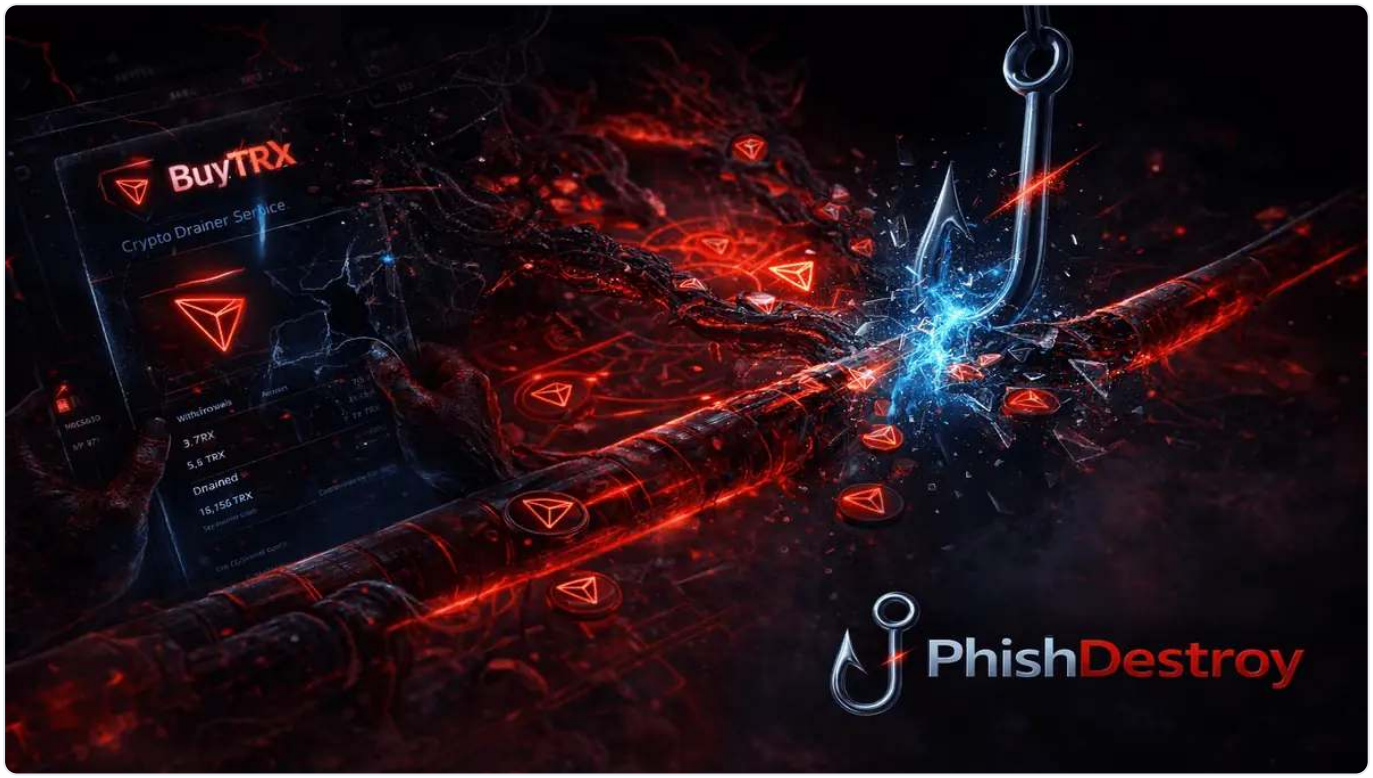
THREAT INTELLIGENCE REPORT

BUYTRX Exposed: 55 Domains, Zero Auth APIs, and a TRON Approval Drainer Dissected

Ref. **PD-TI-2026-11295** Published **10 July 2026** Source **phishdestroy.io/buytrx-drainer-exposed**

DRAINER INFRASTRUCTURE TEARDOWN
TRON USDT approval phishing operation · Exposed backend · On-chain evidence · Google Ads funding

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



0 +
Phishing Domains
0
Exposed Victim Records
0
API Authentication
$0
Cost to Access All Data

What Is BUYTRX?

