



| Flash |

Comprehensive Ponzi Scheme Platform Advertised for Sale

F-2025-05-28a

Classification: TLP:CLEAR

Criticality: LOW

Intelligence Requirements: Deep and Dark Web, Fraud, Social Engineering

May 28, 2025

Scope Note

ZeroFox Intelligence is derived from a variety of sources, including—but not limited to—curated open-source accesses, vetted social media, proprietary data sources, and direct access to threat actors and groups through covert communication channels. Information relied upon to complete any report cannot always be independently verified. As such, ZeroFox applies rigorous analytic standards and tradecraft in accordance with best practices and includes caveat language and source citations to clearly identify the veracity of our Intelligence reporting and substantiate our assessments and recommendations. All sources used in this particular Intelligence product were **identified prior to 9:00 AM (EDT) on May 28, 2025**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

| Flash | Comprehensive Ponzi Scheme Platform Advertised for Sale

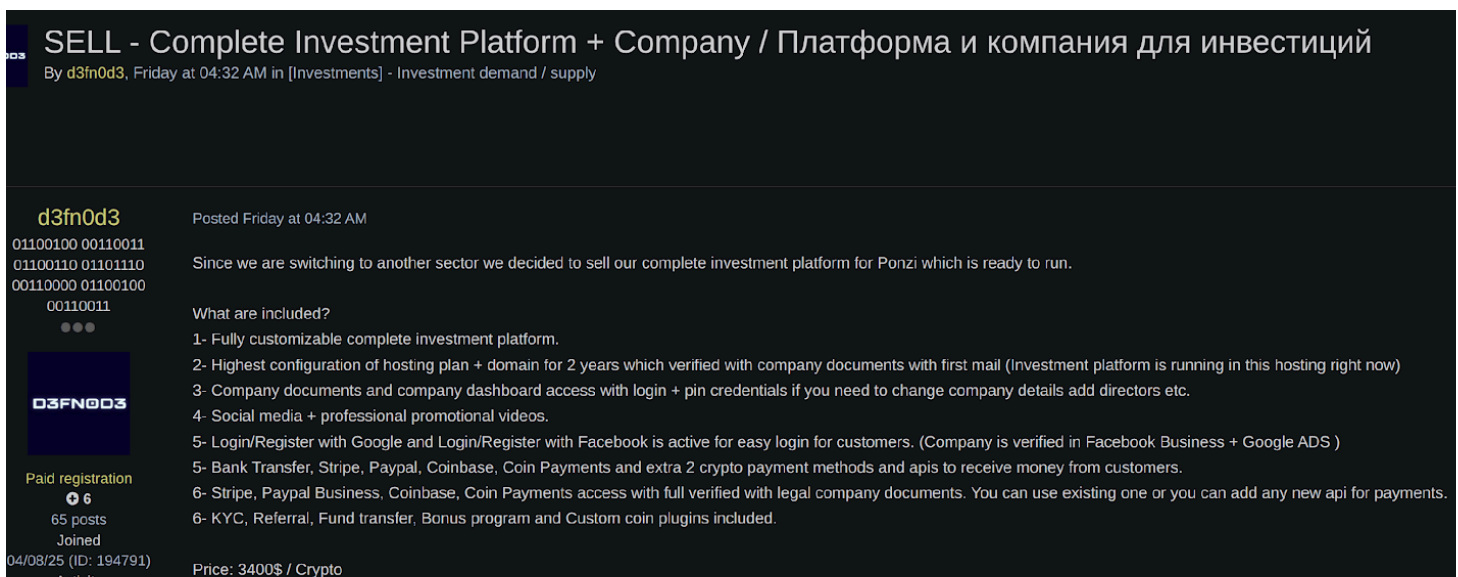
| Key Findings

- On May 23, 2025, an actor using the alias “d3fn0d3” posted on the predominantly Russian-speaking deep and dark web (DDW) forum Exploit advertising the sale of a “complete investment platform” designed to facilitate a Ponzi scheme.
- According to the advertisement, the investment platform includes features and services such as access to a dashboard feature, verified logins for numerous payment platforms, and established know-your-customer (KYC) protocols.
- Although scam-related services are very common in DDW marketplaces and forums, ZeroFox has rarely observed the sale of comprehensive platforms such as the one allegedly advertised by d3fn0d3.
- D3fn0d3’s advertisement is unlikely to reflect a new trend, with a more likely chance that the actor is seeking to recuperate funds from an already established platform they no longer wish to operate.
- While ZeroFox cannot currently ascertain the threat posed by this platform, it is almost certainly heavily dependent upon its post-purchase management.

