the number of operators grows exponentially.

This pattern is consistent across the drainer-as-a-service ecosystem. The kit developers (in this case, Angel Drainer) possess genuine technical ability. The resellers and affiliates deploying these kits often do not. The anti-analysis layer exists not because the operators understand security research -- it exists because the kit ships with it enabled by default.

Evidence & Source Intelligence

All evidence referenced in this investigation is preserved in the PhishDestroy ScamIntelLogs repository. Each operation has its own directory containing configuration files, source code excerpts, domain lists, wallet addresses, and Telegram intelligence.

TRXDrop Evidence

15 domains, source code, XOR keys, WalletConnect ID, operator Telegram, wallet address.

View on GitHub

NiceCrypto Evidence

Configuration files, affiliate payment records, multi-chain expansion plans, forum posts.

View on GitHub

717Team Evidence

Member lists, wallet addresses, domain infrastructure, admin intelligence, disruption timeline.

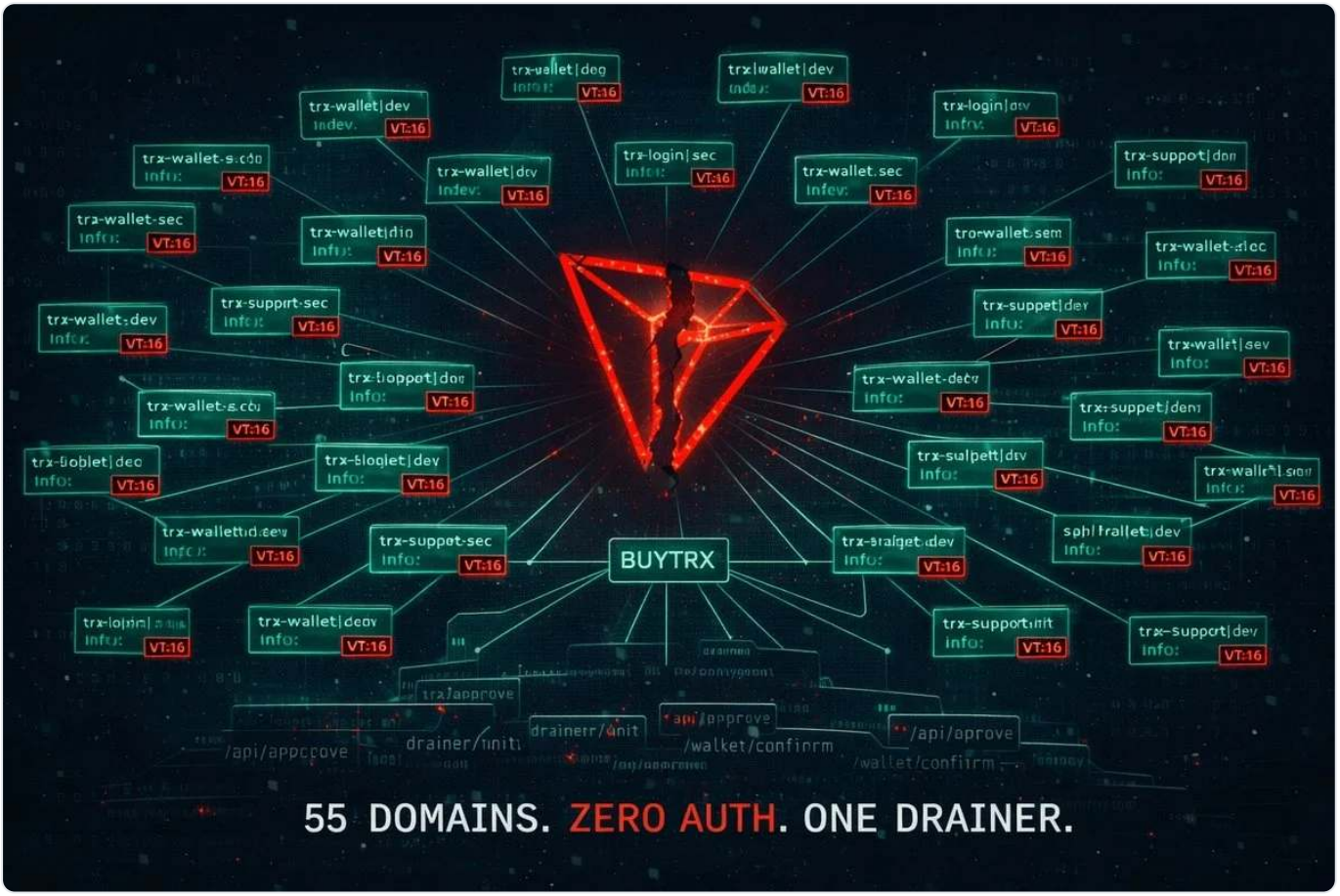
View on GitHub

Responsible Disclosure

All wallet addresses, domain lists, and operator identifiers published in this report have been shared with relevant blockchain security teams and domain registrars prior to publication. The WalletConnect Project ID has been reported for revocation. If you operate infrastructure affected by these IOCs, contact us via @PhishDestroy_bot .

Share This Investigation

Related Investigations



INVESTIGATION

BUYTRX Exposed: 55 Domains & TRON Approval Drainer

DEEP INVESTIGATION

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

DEEP INVESTIGATION

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