BUYTRX is a TRON-based USDT approval drainer operation disguised as a legitimate cryptocurrency swap service. The sites present professional-looking interfaces that promise to convert USDT to TRX

at attractive rates. But the "swap" never happens.

Instead, the victim is prompted to sign an `approve(MAX_UINT256)` transaction on the USDT (TRC-20) smart contract. This single signature grants the attacker's drainer contract **unlimited permission** to transfer the victim's entire USDT balance — now and forever — until the approval is manually revoked.

Once the approval is confirmed on-chain, the operator calls `transferFrom()` to sweep the wallet. The victim sees nothing. No swap. No TRX. Just an empty balance.

One signature. Unlimited access. Permanent drain capability.
The approve() call doesn't transfer tokens — it grants permission. The actual theft happens silently via transferFrom() seconds or hours later. Most victims never connect the two transactions.

The operation has been active since at least **July 2025** , cycling through dozens of domains as old ones get reported and taken down. The infrastructure adapts faster than most registrars and hosting providers can respond.

55+ Domains — One Operation

Our investigation uncovered a sprawling network of phishing domains, all serving identical or near-identical BUYTRX swap interfaces. The domains span Cloudflare Workers, Cloudflare Pages, and bare-metal origin servers.

Currently Active Domains

Domain	Type	Hosting
`trxev.com`	Primary	Cloudflare
`trxmo.com`	Primary + API	Cloudflare
`buytrx.mov`	Active	Cloudflare
`buytrx.cx`	Active	Cloudflare
`trxdc.org`	Active	Cloudflare
`buytrx.bet`	Active	Cloudflare
`buytrx.store`	Active	Cloudflare
`buytrx.click`	Active	Cloudflare
`trxfx.com`	Active	Cloudflare
`trxsw.org`	Active	Cloudflare

Cloudflare Workers & Pages

Subdomain	Platform
`shrill-haze-5ff7.buytrx.workers.dev`	Workers
`exchange.swap-trx.workers.dev`	Workers
`buytrx.pages.dev`	Pages

Subdomain	Platform
`swap-trx.pages.dev`	Pages

Origin Servers

IP Address	Provider	Purpose
`107.155.88.198`	HIVELOCITY (AS29802)	Primary origin
`46.21.151.194`	HVC-AS	Secondary origin

An additional **50+ recycled domains** were identified, including:

`buytrx.net` `buytrx.org` `buytrx.io` `buytrx.co` `buytrx.exchange` `buytrx.app` `buytrx.pro` `buytrx.cc` `buytrx.xyz` `buytrx.site` `buytrx.online` `buytrx.live` `buytrx.fun` `buytrx.top` `buytrx.vip` `trxswap.org` `trxswap.net` `trxswap.io` `trxswap.com` `trxflip.com` `trxev.org` `trxmo.org` `trxnw.com` `trxfn.com` `trxwb.com` `swaptrx.org` `swaptrx.net` `swaptrx.io` and many more.

50+ domains burned and replaced. The infrastructure adapts faster than most registrars respond.

Zero Auth APIs — The Backend Wide Open

The BUYTRX operation runs on **6 Express.js API endpoints** sharing a single database. The primary API is hosted at `api.trxmo.com` . Every single endpoint returns full victim data **without any authentication** .

Unauthenticated Endpoints

Endpoint	Returns
`GET /api/records`	All victim records
`GET /api/records/:id`	Individual victim detail
`GET /api/stats`	Operation statistics
`POST /api/records`	Create new record
`PUT /api/records/:id`	Update record
`DELETE /api/records/:id`	Delete record

Unauthenticated Admin Dashboard

An admin panel is accessible at `/8fb198a6e9b7af32` — a "security by obscurity" hash path with **zero authentication** . It provides a real-time victim feed showing:

- Wallet addresses of every victim
- Transaction IDs (approval hashes)
- IP addresses of victims
- Timestamps of every interaction
- Approval amounts (typically MAX_UINT256)

