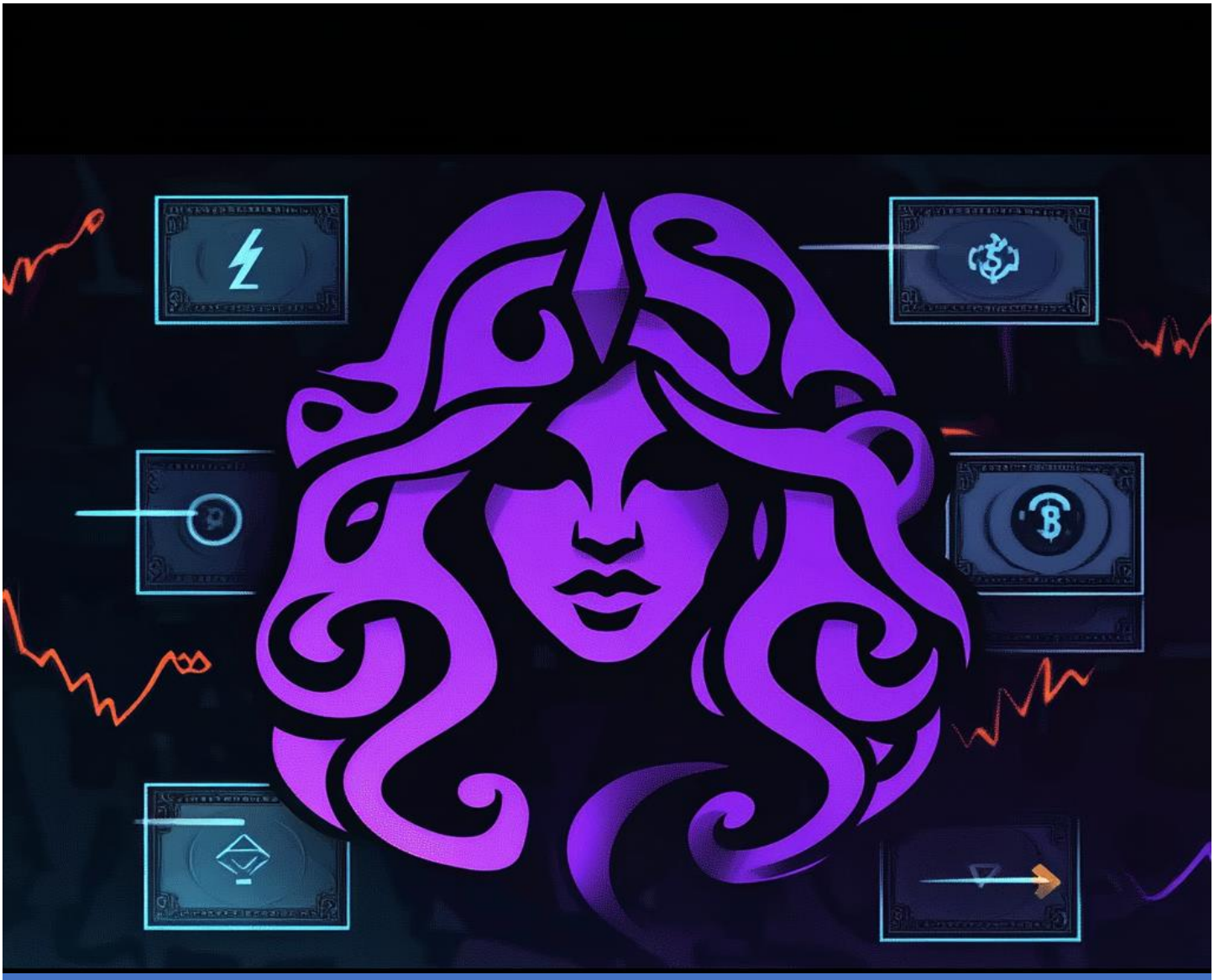


Drainer-as-a-Service (DaaS) Operations: Medusa Drainer

Under-the-radar asset draining from unsuspecting Web3 users

DEEPCODE AMLBot

Disclaimer: This report contains information and intelligence collected from a variety of sources. The data is presented "as is" and reflects the most accurate and current understanding available at the time of writing. While every effort has been made to verify the credibility and reliability of the information, it may be subject to change as new intelligence emerges. The authors make no guarantees regarding the completeness, accuracy, or timeliness of the content and accept no liability for any decisions made based on this report.

DeepCode & AMLBot Joint Investigation Overview

This investigation is the result of a collaborative effort between the **Deepcode** and **AMLBot** teams, combining expertise in blockchain forensics, cybercrime intelligence, and Web3 infrastructure analysis. Our joint mission was not only to uncover the inner workings of the Medusa Drainer operation and associated networks, but also to translate findings into actionable advice.

The investigation aims to provide an in-depth, multi-faceted analysis of the Medusa Drainer operation within the broader context of Drainer-as-a-Service (DaaS) model. We will conduct a deep dive into various key components of the operation to uncover how Medusa Drainer exploits unsuspecting Web3 users. The investigation will include the following:

Social Media Analysis:

We will examine the digital footprint of the Medusa Drainer operation, focusing on social media channels, including Telegram and other platforms, to trace the communication patterns, promotional tactics, and connections to other criminal activities.

On-Chain Advanced Investigation:

Led by AMLBot's subject-matter experts, we will analyze the blockchain transactions related to Medusa Drainer. By tracing the flow of stolen assets, we aim to uncover patterns of movement, identify key addresses, and expose the methods used to obfuscate the origin and destination of these illicit funds.

