

Rublevka Team: Anatomy of a Russian Crypto Drainer Operation

 recordedfuture.com/research/rublevka-team-anatomy-russian-crypto-drainer-operation

Insikt Group®



Executive Summary

Insikt Group has identified a major cybercriminal operation specializing in large-scale cryptocurrency theft, operating under the moniker “Rublevka Team”. Since its inception in 2023, the threat group has generated over \$10 million through affiliate-driven wallet draining campaigns. Rublevka Team is an example of a “traffer team,” composed of a network of thousands of social engineering specialists tasked with directing victim traffic to malicious pages. Unlike traditional malware-based approaches such as those used by the traffer teams Marko Polo and CrazyEvil (previously identified by Insikt Group, both of which distributed infostealer malware), Rublevka Team deploys custom JavaScript scripts via spoofed landing pages that impersonate legitimate crypto services, tricking victims into connecting their wallets and authorizing fraudulent transactions. Their infrastructure is fully automated and scalable, offering affiliates access to Telegram bots, landing page generators, evasion features, and support for over 90 wallet types. By lowering the technical barrier to entry, Rublevka Team has built an extensive ecosystem of global affiliates capable of launching high-volume scams with minimal oversight.

This structure poses a growing threat to cryptocurrency platforms, fintech providers, and brands whose identities are being impersonated. Organizations that facilitate blockchain transactions, particularly fintech firms, exchanges, or wallet providers, face elevated reputational and legal risks if customers fall victim to these scams. Even if the victim’s compromise occurs outside a firm’s platform, failure to detect spoofed landing pages or fraudulent referrals can trigger consumer backlash, loss of trust, or regulatory scrutiny around customer protections and Know Your Customer (KYC) enforcement. The threat group’s agility — evidenced by its use of frequently rotating domains, targeting lower-cost chains like Solana (SOL), and exploiting Remote Procedure Call (RPC) APIs — undermines traditional fraud detection and domain takedown efforts. Their model mirrors ransomware-as-a-service (RaaS) operations, signaling a continuation of the broader shift toward scalable, service-based cybercrime that organizations must proactively monitor, disrupt, and defend against to protect customers and maintain trust.

Key Findings

- The objective of a Rublevka Team scam is to create an attractive SOL-based offer, such as a promotion or an airdrop event, generate traffic to the lure via social media or advertisements, and trick a user into connecting their wallet to the website and signing a transaction that drains their wallet.
- As of writing, Rublevka Team’s primary Telegram channel has approximately 7,000 members. Over 240,000 messages have been posted to Rublevka Team’s automated “profits” channel, indicating at least 240,000 successful wallet drains, with transactions ranging from \$0.16 to over \$20,000.
- Rublevka Team offers a custom JavaScript drainer embedded into their landing pages, which exfiltrates victims’ SOL assets by draining held tokens. The drainer is compatible with over 90 SOL wallet types.
- The threat group’s infrastructure is fully automated via Telegram bots, offering affiliates tools for landing page creation, campaign tracking, cloaking, and distributed denial-of-service (DDoS) protection.
- The drainer campaign, active since 2023, leverages spoofed versions of legitimate services such as Phantom, Bitget, and Jito to maximize user trust and conversion

Background

Insikt Group has been monitoring Rublevka Team since August 2025, when we first encountered the threat group's advertisement banner on Exploit Forum. The name "Rublevka Team" is likely a reference to the Rublevka neighborhood of Moscow, a prestigious and wealthy suburb largely [populated](#) by elite Russian businesspeople and government officials. Like other trafter teams previously reported by Insikt Group, such as [Marko Polo](#) and [Crazy Evil](#), Rublevka Team is a "cryptoscam" team primarily operating on LolzTeam Forum, as well as maintaining a smaller presence on high-tier forums Exploit and XSS. However, in contrast to the trafter teams previously reported by Insikt Group, Rublevka Team does not rely on infostealer malware to target victims; instead, it operates a drainer script embedded in its landing pages to connect to victims' cryptocurrency wallets and drain their funds.



Figure 1: Rublevka Team advertisement banner, as seen on Exploit Forum (Source: Recorded Future)

Based on analysis by Insikt Group, Rublevka Team has been active since 2023, when it was first launched on LolzTeam Forum by the user "denisssss_inactive". Based on an analysis of its reported profits within its private channel, Rublevka Team has a lifetime revenue of over \$10 million USD as of the time of writing. The team's tactics, techniques, and procedures (TTPs) have evolved since it began operations in 2023. Originally, the threat group operated fake cryptocurrency exchanges to convince users to connect their wallets and deposit funds, focusing on generating traffic through Instagram and, later, TikTok. In 2024, however, Rublevka Team fundamentally shifted its tactics to deploy a custom JavaScript-based cryptocurrency wallet drainer on its landing pages, which impersonated cryptocurrency token airdrops and giveaways. The threat group initially targeted The Open Network (TON), then shifted to SOL in spring 2025. Its latest campaign, which is ongoing as of writing, has generated the majority of its total revenue (approximately \$8.2 million).

Rublevka Team Operations

Affiliate Recruitment

Rublevka Team's latest post on LolzTeam Forum, which was published by denisssss_inactive on April 18, 2025, advertises Rublevka Team's SOL drainer scam program. Since Rublevka Team's original postings advertising its cryptocurrency exchange scams and TON token campaigns, the payout rates have shifted significantly in affiliates' favor, with a starting percentage of 75% and 80% for "experienced users." The increase in commission rates for starting affiliates may indicate a shift over time in the team's monetization strategies based on the financial success the threat group has seen; it may now be more favorable to prioritize expanding the pool of workers rather than extracting maximum income from any individual affiliate.

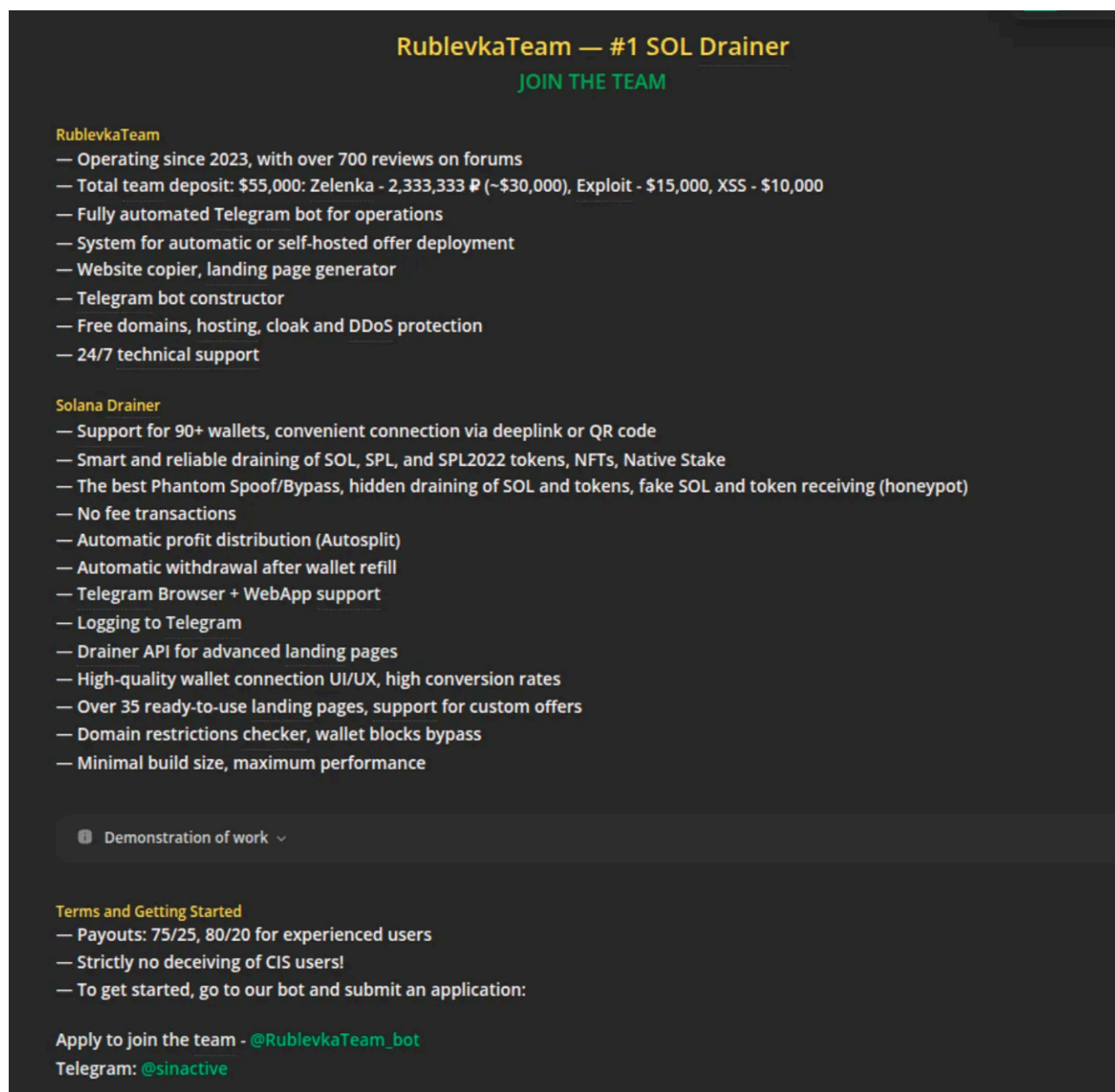


Figure 2: Screenshot of the latest SOL drainer advertisement, posted by denisssss_inactive (Source: LolzTeam Forum).

The post also advertises a fully automated Telegram bot for conducting operations, a landing page generator, and free domains and hosting services with included cloaking features and distributed denial-of-service (DDoS) protections. The advertisement also describes the SOL drainer used on the landing pages, which supports over 90 wallet types, draining capabilities for SOL, [Solana Program Library](#) (SPL) tokens (including SPL2022 extension tokens), [non-fungible tokens](#) (NFTs), and [Native Stake](#), spoofing and bypass features for Phantom wallet, a drainer API, and over 35 ready-to-use landing pages integrated with the drainer.

The posts do not specify any hard requirements for prospective affiliates, who are instructed to apply for the team via the Telegram bot [@]RublevkaTeam_Bot. Applications are likely vetted by Rublevka Team's leader, denisssss_inactive, or the administrative team ("Jesse Pinkman" and "Shell" at the time of writing).

Once an applicant is accepted to Rublevka Team, they are directed to join the following private channels:

- “[RublevkaTeam] Chat”: Closed group chat with messages dating back to May 2024, with 6,821 members as of writing
- “[RublevkaTeam] Profits”: Closed channel with messages dating back to June 2024, with 3,093 subscribers as of this writing
- “[RublevkaTeam] Info”: An informational channel posting updates to the drainer and affiliate program; the threat group also operates a Russian-language version of this channel, “[Rublevka Team] Инфо”
- “[RublevkaTeam] Landing pages”: Repository of screenshots of new landing pages used by Rublevka Team
- “RublevkaTeam_bot (@RublevkaTeam_Bot)”: Handles group applications and serves as an administrative panel for affiliate campaigns
- “Rublevka Utils (@RublevkaUtils_bot)”: Used for generating custom landing pages and video content for traffic generation

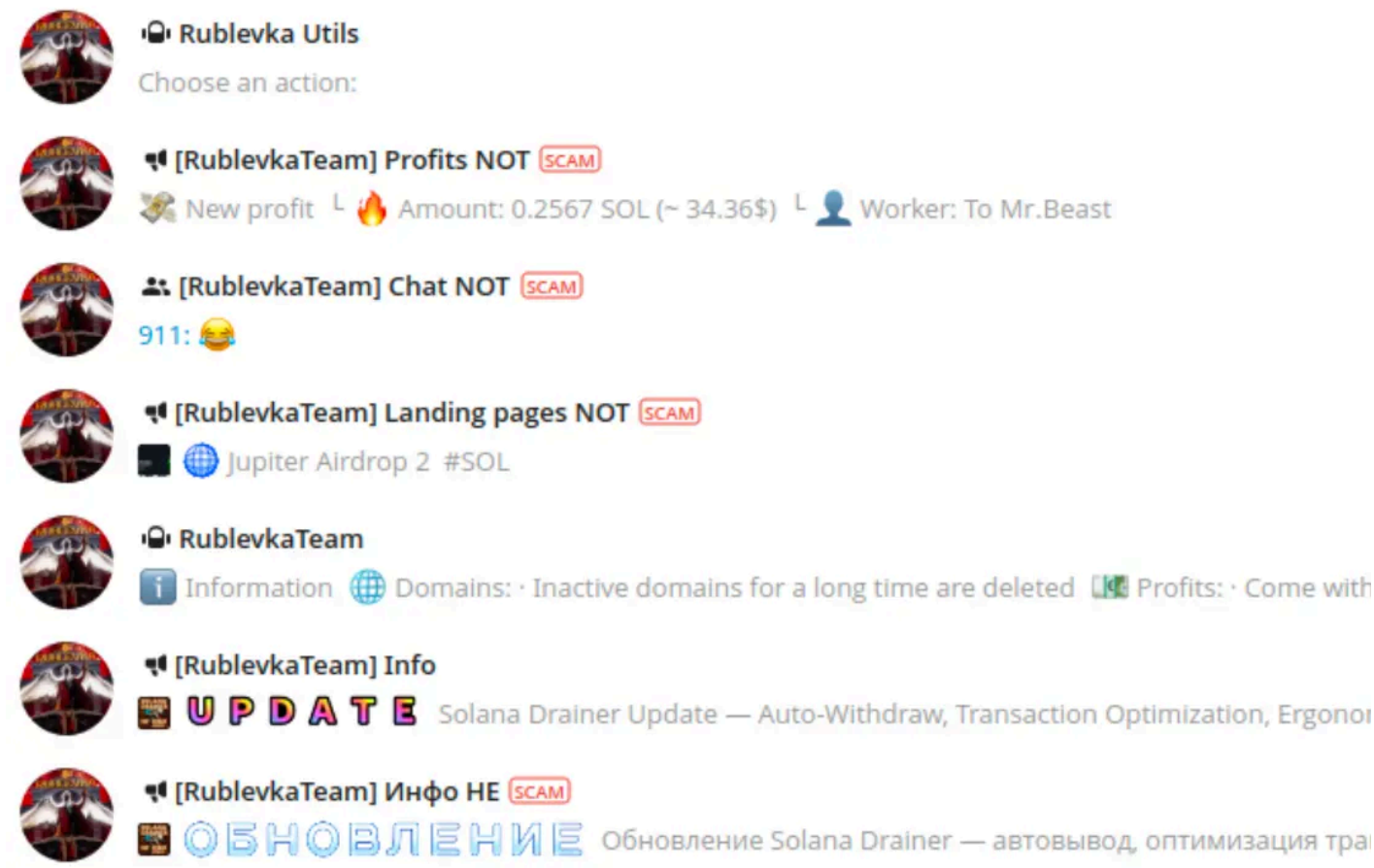


Figure 3: Rublevka Team private channels, accessible only by affiliates (Source: Telegram)

Manual Walkthrough

Rublevka Team hosts an informational manual for affiliates on the domain *rublevkateam[.]cc*. This manual outlines the procedures for working on the team, including how to use the Telegram bot, how to conduct cryptoscams, how to configure the drainer, and more.