UNAUTHENTICATED API RESPONSE — api.trxmo.com

```
{
  "records": [
    {
      "id": 1,
      "wallet": "TKjdnS...redacted",
      "txHash": "a8f3e2...redacted",
      "ip": "185.xxx.xxx.xxx",
      "amount": "115792089237316195423570985008687907853269984665640564039457584007913129639935",
      "status": "approved",
      "createdAt": "2026-02-14T09:23:41.000Z"
    }
  ]
}
```


Additional vulnerabilities discovered:

- **Weak rate limiting:** 6 requests per window, trivially bypassed with IP rotation
- **Express.js header leak:** `X-Powered-By: Express` reveals server technology
- **Potential stored XSS:** Admin panel renders unsanitized user-agent strings

The operators built a drainer but forgot to secure their own backend.
Every victim's wallet address, IP, transaction hash, and approval amount is one unauthenticated GET request away. Zero API keys. Zero tokens. Zero security.

On-Chain Evidence

The drainer contracts are deployed on the TRON network and have been actively used to process approval transactions from victims.

Contract	Label	Deployed	Transactions
`TRnruCYe2k...UPJ8`	SwapTRX (Current)	Dec 13, 2025	Active
`TXwXfz8Bp9...uHnS`	Legacy Contract	Earlier	323 recorded

4 confirmed on-chain approval transactions were matched to victim records in the exposed database (records 1–10). Records 11–30 appear to be **operator test data** — test wallets with small amounts, sequential timing patterns, and identical IP ranges.

WalletConnect Integration

The phishing sites use WalletConnect to trigger the approval signing prompt in mobile wallets. The operation uses a single **WalletConnect Project ID** :

`31eee2e7b3ff1dc4ebdfa6f839467664`
This Project ID should be reported to WalletConnect for immediate blacklisting.

Following the Money — Google Ads & Attribution

Perhaps the most disturbing finding: **BUYTRX operators are paying Google to advertise their drainer** .

Indicator	Value
Google Ads Account	`AW-17287232508`
Conversion Tracking	Tracks successful approvals as conversions
Telegram Contact	`@buytrx9` ("Buytron")
Admin Panel Language	Simplified Chinese

The Google Ads account tracks **successful wallet approvals as conversion events** . This means Google's advertising platform is literally optimizing ad delivery to find more victims for a crypto drainer — and collecting payment for the service.

The admin dashboard is entirely in **Simplified Chinese** , with UI elements like `日間` / `夜間` (day/night mode toggles) and source code comments in Chinese. The Telegram handle `@buytrx9` serves as the primary operator contact channel.

They're running Google Ads campaigns that track successful wallet drains as conversion events. Google is being paid to optimize ad delivery for a phishing operation. The advertisers aren't hiding — they're paying for targeted traffic and measuring "success" by how many wallets get drained.

Takedown Recommendations

This operation touches multiple service providers. Coordinated reporting across all vectors is required:

Cloudflare

Report Workers abuse, Pages abuse, and DNS records for all 55+ domains. Bulk abuse report with full domain list.

Domain Registrars

55+ domains across multiple registrars. Each requires individual abuse reports citing phishing and financial fraud.

HIVELOCITY

Origin server at 107.155.88.198 hosting the backend API. Report for hosting phishing infrastructure.

WalletConnect

Blacklist Project ID `31eee2e7b3ff1dc4ebdfa6f839467664` to prevent phishing sites from triggering wallet signing prompts.

Tronscan

Flag drainer contracts `TRnruCYe2k3kSMYCGwM51rzDD591w7UPJ8` and `TXwXfz8Bp9AoCX79wcHiyB5vWSCtbNuHnS` .

Google Ads

Report account `AW-17287232508` for advertising phishing and financial fraud. Conversion tracking proves malicious intent.

Evidence & Source Data

Full Infrastructure Teardown

Complete technical analysis: domains, APIs, contracts, and attribution.

Domain List & Details

55+ domains with hosting details, registration info, and current status.