Domain and Infrastructure Providers Analysis:

A detailed investigation will be conducted into the domain names, and infrastructure supporting Medusa Drainer's phishing operations. This will include a thorough examination of any associated phishing websites.

Source-Code Analysis of Phishing Sites:

We will conduct a deep analysis of the phishing site code to uncover its underlying structure, techniques for deceiving users, and how it interacts with blockchain protocols.

Connections to Other Drainers:

We will explore the potential links between Medusa Drainer and other notorious drainer operations, such as Pink Drainer, Inferno Drainer, Angel Drainer. By examining shared tactics, infrastructure, and operators involved, we will determine whether Medusa Drainer is part of a larger coordinated effort.

This multi-pronged investigation seeks to identify and expose the full scale of Medusa Drainer's operations, its links to the broader drainer ecosystem, and the methods used to drain assets from Web3 users. Through this effort, we aim to contribute valuable insights into the fight against Web3-based cybercrime and phishing operations.

What are Crypto Drainers?

Crypto drainers have become a major threat in the Web3 ecosystem, responsible for substantial financial losses amounting to millions of dollars stolen from both individuals and organizations. These drainers function as phishing tools that impersonate legitimate crypto platforms, tricking users into signing malicious transactions that silently drain their wallets.

Beneath this broad definition lies a variety of deceptive techniques, often disguised as:

- airdrops
- free mint offers
- smart contracts containing tokens but requiring no gas

These tactics are highly lucrative for scammers because they target Web3 brands and projects directly—resulting not in stolen credentials or database leaks, but in the direct theft of cryptocurrency.

Once funds are drained from victims' wallets, attackers typically engage in laundering to reduce traceability and facilitate conversion to fiat currency. This process often involves routing stolen assets through mixers (hence the term "mixing"), decentralized exchanges, DeFi platforms, gambling sites, and similar services. By 2023, DeFi platforms had emerged as the dominant channel for such laundering operations.

Drainer-as-a-Service (DaaS) is a malicious business model where these tools are leased out to less technically skilled attackers. Similar to Ransomware-as-a-Service (RaaS), DaaS providers offer user-friendly dashboards, custom phishing kits, and even customer support—making wallet theft more accessible to novice cybercriminals.

The earliest crypto drainers emerged on underground forums around 2021, with a primary focus on compromising MetaMask wallet users. Since then, the landscape has evolved significantly. Today, many drainers operate under a "**Drainer-as-a-Service**" (DaaS) model, where experienced developers and cybercriminals offer turnkey infrastructure to affiliates for a one-time payment or a recurring subscription fee.

This model dramatically lowers the barrier to entry for would-be scammers. Every stage of the fraud operation—ranging from phishing page deployment to wallet-draining scripts—is pre-packaged and ready for use, requiring little to no technical expertise or upfront investment. In return, the service providers, or "operators", typically take a cut of the profits, earning between 5% and 25% of the stolen funds.

Market Penetration and Reach of Crypto Drainers

Drainers have seen a sharp rise in popularity in recent years. According to Chainalysis, the industry's quarterly growth rate in early 2023 even outpaced that of ransomware.

In 2024, ScamSniffer reported that the total amount of funds stolen by drainers reached approximately **$494 million**—a **67% increase** compared to the previous year. Interestingly, the number of victims only grew by **3.7%**, indicating that attackers are now extracting significantly larger sums per target.

This surge in drainer activity has been accompanied by increased chatter on underground forums. Kaspersky Labs notes that the number of darknet resources discussing drainer tools rose from **55 in 2022** to **129 in 2024**.

Among blockchain networks, Ethereum suffered the most severe losses. According to Scam Sniffer, the Ethereum network saw **$156.2 million** in total stolen funds, concentrated in some of the largest individual thefts.

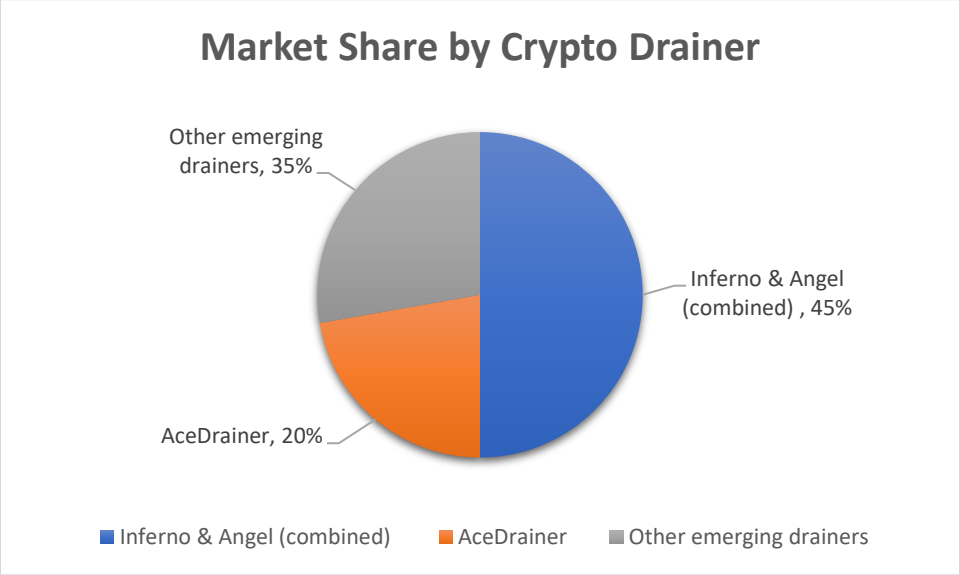
The drainer ecosystem itself began to consolidate and shift throughout 2024. In the first half of the year, three major players dominated the landscape:

- **Angel Drainer** – 42% market share
- **Pink Drainer** – 28%
- **Inferno Drainer** – 22%

By the end of May, **Pink Drainer** exited the market and was absorbed by **Inferno Drainer**. This led to a head-to-head competition in Q3 between **Inferno** (43%) and **Angel** (25%).

