

Drainers as a Service: A Case Study of Medusa and Its Ties to a Broader Ecosystem



What Are Drainers?



A **drainer (also referred to as a Puller)** is a type of malicious tool in the Web3 ecosystem designed to covertly obtain wallet permissions from users — often through social engineering or misleading interfaces. Once granted approval, the drainer enables unauthorized transfers of cryptocurrency from a victim's wallet without further consent. While the mechanics may vary, the underlying goal remains the same: **exploiting wallet approval mechanisms to siphon funds.**

Common Disguises Used in Drainer-Based Attacks Include:

- **Fake Airdrops;**
- **Free NFT Minting Campaigns;**
- **Gasless Token Contracts** (tricking users into approving without realizing the risks).

These scams are often straightforward to execute and highly profitable. Unlike traditional phishing campaigns that seek access to email or login credentials, drainers target direct monetary assets in the form of digital currencies. Once the assets are extracted, perpetrators must obscure the source and ownership of the stolen funds. This laundering process typically involves:

- **Mixers** (e.g., Tornado Cash)
- **Decentralized Exchanges (DEXes)**
- **DeFi Lending/Borrowing Protocols**
- **Gambling Platforms**
- **Bridges to Other Blockchains** (e.g., Solana)

By 2023, DeFi platforms had become the most commonly used laundering channels due to their ease of use, liquidity, and lack of strict KYC requirements.

01 Reduced Risk Exposure:

Developers avoid direct interaction with victims, minimizing the risk of identification or operational errors.

02 Consistent Revenue Streams:

Even if a client fails to profit from fraudulent activities, developers earn from initial access fees, subscriptions, and a percentage of stolen funds.

03 Scalability:

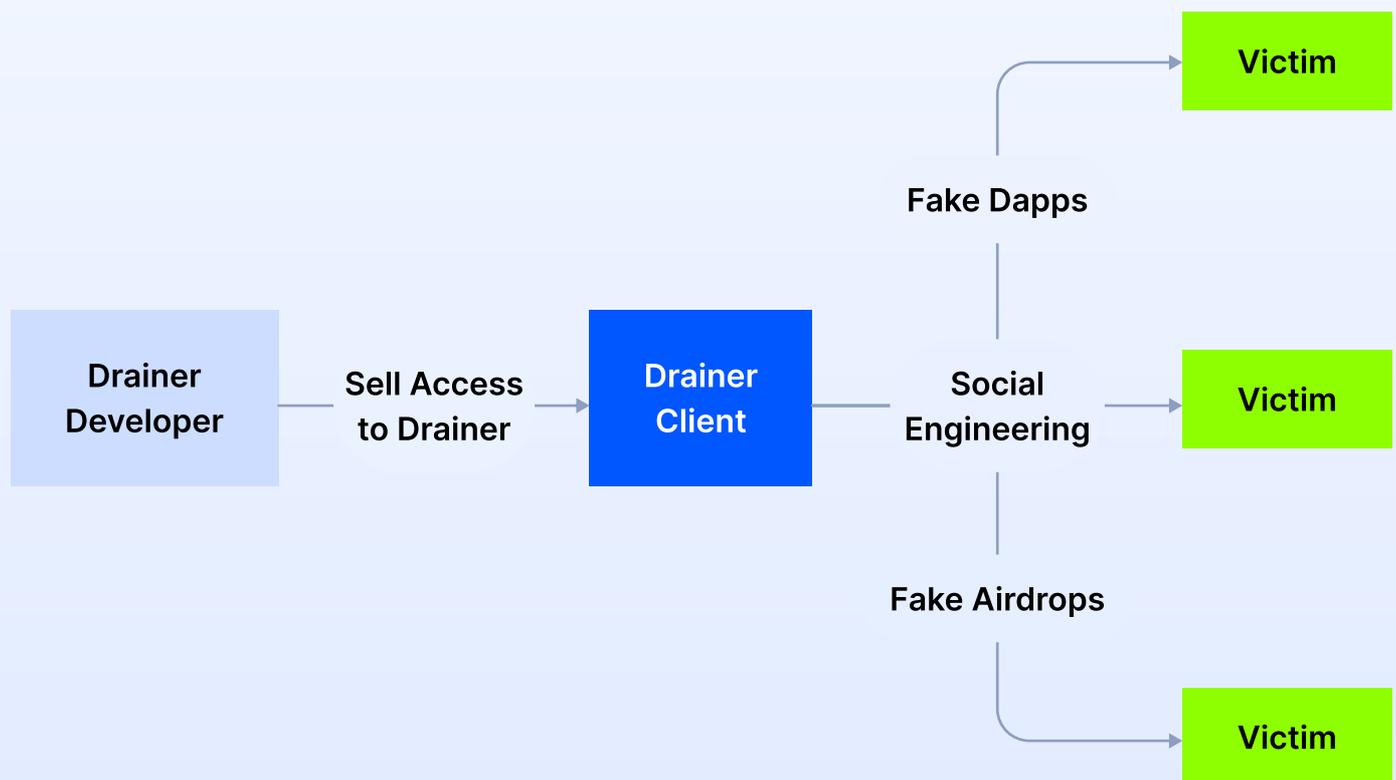
The DaaS model lowers the barrier to entry for fraudsters, eliminating the need for programming expertise and enabling the market to expand rapidly.

How Drainers Operate and Reach Clients

- **Telegram Groups**
- **Discord Servers**
- **ClearNet and DarkNet Forums**

Evolution of Drainers: The Rise of DaaS (Drainer as a Service)

The broader drainer ecosystem has evolved significantly, with many operators, including Medusa Drainer, adopting the Drainer-as-a-Service (DaaS) business model.



In this model, developers provide access to their drainer infrastructure — including control panels, operational proxies, and accounts on major platforms — for a one-time fee or subscription. This shift offers several advantages to developers:

These channels foster public and private communities where scammers can access necessary resources, such as: domain name rentals for cryptocurrency schemes; proxy purchases to obscure online activities; KYC documents for identity verification; hacked or new accounts on platforms like Telegram, Discord, and Twitter/X.

Newcomers gain access to a complete fraud toolkit, while developers benefit from an expanding client base and industry connections.

Investigation on Drainers



The primary objective of this investigation is to identify the potential owners behind **Medusa Drainer** — a malicious Web3 toolkit designed to steal cryptocurrency from users by exploiting wallet permissions — and to uncover its possible links to other major drainer operations.

The Investigation Focuses on the Following Key Areas:

- **Identification of Key Players:** Determining the individuals or entities behind Medusa Drainer, as well as understanding which players have replaced or absorbed their operations after their decline.
- **Distribution and Customer Communication:** Analyzing how Medusa Drainer's infrastructure was distributed, and the methods used to communicate with clients. This includes examining customer onboarding processes, communication channels, and promotional activities.
- **Owner and Support Accounts:** Investigating the primary owner, support accounts, and any related profiles. This involves identifying their roles, interactions, and activities to map their involvement within the ecosystem.

- **Connections to Other Drainers:** Exploring links to other drainer groups or services through shared infrastructure, communication methods, or overlapping personnel. Identifying common channels, forums, or platforms where collaboration or exchanges of information may have occurred.
- **Reasons for Ceasing Operations:** Assessing the circumstances that led to Medusa Drainer exiting the public space, including potential internal issues, competition, enforcement actions, or deliberate fraud against their own clients.

Market Overview: The Growing Reach of Drainers



Drainers have seen a significant rise in popularity and impact within the Web3 ecosystem over recent years.

In 2024, Scam Sniffer [reported](#) that drainers were responsible for the theft of approximately **\$494 million**, marking a **67% increase** compared to the previous year. Interestingly, the number of victims grew by just **3.7%**, indicating that drainers are becoming more effective, targeting higher-value wallets and stealing larger amounts per incident.

The trend is also reflected in dark web activity. According to [Kaspersky](#), the number of online resources dedicated to drainers on darknet forums rose sharply — from **55 in 2022 to 129 in 2024**. This surge points to a growing interest among cybercriminals in drainer tools and their operational models.

Scam Sniffer also notes that **Ethereum** suffered the greatest losses among blockchains, with reported thefts totaling **\$156.2 million**, mostly concentrated in large-scale phishing campaigns.

Throughout 2024, the Drainer Market Underwent a Notable Consolidation:

■ **First Half of the 2024:**

Angel Drainer: 42% / Pink Drainer: 28% / Inferno Drainer: 22%

End of May: Pink Drainer exited the scene and was absorbed by Inferno.

Third Quarter (2024): Inferno took the lead with 43%, followed by Angel at 25%.

End of October (2024): Angel Drainer absorbed Inferno. Together, they now control an estimated 45% of the market.

■ **Q4 2024 Distribution:**

Angel + Inferno: 45% / Ace Drainer: 20% / Other Emerging Drainer Operations: 25%

Previously, drainer activity was mostly linked to phishing websites. However, 2024 marked the beginning of a shift toward mobile vectors. One notable example is the **malicious WalletConnect** app, discovered in **March 2024** on Google Play. This indicates that drainer operators are diversifying their attack surfaces, expanding from browser-based phishing to mobile app-based vectors.



Key Players in the Drainer Ecosystem

The following actors have played a central role in the evolution of wallet drainer operations across Web3 in 2023 – 2024. These entities are responsible for the majority of the high-profile phishing campaigns and large-scale fund thefts.

Top actors:

- Angel
- Cerberus
- Inferno
- Nova
- Pink
- Medusa
- Ace Drainer
- MS Drainer

Inferno Drainer

Launched in **November 2022**, Inferno Drainer was responsible for stealing over **\$80 million** before temporarily halting operations in **November 2023**. It returned in **May 2024** and was eventually **acquired by Angel Drainer**, becoming part of one of the most powerful entities in the space.