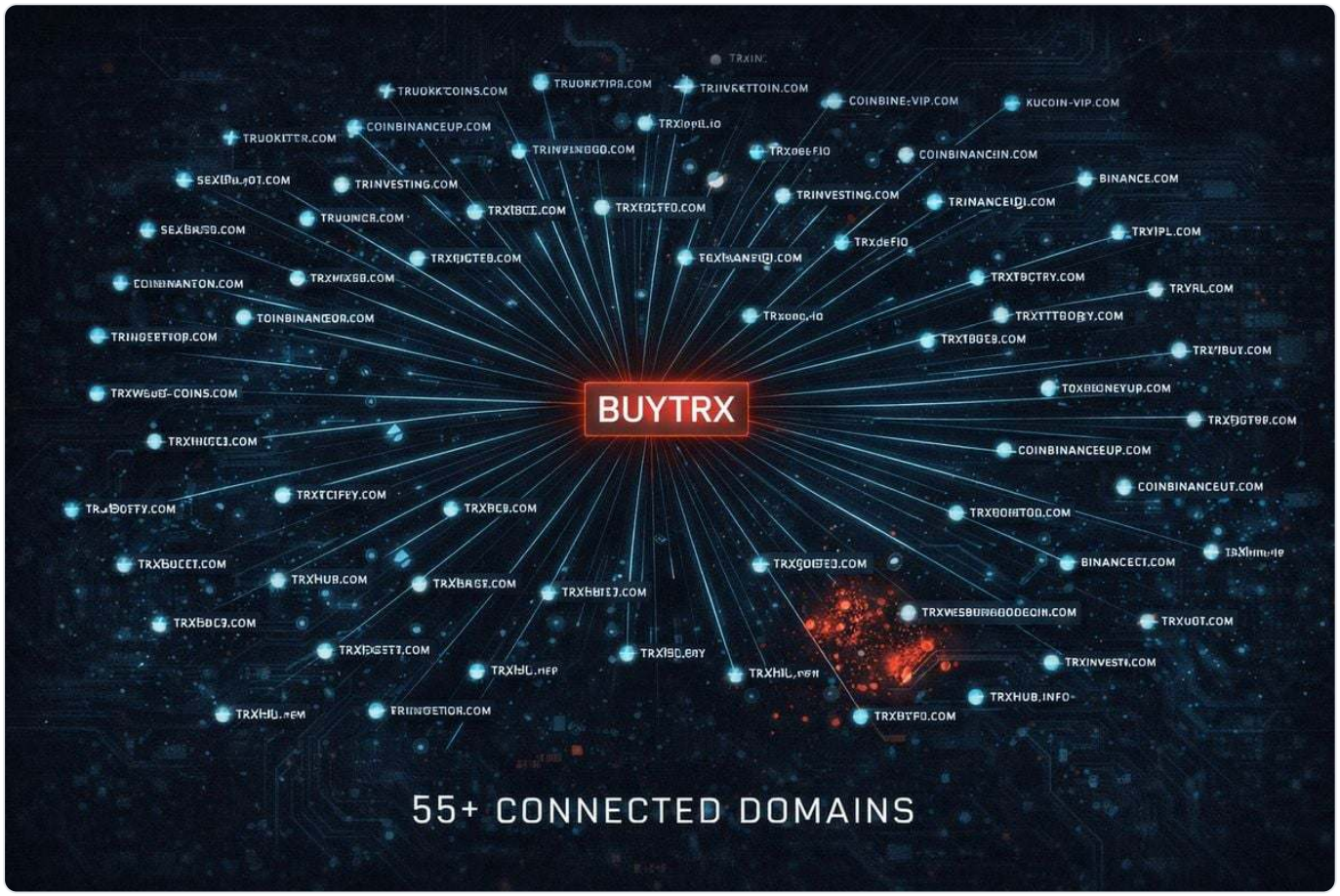
Raw API Victim Data Dump

Unredacted API responses from the unauthenticated backend. 30 records.