In a significant move at the end of October, **Angel Drainer absorbed Inferno**, consolidating their operations. Despite the merger, both entities remained active, now holding a **combined 45%** market share.

In the final quarter of 2024, the market share was distributed as follows:



While drainers were traditionally deployed via phishing websites, 2024 saw their expansion into mobile platforms. In March, a malicious app mimicking **WalletConnect** was discovered on the Google Play Store, targeting Android users as a new vector for drainer-based attacks.

Key Players in the Crypto Drainer Ecosystem

The crypto drainer landscape is shaped by a handful of dominant actors, many of whom have undergone shifts, rebrands, or consolidations over time. Below is an overview of the most prominent players, along with relevant investigations and references.

Inferno Drainer

- **Initial Activity:** Debuted in **November 2022**.
- **Code**: Likely developed by a **Russian programmer** based in **Astrakhan**.
- **First Exit:** Ceased operations after stealing **~$80 million** by **November 2023**.
- **Return & Merger:** Re-emerged in **May 2024**, and was later **acquired by Angel Drainer** in October 2024.
- **Modus Operandi:** Injects malicious JavaScript into phishing sites, exploiting integrations with **Seaport, WalletConnect, Coinbase**, and others.
- **Targeted Brands:** PEPE, COLAB.LAND, zkSync, MetaMask, and more.
- **Current Status:** Merged with Angel; the two now operate as a single entity "**Angelferno**" and collectively hold the **largest share of funds stolen** in recent high-profile thefts.

Angel Drainer / AngelX / Angelferno

- **Original Focus:** Operated across **EVM-compatible chains**, deploying smart contracts and targeting NFTs.
- **Expansion:** Recently added support for **Solana, TON, and Tron**, capitalizing on their relatively weak security tooling.
- **High-Profile Attack:** Gained attention after involvement in a **Ledger Connect Kit phishing incident**.
- **Rebrand:** On **31 August 2024**, relaunched as **AngelX**, introducing improved obfuscation and easier deployment.
- **Security Evasion:** Analysts report that AngelX has a significantly **higher evasion rate**, making detection by security vendors more difficult.
- **Operational Risk:** On **16 July 2024**, the team announced plans to shut down due to fears of their identities being exposed.
- **Merger:** On **20 October 2024** Angel Drainer acquired Inferno Drainer's infrastructure for **$501,000,000**, and rebranded as **Angelferno**. As of Q4 2024, Angel and Inferno together hold **45%** market share.
- **OSINT Links:**
    - **Angelferno** has been traced to **Russia** and is suspected to have ties to the **Crazy Evil** cybercrime group. One of the key **Angelferno** Telegram channels, **@avolneeupd**, is managed by **@avolnee** (ID: 7876081384), who is allegedly named "**Nikolai**". This user is

further linked to the website **angelferno[.]com**. Posts by **@avolnee** have been observed in both **English** and **Russian**.
    - The previous X.com account **"AngelDrainer"** has been linked to the **Telegram user** @Stopppmeeee (ID: 7202038529, display name: *"Drakan | AngelX (Only Real Account)"*), who appears to act as the '**CEO**' or lead operator of **Angelferno**.
    - This same user has also been connected to a **Solana (SOL)** address: 5rigLyzJa6vVDRzkWFntuSm1HJsnRtLh4SkiTWnTXEvx, based on Telegram-linked wallet tracking.
      A deeper analysis of this address can be found on **Arkham.com**.

Pink Drainer

- **Launch: April 2023**, with an early theft of **156 ETH**.
- **Developer Identity:** Allegedly created by a solo actor known as **PinkDeveloper**, previously active as "Blockdev" on **X.com** and **Discord**, posing as a crypto security researcher.
- **Social Media Presence:**
    - **"pinkdrainer_" on X.com / Twitter –** linked to **pink-drainer.eth**
    - **"pinkdrainer" on Instagram** (display name: "**Ace**") and **Discord** (ID: 1185102766440452161; registered: 15 December 2023)
- **Target Audience:** Initially aimed at **Chinese users**, whom the developer controversially criticized.
- **Milestones:** Became **multi-chain** within a month; passed **$1 million** in stolen funds by **July 2023**.
- **Exit:** Ceased activity on **17 March 2024**, accounting for **28%** of major thefts that year.
- **Downfall:** Fell victim to an **address poisoning scam** in **June 2024**, losing **10 ETH** to lookalike wallet addresses.

Ace Drainer

- **First Seen: January 2024**
- **Social Media Presence:**
    - Facebook account "**acedrainer**" links to a previous Telegram account of **Inferno Drainer** (t.me/mr_inferno_drainer) on 16 October 2023
    - Instagram account "**acedrainer**" (display name: "Drake") connects to **Inferno Drainer** logo
- **Notable Attack:** In **October 2024**, compromised over **400 DApps** by targeting the **Lottie Player npm package**, executing a **supply chain attack**.
- **Tactics:** Injected malicious scripts via third-party components used across decentralized apps.
- **Current Status:** Remains active alongside Angel, retaining a **20% market share** in Q4 2024.