Details

On May 23, 2025, the actor d3fn0d3 posted on the predominantly Russian-speaking DDW forum Exploit advertising the sale of a “complete investment platform” designed to facilitate a Ponzi scheme. According to the post, the platform can be purchased for USD 3,400 and is ready to become operational.

- A Ponzi scheme is a type of investment fraud whereby victims are encouraged to invest in a seemingly appealing fabricated or exaggerated business model promising low risk and high returns. However, rather than investing the funds as promised, scammers often use them to pay previous investors under the guise of dividends, while also paying themselves. The scheme can continue until the threat actors can no longer attract new investors, upon which the majority of the existing investors lose their money.



SELL - Complete Investment Platform + Company / Платформа и компания для инвестиций
By d3fn0d3, Friday at 04:32 AM in [Investments] - Investment demand / supply

d3fn0d3
01100100 00110011
01100110 01101110
00110000 01100100
00110011
● ● ●

Posted Friday at 04:32 AM

Since we are switching to another sector we decided to sell our complete investment platform for Ponzi which is ready to run.

What are included?

- 1- Fully customizable complete investment platform.
- 2- Highest configuration of hosting plan + domain for 2 years which verified with company documents with first mail (Investment platform is running in this hosting right now)
- 3- Company documents and company dashboard access with login + pin credentials if you need to change company details add directors etc.
- 4- Social media + professional promotional videos.
- 5- Login/Register with Google and Login/Register with Facebook is active for easy login for customers. (Company is verified in Facebook Business + Google ADS)
- 5- Bank Transfer, Stripe, Paypal, Coinbase, Coin Payments and extra 2 crypto payment methods and apis to receive money from customers.
- 6- Stripe, Paypal Business, Coinbase, Coin Payments access with full verified with legal company documents. You can use existing one or you can add any new api for payments.
- 6- KYC, Referral, Fund transfer, Bonus program and Custom coin plugins included.

Paid registration
6
65 posts
Joined
04/08/25 (ID: 194791)
Activity

Price: 3400\$ / Crypto

d3fn0d3's Exploit post on May 23, 2025

Source: ZeroFox Intelligence

Since joining Exploit on April 8, 2025, d3fn0d3 has established a positive reputation in the forum. ZeroFox observed at least 65 previous posts associated with the actor, the majority of which were related to various types of scamming and social engineering activity. D3fn0d3 is heavily active within two predominantly Turkish-speaking cybercrime

forums, [hacktiviz\[.\]org](https://hacktiviz[.]org) and [spyhackerz\[.\]org](https://spyhackerz[.]org). This, along with Turkey-related posts, indicates d3fn0d3 is likely located in Turkey.

According to the advertisement, the investment platform includes the following features and services:

- A fully customizable, complete investment platform.
- “Highest configuration” of domain hosting plan available for at least two years. D3fn0d3 provided no further detail, but this very likely refers to dedicated hosting, whereby the buyer can exercise a high degree of control over associated servers.
- Access to a dashboard feature, which is likely intended to mimic a legitimate environment whereby investors can manage their portfolios and view investment opportunities. This dashboard is almost certainly intended to increase perceived legitimacy.
- Social media and “professional” promotional videos. No examples of these were provided in the advertisement, though they are likely intended for advertisement purposes.
- Logins for both Google Ads and Facebook Business, likely indicating that d3fn0d3 has already completed the process of providing verification information such as business name and website URL, government-issued identification, and various aspects of company policy.
- “Easy login” procedures for victims, likely referring to Google and Facebook logins that are intended to increase perceived legitimacy and security.
- Verified logins for numerous payment platforms, including Coinbase, Coin Payments, Stripe, and Paypal Business, as well as two other unspecified cryptocurrency services. These are likely intended as a means by which to receive payment from victims, as well as provide payment to existing investors. The platforms also allegedly facilitate customized application programming interfaces (APIs).
- Other additions such as unspecified KYC security protocols and “referrals”—likely alluding to financial incentives available for victims referring new investors.