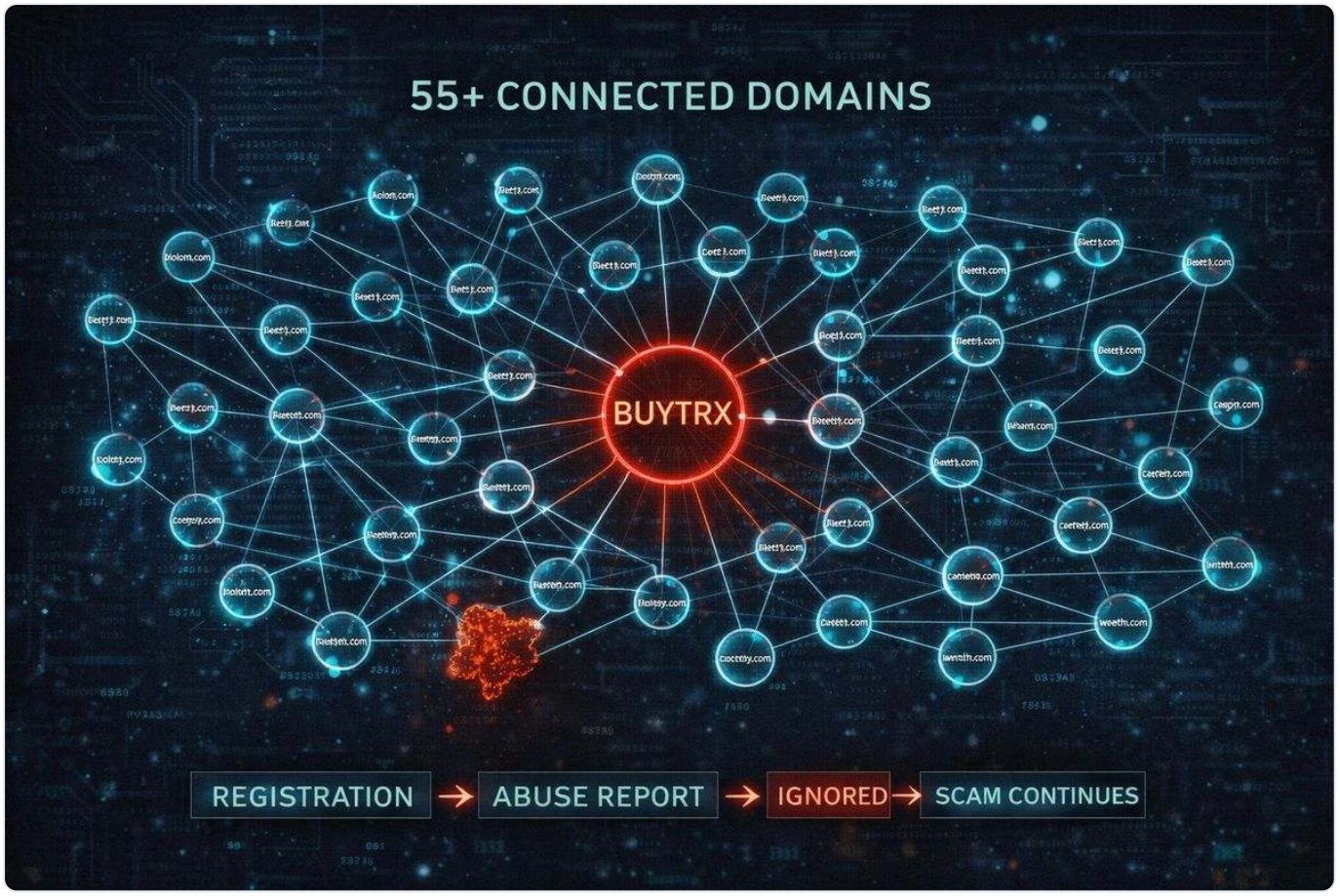
Tronscan: SwapTRX Contract

Active drainer contract on TRON. View transactions and approvals on-chain.