Other Known Drainers

- **Cerberus**
- **Nova** (maintained by **CryptoGrab**, likely operated from **Russia)**
- **Medusa**
- **MS Drainer** (developed by a **Russian programmer**)
- **Venom**
- **Pussy**
- **Monkey** (devildrainer.eth)

🔍 🧩 In-Depth Analysis of Medusa Drainer: Uncovering Connections and Origins

The goal of this investigation is to identify the potential owners of **Medusa Drainer** and uncover any links to other prominent drainers in the ecosystem.

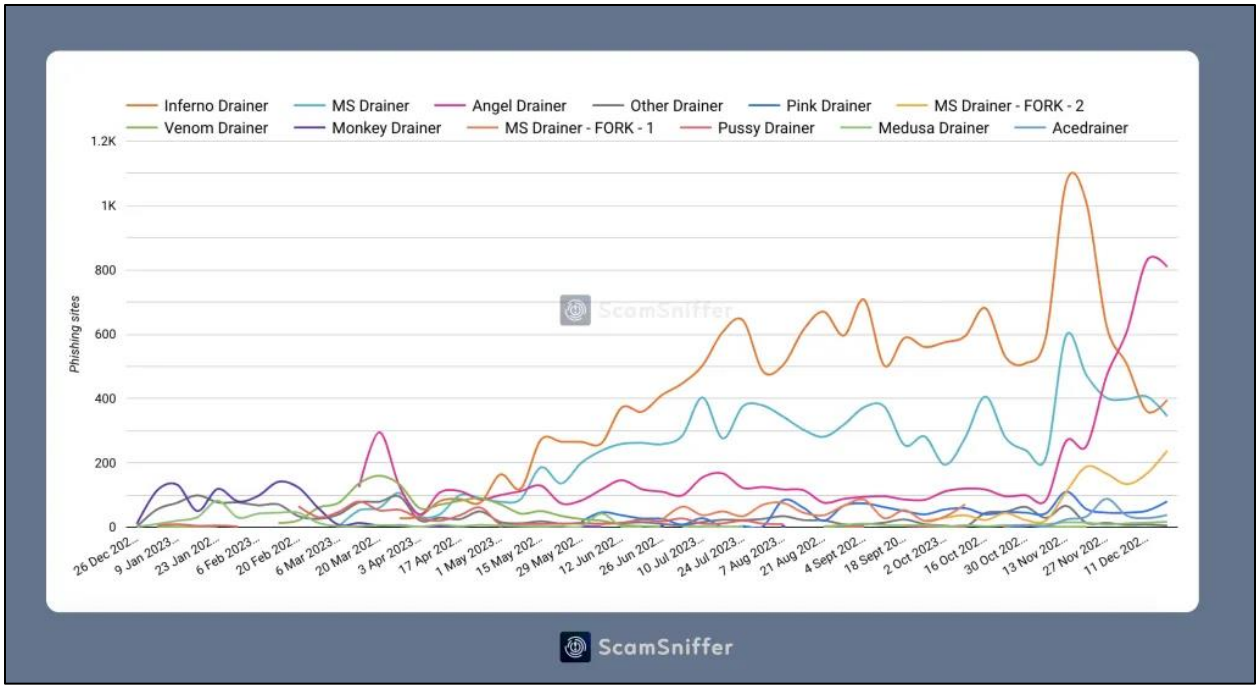
This section explores who the **Medusa Drainer** actors are, their origins, and what entities or operations have since replaced or absorbed them.

Medusa Drainer emerged on the exact day that **Inferno Drainer** announced their exit in November 2023, positioning itself as a successor—and an alternative to **Monkey**, **Venom**, and **Inferno** itself. In early January 2024, Medusa claimed to have drained over **$5 million** from victims, according to quetzal.bitso.com. For a deep dive into **Inferno Drainer**, refer to the comprehensive analysis by Group-IB.

Medusa Drainer and Its High-Profile Mentions

Medusa Drainer stands out as one of the key players in the 2024 drainer landscape, yet, compared to others, it has been less frequently observed in large-scale phishing attacks.

The chart below, sourced from ScamSniffer, illustrates this trend—**the green line represents phishing sites confirmed to be associated with Medusa Drainer, rarely surpassing 100 domains.**

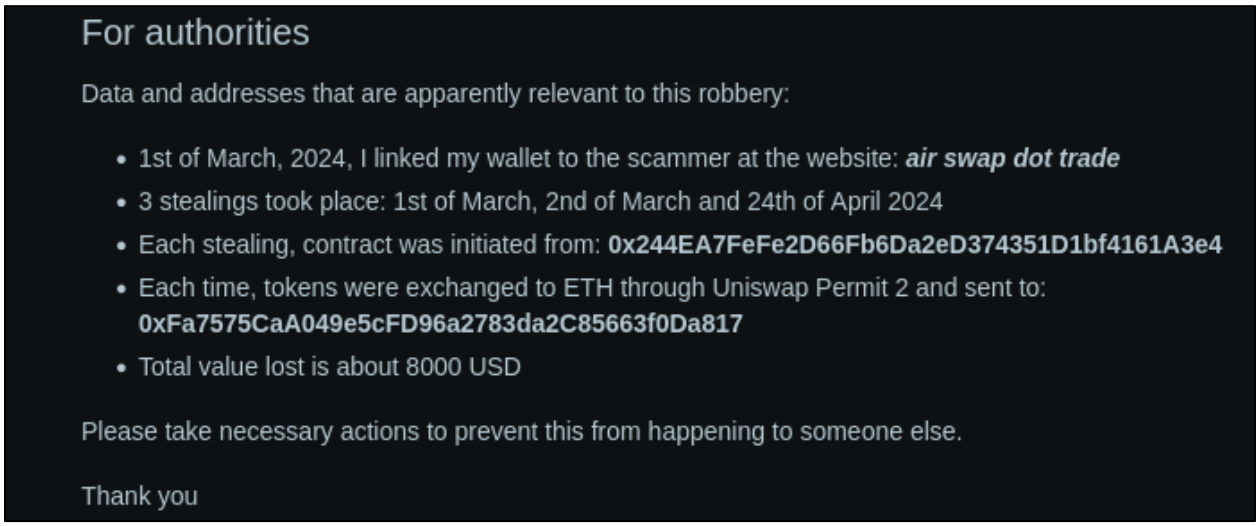


Target Audience and Attack Method:

Medusa Drainer primarily targeted **regular users**, avoiding large-scale, well-known hacks like **Angel** and **Inferno**. Infections often occurred through phishing sites or social engineering tactics. The drainer was frequently disguised as a token distribution (airdrop), prompting users to authorize the flow of funds via **Approval** or **Permit2** functions. This type of fraud is categorized as a **permission scam**.

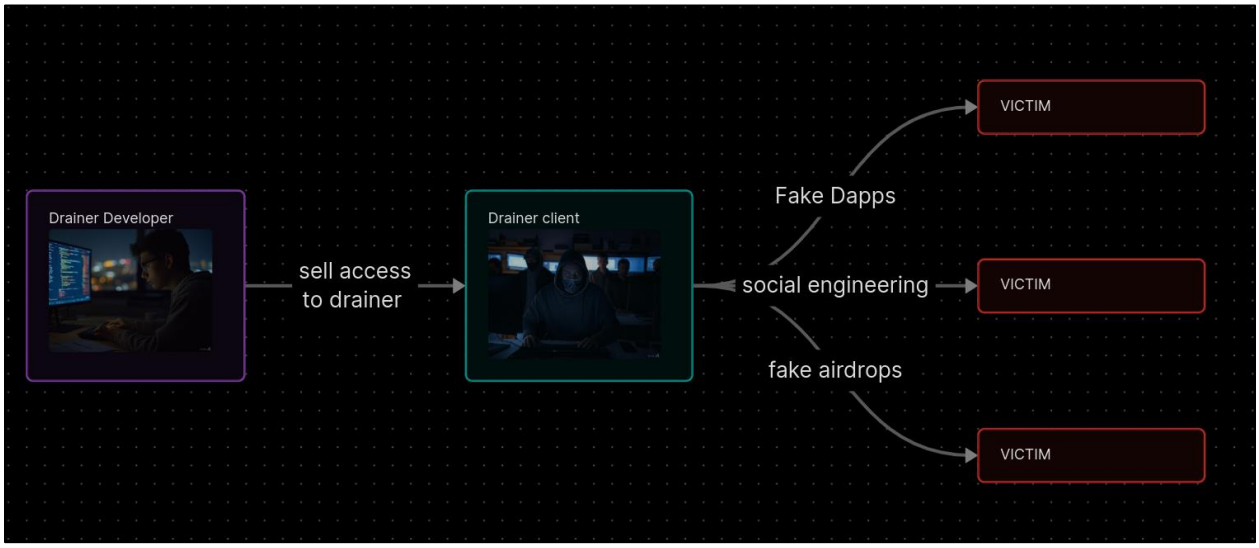
Case Example:

An automated scam report detailing one of Medusa Drainer's operations can be found here. Another notable instance of Medusa Drainer's activity involved scams spreading via **Reddit**, particularly in the UniSwap thread. A screenshot is provided below.



DaaS Model Evolution:

The most prominent drainer operators have transitioned to the **Drainer as a Service (DaaS)** model, marking the next stage in fraud evolution. Developers now act as service providers, offering access to drainers, control panels, operational proxies, and accounts on major platforms. Rather than interacting directly with victims, these developers profit by charging other scammers subscription fees for initial access and ongoing services. This model benefits developers in multiple ways, including broader scalability and reduced risk. The diagram below illustrates the Drainer-as-a-Service (DaaS) model used by Medusa.



How Crypto Drainers Reach Clients

Drainer developers typically acquire customers through three primary channels:

- **Telegram-themed chats**
- **Discord thread-based servers**
- **Clear Web, Deep Web and Dark Web forums**

These platforms host both public and private communities, where a wide range of fraud-enabling services are openly traded. These include:

- Rental of crypto-themed domain names
- Proxy server access
- Purchase of KYC-verified documents
- Hacked or newly registered accounts on platforms popular in the Web3 space (e.g., Telegram, Discord tokens, compromised Twitter/X accounts)

In effect, scammers can gain access to a complete toolkit with minimal effort—simply by joining a few key chat rooms. Developers, in turn, gain both a steady client base and ties to other malicious operators.

Medusa Drainer operated similarly

The developer promoted their services via a public Telegram channel, **@MedusaDrainer** (ID: 1784643705), first detected on **1 February 2024**, by the Telemetr.io monitoring system. At the time of discovery, the channel already had around **1,500 subscribers**. The last post was made on **13 August 2024**. Medusa Drainer reached its peak activity in **March 2024**, when it was associated with the creation of **100 to 200 phishing domains** containing its malicious code.

We found several user complaints and comparisons posted in other channels, suggesting that **Medusa Drainer lagged behind competitors like Angel Drainer** for multiple reasons:

- **Angel Drainer** only takes a **percentage of stolen funds** as payment, while Medusa charges upfront fees for access to files and control panels.