Inferno's phishing operations primarily targeted high-profile crypto ecosystems like **PEPE**, **COLAB.LAND**, **zkSync**, and **MetaMask**. Its method included embedding malicious **JavaScript code** into phishing websites, manipulating protocols such as **Seaport**, **WalletConnect**, and **Coinbase Wallet** to force wallet approvals and unauthorized transfers.

As of late 2024, Inferno and Angel are considered to be part of a **merged infrastructure**.

Angel Drainer

Initially focused on **EVM-compatible blockchains** and NFTs, Angel Drainer later expanded to **Solana**. It gained widespread attention following the **Ledger Connect Kit Phishing Campaign**.

On **August 31, 2024**, Angel rebranded and returned under the name **AngelX**, introducing improved obfuscation mechanisms. New blockchains like **TON** and **Tron** were added, selected for their limited security tooling and fewer detection mechanisms.

Cybersecurity researchers have noted that AngelX has a **high evasion rate**, allowing it to bypass many Web3 security solutions.

On **July 16, 2024**, the team reportedly attempted to shut down operations after concerns that their real-world identities may have been compromised.

October 20, 2024

Benzinga

 **JUST IN:** Angel Drainer has acquired Inferno for the sum of \$501,000,000, as confirmed by [@ripferno](#), verifying that this figure is accurate.

BZ

← 5 00:03

By **October 20**, Angel Drainer had absorbed the infrastructure of Inferno Drainer, consolidating their position as a market leader.

Pink Drainer

First detected in **April 2023**, Pink Drainer quickly became a dominant force, stealing **156 ETH** shortly after launch. The tool was reportedly built by a single developer operating under the alias **PinkDeveloper** (previously known as Blockdev on X.com and Discord), who claimed to focus on targeting **Chinese DeFi users**. Pink Drainer expanded to a multichain tool within one month of release and surpassed **\$1 million in stolen assets by July 2023**.

The operation ceased on **March 17, 2024**, with a notable irony — its own developer fell victim to **address poisoning**, a scam in which attackers mimic legitimate wallet addresses. In June 2024, 10 ETH were mistakenly sent to a fraudulent address.

Ace Drainer

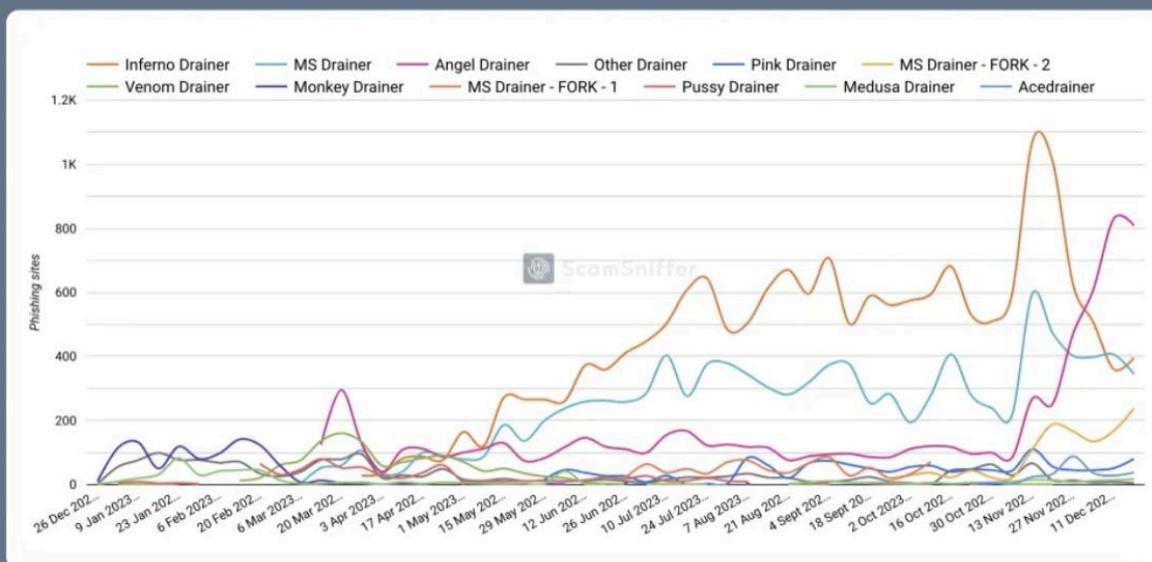
Ace Drainer emerged in **January 2024** and became infamous for its **supply chain attacks**. In **October 2024**, the group exploited the **Lottie Player animation package** on npm, compromising more than **400 Web3 applications** that had integrated the vulnerable package into their decentralized apps (DApps). Unlike Pink, Ace remains active and is considered a direct competitor to Angel.

Medusa Drainer (Subject of This Investigation)



In 2024, Medusa Drainer emerged as one of the most significant players in the cryptocurrency draining ecosystem. Despite its size and influence, it has remained relatively under the radar in terms of large-scale phishing attacks compared to competitors like Angel or Inferno.

Medusa Drainer primarily targeted individual users through phishing websites and social engineering tactics. These schemes often disguised themselves as token distributions, luring users into approving fund transfers via strong Approval or Permit2 functions. This type of fraud falls under the category of “Permission Scams”.



ScamSniffer

Source: ScamSniffer

A detailed analysis of the drainer's activities reveals that the number of phishing domains associated with Medusa Drainer rarely exceeded 100+, as indicated by the green line on the ScamSniffer graph. While less prolific than other players, Medusa's operations were nonetheless impactful.

For instance, [an automated report from MetaSleuth](#) illustrates how such scams unfold, tracing transactions from victim wallets to intermediary addresses where stolen funds are laundered or exchanged. Similarly, a case [highlighted on Reddit](#) showcases how phishing schemes — such as those exploiting Uniswap — successfully deceive users into approving unauthorized token transfers.

For authorities

Data and addresses that are apparently relevant to this robbery:

- 1st of March, 2024, I linked my wallet to the scammer at the website: *air swap dot trade*
- 3 stealings took place: 1st of March, 2nd of March and 24th of April 2024
- Each stealing, contract was initiated from: **0x244EA7FeFe2D66Fb6Da2eD374351D1bf4161A3e4**
- Each time, tokens were exchanged to ETH through Uniswap Permit 2 and sent to:
0xFa7575CaA049e5cFD96a2783da2C85663f0Da817
- Total value lost is about 8000 USD

Please take necessary actions to prevent this from happening to someone else.

Thank you

Medusa Drainer's Public Activity



Medusa Drainer followed this model closely, leveraging Telegram as a primary communication platform. The public Telegram channel @MedusaDrainer was first monitored on **February 1, 2024, with 1,500 subscribers.**

The channel reached its peak in **March 2024, when up to 200 phishing domains** linked to Medusa were created. By **August 2024**, activity had ceased, with the channel's final post dated **August 13, 2024.**

Source: https://telemetr.io/ru/channels/1916540595-medusadrainer_scam/about

User Feedback on Medusa Drainer Highlights Several Shortcomings Compared to Competitors:

- **High Fees:** Unlike Angel Drainer, which charges only a percentage of stolen funds, Medusa required upfront payments for access.
- **Unreliable Support:** Users frequently complained about unprofessional and unresponsive customer service. (Source: <https://t.me/yellowlean/30852>)

- **Internal Fraud:** Reports suggest the Medusa team defrauded its own clients, abandoning operations while withholding client funds. (Source: <https://t.me/yellowlean/53372>)

Intelligence Insights from Community Analysis

Telegram chats associated with Medusa Drainer offer valuable insights into the broader fraud ecosystem. Public and private discussions reveal connections between members of similar communities, shared operational techniques, and overlapping clientele.

Report

This list exposes a concerning network of individuals and groups involved in cryptocurrency fraud, primarily through sim-swapping and draining techniques. Sim-swapping involves hijacking a victim's phone number to gain access to their cryptocurrency accounts. Drainers, on the other hand, exploit vulnerabilities in platforms to steal funds.

Notable Individuals and Groups:

- @swat, @dare, @june, @dead, @crazy: These individuals are known Coinbase sim-swappers, with confirmed thefts ranging from over \$100,000 to over \$5 million.
- @goth, @perc, @kill, @meth, @dislike: These individuals are also Coinbase sim-swappers, with confirmed thefts exceeding \$100,000 and reaching over \$500,000.
- @griddy, @larp, @lonely: These individuals are classified as drainers, with confirmed thefts ranging from \$100,000 to \$200,000.
- @yeah, @virgin, @dirty: This team of drainers has stolen over \$1 million.
- @zombie, @villain: This team of Coinbase sim-swappers has stolen over \$1 million.
- @patelco: This individual engages in both bank fraud and sim-swapping, with confirmed thefts exceeding \$200,000.

- @twink, @happy, @rumor: These individuals are Coinbase sim-swappers, with confirmed thefts ranging from \$100,000 to \$200,000.
- @spirit, @amulet, @three, @emotion, @weed, @sleepy, @insecure, @favorite, @fate, @cuter, @demise, @PermBigSir, @stand, @regret: These individuals are known to be involved in sim-swapping but with varying degrees of confirmed stolen amounts.
- @stop: The developer of the "angel drainer" tool, with over \$50 million in confirmed thefts.
- @infernoDrainerSupport: The developer of the "inferno drainer" tool, with over \$200 million in confirmed thefts.
- @bigego: A Coinbase sim-swapper with confirmed thefts exceeding \$200,000.
- @tempt, @offthat: Developers of illegal sim-swapping and automated tools, with unknown stolen amounts.

Illegal Tools Facilitating Fraud:

These individuals and groups rely on tools specifically designed for illegal sim-swapping and draining activities:

- @breachly, @carrier, @suite, @ogbluvouches, @gorillacallbot, @kittymailer, @infernoReborn: These are the names of tools or services that facilitate the illegal activities mentioned above.