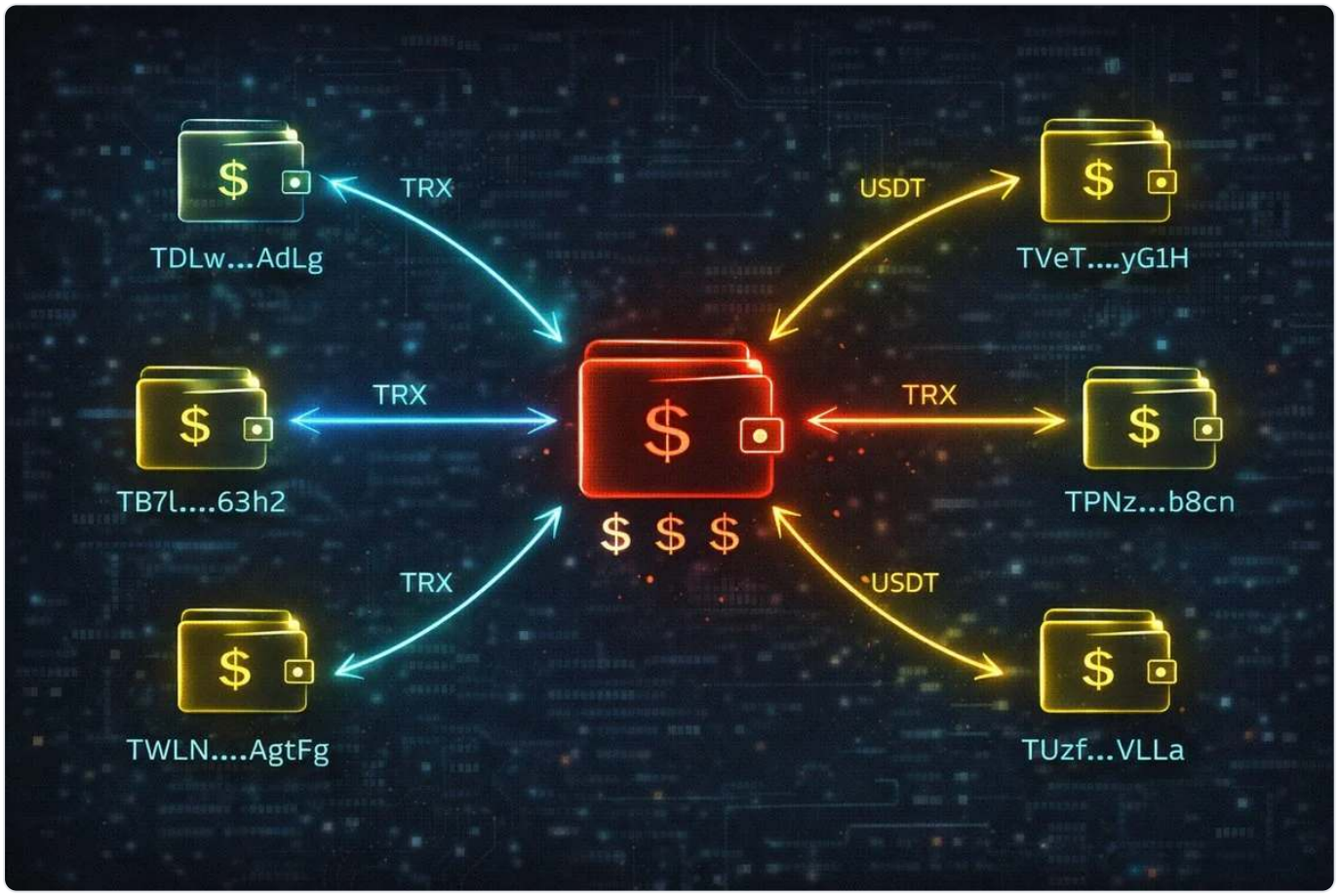
Check. Revoke. Report.