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 Emplo..., edited 3:24 PM

• Users reported **poor support** from the Medusa team, citing "stupidity and unprofessionalism" (source).

• Some alleged that **Medusa's developers defrauded their own customers**, disappearing with their money (source).

Studying these discussions also yields valuable OSINT about members of adjacent Telegram communities and the nature of their operations. For example, the top-right analysis posted on Telegram shows various Telegram users involved in cryptocurrency fraud.

TaoMazov – Alleged Creator of Medusa Drainer

The primary operator behind Medusa Drainer goes by the alias **"Tao"**, active on Telegram since at least August 2023. Previous usernames include **"taomazov"** and **"ycmarginal"**, both tied to Telegram ID: **6695770377**. Tao's current username is **"mazovdusa"** (ID: **109327337**), who has been linked to at least **26 Farsi-speaking or Iran-based Telegram groups**.

These Telegram groups show signs of suspicious and potentially harmful activity. Many pretend to offer financial help, jobs, or rewards for adding members, often using names of well-known Iranian figures to seem credible. Others promote temporary marriage or adult services disguised with religious language. Some groups use strange or random usernames (e.g., "jdjdjdbbrbrb", "dkcfkddksk", "jkgfddyii9") suggesting they might be run by bots or used for spam or scams. Taken together, these groups appear to be part of a wider network that takes advantage of people's financial needs, religious beliefs, or curiosity to deceive or exploit them.

User **"Tao"** (ID: **6695770377**) first appeared on **19 August 2023**, in the Telegram group **@curvefi** (ID: **1357982180**), introducing themselves with:

"hi i'm a beginner, can someone tell me whats the benefit to stake funds into a curve pool? sorry for dumb questions hehe".

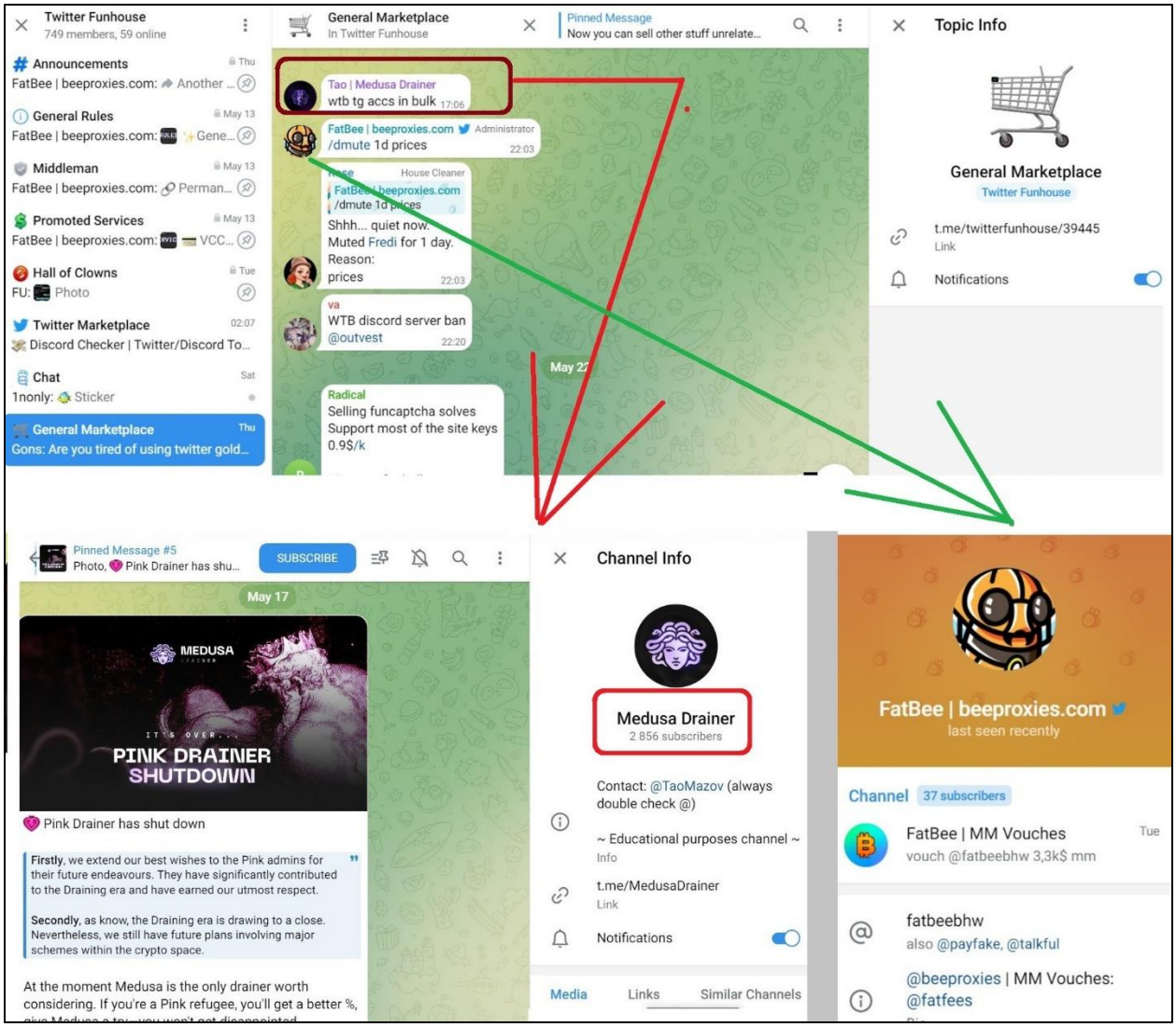
Interestingly, **Curve Finance** (curve.fi) was identified as one of the decentralized liquidity pools through which Medusa Drainer received transactions. A day later, on **20 August**, **"Tao"** (ID: **6695770377**) posted:

> *"I heard about **conic.fi** hack but you refunded ppls/gonna then its all good, and I have many friends investing in pools".*

Archived data from the Medusa Drainer Telegram channel (ID: 1784643705) also lists @**taomazov** (ID: 6695770377) as the official support and developer account. The account @**taomazov** is currently either deleted or banned, likely due to violation of Telegram's TOS. Message history indicates that the user was active between 19 August 2023, and 4 August 2024—a timeframe that aligns with the decline in activity on the @MedusaDrainer channel (ID: 1784643705).