👍 13 🤔 5 👍 2

👁 1688 Empla..., edited 3:24 PM

Analysis of the Telegram Account @TaoMazov and its Role in Medusa Drainer Operations

The **Medusa Drainer** channel's archived data indicates the involvement of the Telegram account **@taomazov**, linked to its development and support activities. A deeper analysis of this account and its history reveals significant connections and operations within various Telegram communities.

Account Details

The **@taomazov account was active from August 19, 2023, until August 4, 2024**, coinciding with the decline of activity on the Medusa Drainer channel. As of now, the account appears deleted or banned following Telegram's policy changes regarding fraudulent accounts. During its active period, the account generated 63 messages across 6 different chat rooms.

Technical and Historical Details

Telegram chats associated with Medusa Drainer offer valuable insights into the broader fraud ecosystem. Public and private discussions reveal connections between members of similar communities, shared operational techniques, and overlapping clientele.

- **Telegram Link:** t.me/taomazov
- **Names:**
 - February 1, 2024: Tao | Medusa Drainer
 - January 10, 2024: YC
- **Usernames:**
 - @ycmarginal (as of January 10, 2024)
 - @taomazov (as of February 1, 2024)
- **Account ID:** 6695770377

Chatroom Presence and Message Activity

Channel Name	Link	Count of Messages
Crypto4domain	https://t.me/crypto4domain	2
Twitter Funhouse	https://t.me/c/2014336909/42226	1
	https://t.me/c/1841068709/65057	1
Scam Sniffer Official	https://t.me/scamsniffer/64498	33
Sim Land 🍊	https://t.me/c/2068592120/369018	14
Curve Finance	https://t.me/curvefi/590548	12
Drainer's Haven	https://t.me/c/2123758786	No Messages
HyperCycle	https://t.me/hypercycle_ai	No Messages

 Alert Pump Unit – Exclusive Community Tips	https://t.me/ CryptoInsightPumpHub	No Messages
Crypto Insight Hub – Expert Analysis 	https://t.me/ GlobalPumpSyndicate	No Messages

Observations from Specific Chatrooms

01 Scam Sniffer Official:

This chat room provides a wealth of information about the behavior and operations of the account user. The user displayed dismissive and mocking behavior toward others, often ridiculing victims. Interestingly, early messages in this group appear contradictory, with some users claiming that the drainer code was exclusive and accessible only to select clients, while others argued that it was more widely available. This points to possible misinformation within the community. The chat also suggests the existence of a reputation system for drainer clients, akin to those found on darknet forums. Such systems likely serve as a protective measure to shield trusted users from external intelligence or law enforcement interventions.

02**Sim Land 🍊:**

Sim Land is a private chat room centered around SIM card swapping scams, a type of fraud closely linked to drainer activities. The overlap between these communities indicates a tight-knit network of individuals engaging in various types of cyber fraud. The recurring interaction between drainers and SIM-swapping groups highlights the integrated nature of these illicit activities.

03**Curve Finance:**

This crypto project chatroom provides further insight into the interests and activities of the Medusa Drainer developer. The user interacted within the group, notably using branded community stickers, which suggests an effort to blend into legitimate discussions while possibly scouting for targets or opportunities.

04**Crypto4Domain:**

This chat focuses on services for acquiring domain names for cryptocurrency operations, likely including phishing activities. Messages from the user inquire about the disappearance of the chat owner, implying prior business dealings or reliance on the group's services. This indicates that @taomazov may have used these domains for establishing phishing sites or other fraudulent operations.

Mentions and References

Analyzing mentions of @taomazov and the @MedusaDrainer channel reveals significant interactions and references across various Telegram discussions.

■ Reference to MedusaDrainer

Message: "U must sold it to @medusadrainer"

Context: This statement suggests a transaction or ownership transfer related to @medusadrainer, indicating its active involvement in acquiring or managing drainer-related assets.

■ Direct Mention of MedusaDrainer

Message: "@medusadrainer"

Context: A simple yet noteworthy mention that situates the channel within a broader discussion, likely highlighting its activities or role within the ecosystem.

■ Hostile Interactions Involving @taomazov

Messages:

"@taomazov u r a retard get beamed nigga"

"bro this nigga rlly thought he getting src"

"nigga tryna leech"

Context: These messages appear to reflect confrontations between parties, possibly regarding disputes over access to source code ("src") or accusations of exploitative behavior. The tone suggests rivalry or disagreements within the drainer community.

In the final instance, more than 20 identical messages containing the same content were posted by a user identified as Edison (ID: 6091523852) in both the "Drainer's Heaven" and "Guardian Chat" Telegram groups. Upon further investigation, this user was traced to the "Aiden Test Group" chat (accessible at <https://t.me/aidenchattest>). This group references a Telegram bot capable of replicating entire messages, chats, or groups by simply following a link.

Significantly, this group appears to host several accounts associated with another major actor in the ecosystem: Angel Drainer. Within this network, "Stop Me | Angel Drainer" is identified as one of the primary accounts linked to AngelDrainer's ownership. The overlapping presence of these accounts in related groups underscores a clear connection between individuals operating in the drainer ecosystem, hinting at a broader collaborative or competitive relationship among these actors.

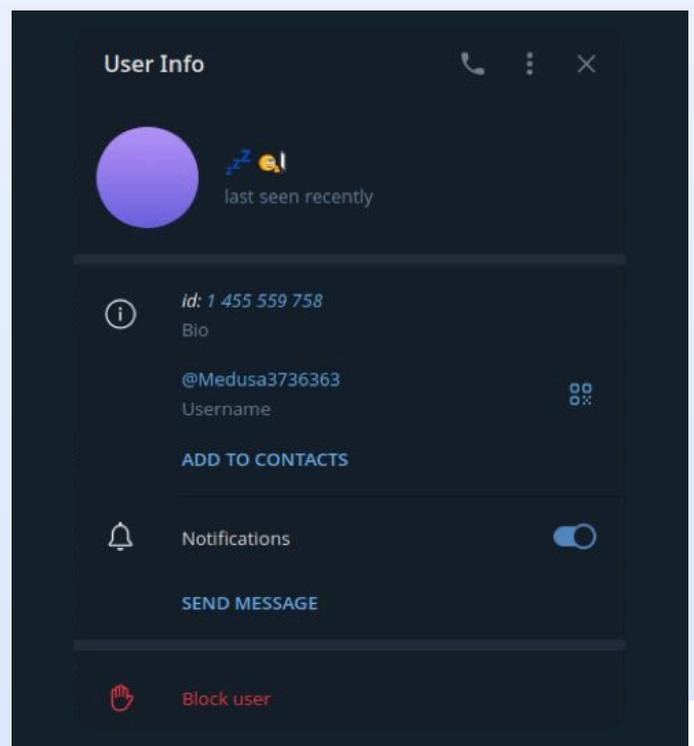
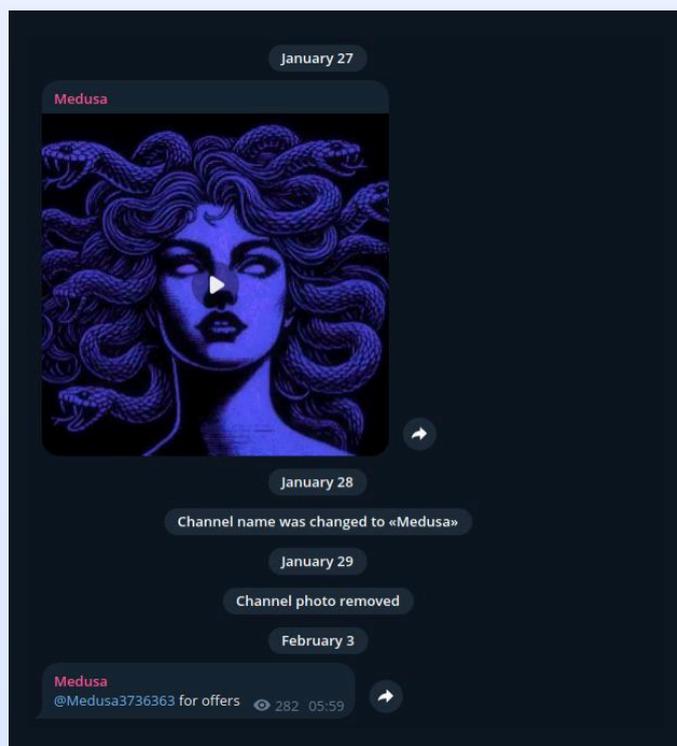


It is notable that the first referenced chat serves as a marketplace for trading high-value, aesthetically appealing usernames. Within this chat, users interested in acquiring or selling the username @medusa were active. This raises the possibility that the operator of the Medusa Drainer may have shown interest in obtaining or leveraging this username, potentially for branding or operational purposes. The identified individuals engaged in discussions about the username are flagged as persons of interest.