The stated goal of the Rublevka Team scam is to create a “drainer-based offer” (usually a promotion, an airdrop notice, a KYC request, or other) and to attract traffic to the website. From the perspective of a victim (referred to as a “lead”), they will encounter the website, connect their cryptocurrency wallet to the website, and then receive an offer to perform a crypto transaction. Upon confirming and signing the transaction, all assets from the lead’s wallet are transferred to the website’s operator.

According to the manual, the team opted for SOL due to its fast transaction time and low fees, as well as its support for smart contracts, [decentralized apps](#) (dApps), and NFTs. The manual includes a table of popular wallets that support SOL and are compatible with the Rublevka drainer, which includes Solflare, Phantom, Backpack, Coinbase, Bitget, OKX, Metamask, and others.

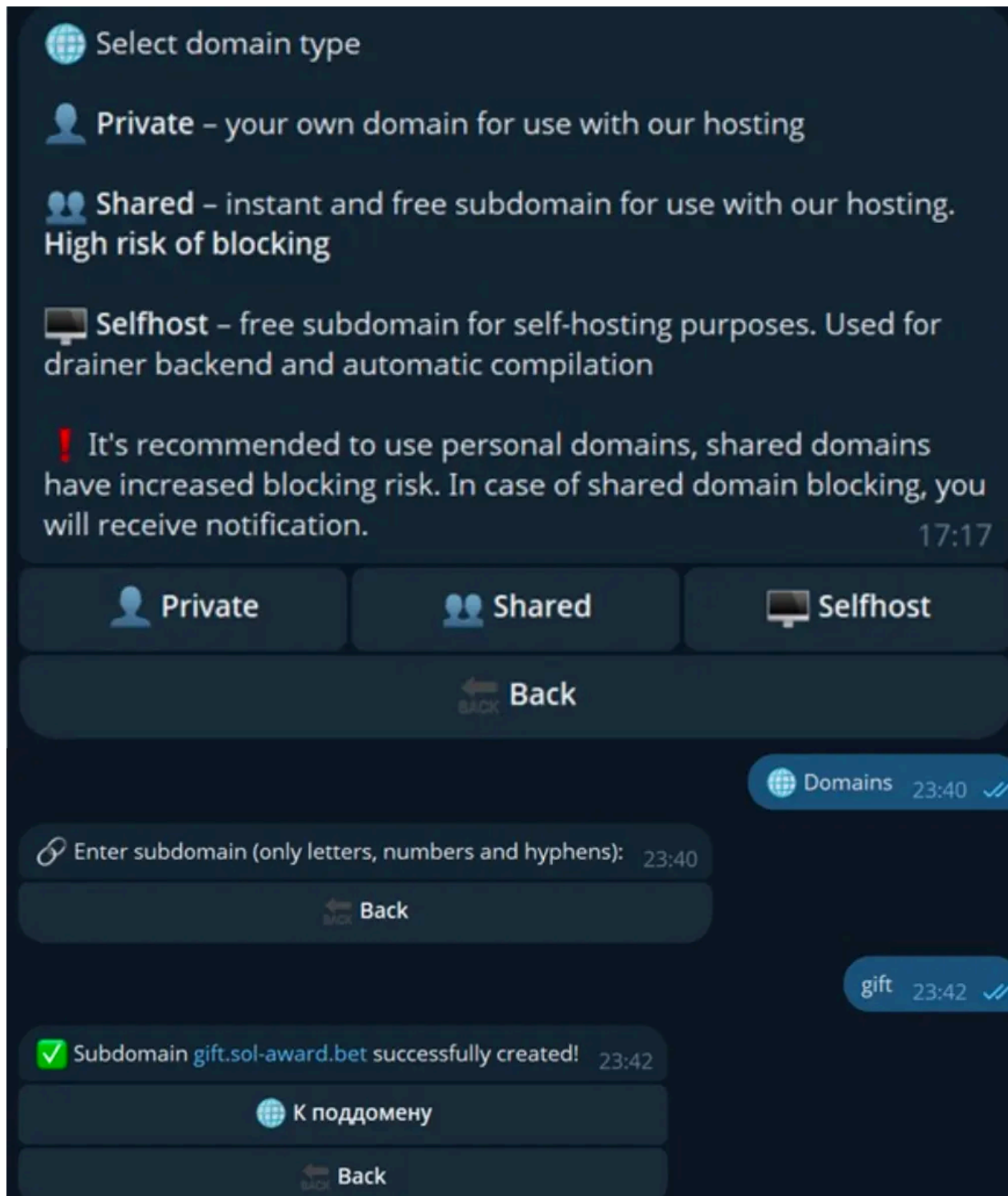
Notably, configuration for an affiliate's campaign is done within the [@]RublevkaTeam_bot, which is available in English, Russian, and Chinese, and in most cases requires no interaction with the support team. This provides affiliates with full control and visibility into their own campaigns.

Domains

Rublevka Team affiliates have three options when creating a domain for hosting a landing page:

- **“Shared domain”**: This type of domain is provided by Rublevka Team and is shared among multiple team members. This option is free of charge but has a higher chance of being blocked and comes with a preset list of names. With this option, a user chooses a custom subdomain, which is hosted under a shared apex domain managed by Rublevka Team and periodically rotated by administrators. Users on a shared domain have no control over the IP address of their website. This option has experienced continuous disruptions from December 2025 into 2026.
- **“Private domain”**: An affiliate provides a private domain, which they purchase and configure themselves. This option has minimal risk of being blocked and provides users with full control over their own hosting.
- **“Self-host”**: With this option, the affiliate can host the SOL drainer backend on a Rublevka Team-operated domain for free, with the intent that the affiliate invokes the script from their own privately hosted website.

Users can also choose to register subdomains of their private domain using the bot, with each subdomain functioning as a fully autonomous landing page.



Figures 4 and 5: Options to add a domain and subdomain in RublevkaTeam_bot (Source: Recorded Future)

Landing Pages

Once a domain is created, the affiliate can configure their landing page. Within the bot, the user has the option to create either a “regular” page, which includes a drainer, or a “white” page, which does not have a drainer and is used to evade abuse detection services. The white pages are used as part of the “Red Table Bypass” feature, designed to unblock a domain that has been blocked by Google by temporarily displaying a harmless web page. In both cases, the user has the option to choose from a wide selection of pre-created landing pages.

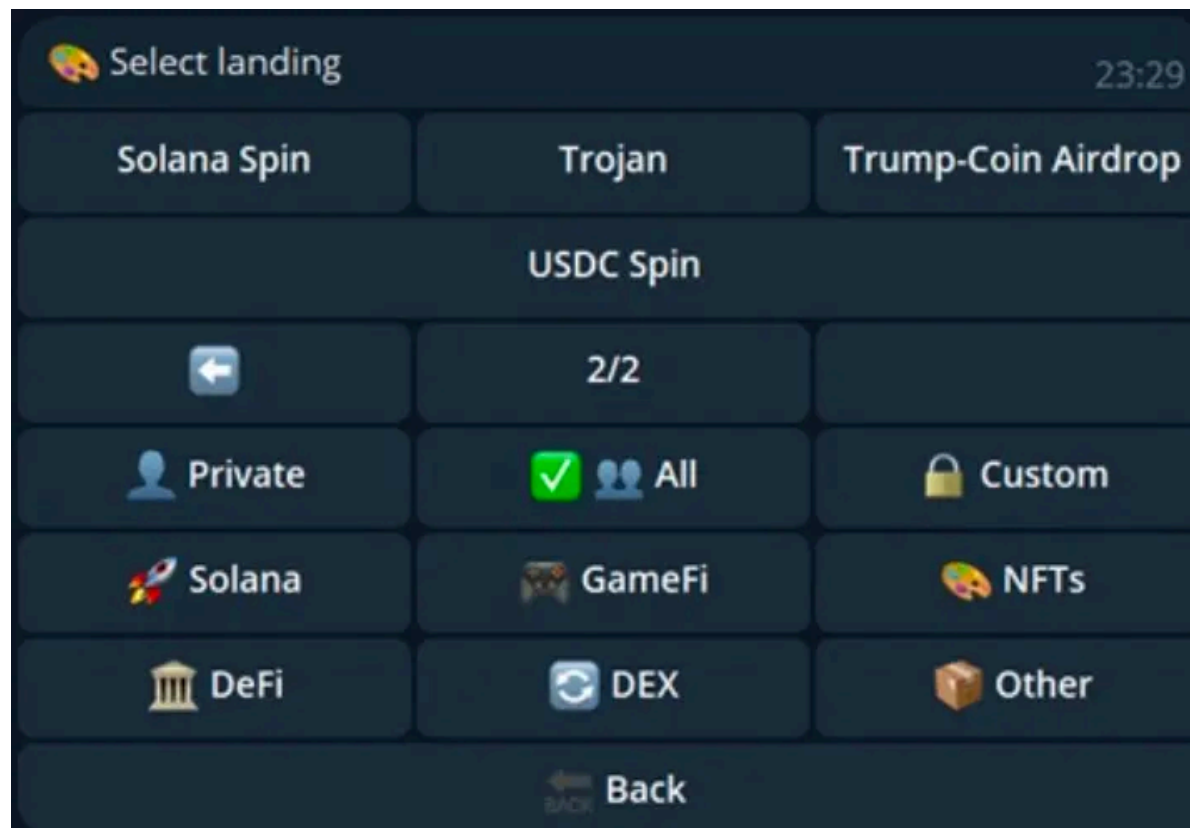


Figure 6: Options to choose a “regular” landing page, as per the Rublevka Team manual (Source: Recorded Future)

Alternatively, users can choose to generate their own landing page based on a template, which can be customized to a token of the user’s choice. They can also choose to “copy” an existing website by providing a URL to the bot; however, as of writing, this functionality appears to be broken.

Official airdrop

Discover Exclusive TRUMP Airdrop

Get direct TRUMP airdrop and never miss out on free crypto rewards. Track, participate, and claim airdrop from top blockchain projects across Solana ecosystem. [Hurry up!](#)

Get Started

Learn More

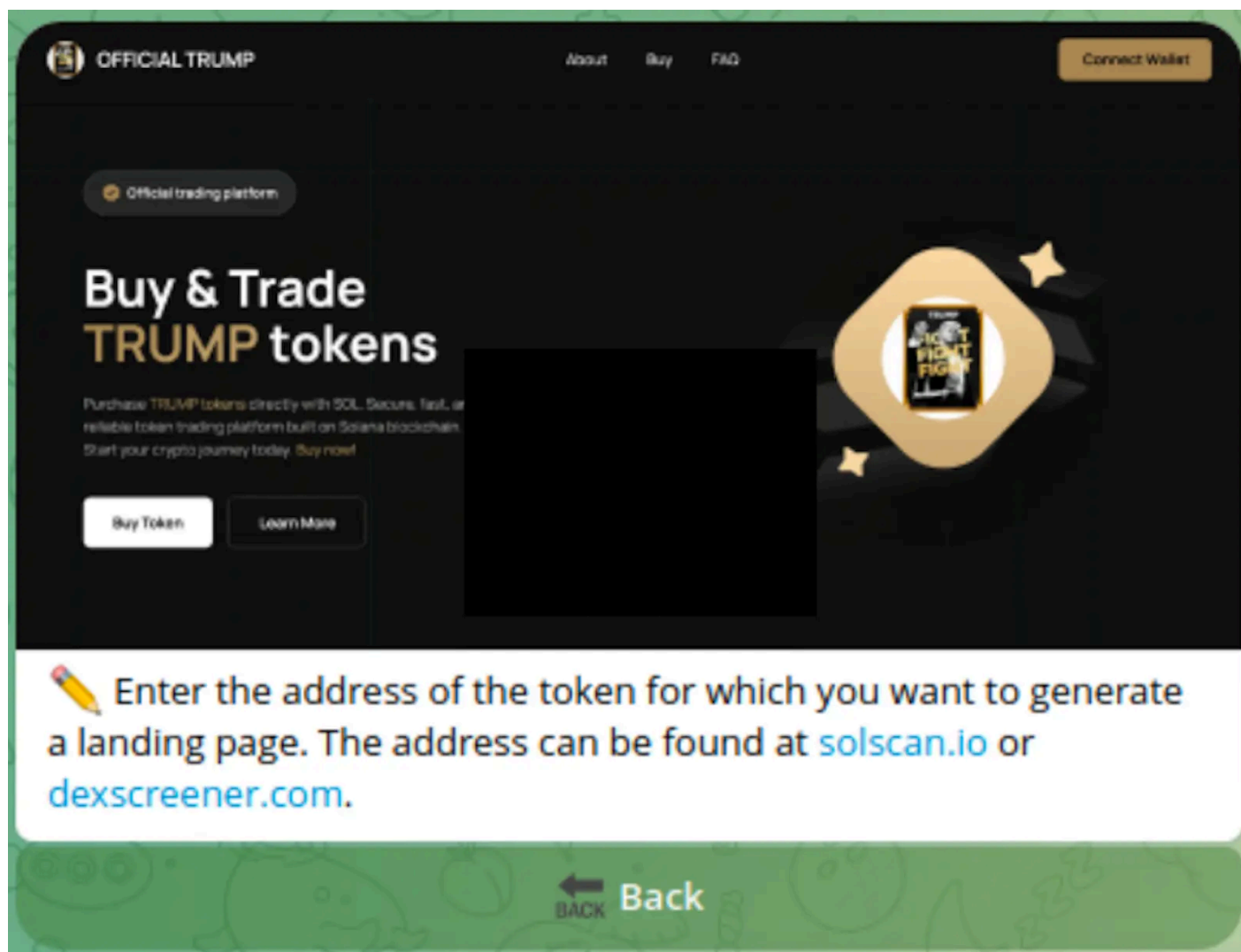


ORCA PYTH SolBlaze BONK Jito Marinade

 Enter the address of the token for which you want to generate a landing page. The address can be found at solscan.io or dexscreener.com.