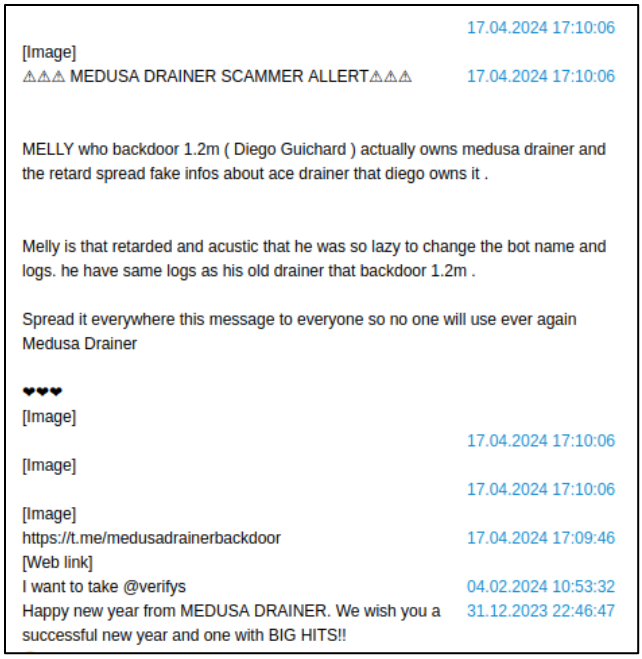
Further investigations show that **@mazovdusa** is a member of a private Telegram group named **"Drainer's Heaven"** (ID: **2398309960**), which has **1,002 members**. Among the participants is **@Angelferno_Admin** (ID: **7578452222**), who claimed that **Inferno Drainer** was sold and rebranded as **Angel Drainer**, now operating under the name **Angelferno**.

Additionally, a Telegram search disclosed a discussion within the ETHSecurityCommunity chatroom (ID: -1001372269197) about an investigation into another drainer—**Pink Drainer**—and its connections to the account and proxy provider FatBee (@fatbeebhw; beeproxies.com). A screenshot is provided below.



This chatroom had previously appeared in group discussions involving the user **@taomazov**.

Additional analysis of Telegram messages referencing Medusa Drainer—particularly in groups like “Drainer's Heaven” (ID: 2398309960) and “Twitter Funhouse” (ID: 2014336909)—has uncovered further insights into the group’s operational methods. Relevant screenshots are included below.



17.04.2024 17:10:06

[Image]

⚠⚠⚠ MEDUSA DRAINER SCAMMER ALLERT⚠⚠⚠ 17.04.2024 17:10:06

MELLY who backdoor 1.2m (Diego Guichard) actually owns medusa drainer and the retard spread fake infos about ace drainer that diego owns it .

Melly is that retarded and acustic that he was so lazy to change the bot name and logs. he have same logs as his old drainer that backdoor 1.2m .

Spread it everywhere this message to everyone so no one will use ever again Medusa Drainer

❤❤❤

[Image]

17.04.2024 17:10:06

[Image]

17.04.2024 17:10:06

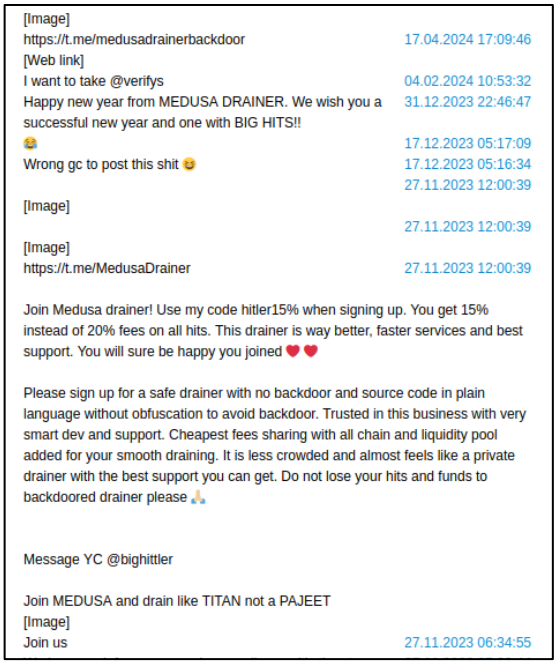
[Image]

https://t.me/medusadrainerbackdoor 17.04.2024 17:09:46

[Web link]

I want to take @verifys 04.02.2024 10:53:32

Happy new year from MEDUSA DRAINER. We wish you a successful new year and one with BIG HITS!! 31.12.2023 22:46:47



[Image]

https://t.me/medusadrainerbackdoor 17.04.2024 17:09:46

[Web link]

I want to take @verifys 04.02.2024 10:53:32

Happy new year from MEDUSA DRAINER. We wish you a successful new year and one with BIG HITS!! 31.12.2023 22:46:47