Link	Message	ID
https://t.me/c/1418416872/838132	Who owns @medusa? do you @liar?	7311703812
https://t.me/c/1418416872/846922	I tried. He blocked me. @mazovdusa	1455559758

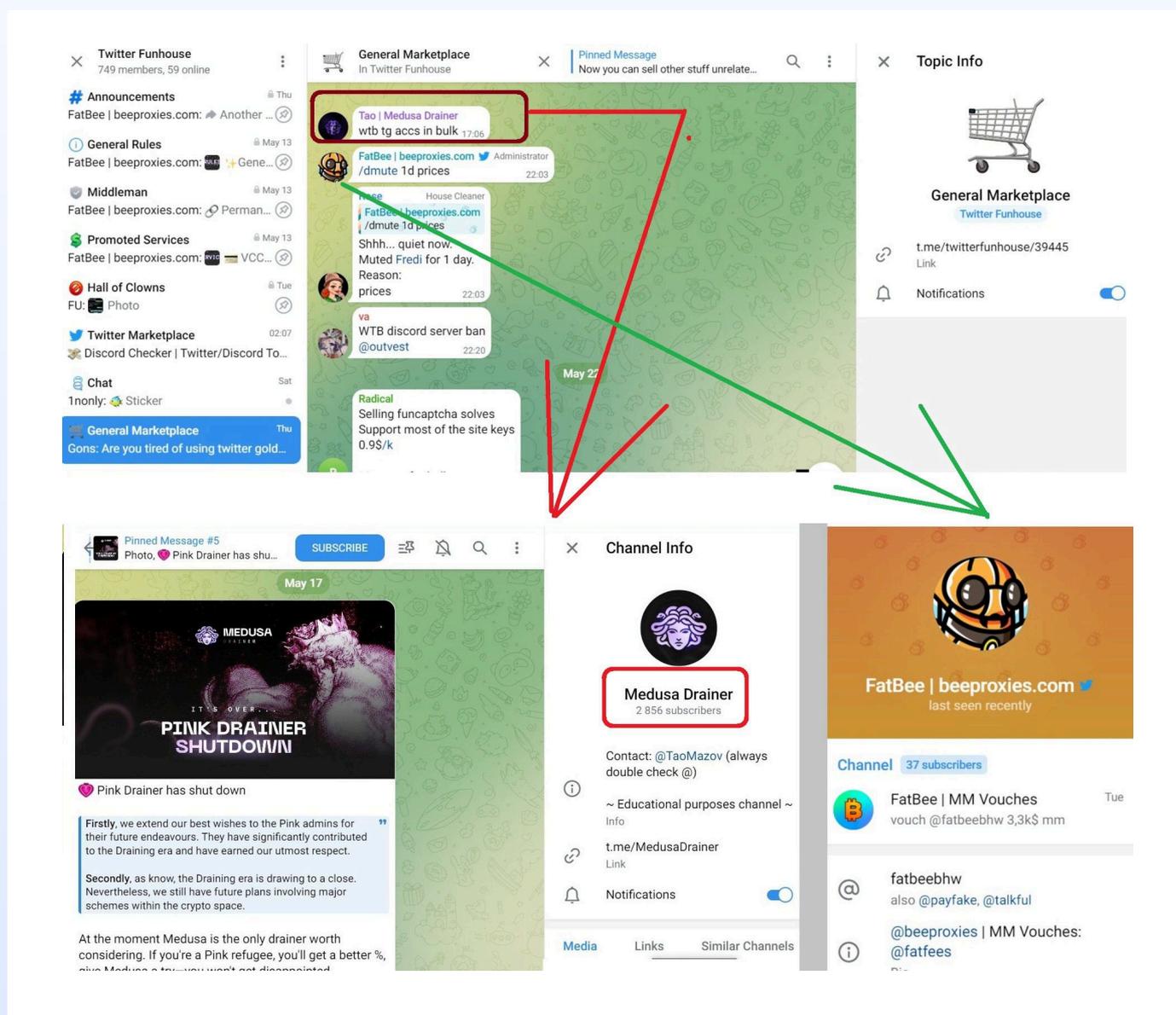
The current owner of @medusa is user @Medusa3736363, ID 1455559758.

At present, there is no traceable activity from the main account, **@TaoMazov**, which is associated with the MedusaDrainer channel. This account, believed to be linked to the drainer's development or representation, remains inactive. This inactivity could suggest deliberate concealment or an operational pause. Further investigation is required to determine the current state of the individual or group behind the account.



A search on Telegram led to a discussion within the ETHSecurityCommunity chatroom, which detailed an investigation into Pink Drainer. This investigation [uncovered connections](#) between Pink Drainer and the proxy and account provider FatBee.

<https://web.archive.org/web/20240524204647/https://medium.com/@Heiner./scam-as-a-service-pink-drainer-5b4165371916>



Source: [ETHSecurity Community](#)

“I think that the person you identified is an accomplice through whom Drainers pawns purchase hacked and other social media accounts, primarily Twitter accounts. For example, in the telegram group [@twitterfunhouse](#) (Section General Marketplace), you can see the official representative of Medusa Drainer.”

Evidence suggests that **@taomazov**, an account linked to Medusa Drainer, was also active in groups where Pink Drainer was mentioned. This overlap indicates potential ties or shared networks between the actors behind these drainers.

Additionally, further investigation using keyword searches identified two other Telegram accounts: **@mazovdusa** and **@medusadrainersupport**. These accounts are directly connected to Medusa Drainer's operations and may provide additional insights into the organizational structure and affiliations of this actor. Further analysis of these accounts and their activity is underway to uncover more links to related entities.



MazovDusa Telegram Account Research

A search on the account @mazovdusa, along with related keywords such as “Medusa,” “MedusaDrainer,” and “taomazov,” revealed additional connections, including the newly registered site medusa.services. This site prominently features a link to the @mazovdusa Telegram account in its “Contact Us” section.

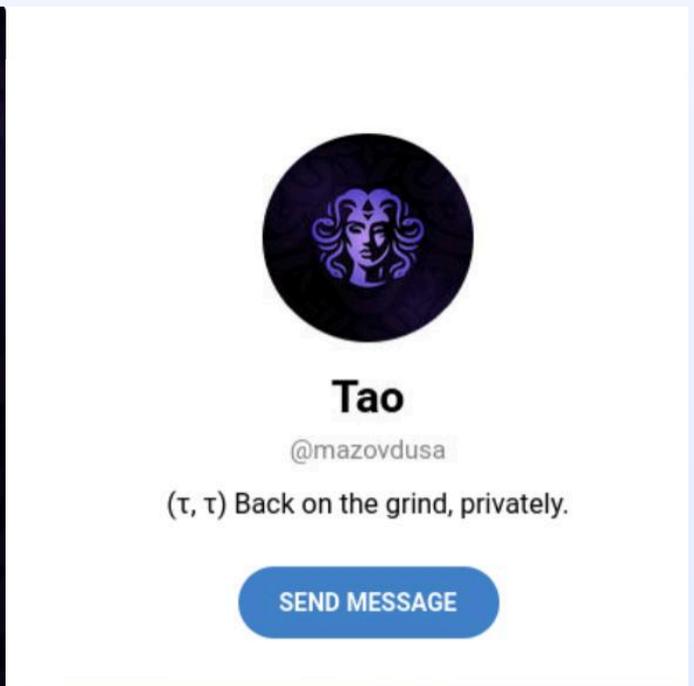
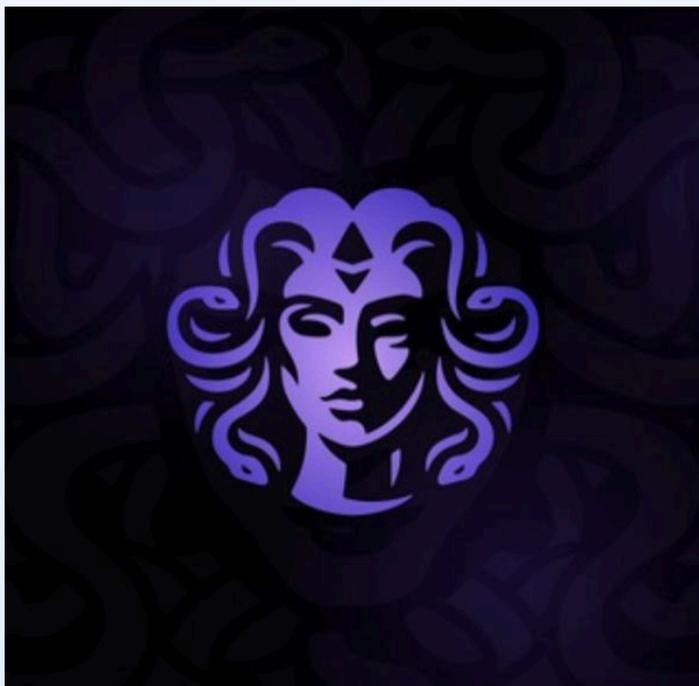


Photo uploaded 20.10.2024 at 17.00 UTC +5.

Brief Technical Information:

- **TG Link:** t.me/mazovdusa

Name Changes:

October 29, 2024 → **Tao**

October 29, 2024 → **2015**

October 18, 2024 → **Fatme tvkli**

- **Username:** @mazovdusa

- **Telegram ID:** 109327337

- **Registration Date:** Approx. August 2015

- **Bio:** (τ, τ) Back on the grind, privately.

- **Photo:** View Archived Image https://cdn4.cdn-telegram.org/file/KZraCU5VfDv3zy3kWJuipLvz6633XAPIW-hShNHx7LLI9nly-hYZQ0FBZKUKMnhSA1bMa-0NW109S3o2yFzVn_s6SMYVFp2VlyRvSnK6GzQMwrBUFu5oGAuHMy0ZP97cFGfscK6N6YRckgwXclWw5vrg5KONJYzZzb8i5vTKtrUTwoTUZ7sKTqIMMEMRCpN9dEQIYBC4sZAqOGd2es6p1QB0w_cNdkOh5NSECUQW1o_PjF72CjhnPUhTanQu9t0PW8bsB7j0S5fWEqo8_8WYscC95eAueAi84weualdRXaLP_AJ3CbejxkELbmvPb7ZKA4XMZbL7i8GPbgJUHL3uA.jpg

User Was Found in Chats:

Channel Name	Link	Count of Messages
Drainer's Heaven	https://t.me/c/2398309960/158387	14
[chat]	https://t.me/draingc/1252	2
Scam Sniffer Channel	https://t.me/scamsniffer/70303	3
Faded MP	https://t.me/c/2397156301/7395	1
ETHSecurity Community	@ethsecurity	No Messages
گروه VIP تیم هلاکویی 💰	@halakooii_vvip	No Messages
صیغه حلال	@asmilmirrjab640	No Messages
طهره ✿ پان پکت هک راج	@tehrankarraji	No Messages
مایت از بانک ملی	@kakhazinemardomii	No Messages

مشاور پاسخگویی	@jumivuygukj	No Messages
صیغه ونکاح موقت	@chaneelavalfvvv	No Messages
موسسه رسمی سرو	@jsksklwlkwkske	No Messages
.	@tvnpersian	No Messages
چتکده	@chat_kadeeeehw	No Messages
سهم بانک ملی ایران	@bfxmgcbk	No Messages
صیغه و سکس حضوری ساحره	@hozori_sahere_jon	No Messages

The most noteworthy activity stems from recent posts in the closed Telegram chat **Drainer's Heaven**, which is explicitly designed for developers, clients, and enthusiasts involved in drainer-related cryptocurrency activities. Access to such chats is restricted and typically requires an invitation link. However, all links we discovered have since expired or become invalid.