Back



Figures 7 and 8: Two of the template options for generating a custom landing page for either an airdrop or token-buying scam (Source: Recorded Future)

In addition to generating landing pages, the Telegram bot also allows users to configure “cloaking settings” for their domains. Cloaking is a technique used by cybercriminals that involves presenting website content to a search engine in a way that differs from what the victim will see after navigating to the website. However, Rublevka Team uses the term to describe access restrictions for users from certain countries, IP addresses, internet service providers (ISPs), or virtual private network (VPN) or proxy users. Affiliates can also configure redirect logic and CAPTCHAs via Cloudflare to redirect victims to another landing page if the primary domain is blocked; they can also filter out bots to reduce the likelihood of the domain being blocked. The Telegram bot also supports configurations that allow only the user’s domain to open as a Telegram Mini App for Telegram-based traffic schemes, as well as the option to block specific “leads” (victims).

Drainer Logic and Configuration

Rublevka Team affiliates can configure the settings for the drainer to fit their specific needs. The drainer can display a custom fake transaction for receiving SOL or a fake token, based on the contents of an affiliate’s landing page, and can be configured to display a fake credit for each asset drain operation on the wallet. Affiliates can also set up minimum balance alerts to lure victims into buying additional SOL to use on their landing page.

The drainer has additional settings specifically for Phantom wallet, which the manual states is one of the most popular SOL wallets and can allow for a significant boost in “traffic conversion.” The drainer supports the following Phantom wallet “modes,” which are ways to connect with a user’s Phantom wallet to convince a user to sign a malicious drainer

transaction:

- **“Honeypot”**: This mode relies on a fake incoming token or SOL receipt to prime the user before initiating a visible drain transaction. The drain is shown as an outgoing transfer, but Phantom does not flag it as risky. Fake receipts only render correctly for tokens installable through Phantom’s UI (not arbitrary custom tokens). A modal window falsely claims that the drained assets will be returned via a second transaction.
- **“Honeypot2”**: Honeypot2 expands on Honeypot by requiring two transactions. The user first sees a fake inbound transfer, then approves a follow-on transaction that performs the drain. When combined with Crasher, the second transaction may appear as a simulation error rather than a clear debit. As with Honeypot, a modal window falsely claims that a refund will follow.
- **“Fake Return”**: Unlike Honeypot, this mode does not simulate inbound funds; instead, it shows a straightforward outgoing transfer that appears legitimate. After a user signs the transaction, a modal window falsely claims that a second “return” transaction will refund the assets.
- **“Crasher”**: This is a stealth-focused drain designed to complete in one interaction with minimal user review. Phantom displays a generic warning commonly seen on legitimate sites, reducing suspicion through familiarity. There is no fake inbound activity or refund narrative. This mode is considered experimental and is replaced by Honeypot behavior on mobile devices.
- **“Whitelist”**: This mode is intended for domains explicitly whitelisted by Phantom, and is used in conjunction with other modes. When active on a whitelisted domain, it enables hidden draining and fake inbound token displays. If enabled on a non-whitelisted domain, Phantom blocks all draining activity, rendering the mode ineffective.
- **“Warning”**: Unlike other modes that suppress warnings, this mode intentionally displays a Phantom warning banner while concealing the drain mechanics, aiming to exploit warning fatigue in users. A modal window instructs the user to proceed despite the warning. Default warnings include:
 - “This dApp could be malicious”
 - “You are approving over 200 transactions”
- **“Remove Phantom”**: This mode restricts Phantom wallet use by hiding it from wallet selectors or blocking connection attempts.



Confirm Transaction

passive-validator.online

Balance changes are estimated. Amounts and assets involved are not guaranteed.



Solana

-0.00844 SOL



Pudgy
Penguins

-394.24909
PENGU



USD Coin

+1,000 USDC



Bonk

-1,333,131 Bonk

Cancel

Confirm



Confirm Transactions

Balance changes are estimated. Amounts and assets involved are not guaranteed.



Failed to simulate the results of this request. Confirming is unsafe and may lead to losses.

Network



Solana

Network Fee

0.00034 SOL

► Advanced

Only confirm if you trust this website.

Cancel

Confirm



Warning



-0.0361 SOL

 Solana

< 0.00001 SOL

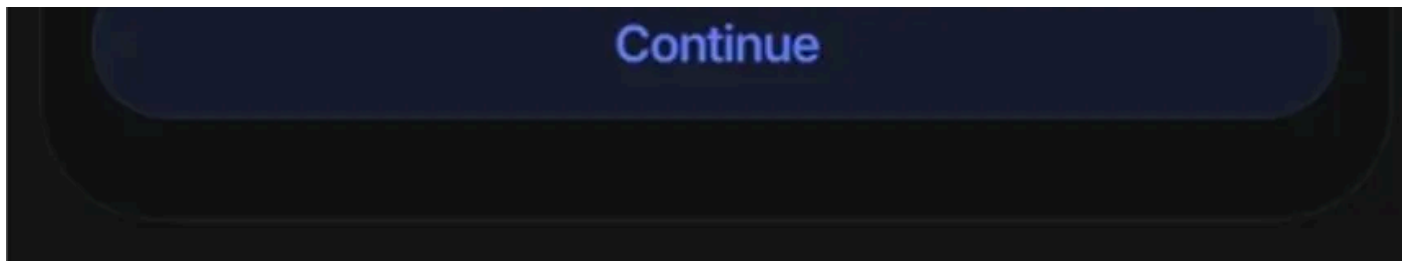
Confirm if you trust this website.

Cancel

Confirm



Note: This dApp uses Abuse Protection to prevent misuse of platform. You'll need to complete a quick verification of your transaction history. It's completely safe and only takes a few seconds.



Figures 9–11: Screenshots of “Honeypot,” “Crasher,” and “Fake return” modes (Source: Recorded Future)

The user can configure notifications in Telegram to notify them when a user visits their website, receives a withdrawal request, does not have funds, and more. Additionally, they can use the “Autosplit” feature, which will send any stolen funds directly to their private wallet, bypassing any intermediaries such as smart contracts or the shared Rublevka Team wallet, which is the default behavior. In this case, the profits are sent as they are, with each drained token being sent without conversion to the threat actor’s wallet.

Additionally, Rublevka Team provides an API (PiterAPI) stored in the `piter` variable within the JavaScript code to allow more advanced users to further customize drainer behavior. This API includes the following functions:

- “connect”: Opens the modal window to connect to a victim’s wallet
- “process”: Prompts the user to sign the transaction
- “onConnect”: Sets the function to be called when a user connects their wallet
- “getBalance,” “getAddress”: Gets victim wallet information
- “setToken”: Sets up context for a specific token to be drained, including the token account address, mint, victim address, price, amount, and whether it’s an SPL-2022 token

Landing Pages and Content

Through the Telegram bot, Rublevka Team provides affiliates with an extensive catalog of landing pages available for use in their campaigns. As of October 2025, the Insikt Group identified 50 unique drainer landing pages and eleven “white” landing pages provided to affiliates. It is possible that additional landing pages have been added to the Telegram bot since then.

The drainer landing pages spoofed meme coin and stablecoin token airdrops, token mints, decentralized finance (DeFi) trading platforms, SOL staking services, and more. For the most part, the landing pages impersonate existing “legitimate” services, such as Axiom, Bitget, Photon, Jito, and Marinade. The landing pages also impersonate existing meme coin and social coin tokens for airdrops, including “Bonk,” “DogWifHat,” “Trump,” “Pengu,” and “Fartcoin.” The SOL-specific services pages typically reference SOL liquid staking, “burning” or “incineration,” faucets, airdrops, snipers, and multipliers. Generally, the landing pages included social media and informational links to the actual websites of the coins and services they were impersonating, likely to appear legitimate in a cursory check.



TRUMP COIN



CLAIM REWARD

TAKE PART IN THE **BIGGEST** **TRUMP COIN** AIRDROP

THE FIRST OFFICIAL AIRDROP FROM THE PRESIDENT OF AN ENTIRE
COUNTRY, AIMED AT HELPING ACTIVE PARTICIPANTS.

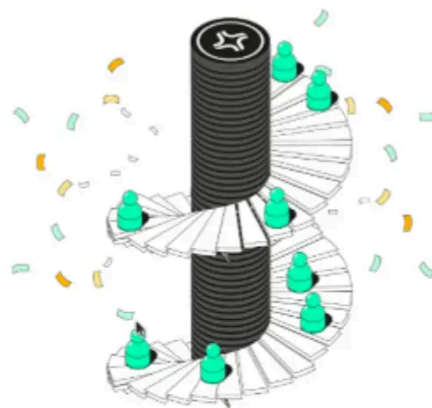
CLAIM REWARD

LEARN MORE



Welcome to the future of Jito governance

Introducing JTO token: empowering our community to directly shape the Jito Network's evolution. Search below to verify eligibility of your Solana wallet address

[Check eligibility](#)[About Airdrop](#)

Want To Know If You Are Eligible?

[Connect Wallet](#) or search a wallet address

Only 22 days left to claim...

Native staking

Automatically stake SOL with top performing validators. [How it works](#) ➤

[Stake SOL](#)
[Migrate stake](#)

Stake



 SOL

0.0

Delegation strategy ⓘ

Max Yield 8.73% APY

Stake is delegated to 100+ bidding validators to maximize yield.

Connect wallet

By connecting your wallet, you agree to our
[Terms of use](#), [Referral Program Terms](#) and [Privacy Policy](#)



Interested in Liquid Staking?

Stake with mSOL and get instant liquidity

[Stake with mSOL](#)



CONNECT WALLET >

Official from Bitget

Official Solana Airdrop by Bitget

Community support from the biggest crypto exchange
Luck will turn to you! The odds are the same for everyone.

CONNECT WALLET >

What is SOL Airdrop?





SOL SNIPER BOT

 Automate Your Trades and Dominate the Solana Market with Precision Sniping!

[Open SOL Sniper Bot](#)[Check Safer Solana Sniper](#)



Figures 12–17: Sample of Rublevka Team drainer landing pages impersonating Trump Coin, Jito, Marinade, Bitget, and Jupiter (Source: Recorded Future)

The landing page generator also included a panel for selecting a crypto wallet to connect to the malicious page, which prompts users to either connect an existing wallet or create a new one.