BuyTRX phishing domain network — detailed cluster map



BuyTRX domain network overview — interconnected phishing infrastructure



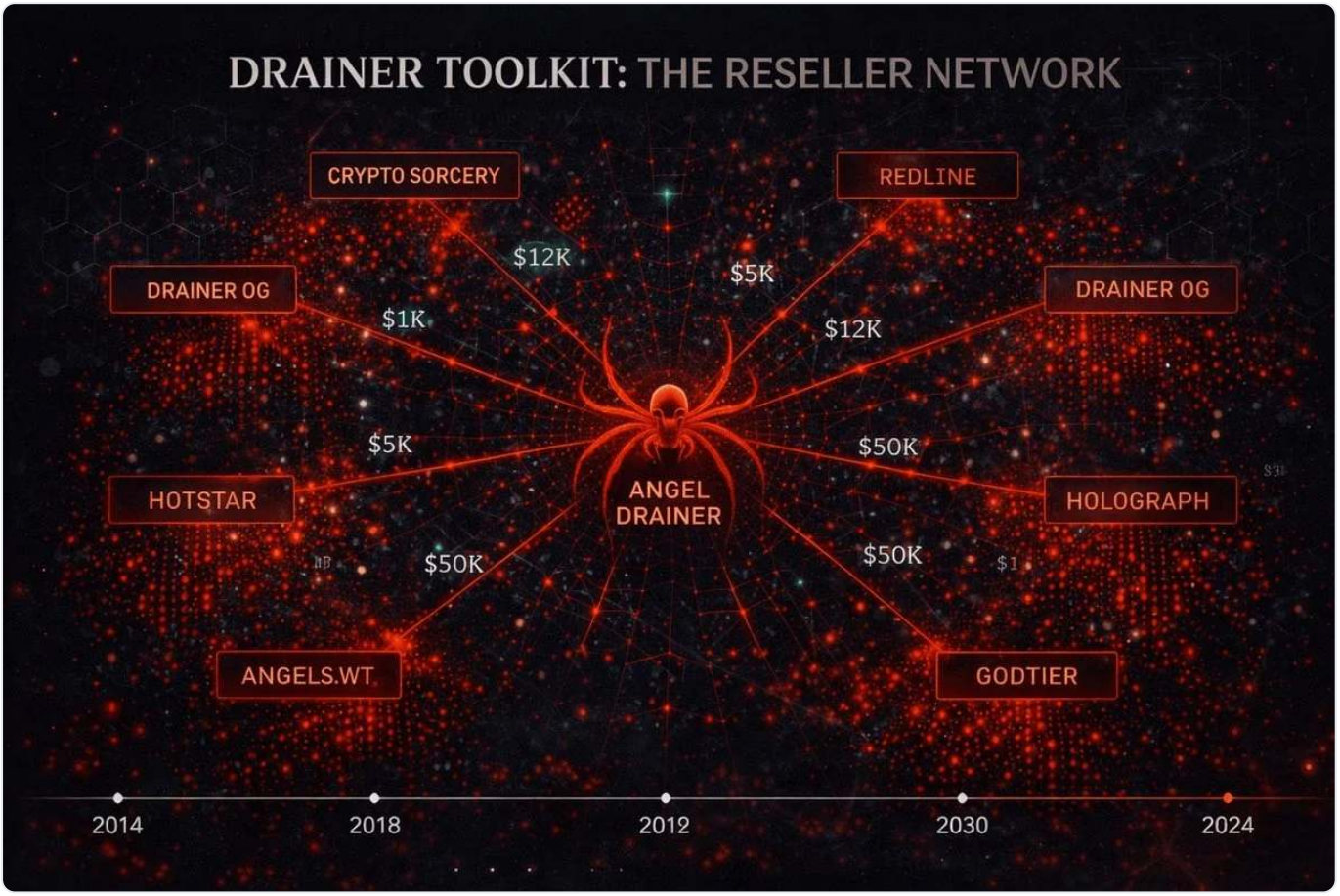
BuyTRX money flow — how stolen TRX moves through laundering chain

If you've interacted with any BUYTRX domain, check your TRON token approvals immediately. Revoke any suspicious approvals and report the domains.

Revoke Token Approvals Report a Domain DestroyList Tools

#CryptoDrainer #BuyTRX #OSINT #PhishingInfrastructure #TronScam

Related Investigations



DEEP INVESTIGATION

Crypto Drainer Toolkit: Angel Drainer Resellers Exposed

DEEP INVESTIGATION

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