Highlights of Activity in Drainer's Heaven:

- **08 Dec:** [Message](#) - "Who still has Twitter marketplace @s?"
This suggests interest in Twitter-related accounts or tools, potentially for exploitation or sale.
- **03 Dec:** [Message](#) - "R how much is this selling for xd"
This indicates active discussions about the value and sale of certain items or services within the drainer ecosystem.
- **03 Dec:** [Message](#) - "He meant that"
Likely a continuation of a thread discussing a specific topic or clarification within the community.
- **03 Dec:** [Message](#) - "They're terming our channels"
Suggests concerns about channels being flagged, terminated, or monitored, reflecting an ongoing effort to evade detection or censorship.

And in ScamSniffer Telegram Channel:



From this, we can infer the possible reasons behind the Medusa Drainer team's retreat from the public space. It is highly likely that, as suggested by previous mentions, they have transitioned to operating within private chats dedicated to users and technical support. However, their public channel and primary profile appear to have been removed, either as a result of actions taken by the Telegram platform — potentially in response to fraudulent activities — or due to coordinated complaints from competitors. This remains speculative, as no concrete evidence has yet been discovered to confirm these claims.

MedusaDrainerSupport Telegram Account Research



Key Information:

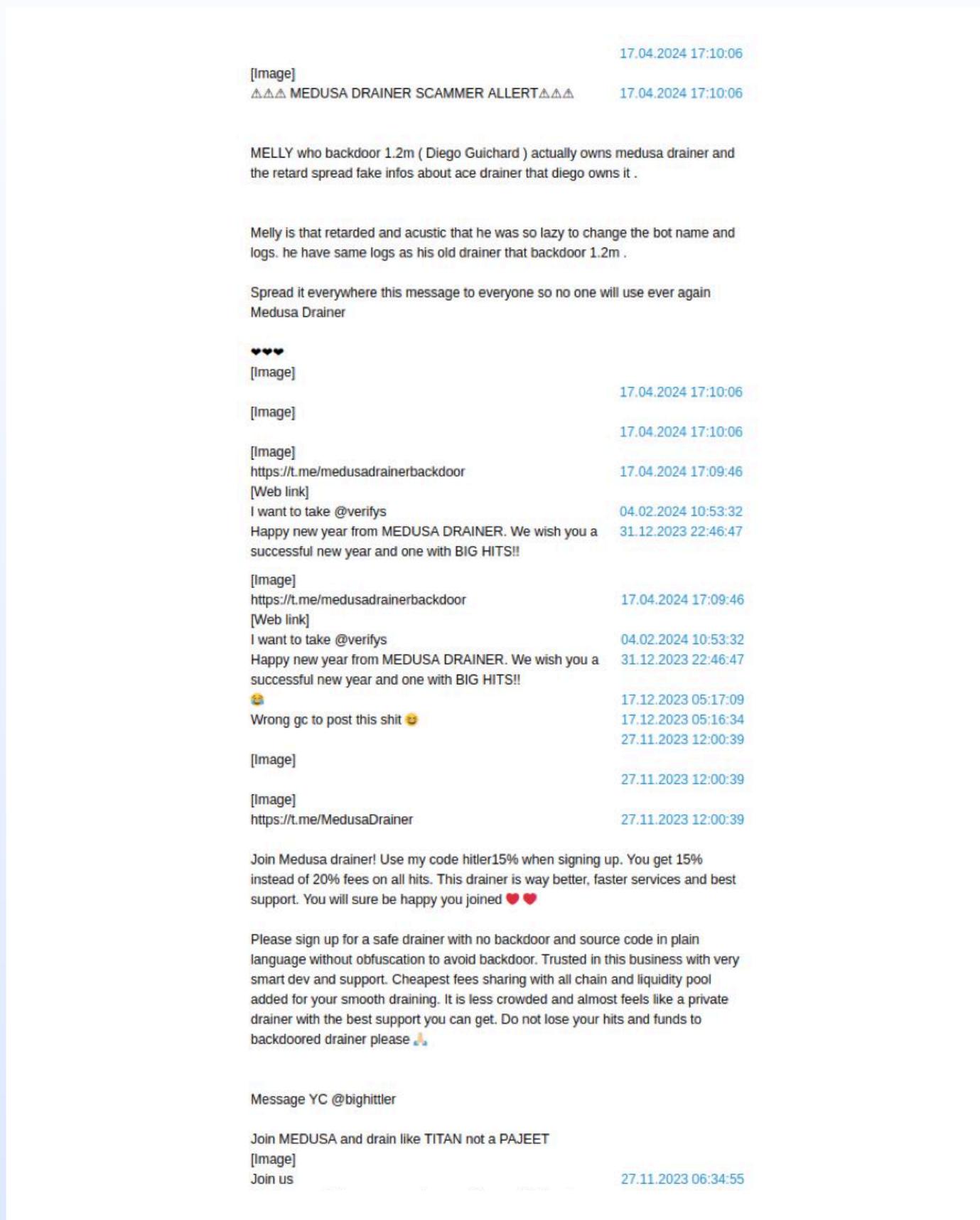
- **TG Link:** t.me/medusadrainersupport
- **Account Names:**
 - 16.01.2024** → Hitler | Medusa Drainer
 - 16.01.2024** → Medusa Drainer
 - 30.12.2023** → Hitler (Medusa Drainer Support Team)
- **Associated Usernames:**
 - @bighittler
 - @MrBBonly
 - @mrbigbags
 - @ebetins
 - @grokcommunityairdrop
- **User ID:** 5545771645

User Was Found in Chats:

Channel Name	Link	Count of Messages
.	https://t.me/c/1841068709/61787	33
@Verifys - Chat	https://t.me/verifys	1
CB MARKETPLACE	https://t.me/nftdrainers2/10582	21
ChangeNOW Community	https://t.me/ChangeNOW_chat/213357	3
Ottoman Cloud	https://t.me/c/1571072328/186	1
Angel X Drainer	https://t.me/+Zn84U2JSMGMxZDMx	271
Bloktopia Official Chat	https://t.me/BloktopiaChat/496051	2
TrackTX Community	https://t.me/tracktx	No data, Exited
	https://t.me/kaonlabs	No data, Exited

	https://t.me/angel_drainer_eth	No data, Exited
	https://t.me/c/1382061287	No data, Exited
	https://t.me/updteamchat	No data, Exited
	https://t.me/scamsniffer	No data, Exited
	https://t.me/cryptoo_Red	No data, Exited
	https://t.me/c/1898813951	No data, Exited
	https://t.me/Radio_Biafra	No data, Exited
Freelancer Upwork Fiverr PeoplePerHour	https://t.me/Freelancer_Upwork_Fiverr	No data, Exited
	https://t.me/financeboys	No data, Exited
	https://t.me/PAXworldOFFICIAL	No data, Exited
Hacker Legion	@hackersy	No data

The archived messages provide significant insights into the Medusa Drainer operations and its key figures. Here's a detailed analysis:



Key Observations:

01 Involvement of Diego Guichard and Melly:

The messages indicate that Melly is identified as the owner of Medusa Drainer. Melly has been accused of hacking Diego Guichard and falsely attributing the ownership of Ace Drainer to him. Claims suggest that Melly used unchanged bot names and logs from his previous drainer operation, which resulted in a loss of 1.2 million USD. This aligns with accusations of negligence and an attempt to shift blame.

02 Medusa Drainer's Decline:

The suggestion that Medusa Drainer went into obscurity by defrauding its customers gains credibility. This is consistent with the allegations and observed changes in its operational style.

03 Connection Between @MedusaDrainerSupport and @TaoMazov:

Similarities in writing style and overlapping participation in specific Telegram groups suggest a possible link between the two accounts. This raises questions about the coordination of Medusa Drainer's activities across multiple aliases.

04 Drainer Airdrop Giveaways:

Past usernames and promotional strategies hint at involvement in typical scam tactics such as drainer airdrop giveaways, a common scheme for luring unsuspecting users.

05 Awareness and Response from the Drainer Community:

The ETHSecurityCommunity investigation highlighted connections between scam service providers and drainer developers, specifically pointing to Pink Drainer. The drainer community appears to be aware of these investigations, as evidenced by the removal of the original report from Medium and the subsequent privatization of many Telegram groups, including Twitter Funhouse.

Estimated Impact of Medusa Drainer



Estimated Total Funds Stolen:

Approximately **\$5.5 million USD** across all identified addresses, based on historical incoming transactions and the USD rate at the time of each transfer.

- While the drainer's creators claimed to have stolen over **\$5 million** in just the first week of operation, the actual on-chain data suggests this may be an exaggeration.
- The total observed across all tracked addresses (Medusa Drainer 1, Medusa Drainer 2, and related phishing addresses) matches this figure but appears to reflect the entirety of the operation's lifespan, not just one week.

Median Amount Stolen Per Victim:

It is roughly **\$3,800 USD** per transaction. The distribution is highly uneven, skewed by a small number of large-scale thefts. This is consistent with alerts issued by MistTrack, which highlight individual thefts in the **\$800k–\$900k** range.

📌 Number of Unique Transactions:

~**1,547** incoming transactions across all identified addresses. This represents the upper bound of victim interactions with the Medusa Drainer.