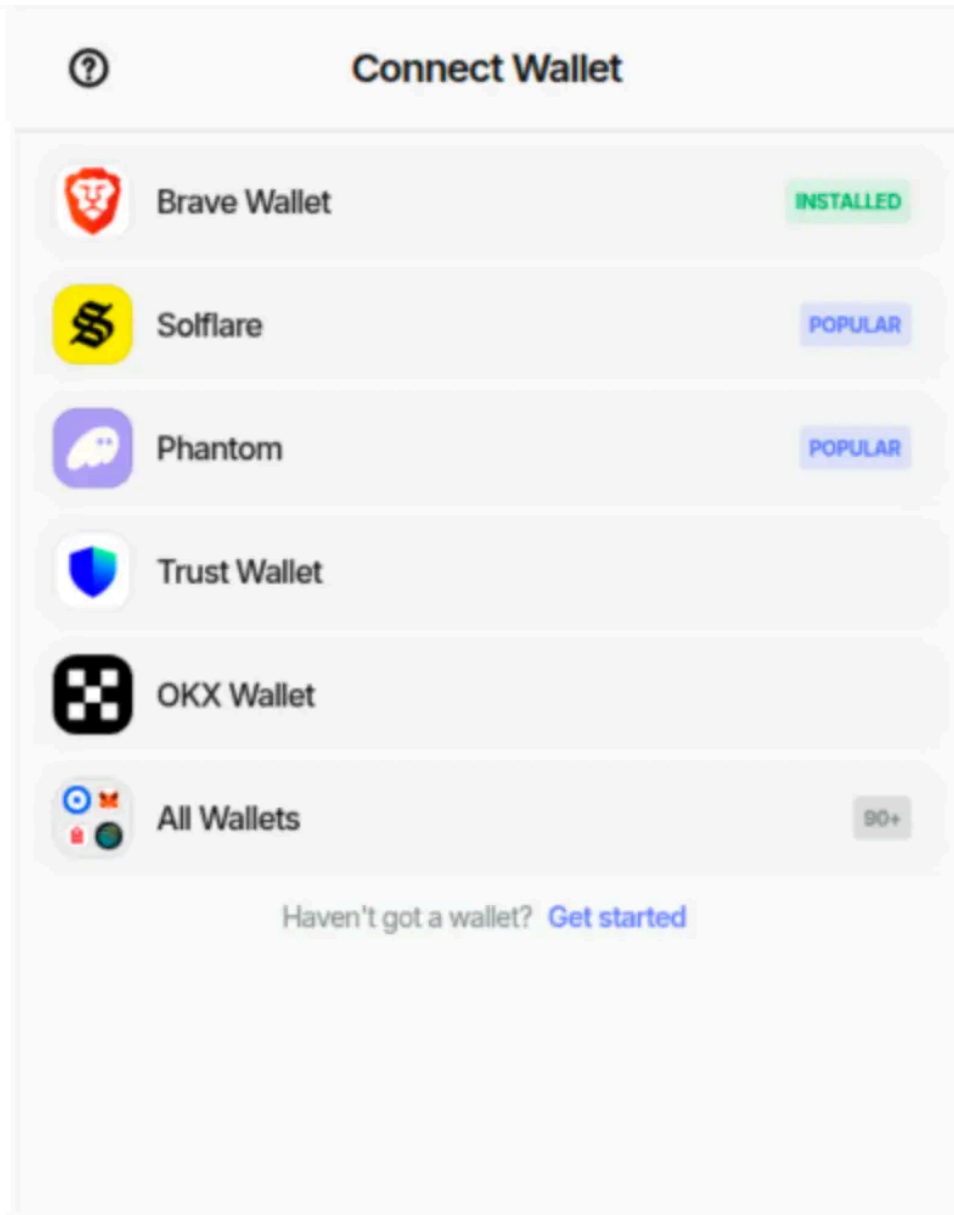


Figure 18: The “Connect Wallet” landing page prompting users to connect a supported wallet to the drainer (Source: Recorded Future)

It is likely that these landing pages are used to lure victims to connect their wallet to the website, after which the embedded drainer script, `index.js`, will enumerate the wallet’s holdings, trick the user into signing a malicious transaction, and drain all held funds.

JavaScript Drainer Analysis

Based on Insikt Group’s analysis of the malicious landing pages, we identified that each page contained the file `index.js` (`9c21d538c2a556f4a5b351b29f3513097ac57643f291ff6d751400d8dbc69489`). This file is heavily obfuscated; Insikt Group assesses that the authors possibly used [js-confuser](#), a free open-source JavaScript obfuscation tool with no available deobfuscator. However, Insikt Group was still able to identify strings of interest within the code, including indicators that may suggest parts of the script’s functionality.

The drainer includes the following URLs:

- `hxxps://mainnet[.]helius-rpc[.]com/?api-key=`
- `hxxps://mainnet[.]helius-rpc[.]com/?api-key=8e0e9a34-2648-421a-8f22-6460b4a68705`

- `hxxps://mainnet[.]helius-rpc[.]com/?api-key=55065729-bda8-4cf8-87a1-7bd64cf22726`
- `hxxps://mainnet[.]helius-rpc[.]com/?api-key=db25ae76-7277-45ce-b21a-5be1a61f2f04`
- `hxxps://mainnet[.]helius-rpc[.]com/?api-key=44b7171f-7de7-4e68-9d08-eff1ef7529bd`
- `hxxps://mainnet[.]helius-rpc[.]com/?api-key=bfd713ef-c9a7-404f-804c-e682c2bd0d3b`
- `hxxps://mainnet[.]helius-rpc[.]com/?api-key=f30d6a96-5fa2-4318-b2da-0f6d1deb5c83`
- `hxxps://mainnet[.]helius-rpc[.]com/?api-key=3b5315ac-170e-4e0e-a60e-4ff5b444fbcf`
- `hxxps://rpc[.]walletconnect[.]org/v1/?chainId=solana%3A5eykt4UsFv8P8NJdTREpY1vzqKqZKvdp&projectId=730eede4c040eafa7a928a503b6cd650`
- `hxxps://solana-rpc[.]publicnode[.]com`
- `hxxps://wallet-api[.]solflare[.]com`

These are likely authorization calls to the Solana remote procedure call (RPC) API endpoints provided by RPC platforms Helius and WalletConnect, as well as the free Solana RPC endpoint provided by PublicNode. These endpoints are likely used to conduct the malicious drainer transactions. Notably, the Helius and WalletConnect URLs include API keys, as both services require sign-up and have various service tiers. As such, these API keys likely belong to Rublevka Team developers. The Solflare endpoint is likely used to connect to a victim's wallet for enumeration and draining. The strings also included the domain *efficient-endpoint[.]site* (discussed further in the **Domains and Infrastructure** section below).

The drainer code also includes the following strings (verbatim):

- Strings related to building SOL [transactions](#) and [address tables](#), including:
 - "numSignerAccounts"
 - "programAddressIndex"
 - "lookupTableAddress"
 - "addressTableLookups"
 - "solana:101/nativeToken:501"
 - "solana:mainnet"
 - "standard:connect"
 - "solana:signTransaction"
 - "solana:signAllTransactions"
 - "solana:signMessage"
- Instructional and error messages related to wallet transactions:
 - "Transactions are reverted. Sign all transactions to verificate your account"
 - "Phantom is temporarily unsupported, please choose another wallet"
 - "You have an insufficient balance. Top-up your balance by at least {fee} SOL"
 - "This DApp would like to connect your wallet"
 - "You are allowing this DApp to"
 - "View wallet balance & activity"
 - "Request approval for transactions"
 - "Perform transactions without confirmation"
 - "\n\nWelcome to our DApp. Signing is the only way we can truly know that you are the owner of the wallet you are connecting. Signing is a safe, gas-less transaction that does not in any way give us permission to perform any transactions with your wallet.\n\nURI: https://"
 - "A wallet lets you store, send and receive digital assets like cryptocurrencies and NFTs."

- Messages stating that the dApp can be trusted:
 - “This application hasn’t been reviewed by Phantom yet, but it is listed in trusted community-maintained safety databases. You can proceed with confidence — this app is recognized as safe.”
 - “This dApp uses a new, optimized transaction delivery method that is not yet displayed correctly in Phantom. You can proceed with confidence — this app is recognized as safe.”
 - “This dApp uses Abuse Protection to prevent misuse of platform. You’ll need to complete a quick verification of your transaction history. It’s completely safe and only takes a few seconds.”
- String related to Telegram integration:
 - “TelegramWebview”
 - “TelegramWebviewProxy”
 - “tgWebAppVersion”
 - “TelegramGameProxy”
 - “[Telegram.WebView] < receiveEvent”
- A catalog of supported wallets, including wallet display names, URI schemes, iOS and Android package identifiers, and deeplinks, including Arculus, Blockchain, Ledger, KuCoin, Atomic, CoinEx, Trezor, and others.

Insikt Group also identified approximately 160 unique strings within the drainer that resembled SOL addresses. Of these, approximately 30 corresponded to known addresses in the SOL ecosystem, including system programs and token mints. The remaining approximately 130 addresses do not have any official SOL affiliation and are likely private addresses linked to attacker infrastructure. These addresses are discussed further in the **Cryptocurrency Addresses** section below.

Profits and Top Earners

Rublevka Team has tracked their profits in the closed Telegram channel “[RublevkaTeam] Profits” since at least June 2024. Each entry contains a user’s “Worker” name (sometimes hidden) and the profit from a single transaction in SOL (or TON, during their previous campaign) and USD. As of this writing, the channel has over 240,000 messages and approximately 3,000 subscribers. Insikt Group performed an analysis of the total sum of profits generated by affiliates since the channel’s inception, totaling approximately \$10.9 million USD as of December 8, 2025. The sums for individual profit messages span from as little as \$0.16 per transaction to upwards of \$20,000.

[RublevkaTeam] Profits NOT



New profit

L



Amount: 2.4197 SOL (~ 329.48\$)

L



Worker: Pivo Boss

[RublevkaTeam] Profits NOT



New profit

L



Amount: 0.3277 SOL (~ 44.47\$)

L



Worker: Hidden

[RublevkaTeam] Profits NOT



New profit

L



Amount: 0.0769 SOL (~ 10.43\$)

L



Worker: 🤔

[RublevkaTeam] Profits NOT



New profit

L



Amount: 19.5665 SOL (~ 2,652.17\$)

L



Worker: LL

[RublevkaTeam] Profits NOT



New profit

L



Amount: 1.9636 SOL (~ 265.51\$)

L



Worker: fifi

[RublevkaTeam] Profits NOT



New profit

L



Amount: 6.1992 SOL (~ 838.25\$)

L



Worker: John Berlin

Rublevka Team Top Earners (June 2024 – December 2025)

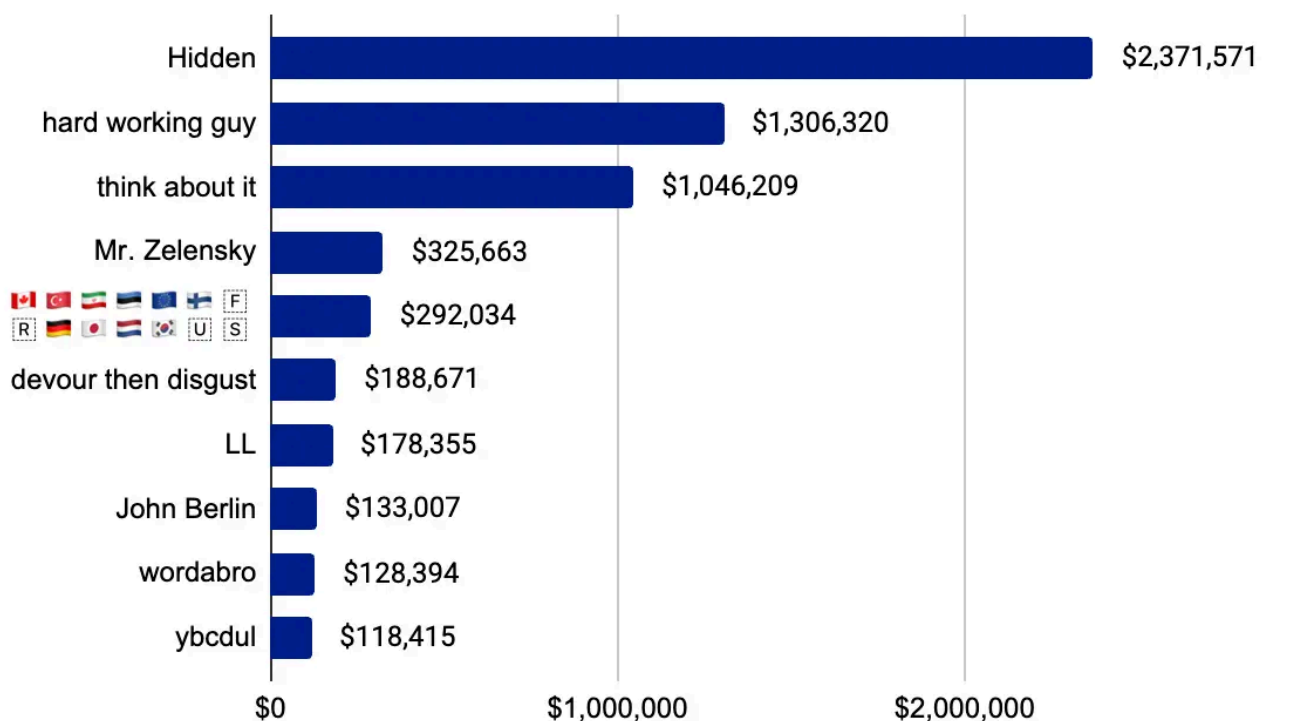


Figure 20: Top named earners on Rublevka Team between June 2024 and December 2025, based on the threat group’s Telegram profits channel, where “Hidden” users amassed the most combined profits (Source: Recorded Future)

Domains and Infrastructure

Insikt Group collected a sample of domains associated with Rublevka Team based on the Telegram bot and channels linked to the threat group. Based on proprietary sources, it is evident that Rublevka Team is constantly changing and rotating their infrastructure, including the domains used to host their shared pages for affiliate use, as well as other staging infrastructure to host aspects of their drainer. Over the last year, shared Rublevka Team domains have included:

- *open-sol[.]jcc*
- *sol-galaxy[.]jcc*
- *web-core[.]jcc*
- *sol-hook[.]jorg*
- *sol-coin[.]xyz*

Using open-source intelligence (OSINT) tools, Insikt Group identified approximately 70 unique subdomains historically associated with *open-sol[.]jcc*, 400 associated with *sol-hook[.]jorg*, 300 associated with *sol-galaxy[.]jcc*, 30 associated with *web-core[.]jcc*, and 40 associated with *sol-coin[.]xyz*, as of writing. A cursory analysis of these domains’ hosting information showed that Rublevka Team primarily hides their shared infrastructure behind Cloudflare, with variation in registrars (using CNOBIN, Public Domain Registry, and an unspecified Hong Kong-based registrar). Notably, in November and December 2025, three of the domains (*sol-galaxy[.]jcc*, *web-core[.]jcc*, and *sol-coin[.]xyz*) migrated to IP address 158[.]94[.]208[.]165, registered to “Lanedonet Datacenter,” previously named “Metaspinner Net GmbH.” Insikt Group recently identified Metaspinner net GmbH as a fraudulently registered hosting network that impersonated a

legitimate German software company. Following RIPE NCC intervention, the network was re-registered under Lanedonet Datacenter. Insikt Group assessed with high confidence that Lanedonet Datacenter is operated by threat activity enabler (TAE) Virtualine Technologies.