Although scam-related services are very common in DDW marketplaces and forums, ZeroFox has rarely observed the sale of comprehensive platforms such as the one advertised by d3fn0d3. The advertised price of USD 3,400 is unusually low—particularly if

the service sold is as described by d3fn0d3, inclusive of all the alleged features (many of which likely required significant effort to establish). However, d3fn0d3 claimed in the post that the reason for selling the product is that they are “changing sectors”, reflecting a likely chance that they seek a quick sale.

As of the writing of this report, d3fn0d3’s post has received several positive comments from other actors within Exploit, though the majority are discussing general advice for conducting scamming activity rather than an imminent purchase. However, the platform is very likely to appeal to some financially motivated actors—particularly those familiar with conducting Ponzi schemes and those willing to invest time in managing, growing, and advertising the platform. Due to the limited detail provided by d3fn0d3, ZeroFox cannot ascertain the threat posed by the platform, though it is almost certainly heavily dependent upon its post-purchase management.

| Recommendations

- Be wary of any entity offering guaranteed financial returns—particularly with no or minimal risk or if pressured to invest within a limited timeframe.
- Examine investment platforms thoroughly, and exercise increased caution if the entity structure, personnel, or strategy appear opaque.
- Exercise caution if a platform offers to invest money on your behalf, without providing transparency as to where it will go or how it will be managed.
- Be aware that scammers leveraging Ponzi schemes will often seek to confuse a victim by using convoluted terminology and conveying difficult procedures for withdrawing funds.
- Take time to examine online reviews associated with the organization, including commentary on its social media accounts.
- Be aware that financial scams such as Ponzi and Pyramid schemes will often place great emphasis on recruitment and referrals in order to generate new funds and stay afloat.
- Check that an organization is registered with an authoritative body, such as the Financial Conduct Authority (FCA) in the United Kingdom or the Securities and Exchange Commission (SEC) in the United States. While their registration does not guarantee legitimate trading practices, it reflects a lower risk of malicious activity.

Appendix A: Traffic Light Protocol for Information Dissemination

WHEN SHOULD IT BE USED?

Red

Sources may use

TLP:RED when information cannot be effectively acted upon by additional parties and could lead to impacts on a party's privacy, reputation, or operations if misused.

Amber

Sources may use

TLP:AMBER when information requires support to be effectively acted upon but carries risks to privacy, reputation, or operations if shared outside of the organizations involved.

HOW MAY IT BE SHARED?

Recipients may NOT share

TLP:RED with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.

Recipients may ONLY share

TLP:AMBER information with members of their own organization and its clients, but only on a need-to-know basis to protect their organization and its clients and prevent further harm.

Note that

TLP:AMBER+STRICT restricts sharing to the organization only.

Green

WHEN SHOULD IT BE USED?

Sources may use

TLP:GREEN when information is useful for the awareness of all participating organizations, as well as with peers within the broader community or sector.

Clear

Sources may use

TLP:CLEAR when information carries minimal or no risk of misuse in accordance with applicable rules and procedures for public release.

HOW MAY IT BE SHARED?

Recipients may share

TLP:GREEN information with peers and partner organizations within their sector or community but not via publicly accessible channels.

Recipients may share

TLP:CLEAR information without restriction, subject to copyright controls.

| Appendix B: ZeroFox Intelligence Probability Scale

All ZeroFox intelligence products leverage probabilistic assessment language in analytic judgments. Qualitative statements used in these judgments refer to associated probability ranges, which state the likelihood of occurrence of an event or development. Ranges are used to avoid a false impression of accuracy. This scale is a standard that aligns with how readers should interpret such terms.

Almost No Chance	Very Unlikely	Unlikely	Roughly Even Chance	Likely	Very Likely	Almost Certain
1-5%	5-20%	20-45%	45-55%	55-80%	80-95%	95-99%