📌 Estimated Number of Unique Victims:

~**870 individuals**. This estimate is based on the count of unique sender addresses to Medusa-Associated contracts.

Publicly Tracked Cases and Supporting Alerts

- **\$792.5k:** [MistTrack Alert 1](#)
- **300 ETH (±\$537 as of April 2025):** [MistTrack Alert 2](#)
- **~\$800k:** [MistTrack Alert 3](#)
- **~\$300k (Dashboard Screenshot):** [Quetzal Article](#)

Medusa team's claimed \$5M+ within the **first week** is unverified but aligns with the cumulative total of observed funds.

Key Medusa-Linked Wallet Addresses

Known Tagged Addresses

- [0xFa757575CaA049e5cFD96a2783da2C85663f0Da817](#)
(Medusa Drainer 1)
- [0x111117d0c05573b49B32eF30Dc031dD9eD022099](#)
(Medusa Drainer 2)

Additional Potentially Linked Wallets:

- [0x1x1a42605d92c210e4be47a6363046c591659ab444](#)
(Fake_Phishing26988, MistTrack Alert)
- [0x009515EfabCccdBAfA485f3919d94C85Ff23Ba75D](#)
Fake_Phishing268902, Quetzal Ref)
- [0xaC65360aF5a8AE5ec45AD0Bf2A7Ec063a38e2161](#)
Fake_Phishing328573, linked to Withdrawals)
- [0xda2dF35CDDA2C26D2473AAB2Ca1d6C15d58Ddd96e](#)
(Fake_Phishing328557)

These were flagged in MistTrack and Quetzal reports for exhibiting behavior linked to Medusa activity.

On-chain Transaction Analysis with AMLBot PRO



Our team utilized [AMLBot Pro](#) to build a comprehensive transaction flow graph tracking Medusa Drainer funds: [Visualization Link](#)

We began our analysis by focusing on two key addresses previously identified as being associated with the Medusa Drainer operation:

- **Medusa Drainer 1:**

`0xFa7575CaA049e5cFD96a2783da2C85663f0Da817`

- **Medusa Drainer 2:**

`0x11117d0c05573b49B32eF30Dc031dD9eD022099`

This second address was primarily used to activate new addresses and deploy multiple phishing smart contracts.

Transaction Tracing: Medusa Drainer 2

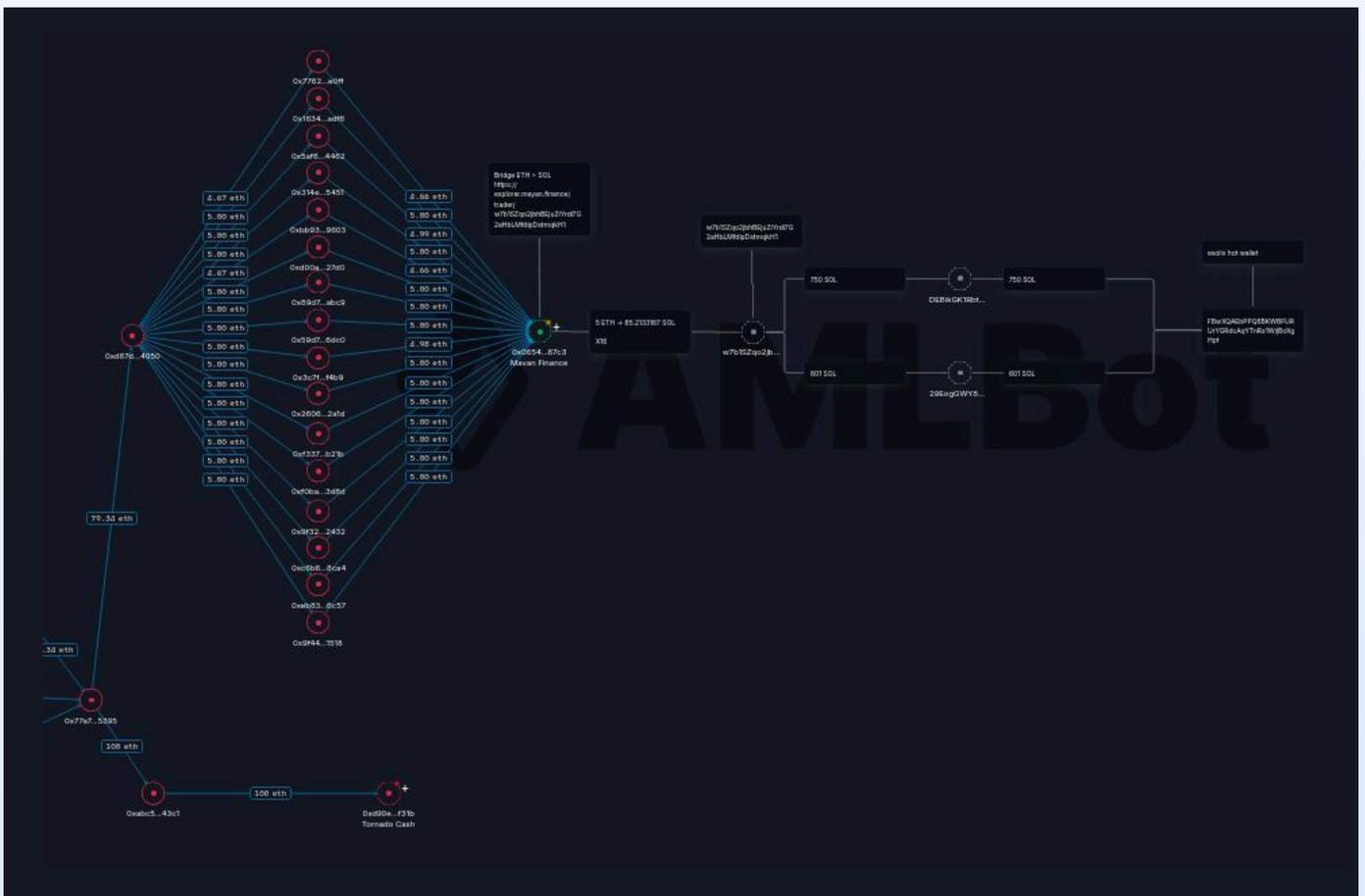
According to a report by [user X](#), approximately **180 ETH** originating from Medusa Drainer 1 was combined with funds from other victims. The funds were funneled through several disposable wallets and consolidated at the following **intermediate address:**

`0x77a78d9e12b94825c02595aebc208915df495395`



[Full Visualization Link](#)

From this point, the assets were divided into two separate transactions:



[Full Visualization Link](#)

- **October 18, 2024:** 100 ETH was transferred to **Tornado Cash**, a known Ethereum mixer. The transaction trail ends here due to the anonymization process used by Tornado.
- **October 18–19, 2024:** 80 ETH was bridged via **Mayan Finance** to the **Solana** blockchain, where it was converted into **1350 SOL**. These funds were subsequently sent to the **EXOLIX** exchange. Further tracing could not continue due to lack of public data from the exchange.

Transaction Tracing: Medusa Drainer 1

While less active than before, Medusa Drainer 1 ([0xFa7575CaA049e5cFD96a2783da2C85663f0Da817](#)) still shows evidence of transactional activity. The bulk of stolen Ethereum (ETH) was routed through several services in an apparent effort to obscure its origin and convert it into usable assets. The laundering path involved the following:

- An estimated **~312 ETH** was sent to **TradeOgre** and **Railgun** between February 22 and May 23, 2024.
- From **May 24 to October 18**, another **180 Ethereum (ETH)** was funneled through **Mayan Finance** and **Tornado Cash**.
- Approximately **8 Ethereum (ETH)** was moved to **Bybit** via an intermediary wallet. This address remained active in sending funds from Bybit between **April 21 and August 30**.

Throughout these transactions, **COW Protocol** was used extensively as a conversion tool to move stolen funds through decentralized exchanges before routing them to final destinations such as **Stake (a gambling platform), Bybit, or TradeOgre**.

Initially, the attacker opted to move funds directly to **Bybit** and **TradeOgre** using a network of intermediate addresses. However, over time, the laundering strategy evolved to incorporate multiple obfuscation layers.

The revised scheme followed the path: COW Protocol → Intermediate Addresses → Stake / Bybit / TradeOgre.

- The majority of funds — approximately **300 ETH** — were funneled to **TradeOgre** between **February 22 and May 23, 2024**.
- Between **May 24 and October 18**, an additional **180 Ethereum (ETH)** was processed through the **Mayan Finance Bridge** and **Tornado Cash**, further complicating traceability.
- Roughly **8 Ethereum (ETH)** was routed through an intermediary wallet and eventually deposited to **Bybit**. This address exhibited ongoing transactional activity with Bybit between **April 21 and August 30**.

Additional Findings on an Intermediate Address

Further analysis revealed notable activity surrounding one of the intermediate addresses in the laundering path:

0x2519a02e924767d7e0dc97596d8089db5b5ef62a. This address received funds directly from

0xfC6C479CBB9dB178E5F959CFc56d790B1D3eA3Bc, which is tied to multiple **ENS (Ethereum Name Service) domains** — a blockchain-based naming system analogous to domain names in traditional web infrastructure.

The following ENS domains have been registered by the user of the 0xfC6...3Bc address:

- **withdrawal-pendle.eth**
- **swapdex.eth**
- **taobridge.eth** ([Reported as scam](#))
- **swapfinance.eth**
- **eligibility-zksync.eth**

This address also shows inbound transactions from **TradeOgre**, consistent with other addresses used in the laundering chain.

Notably, it interacted with **fatfeemiffleman.eth**, an ENS address that appears to be linked to **TwitterFunhouse**, a community previously investigated in connection with **Angel Drainer**.

Fatfeemiffleman.eth acted as a **guarantor** — a trusted role within Telegram-based scammer ecosystems.