The image is a screenshot of a website banner for SOLANA. The background is a dark purple gradient with faint, abstract patterns. At the top, there is a dark purple navigation bar containing the SOLANA logo on the left and four links: Home, About Event, Live Vouchers, and FAQ. On the right side of the navigation bar is a purple button with the text "Activate Voucher". Below the navigation bar, centered, is a purple pill-shaped button with the text "EVENT" in white, followed by the text "Voucher Event is now available!". The main headline is "Free USDC vouchers available now." in large, white, sans-serif font. Below the headline, there is a paragraph of text: "Exclusive closed event with powerful rewards and analytics. Supercharge your DeFi journey & get exclusive USDC vouchers from anywhere." Below this text are two buttons: a purple "Activate Voucher" button and a white "Learn More" button. Further down, centered, is the text "Trusted by 500+ Solana developers". At the bottom, there is a row of logos for various Solana ecosystem projects: Jito, Marinade, METAPLEX, ORCA, and a partially visible logo on the right.

SOLANA Home About Event Live Vouchers FAQ [Activate Voucher](#)

EVENT Voucher Event is now available!

Free USDC vouchers available now.

Exclusive closed event with powerful rewards and analytics.
Supercharge your DeFi journey & get exclusive USDC vouchers from anywhere.

[Activate Voucher](#) [Learn More](#)

Trusted by 500+ Solana developers

Jito Marinade METAPLEX ORCA



CONNECT WALLET >

Official from Bitget

Official Solana Airdrop by Bitget

Community support from the biggest crypto exchange
Luck will turn to you! The odds are the same for everyone.

CONNECT WALLET >



What is SOL Airdrop?

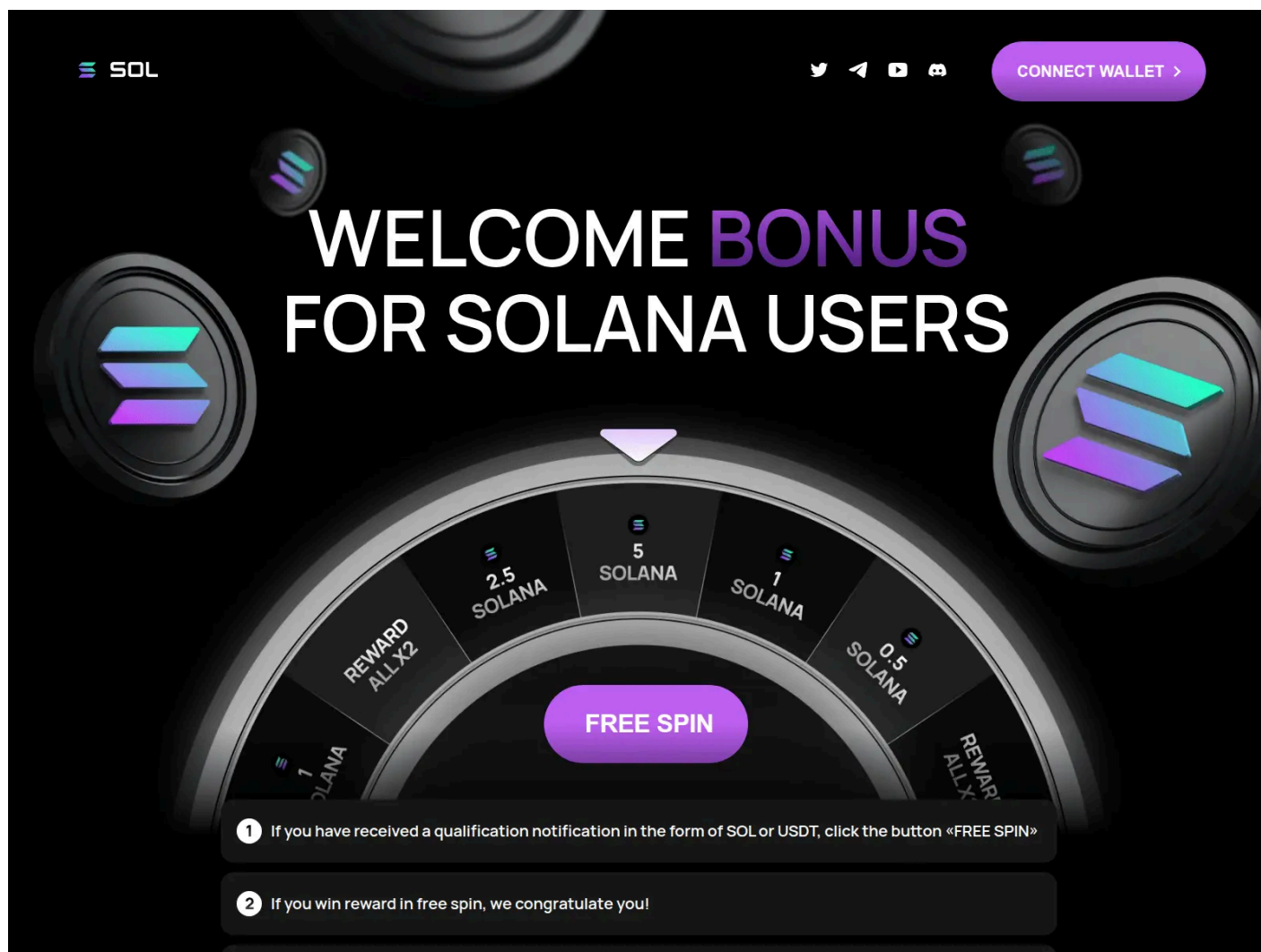


How do I get tokens as part of the SOL Airdrop?



How do I use tokens after receiving them in SOL Airdrop?





Figures 21–23: Sample of subdomains associated with *sol-galaxy[.]cc*; from left to right: *usdcoin.sol-galaxy[.]cc*, *rewards.sol-galaxy[.]cc*, *fortunawheel[.]sol-galaxy[.]cc* (Source: Recorded Future)

Insikt Group also identified several domains used for Rublevka Team’s shared drainer backend hosting (“selfhost”) service: *g-app-d[.]cc*, *fontmaxplugin[.]cc*, and *commontechrepo[.]cc*. These domains are also behind Cloudflare and have obfuscated registration information. We identified approximately 60 unique subdomains under *g-app-d[.]cc*, approximately 20 under *fontmaxplugin[.]cc*, and approximately 40 under *commontechrepo[.]cc*, all of which followed the naming convention “[word1]-[word2].[domain].cc,” where “word1” and “word2” appeared to be randomly selected words. This is likely due to the specific domain generation algorithm (DGA) used by Rublevka Team to automatically spin up domains as they rotate them.

Insikt Group also identified the domain *efficient-endpoint[.]site* contained within the drainer file *index.js*. This domain was registered on September 24, 2025, and was hosted behind Cloudflare until December 12, 2025. After this date, the WHOIS record indicated it was registered via Namecheap to “Alexander Petrov,” with a physical address at 742 Evergreen Drive, Springfield, OR (likely fake), and the email address *alex[.]petrov[.]domain[.]emailsecure[.]tech*.

Insikt Group identified additional domains registered to this individual and email address, with over 900 registered since April 2025. These subdomains followed several DGA patterns since first being registered, including “[word 1]-[word 2]-[word 3]” and “[word 1][word 2][word 3]” (where each word is themed around decentralized finance and technology), “[word 1][word 2]”, and “[word 1]-[word 2]”. They used the top-level domains .xyz, .online, .site, .store, .space, .online, and .com.

The first website observed in OSINT sources registered to the email address *alex[.]petrov[.]domain[.]emailsecure[.]tech* is *burn-shard-bridge[.]xyz*, first observed on April 15, 2025. Around this time, the website displayed a “Connect Wallet” window similar to that observed in the Rublevka Team landing page generator, and an analysis of calls made by the website included */piter/visit* and */piter/fetch*, matching the name of the “Piter” drainer API described in Rublevka Team’s manual. We identified the following five additional domains that shared similar features and were registered to the same email address:

- *public-proof[.]online*
- *private-peer[.]store*
- *highperformance-kit[.]online*
- *instant-automated-matrix[.]website*
- *highperformance-shard[.]online*

All of these websites demonstrated similar behavior, including displaying the same “Connect Wallet” window, calls to the PiterAPI function *openModal()*, and references to a JavaScript file that is highly similar to the drainer analyzed by Insikt Group. Hashes for the JavaScript drainer files observed on these websites are included in **Appendix A**.

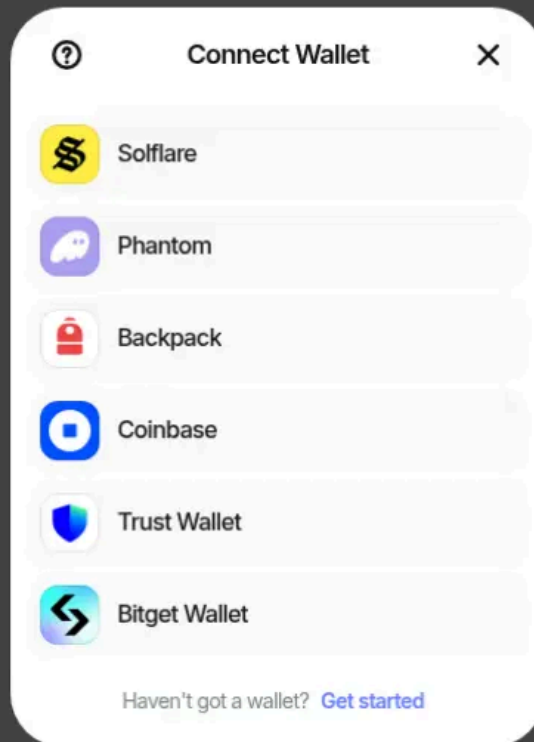


Figure 24: The page displayed by *burn-shard-bridge[.]xyz* in April 2025, which made HTTP requests to endpoints referencing “*piler*” (Source: Recorded Future).

We assess that the domains registered to Alexander Petrov are possibly automatically generated infrastructure for use by Rublevka Team to host backend functions of their drainer operation, where the high volume of the domains is likely intended to enable the threat group to frequently rotate their infrastructure.

Cryptocurrency Addresses

Insikt Group identified a set of cryptocurrency addresses connected to Rublevka Team operations. Approximately 160 unique strings resembling SOL addresses were extracted from the JavaScript drainer attached to the team’s malicious landing pages, and several others were obtained by tracing transactions within affiliate screenshots showing proof of their payouts on forums and the “[RublevkaTeam] Chat” Telegram channel. We focused on the following addresses for further analysis:

- EAsyxEjYKbDSVi6JbGYF1v9Jq1QyTSghRc8aqCeq7Ub3 (“Address A”, [Transaction History](#))
- EkaGjTVHDiRTYqSiup6TQs2QXfqSnEcrWN61dC8UVK21 (“Address B”, [Transaction History](#))
- CRnuwdpi3HGvFU5gGnvZAA9rV7AWe12v3sap8H3vXFY4 (“Address C”, [Transaction History](#))
- DD6vCVa4NEYRKA7K93rYZSKuY7REydFbqB3rog149ySx (“Address D”, [Transaction History](#))
- 8e8kiGgEMCxYYx2vuSf2iPo859QjE7ojkY6yGWDez9pW (“Address E”, [Transaction History](#))
- 4Ri6Rd7zN6M6H8jF3vPc6MqnmFioVcPaizZt3crLVGXd (“Address F”, [Transaction History](#))

Insikt Group identified seventeen references to the above addresses in the Recorded Future Platform, all of which involved posts from users on social media and Telegram stating that those addresses had stolen crypto assets from them, with the earliest post dated July 10, 2025. One such post specifically named *pumptoken[.]net* as the phishing website that had initiated the transaction; via further historical analysis, Insikt Group identified a JavaScript file linked to this website ([b9157f6bff6a6ee6ba5932ebac2c8796836b21eb3c69df08fbeb102e9228ba15](#)) that had a high degree of similarity with the drainer file analyzed above, including the same obfuscation technique and overlap in listed addresses. We assess that these users were likely victims of Rublevka Team.

OsaiThe3rd (🎮🎮) **MMT**
@Ragnarbjoarnivar

4Ri6Rd7zN6M6H8jF3vPc6MqnmFioVcPaizZt3crLVGXd

This is the wallet address of the guy that hacked my wallet

Like bro over 1.8m in your wallet but still taking our few hundreds

Cmon!!!

Wed Oct 22 2025 07:46:11 GMT-0400 (Eastern Daylight Time)



GIO
@giogio1483733

@cipher_elite My wallet just got drained. They took all my ISO20022 coin. Can you help me to recover them. Here is the address they have.

DD6vCVa4NEYRKA7K93rYZSKuY7REydfbqB3rog149ySx   

CRYPTO RECOVERY FIRM

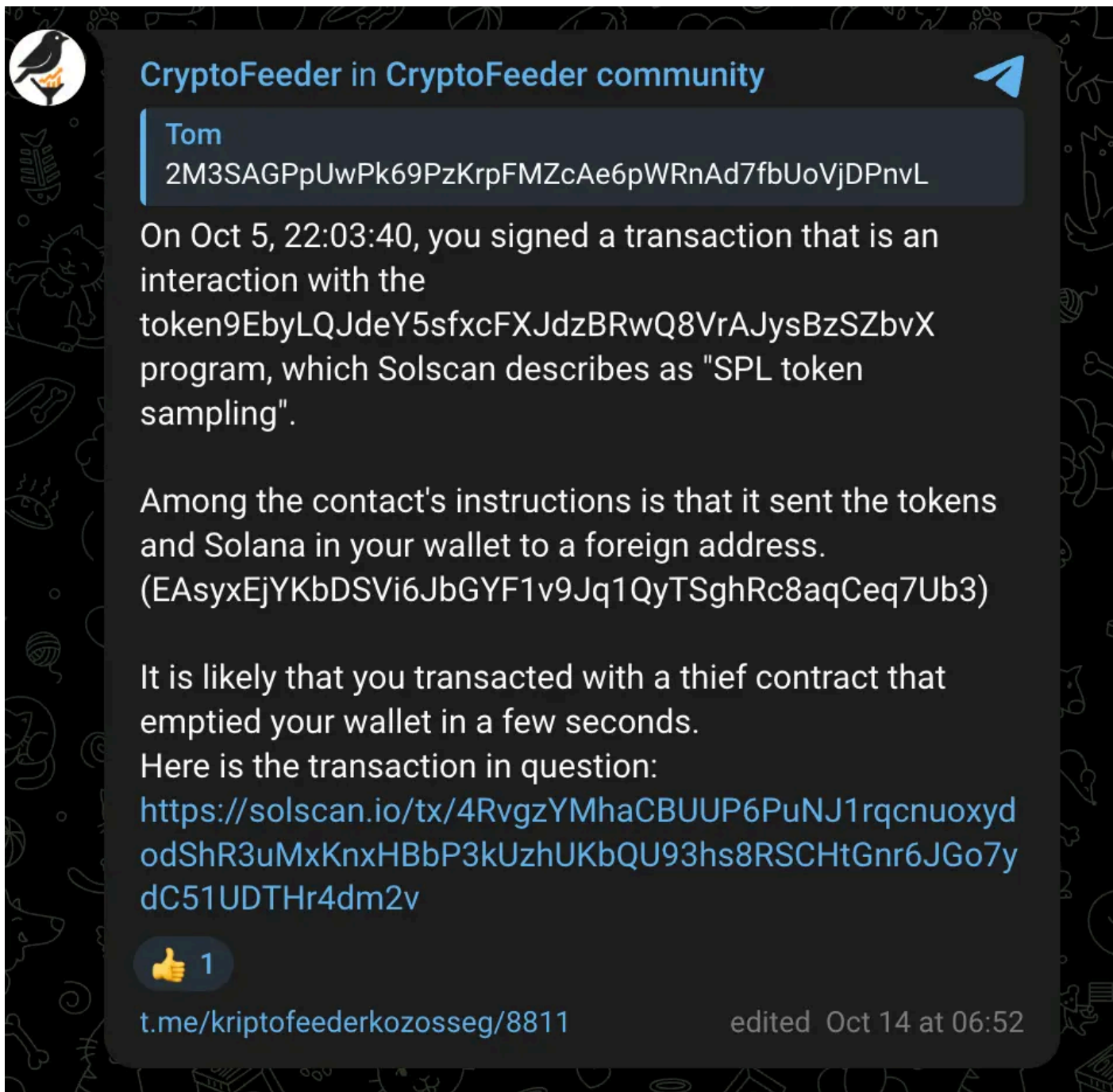
@cipher_elite

Securing your blockchain assets requires vigilance and best practices. Here are key tips to enhance blockchain security:

1. Use Strong, Unique Passwords: Create complex passwords with a mix of letters, numbers, and symbols. Avoid reusing passwords across platforms. Use a

Sun Jul 06 2025 17:40:52 GMT-0400 (Eastern Daylight Time)

Thu Jul 10 2025 15:46:49 GMT-0400 (Eastern Daylight Time)



Figures 25–27: Social media posts by users claiming that their crypto assets were routed to Address C and Address E
(Source: Recorded Future)

Both Address A and Address B were contained in the JavaScript drainer code as base64-encoded strings, indicating an attempt by the threat actor to further obfuscate these specific addresses, while all others were available in plaintext. Based on SOL blockchain data, Address A is listed as the “owner” for 31 of the identified addresses within the drainer JavaScript file, corresponding to its Associated Token Accounts (ATAs). As such, these ATAs are almost certainly used as part of the drainer logic. Additionally, the address appeared to be making a high number of conversions to wrapped SOL (wSOL), potentially to use on or swap to compatible blockchains. Insikt Group observed that in fall 2025, Address A followed a pattern of transferring large amounts in and out on the same day, with \$50,000 to \$80,000 moving through the wallet each day over a several-week period. On October 6, 2025, approximately \$1.2 million worth of assets were transferred in and out of the address. This pattern suggests that the wallet was likely used by Rublevka Team as a conduit for transferring and laundering stolen funds before cashing them out. Based on [SOL blockchain](#) data, the address first came into use in September 2025.

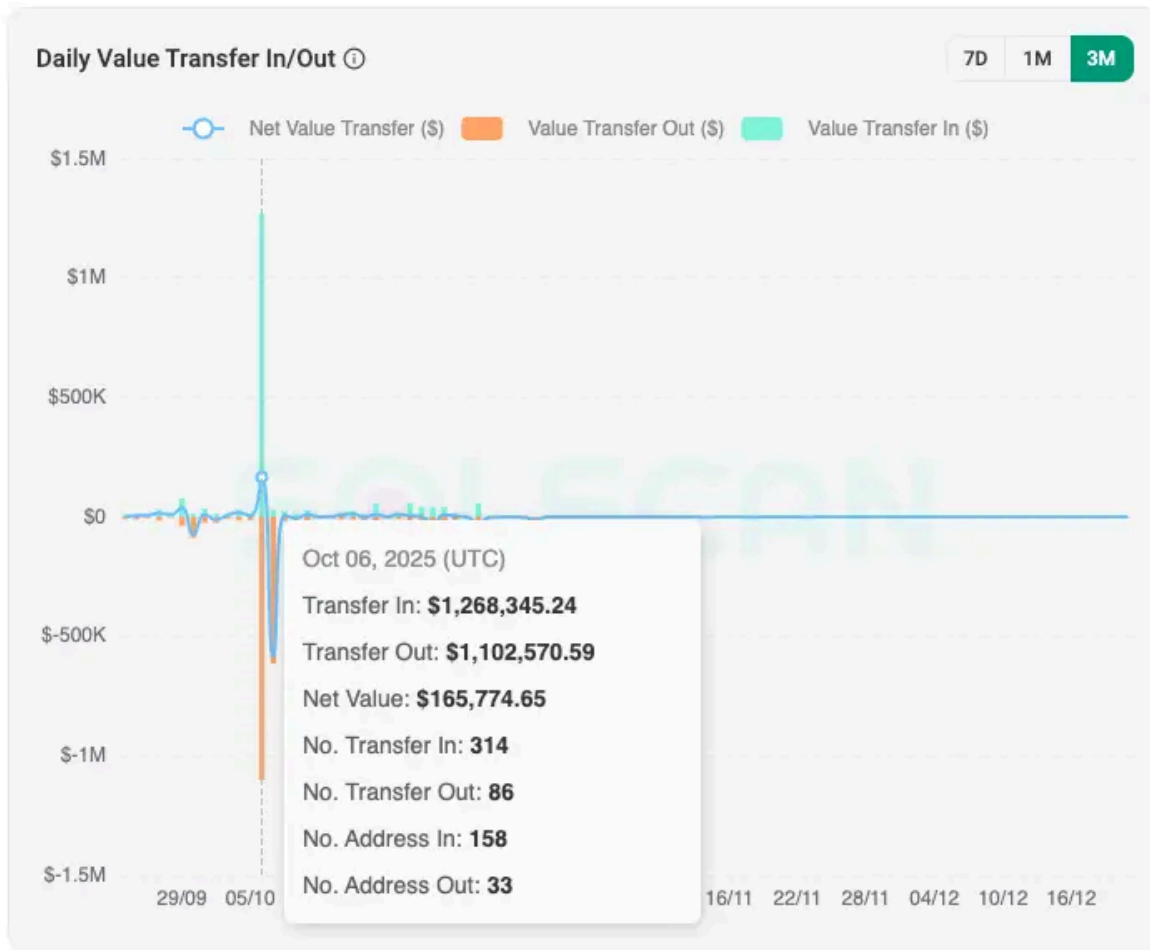


Figure 28: Analytics for transfers in and out of Address A, showing a transfer in of approximately \$1.2 million, and a transfer out of \$1.1 million on the same day (Source: solscan[.jio])



Figure 29: Analytics for transfers in and out of Address A, showing a series of same-day high-value transactions throughout October 2025 (Source: solscan[.]io)

Insikt Group also identified an account associated with Address A on *pump[.]fun*, a platform for users to launch their own meme coins. This account holds low balances in over 600 tokens and was first funded by a transaction from Fixed Float Exchange on September 22, 2025.

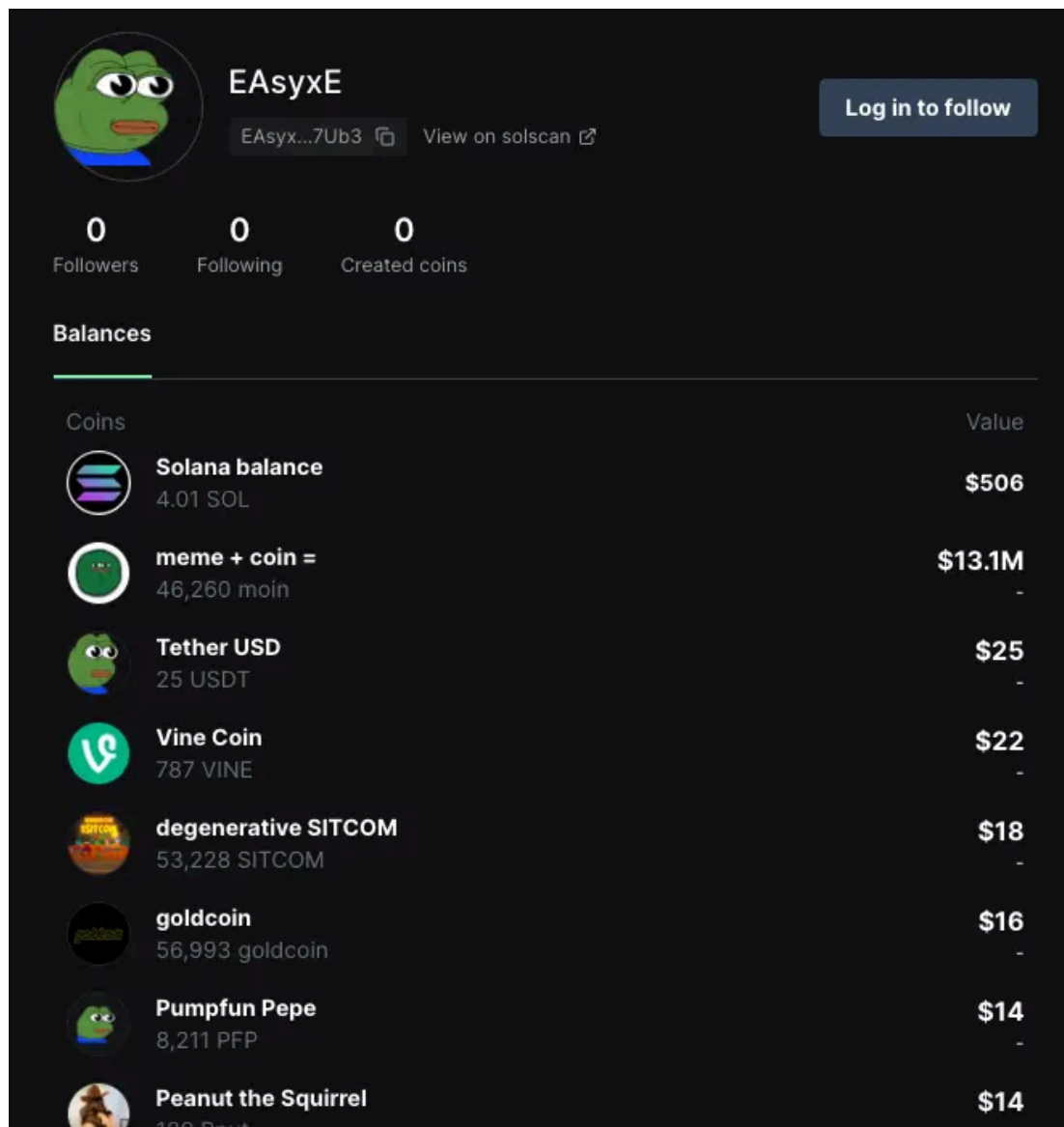


Figure 30: Profile on pump.fun associated with Address A (Source: pump.fun)

The account associated with Address B currently holds over 100 tokens and is associated with a high volume of token swap activity. Notably, Address B's first funder is Address C, which was mentioned in several social media posts as a malicious wallet between July and August 2025. It was also mentioned in a Reddit thread from August 2025, where users discussed having their funds stolen. One user stated that they were signing up for Axiom and connected their Phantom wallet to the service website, and once they authenticated the service took \$50 worth of SOL from their wallet and transferred it to Address C. Based on the wallet address and TTPs (using an Axiom-themed landing page and Phantom wallet), we assess that this individual was likely another victim of Rublevka Team.