The same user was previously exposed in a separate investigation as a Macedonian developer tied to multiple illicit activities. Importantly, the address 0xfC6...3Bc appears to intersect with key infrastructure used by **Angel, Inferno, Pink, and Ace Drainer**, suggesting a broader operational overlap within the ecosystem of major drainer actors.

Address 0x2519A02E924767d7e0dC97596d8089db5B5eF62a

Sponsored: Join Lightchain Protocol AI Presale Today Before Tokens Sell Out. [Explore Now!](#)

Warning! This address is involved with a phishing campaign. Reported by BlockSec.

Fake_Phishing940317 Phish / Hack

Overview

ETH BALANCE
0.094661715608689959 ETH

ETH VALUE
\$194.17 (@ \$2,051.25/ETH)

TOKEN HOLDINGS
\$127.53 (34 Tokens)

More Info

PRIVATE NAME TAGS
[+ Add](#)

TRANSACTIONS SENT
Latest: 4 days ago First: 303 days ago

FUNDED BY
[withdrawal-pendle.eth](#) at txn 0x2ecf86718d3...

0xfC6...eA3Bc Etherscan

withdrawal-pendle.eth View Profile

Expiration Date Search

- withdrawal-pendle.eth** Expires in 1 month Owner
- swaprfinance.eth** Expires in 1 month Owner
- taobridge.eth** Expires in 1 month Owner
- swapr.dex** Expires in 1 month Owner
- eligibility-zksync.eth** Expires in 1 month Owner

Latest Known Destination of Stolen Funds

Following the path of stolen funds through intermediate address: `0x8fc43d983a8e807705120f5ec6493c561f6db33c`, a notable transaction of **25 ETH** was identified, sent to wallet `0xb83b5790f2bb98f72cf7294e71d56e3c0ba5363b`. This **wallet** currently holds approximately **50 ETH**, and has processed substantial volumes of high-value assets. Specifically, it facilitated:

- **445 weETH** (~\$973,000)
- **178 wstETH** (~\$441,000)

Both transfers were made to the **Zircuit Restaking Pool**, indicating an attempt to embed the funds deeper into DeFi infrastructure. This wallet exhibits behavior consistent with previously attributed **Medusa Drainer** infrastructure. It receives ETH via **COW Protocol**, then systematically converts funds through a layered token sequence:

ETH → eETH → weETH or wstETH → stETH → wstETH

Such a conversion pattern is frequently used to obscure fund origin and facilitate integration into staking or restaking mechanisms. The address and its activities raise strong red flags due to the transaction volumes, conversion strategy, and connection to mixers and DeFi platforms already tied to Medusa-linked wallets.

Wallet Overview:

[Etherscan Transaction History – 0xb83b5790...](#)

Zircuit Deposit Transactions:

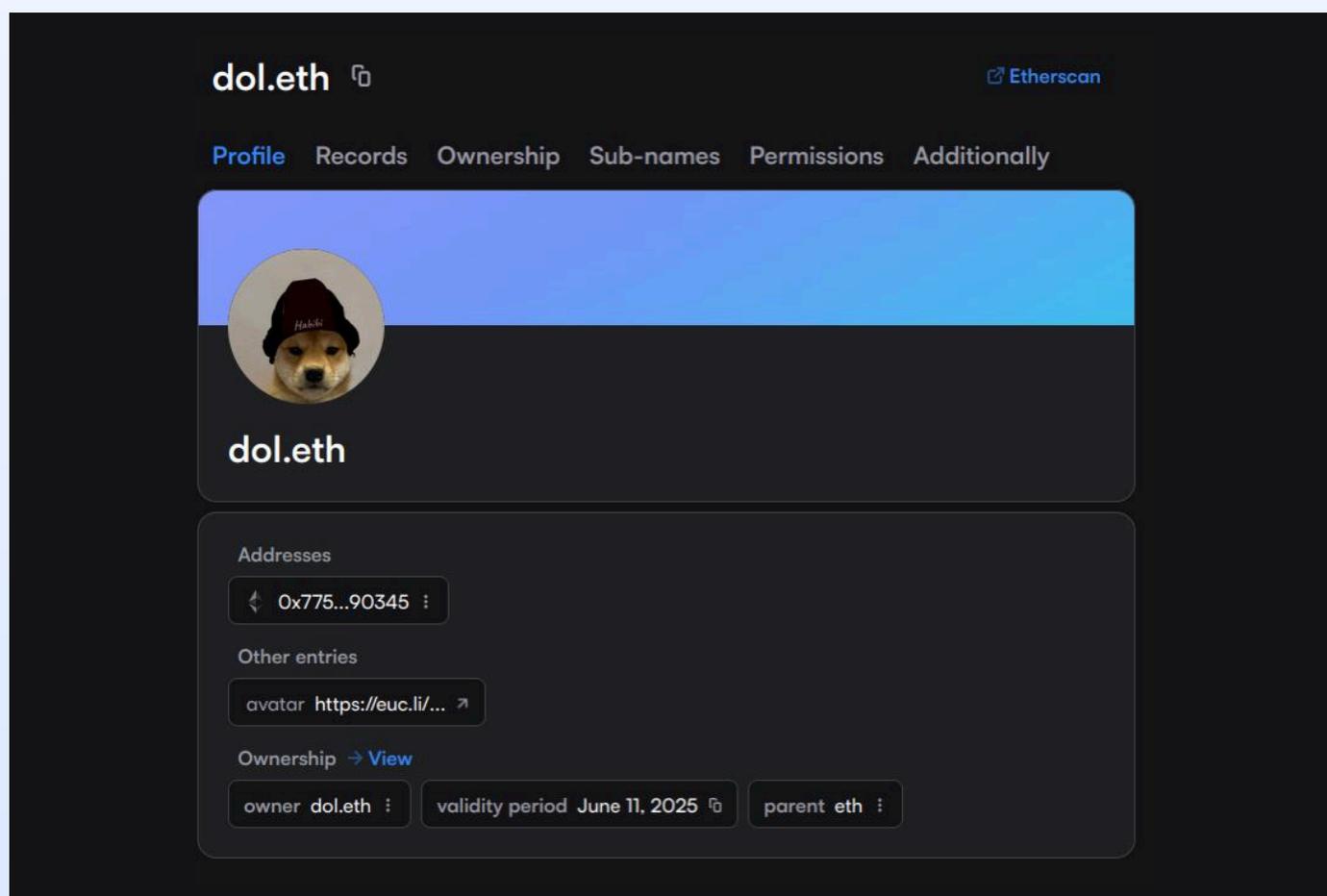
- [445 weETH](#)

- [178 wstETH](#)

This address currently represents the latest known location of funds attributed to the Medusa Drainer operation.

Connection Between Medusa Drainer 1 and ENS Domain Holder dol.eth

A notable address, [0x775b404e48ff523032ce9cc5483de2fef7690345](#), has been identified in association with **Medusa Drainer 2**, participating in a sequence of related transactions. This address is also the registered owner of the **ENS domain dol.eth**, suggesting a degree of user personalization or branding.



The screenshot displays the ENS domain profile for **dol.eth** on the Etherscan website. The profile includes a circular avatar of a dog wearing a red beanie with the word "Hakobi" on it. Below the avatar, the domain name "dol.eth" is shown. The "Addresses" section lists the address [0x775...90345](#). The "Other entries" section shows an "avatar" entry with the URL <https://euc.li/...>. The "Ownership" section indicates the owner is "dol.eth", the validity period is "June 11, 2025", and the parent domain is "eth".

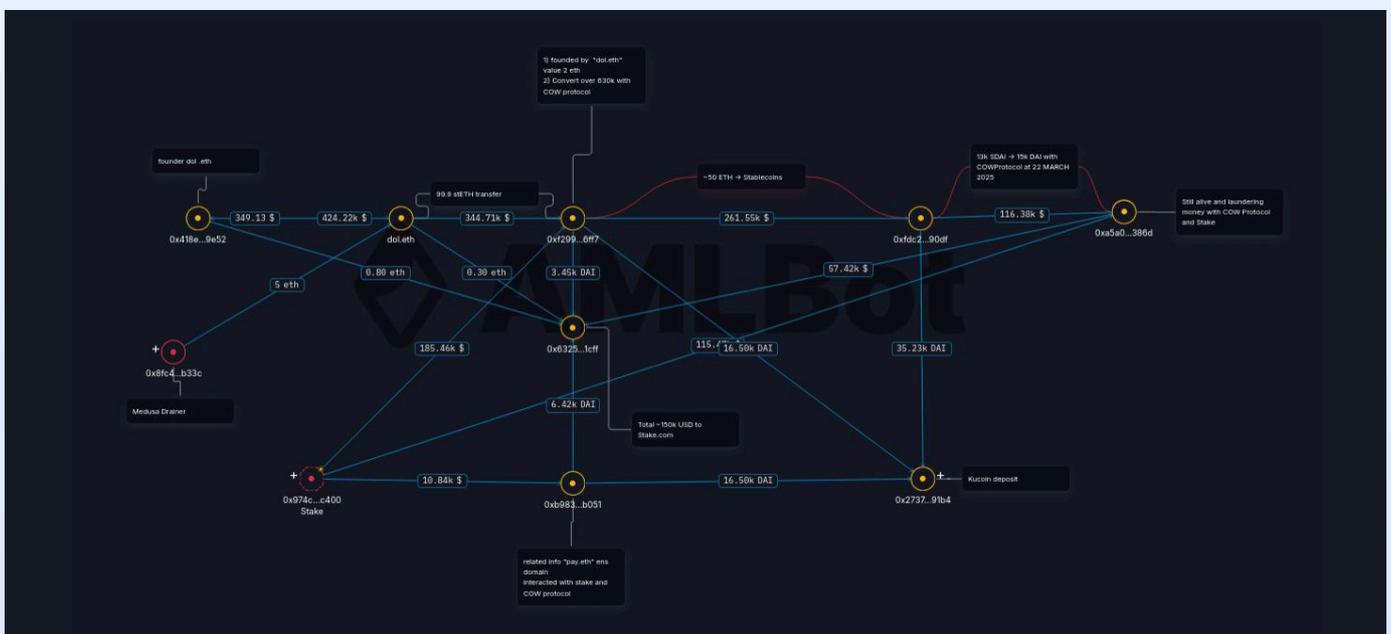
This wallet has shown significant activity on **COW Protocol**, where it repeatedly converted **ETH** and **stETH** into stablecoins — namely **USDT, USDC, sDAI, and DAI** — a common laundering pattern to prepare funds for off-chain conversion or low-risk storage.