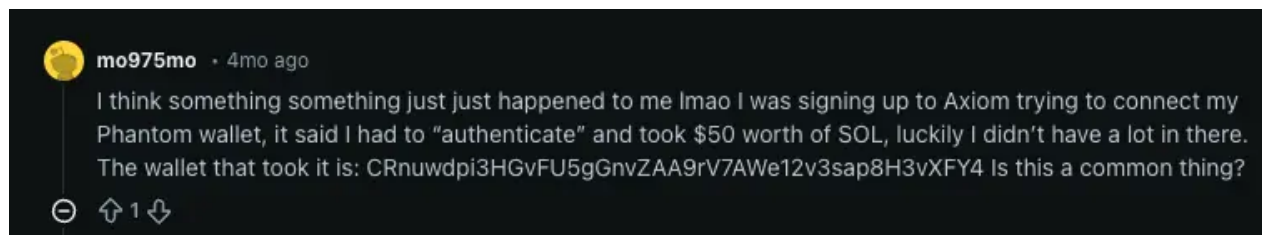


Figure 31: Reddit user stating that their funds were stolen when connecting to an Axiom service; these funds were transferred to Address C (Source: Reddit)

Insikt Group identified Addresses D and E in several affiliate reviews of Rublevka Team, namely in posts showing proof of funds disbursement to their personal wallets from those addresses. These addresses also appeared in screenshots of the [@]RublevkaTeam_bot “profits” notifications, posted by individual affiliates to the chat channel, many of which did not obfuscate the victim wallet ID, allowing Insikt Group to trace the transaction. Several of these transactions were made directly to Address D and E. Based on this, we assess that these are likely two of the “shared” Rublevka addresses used to collect stolen assets and then disburse affiliates’ cuts. We also note that Address E is the first funder of Address D.

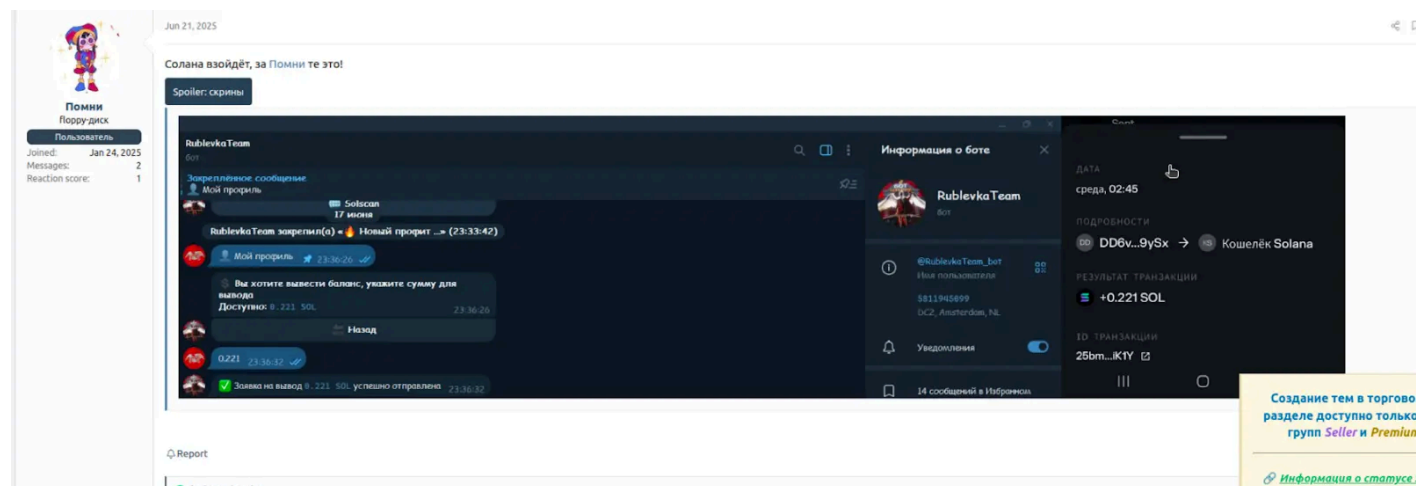


Figure 32: Exploit user posting a screenshot showing funds flowing from Address D to their personal wallet (Source: Recorded Future)

In addition to the above, Insikt Group identified 28 abuse reports for SOL addresses contained in the drainer file (including Addresses A to E) within other open sources, made between April and October 2025. Users reported a variety of scams in which these addresses drained their funds. These scams involved web pages shared on Telegram, social media, and crypto investment advice groups that prompted users to connect their wallets and sign transactions, resulting in the loss of all their funds. The TTPs and timeframe described in these reports match those associated with Rublevka Team, and we assess that these reports were highly likely made by Rublevka Team victims. Notably, in at least one report, users [reported](#) that in addition to their wallet funds being drained, they experienced a breach of their personal data and accounts; this may indicate that some Rublevka Team affiliates possibly conduct additional follow-on activity as part of their scams, such as credential theft. For a full list of the domains and malicious social media accounts listed in these reports, see **Appendix C**.

A complete list of SOL addresses extracted from the drainer script can be found in **Appendix D**; this section excludes addresses corresponding to SOL system programs and official token mints.

Outlook

Rublevka Team represents the maturation of cybercrime-as-a-service within the cryptocurrency threat landscape, signaling that sophisticated social engineering and scalable infrastructure now rival malware as the primary tool set for digital asset theft. As this affiliate-driven drainer ecosystem continues to expand, we expect similar models to proliferate across other blockchain ecosystems and decentralized platforms, particularly those with low transaction fees and fast settlement times, such as SOL. The low barrier to entry, combined with high financial incentives, will continue to attract a global pool of cybercriminals, accelerating the volume, complexity, and geographic diversity of crypto-targeted scams in the near term.

Looking ahead, brand impersonation campaigns tied to crypto drainers will become a strategic reputational risk for exchanges, Web3 platforms, and fintech providers. The effectiveness of these spoofing campaigns, especially those that mimic legitimate token airdrops or DeFi services, will continue to erode user trust in the broader crypto ecosystem.

As threat actors like Rublevka Team improve their social engineering tactics, abuse of RPC APIs, and cloaking techniques to bypass detection, more platforms will likely come under regulatory pressure to implement proactive monitoring, takedown partnerships, and user verification mechanisms to mitigate liability.

Appendix A: Indicators of Compromise

Domains:
open-sol[.]cc
sol-galaxy[.]cc
web-core[.]cc
sol-hook[.]org
efficient-endpoint[.]site
g-app-d[.]cc
fontmaxplugin[.]cc
commontechrepo[.]cc
burn-shard-bridge[.]xyz
pumptoken[.]net
emailsecure[.]tech

Email Addresses:
alex.petrov.domain[@]emailsecure[.]tech

IP Addresses:
158[.]94[.]208[.]165

File Hashes:
9c21d538c2a556f4a5b351b29f3513097ac57643f291ff6d751400d8dbc69489
b9157f6bff6a6ee6ba5932ebac2c8796836b21eb3c69df08fbefb102e9228ba15
fcf1bbac7dae24b6e0357bee6e8e184dfd193ddf8b341feaa9a3d83265af8f0a
ea8e780d0c292bfd1a3ee6bd9b8d77900a545bd3be3105891816c8f561eeb302
78bfb193ba291e17360126796ec9b93acdfec75867619fc50c5d45d7081009b6
93288b95db8cba2b8d3f38246be46e383990a9fcdd06bf26417a5935a8fe0a27
af5bed914f5406e7c1a3f30f91dfe34d81c5b06c571c59417fe4e2bde966325c

URLs:
hxxps://mainnet[.]helius-rpc[.]com/?api-key=
hxxps://mainnet[.]helius-rpc[.]com/?api-key=8e0e9a34-2648-421a-8f22-6460b4a68705
hxxps://mainnet[.]helius-rpc[.]com/?api-key=55065729-bda8-4cf8-87a1-7bd64cf22726
hxxps://mainnet[.]helius-rpc[.]com/?api-key=db25ae76-7277-45ce-b21a-5be1a61f2f04
hxxps://mainnet[.]helius-rpc[.]com/?api-key=44b7171f-7de7-4e68-9d08-eff1ef7529bd
hxxps://mainnet[.]helius-rpc[.]com/?api-key=bfd713ef-c9a7-404f-804c-e682c2bd0d3b
hxxps://mainnet[.]helius-rpc[.]com/?api-key=f30d6a96-5fa2-4318-b2da-0f6d1deb5c83
hxxps://mainnet[.]helius-rpc[.]com/?api-key=3b5315ac-170e-4e0e-a60e-4ff5b444fbcf
hxxps://rpc[.]walletconnect[.]org/v1/?
chainId=solana%3A5eykt4UsFv8P8NJdTREpY1vzqKqZKvdp&projectId=730eede4c040eafa7a928a503b6cd650
hxxps://solana-rpc[.]publicnode[.]com
hxxps://wallet-api[.]solflare[.]com

Appendix B: MITRE ATT&CK Techniques

Tactic: Technique	ATT&CK Code
Initial Access: Phishing	T1566
Defense Evasion: Obfuscated Files or Information	T1027

Tactic: Technique	ATT&CK Code
Command and Control: Application Layer Protocol: Web Protocols	T1071.001
Command and Control: Dynamic Resolution: Domain Generation Algorithms	T1568.002
Command and Control: Hide Infrastructure	T1665
Impact: Financial Theft	T1657

Appendix C: Domains Included in Scam Reports for Rublevka-Affiliated Cryptocurrency Addresses

Domains:

minordao[.]co
 token[.]pump-launch[.]fun
 events-dege[.]com
 soldrop[.]solvault[.]ws
 check[.]me-fnd[.]com
 vwa[.]lat
 luna-memex[.]com
 rugchecker[.]fun
 sol-chey[.]com
 pump-foundation[.]xyz
 claim[.]juplter[.]app

Social media channels:

t[.]me/crypto_arbitrage_signal
 t[.]me/solanadropper_bot/getrewardsol
 x[.]com/Alien2Solana

Appendix D: Unattributed Cryptocurrency Addresses Contained in Rublevka Team SOL

- 9DrvZvyWh1HuAoZxvYWMvkf2XCzryCpGgHqrMjyDwpmo
- FsTb6bdeomvCh7pJsd37Ay7moqGK7wvaihUPDWF3qyg
- FeeZVq5GGCMgM5z4nNVK9YB5s2aaAYoPmWtAaGQeYhT
- CuTbjikN9pCJdbH46oVuuQmgdGfDd33TG4x7ZK52uEnU
- Bj4p6uY4WJRLCH3Zk4Dp27UP2MgJ9JBpTH9ZJR1unCsD
- BF7HTg1J4joSvMwJuz7EUX2TJ3Z3SkrELJwov22ccfffb
- 5VM3FEDPAzazHFHGGCz5bSCd1paoxkdXM4kmxuXQxyDj
- 2d2Zbkrjrrk7X7VLqyg99yXbfy9BKBdYB2SRiUZ1mKsR
- 2c1vZ652u9whxguGxvyJ6HrFDkskcegcgpaMDUeQNoJK
- JCNCFXo5M5qwUPg2Utu1u6YWp3MbygxqBsBeXXJfrw
- FpZi3mRsewmMyJnsVFDXch4qNx5HNFhMnW2k2pMP2HAF
- Fp49M425pwahRPZ1RV89SWnw3qbwPpGHkbFDrVKiov3
- EwPCxMGGMnCoYnH4D3wu5wc1Lm9GGVwEjo39Cn6r8p1s
- EkYa2Tj2tKRptJ9RA5eBhchNh4UpwLurc41w1zXbL9Zh
- CMwrBsnX8HovgR64k3cbhmutBBbTHpMoASAUkZqtVJn1
- AKkWCmk4jpfY1mcRriGR48VqTZUG2MtdKK3wzXhVDxM3
- AEHejaxWe6wBzrU5Pa9KwQMxG7GyCDj7t1vHwbuWB266
- 9PVZ8Cahy156mTYB3g6Be4S17F9vKEGy4ekkaieiGtwa
- 9gt2gxSrrZmP9nBPYdAgViEt9mD6cayuDQCdCYMCzm
- 9BB6NFECjBCtnNLFko2FqVQBq8HHM13kCyYcdQbqump
- 7FPu8A89YTzvm8ZnhzsHFGCoCDg28XYKGANPUSLe7iixj
- 6p6xgHyF7AeE6TZkSmFsko444wqoP15icUSqi2jfgiPN
- 6G3SCdRnCBPuGBpFEZiRABpjoXorS3dqAHGY5NPCtcaj
- 6FN58cdsazwFA5r8EXzMjVoV6rBFXZjhDVMbm7rS93NE
- 5UUH9RTDiSpq6HKS6bp4NdU9PNJpXRxiw6ShBTBhgH2
- 4tyVZQJc2NUMjZs5pJi5Zyz2pi4uTJmxge1mrxt9KQxV
- 27G8MtK7VtTcCHKpASjSDdkwWYfoqT6ggEuKidVJidD4
- ZBCNpuD7YMXzTHB2fhGkGi78MNSHGLRXUhRwNRM9RU
- WLFInEv6ypjkczcS83FzQfPgFZYwQXutRbxGe7oC16g
- UPTx1d24aBWuRgwxVnFmX4gNraj3QGfZL3QBgxtWQG
- rndrizKT3MK1iimdxRdWabcF7Zg7AR5T4nud4EkHBoF
- pumpCmXqMfrsAKQ5r49WcJnRayYRqmXz6ae8H7H9Dfn
- MEFNBXixkEbait3xn9bkm8WsJzXtVsaJEn4c8Sam21u
- J3NKxxXZcnNiMjKw9hY2K4LUxgwB6t1FtPtQVsv3KFr
- J1toso1uCK3RLmJorTtrVwY9HJ7X8V9yYac6Y7kGCPn
- HzwqBKZw8HxMN6bF2yFZNRht3c2iXXzpKcFu7uBEDKtr
- HZ1JovNiVvGrGNiiYvEozEVgZ58xaU3RKwX8eACQBct3
- H1dJF68xpDXfawz2snUjw4Y3GnN3dgyfmzkhaUSbhra
- GNVjeQPrCUu679o1x7DBciGyeKVJPScze9QgiXMa863A
- FeNABkgsWfyuvYBxMMi7BfK1ezDq6rJXZer4d49JF7TU
- DvjbEsdca43oQcw2h3HW1CT7N3x5vRcr3QrvTUHNxvgV
- CB9dDufT3ZuQXqqSfa1c5KY935TEreyBw9XJXxHKpump
- BLZEEuZUBVqFhj8adccFPJvPVCiCyVmh3hkJMrU8KuJA
- B89Hd5Juz7JP2dxcZXfJWk4tMTcbw7feDhuWGb3kq5qE
- 8xJiLn7RnWpUGA6vsAjhNiGaixiJfEQFbeXHA3eEDP6
- 8Rcpbksb5GE6BJpYL5juzSZJhwiP8HVYQa2tqAEmwhkM
- 8a5o2DiD5dGxE93374Ft5hVM3Q87faBgtCrrqqv3j6Aj
- 7wtvexodFHEXEQLuQWdi6tBtAyQRkwZ2DYX2hLeraarg
- 7kixES9AGA9jzFtmdYXDwwkFywhsFuF7jjhig9FVWxGr
- 7atgF8KQo4wJrD5ATGX7t1V2zVvykPJbFNeVf1icFv1
- 6AJcP7wuLwmRYLBNbi825wgguaPswZPBEHCHndpRump
- 3TTKJZbaBHCQAWEUqP9CE7RsTeFjbdfe2MjrKrxPiq2Q
- 3NZ9JMVBMGAQocybic2c7LQCJScmgsAZ6vQqTDzcqmJh
- 2zMmhcvQEXDtdE6vsFS7S7D5oUodfJHE8vd1gnBouaUV
- 25hAyBQfoDhfw9ay6rarbgvWgWdDnqcHsXS3jQ3mTDJ
- nEeteqhnXLNVbnkQfPsg1xCLqKBGnm86Nf7e2hu8K2i
- JDudMa32AMG7qNrMJBEEVSPu59TPpp5fZoxMM8JbUL1
- J8TwdioMgeDvnjcsT19dDA5H9D4nhZsLLHpzbmuQoyiC
- HvPWgZobdKrgCkAKFZeKygKHDnJy7eK56CKqWzpxYfy9
- 8VHDwr45BNnyMpMvfGFZwvoUXU4ZPQk4Yfj6b5V2Duzd
- 8tzYaoRju2KwLqYD1LSrcvAEfXJQi7f6aw1aYb9MUqew
- 8tr7rgDnLv2ZpqcGGRM5QuNBGkPnu3PRWBmNBVFPPoa1
- 8SZRBhepUNSoPn3FaTWiHzzv51XDFK84hN6kHDL1MbPr
- 8sJamT7N8oaPHvdWfse4YwS7Tf9DxMu3WnjZCrpJ3Yfw
- 8rFSGrUJUNr7zt65Kc4rTDnroLRhyXuaaESmLu2Pf6R8
- 8pFhUqCU7FkxfG2DLytrDF7a9oK4XGtN92PrYwtVQc6G
- 8K2Nvr695p77cfPGsMvbyz3fhkzvwXo6XcMZPsV42vir
- 89LjSs8wP3EZNCkcs8aCxnGQaEuyhUYGE4STkFwNgRT3
- 7zND8YAtCYehNoa1JrFDLQZi44xJkEuPWK5b4CkiuFpo
- 7XX64f8UKE1nxNCswncCUj3c2FJYdXhMDV5xd5DRdFky
- 7VHUfJHWu2CuExkJcJrzhQPJ2oygUpTWkL2A2For4BmE
- 7oMjvD5MwttpfwA5mDx9aV7aLE8GkMCYeELxqckXKX3n
- 7mhcgF1DVsj5iv4CxZDgp51H6MBBwqamsH1KnqXhSRc5
- 7dF8SFvjBgfEvMkK6uRBkdRXbop4GxbutyAhCqa3JSUn
- 7cAui6ADtxLnpRr2wYvwJWtkzwgmVF2LYKnjKTLx4xR8
- 7AN6avKCJPMkXkx8kPwMuHmaWvJehH69e8rKpLf9rdfk
- 7AB9DJVwmhjuXsa59sxZseiQyWyHobkykEgy7drd1Gx
- 7A4XK9TQrX1YruPZ6B4Qiy1itEWmgXADKES56ud9ESW
- 6tQPS58X6fdEDdtxuTKQRRqakYcVMuhyVj77YhgPF3ro2
- 6TpuRiQ7KEwQt9A4PchnWD5dHGU2FjXRP2ZJZkzFaiQu
- 6sga1yRARGQRqa8Darhm54EBromEpV3z8iDAvMTVYXB3
- 6LY1JzAFVZsP2a2xKrtU6znQMq5h4i7tocWdgrkZzkzF
- 6g3aqiR59BzWLkdpweVyxVDicPoJFsX1k4DquFZR3GZ5
- 6CUV3vQ8wfAvz1ogmT7Wp7mSKReECFxuLakm9nQrS4EK
- 61aq585V8cR2sZBeawJft2NPqmN7zDi1sWS4KLs5xHXV
- 5WumPYv4jDPRQWjW3EeybLczpcohHrMPShK9WQ85qfY
- 5rhms6jZQaXnQc6wbicnrxDTkKqKi4iWfWW3612r5rHb
- 5Q544fKrFoe6tsEbD7S8EmxGTJYAKtTVhAw5Q5pge4j1
- 5N56aAcpKrdJovtw8QCLLfz7v67q2yV6k23ex5iS4PMz
- 5LZkATrLwHYCQj2YuVbjjgsDZzBk6YfL4pFQRJmtboT2
- 5hpfC9VBxVcoW9opCnM2PqR6YWRLBzrBpabJTznwNiw
- 5FeTzLNqwrsvSzezFujeV62a2v4kmQURBnQjJANStMXj
- 5E2d6Z5FRE4584RTmJpyjg8yRtHG1YeorKbFSA1BpkPq
- 584apKZB85789eCoB5Krr1cdUbfTGn8ES1WjGKgCHQRVU
- 5550NTKdRECgyLn8fBvySoN6hXMCszFq1Y4oea9p3ZFB
- 4yCsNPifcJYT7BQWFzYyrSCCzWxo56Qr2c4MugLEmpjj
- 4tkNAaqmfSVaAuCKbxuxoVFXfu2fZu5o9jx8j6AdCjfg2
- 4QtCFWoMcMrxfGcfa3HfHU8TqZrJWGBmFaftyS5DvaMC
- 4pBDBu1K3Zsx9FAX39j3dXfKkJESosqVUSPV9tAUmmNxj
- 4hKiMS1gCybw2RnHiuwSb8fcdJM63bDunaJkw1uETBkj
- 4aE6ow1YNDm9MRNdK8HRZFFzvs9FXBgEttWSMrH6hupD
- 43PyQ5EEv45Z8s7KECsD6w1peA8svzKYWH2VeNpByUdr
- 3Zaz6vATY8br9WceXWD1Xa7fCyCpKSnanWFDRTejjPqb
- 3tfdiewFQC1zsp97VF5kQyuw5a38rYzkioBLhyzSCRCL
- 3nECyn3B2TL5BQLBZJU7V1t3ddqVZUio76oBCTNFWvhJ
- 38BcC22ZSXxjqBmjA36fCe6BQRxn1k8HHcpz6EKdWUH
- 31rYartQwHeBMjAe2MgGpffGV57fQY3kug4BDN8tLGqQ
- 2THWjMryk7FzaCiJv1M66gaYfPDw6vf93KmVtd5XwxZj
- 2znNjDgrRwkkSyhyUCMD1n76deGz5m4fvF6MztzqPFq1
- 2nrDrMP9ZVqsmu5hmaqk3e612YoCmKHCPsm1bMsbvU8E
- 2LoNg8b8wYneseTQ4FYEVQxSJWp12tsLE799oUDYPDHB
- 2F5bzLu6mNwzNpwwgQNVuNF2QcmobtLswtRxaf39N9uUd
- 26ddLrQXDext6caX1gRxAREPN4kzajyGiAUz9JmzmTGQ
- 23KfDBTdpabQfn8aUeoEDgFGJ5368gpnYGFnkKCECqM

- HQBDTnf2gMkPbn7Q1LcmigKBuQScquR1mnQpKgbCzAaa
- HKzK6FwPQXGGow2TNZJxr6dXxo5opBgYKvw3GRYan6c8
- Hhdix4PLJmHzUFN4aJrUjYcJvx7N8LnMWJUGR6Q7AxXp
- HF9X8puGwFMN5qdfx4qbiz9RwtktTXNR9AS4ctgswkeY
- He79tJD1EW7cGC4xFpB2ugVQ5pRgBS4xk8PM4L9QUTSh
- H21vVC1WthyNwsrbXq4yokGZufyL1GhMR1tNjNs79cqr
- GRGmgWor2PX3sNkoA5wZuNBBYoCnZPoiAufAvvG3WDEi
- GgYLqrHteZTnFdG5sEUhZfmPUBXEvH6W1guVKo7mLKJJ
- GcEXZEUhbk4KyFV7B7q28Zh7PKzGsC3oqgjvGRLaZJZu
- GafNuUXj9rxGLn4y79dPu6MHSuPWeJR6UtTWuexpGh3U
- FP8dLEpT5Pr2FLjGzJ99cnECHtN6qFYX18gFqSn8MiKR
- FJUszQzUsLMBd2T6H7iL3y5N3Vp2ztKUKTKcCvnJTXie
- FJhg2bE1PZEedxpqpXZpJKCfF2m9Z6n9MtLSe2zNo4XY
- FDZ6ocTQnX3HHuf9bxgUAgQWiefcy9PG1jSoGXWvGASr
- Fd6wohshhx61RtYCSMfRBB6qRjsTQtcdNU8PKHxX7CL6
- FbcYcJVccCdNzq5CdMrwzUfsJD3duf4yitRcJAubQgvz
- F5o3MLS12oCcZ7u8pwzSDVXxMMUtqDoFar6DQNYEnSiU
- EXSTAHhnYebGtnSeioFmUCi6NyKE7RMcXJF5sGaXe9ca
- ETrTi8Xhng2wGTUPxYUPTxq6taJh34ejoZTEM27h9Qmd
- ErJLDKQy1Jna9m1LpbLJEXGiEc6yDFxkBu1mXAEZea5o
- ERCSpGu567Bd6r6i2CT3u2uNauAkPzHaprcn6NCqWpP
- EntJvjbs3bZqMCJXXGH7FauSHWwH8hrUwBdSafqXUAKe
- EKpQGSJtjMFqKZ9KQanSqYXRcF8fBopzLHYxdM65zcjm
- EAsyxEjYKbDSVi6JbGYF1v9Jq1QyTSghRc8aqCeq7Ub3
- E3iDU6nhniKiaAp8WUfu2181UNYDnoYGGqodWE9HbJN7
- Dz9mQ9NzkBcCsuGPFJ3r1bS4wgqKMHBPIvuniW8Mbonk
- DNyd87a6uL61EpTXNS1zKwmZXxpRvP6oYfBEaiQk3oc
- DmKR61BQk5zJTNCK9rrt8fM8HrDH6DSdE3Rt7sXKoAKb
- DGB4xJ2FDUJmZkUr8uMsnqCCY9uWXAaf8TPfwtNXGn37
- D7gyNb1vVQaeeXcgyPHYMvrnRRyxxtRJYGQFqtBko5yo
- CVFLDY7oaToBr8vVHaYQvfEcTDSuZF9k9WxoVDH5Rvre
- CtNY5YS7ieorQake2kmt5sTJmveKbXTWF33Zsz11Ugq
- CSSJFgoeqidqVtHKSnp7i7s6WX8APHfH2kyGdLV195Jb
- CQWUdThEbNMjcoEjGyCMTGXHpKvW1aB8JF31hKa1FQQN
- CGD7B6q729P6BS1r8CwskpaKarP95q5EUXxFgukFoicK
- Cg3z44Jnr4KNGf8Cs6p7XXiSR8LAELr4mcCdkqQ4Zbkv
- Cfq1ts1iFr1eUWWBm8eFxUzm5R3YA3UvMZznwiShbgZt
- Cbx5qRLx8CgJ43e4UuaMpHEV34Vh6CA2hva66J2fC5U3
- CBEADkb8TZXHjVE3zwad4L995GZE7rJcacJ7asebkVG
- C4q2QdKe6C6Nhkc2Kk9JNca7L8CxpGBipVzjcDJwB3cH
- C1kvEAHXrDCv6FwcNn3iwyUJqAeXxWrKzm5NXSppBdL
- BwnzGfpDTBDzWAwWmPjZjcgXXFZmzgjlhEhNFWGkb8Nj
- AzcBxq9NMovXBfvXcuc1Df3vrSwLAa2ZiMstsvSA91jn
- AZB72txkm2Ky2TramPF5FaiBtP13drQ2PFjbUum2qAdC
- AyzyikXL9kKs2cwyHswLEe22aRYAvhbWwFn9TKrgmMx
- AUaG3qcYzTNRRCsxDUWyvqdz4AP3cF1yiNLm4f2fnhpt
- ArcckXWCZ8vaUY9DQNiuii51YZHnt8UMmoLCJKKbiL8E
- AoTXgHCVTxCxb3NcF6bmNANBv9p2pa6eDPCXU8VPKUdY
- AHwhic8fhWwMRPGUCPfT2oUdNNAQjLFfNX4u6vr8Dxq
- abvgNpWrqMPsZ8yequUm2795boKrZ6yj7g5w7wih3Ag
- 9SLPTL41SPsYkgdsMzdfJsxymEANKr5bYoBsQzJyKpKS
- 9R9u9dEDngmaHRGUVUqtG6pUFuqnQ9no4gCx8vocY8q4
- 9nFJQ79FNKYvY7c7d9ULeeQLoFjHsBLV4bQLMYMqRmC
- 9J4kxVHDYPJ1ymaHuQkvQurziLARKpVMmmBeFHSaa4Ja
- 9BSY53N64xgbocqA6j2mwx3WwEGenW1xQqkcTfNqaPN2