One transaction of interest includes the handling of approximately **100 stETH**, which is believed to be linked to illicit activities.

The Flow of These Funds Proceeded As Follows:

- The stETH was first transferred to:
0xf2999210f49f5210ffcbdb07b14d3b8792236ff7.
- The total was then split evenly:
One half was routed through **COW Protocol**.
The other half was sent to the **intermediate address**:
0xfdc2790f3c0186f914b914b43c3be47bcbffabb290df.

The funds arriving at this address were subsequently forwarded to a previously identified wallet already associated with the Medusa Drainer operation — reinforcing the linkage between dol.eth and the laundering infrastructure of this drainer.



Withdrawal Analysis from Stake Linked to Medusa Drainer

As part of our ongoing investigation into the Medusa Drainer infrastructure, our team requested and obtained withdrawal data from the Stake platform concerning two deposit addresses previously linked to Medusa Drainer 1:

- 0x8261f516b0221633f2343baa5944f9f67874dbda
- 0xe7d6bd1b2a8a764ef2722f41e939db4936ff048b

Withdrawal Data – Stake-Linked Address 1

Type	Information
Deposit Address	0x8261f516b0221633f2343baa5944f9f67874dbda
Blockchain	Ethereum
Withdrawals In	ETH, USDT
Approx. Withdrawal Total	~\$300,000 USD
Activity Period	From July 26, 2024 to January 20, 2025
Associated Addresses	0xA5A062cEadC6C212b04C76987354372327be386D

0xf2999210F49F5210FfcBDb07b14d3b
8792236FF7

0xE4e2620d05D4B2004A6EE3E183b9
4D0DEB881B98

0x5022F184b7E9E05A0cc60811806Ad
7Bc6A972b61

0xB98310E85D68b888eEc216cDFb9C
e1Ef545cB051

0xb09e1335aE962c6a88C7018e33937
84b760638B2

0x0DDbAb11Aac0301f32964F76a029B
def0c92f6f5

0x6cB33dF933eC7aac60F2640D07a5
E744317651Af

Withdrawal Data – Stake-Linked Address 2

Type	Information
Deposit Address	0xe7d6bd1b2a8a764ef2722f41e939db 4936ff048b
Blockchain	Ethereum

Approx. Withdrawal Total ~\$650,000 USD (in stablecoins),
~\$450,000 USD (in XMR)

Activity Period From **October 6, 2024** to **December 14, 2024**

Associated Addresses 0x86e5d3c1edfe442bd276508ad897e
6154cb05c39

rffGCKC7Mk4cQ5aUGg8pfRe3MPC7Cy8gfe:661320

rdPeCfko28cCLNbY8noXGV4ycZ3TGCSnM:0

rffGCKC7Mk4cQ5aUGg8pfRe3MPC7Cy8gfe:441743

TTt4eiHpCXxMToHvhbwDy9AYgbvNkjhcfn

THqqfBjJLm5S8SS4dhUSnCEksyZJ1LrW6i

TJaRSHSicV51wbJ6RAzK53WUVPNjE6FTD8

TQDMqzNgpCeBo7G8WNQazckRAXikWdCeX1

TAHvN5vBJGwY2g2TWDvpJ5VQL62bbGVJjy

TJZ2MNXdhSLgknNvmDRPNbppHaLn4VjzcS

0x0CB6aa8C9fBe844ba979Fa6DAD1473bD394a2db1

TNN36i7aD4c26wJTZLtUS2tUFVV2WW5dLz

TM2KGMRG5KzsMbQWSdDh9ByShknm1zkh5j

bc1qvg7nrph4pgqpjrlpj6rqf8hnamsvg3r6k0yvrn

bc1qv0y2d8vcnu38tcf0xu8v7nx2xhtzzdcl94s3xf

bc1q0fztyvvf6lr35serala4g8tg54uav3w9azds50

0xa3442e789768C43Bd6DA036d1F6F26998432dc58

TQuvUgiipVEu1wTonkh1sRgjAqJwN48R5i

0xe8c8E2bfa900A05E8B2115b8f3Efeb9D17F9FdAB

TYmmUt6R4db6oW8DNwUxMgb18VNgbUD6MH

Important Note: The total withdrawal figures provided reflect only the volume withdrawn directly from the listed Stake deposit addresses. These do not represent the full scope of funds stolen by Medusa Drainer, as assets may have cycled through these addresses multiple times — via bridges, liquidity pools, or token swaps — and could have re-entered the same wallets in different forms or currencies.

Key Findings Overview



- **Initial Fund Flows:** In the early stages, the stolen assets were directly withdrawn to centralized platforms such as **TradeOgre** and **Binance**. However, over time, likely due to operational security considerations, the withdrawal patterns shifted. Currently, stolen funds are typically split into two (occasionally three) paths:
 - One route passes through the **COW Protocol**, where assets are exchanged and eventually sent to **Stake** via intermediary addresses.
 - The remaining paths cycle repeatedly between addresses, using the **COW Protocol** to convert assets into stablecoins or native ETH, before reaching their final destinations — or returning to **Stake** for additional laundering cycles.
- **Major Mixing Event – May 24, 2024:** On this date, funds from **Medusa Drainer 2** were combined with proceeds linked to **Pink Drainer**, split into three transactions of 60 ETH each, and sent to address [0x77a78d9e12b94825c02595aebc208915df495395](#). A portion of the funds was subsequently bridged via **Mayan Finance** to the **Solana** blockchain and withdrawn through the **EXOLIX** exchange.

- **Latest Stake Withdrawals:** The most recent confirmed withdrawal activity was observed at address [0xa5a062ceadc6c212b04c76987354372327be386d](#), involving:
 - **445 weETH**
 - **178 wstETH**
 - These assets were deposited into the **Zircuit Restaking Pool**. As of the latest observation, this address remains **active** and is considered the most operationally “alive” among all addresses associated with the Medusa Drainer ecosystem.
- **Most Personalized Entity – dol.eth:** The address [0x775b404e48ff523032ce9cc5483de2fef7690345](#), which appears in transaction chains alongside **Medusa Drainer 2** and **Stake**, has registered the ENS domain **dol.eth**, making it the most identifiable address in the flow. This wallet received **5 ETH** via a direct transfer from Medusa Drainer 2.

Summary



MedusaDrainer demonstrates typical behavioral patterns associated with wallet drainer operations: a rapid appearance, short-term activity, and eventual disappearance. Telegram accounts directly connected to the group — **@taomazov**, **@mazotao**, **@medusadrainersupport**, and **@mazovdusa** — have been observed participating in key drainer development communities such as **Drainer's Heaven**. Based on recent messages from the account **@mazovdusa**, it is likely that the operators have ceased activity and that MedusaDrainer will not return.

However, the official website **medusa.services** remains **online**, indicating the potential for reactivation under the same or a different brand.

According to ScamSniffer's 2024 drainer activity data, the number of phishing sites associated with MedusaDrainer began declining after their active period in March. This timeline coincides with the publication of the "Medusa Drainer Scammer Alert" message, suggesting that this marked the start of their operational decline.

A notable development occurred in the [ETHSecurityCommunity](#) chat, where a public investigation revealed links between scam service providers, drainer developers, and one of the space's most prominent actors — **Pink Drainer**.

Following this investigation, which has since been removed from Medium and is now accessible only via [web archive](#), many Telegram channels related to this ecosystem (including [Twitter Funhouse](#)) restricted public access or became private.

The **on-chain analysis** showed that the final destinations for MedusaDrainer funds included: **TornadoCash, Exolix, Bybit, Railgun, TradeOgre, and Stake.**

A particularly significant portion — approximately **\$445,000** — was traced to **Zircuit** via wallet [0xb83b5790f2bb98f72cf7294e71d56e3c0ba5363b](#), which still holds around **50 ETH**. Throughout their movement, the funds were often converted via **COW Protocol**. It was also established that **180 ETH** associated with Medusa Drainer 2 was mixed with funds tied to **Pink Drainer**, further confirming operational overlaps between the two.

How Not to Get Caught by Drainers



To protect yourself from wallet drainers, both technical and behavioral precautions should be taken:

Key Recommendations:

- **Zero Trust Approach.** Only interact with trusted, verified websites and official sources. Suspicious links should be analyzed using isolated environments (e.g., [Browser.lol](#), [any.run](#)) or scanned with [VirusTotal](#) or [Urlscan](#).
- **Diversification.** Avoid storing all assets in one wallet. Use separate wallets or devices for different purposes. If devices are unavailable, use separate browser containers (e.g., Firefox Multi-Account Containers) and disable JavaScript when possible.
- **Hardware Wallets.** Use hardware wallets to store private keys offline. This provides protection against phishing and malware.
- **Multisignature (Multisig) Wallets.** Require multiple approvals for transactions. Even if one key is compromised, funds remain protected.

- **Two-Factor Authentication (2FA):** Enable 2FA on all accounts, preferably using authenticators or hardware devices. Avoid SMS or voice-based 2FA due to vulnerability to SIM swapping.
- **Strong Passwords + Password Manager.** Use complex, unique passwords and manage them with a secure password manager.
- **Keep Software Updated.** Regular updates ensure protection against known vulnerabilities.
- **Verify All Addresses.** Clipboard hijacking and QR-based attacks are common. Always double-check recipient addresses before transferring assets.