😂 17.12.2023 05:17:09

Wrong gc to post this shit 😊 17.12.2023 05:16:34

27.11.2023 12:00:39

[Image]

27.11.2023 12:00:39

[Image]

https://t.me/MedusaDrainer 27.11.2023 12:00:39

Join Medusa drainer! Use my code hitler15% when signing up. You get 15% instead of 20% fees on all hits. This drainer is way better, faster services and best support. You will sure be happy you joined ❤️❤️

Please sign up for a safe drainer with no backdoor and source code in plain language without obfuscation to avoid backdoor. Trusted in this business with very smart dev and support. Cheapest fees sharing with all chain and liquidity pool added for your smooth draining. It is less crowded and almost feels like a private drainer with the best support you can get. Do not lose your hits and funds to backdoored drainer please 🙏

Message YC @bighittler

Join MEDUSA and drain like TITAN not a PAJEET

[Image]

Join us 27.11.2023 06:34:55

The messages initially point to two individuals—Diego Guichard and Melly

Based on the context, Melly is suggested to be the true operator behind Medusa Drainer. Allegedly, Melly previously compromised Diego's account and falsely accused him of being the owner of **Ace Drainer**, another major drainer that remains active in the ecosystem. If this narrative holds true, it lends additional credibility to reports that Medusa Drainer vanished after defrauding its own customers. Alternatively, this could represent a targeted disinformation campaign by the **MedusaDrainerSupport** (ID: 5545771645) account aimed at discrediting Melly.

Further analysis of a promotional post reveals similarities in writing style between @MedusaDrainerSupport and @TaoMazov, suggesting a likely link between the two. This is reinforced by overlapping Telegram group activity, with both accounts appearing in the same clusters of drainer-related chats.

The account's history of usernames and aliases also reflects ideological views and offers direct ties to common scam tactics, including fake airdrop giveaways used to distribute drainer malware.

In a broader context, the **ETHSecurityCommunity** group (ID: -1001372269197) published an investigation exposing connections between scam infrastructure providers and key drainer developers—including ties to **Pink Drainer**. This indicates that drainer communities are aware of active investigations, which may explain why the original Medium article detailing this case has since been taken down. It remains accessible only via the WebArchive.org. Following this exposure, several drainer-themed Telegram chats—including **Twitter Funhouse** (ID: 2014336909), which is referenced in the report—have gone private or switched to restricted-access modes.

Mapping Online Activity of Medusa Drainer

The table below presents a summary of online accounts linked to Medusa Drainer.

Platform	Username / ID	Notes

Telegram	mazovdusa / 109327337	– Name: “Tao” – Historic Name: “**Fatme tvkli**” – Account: Premium – Profile photo uploaded on **20 October 2024** at 17.00 UTC +5. – Member of at least **29** Telegram groups / channels – **26** Telegram groups have content in Farsi language or are operated from Iran – Relevant cryptocurrency-related groups: o t.me/c/**2398309960 (“Drainer's Heaven”) – 14 messages** o t.me/**scamsniffer** (**3 messages**) o t.me/**ETHSecurity**
Telegram	taomazov / 6695770377	– Registration: 16 October 2023 – Historic username 1: ycmarginal – Historic username 2: ycmacn – Historic Names: o “Tao | Medusa Drainer” o “YC” – Account: Premium – Member of over **9** Telegram groups / channels – Relevant cryptocurrency-related groups: o t.me/**crypto4domain (2 messages)** o t.me/**extorters** o t.me/c/**2014336909 (1 message)** o t.me/**CryptoInsightPumpHub** o t.me/**scamsniffer (33 messages)** o t.me/**hypercycle_ai** o t.me/**GlobalPumpSyndicate** o t.me/**LayerZeroOfficialChat** o t.me/**curvefi (12 messages)** o t.me/c/**2068592120 (Sim land)** – **14 messages**
Discord	taomazov	– N/A
Telegram (Channel – historic; inactive)	Medusadrainer / 1784643705	– Admin: taomazov
Telegram (account; historic; inactive)	MedusaDrainerSupport / 5545771645	– Historic display names: o 16.01.2024 -> Hitler | Medusa drainer o 16.01.2024 -> Medusa drainer o 30.12.2023 -> Hitler (Medusa drainer support team) – Older display names: o Mr.BigBagsOnly(active) o Star d king

		○ Hitler (Medusa drainer support team) ○ Mr.Money(active) ○ Starbragger ○ Mr.Money – Historic usernames: ○ @bighittler ○ @MrBBonly ○ @mrbigbags ○ @ebetins ○ @grokcommunityairdrop – Member of over **20** Telegram groups / channels – Relevant cryptocurrency-related groups: ○ t.me/c/**1841068709** (**33 messages**) ○ t.me**/+Zn84U2JSMGMxZDMx** (**Angel X | Drainer**) – **271 messages** ○ t.me/**nftdrainers2** (**21 messages**) ○ t.me/**ChangeNOW_chat** (**3 messages**) ○ t.me/**verifys** (**1 message**)
Telegram (Channel – historic)	Ycmarginal / -1002203693502	– Name: "MEDUSA DRAINER SCAM" – 1 subscriber
Telegram (Channel – historic)	Ycmacn / -1001851253491	– Registration: 26 August 2023 – Name: "YC" – 4 subscribers

Estimated Number of Victims and Total Funds Stolen by Medusa Drainer

Public Reports and Alerts:

Several credible alerts have documented major thefts attributed to Medusa Drainer:

- $792,496 (USDC) — reported by MistTrack (MistTrack.io) on 11 January 2024
- ~$900,000 (299 ETH) — reported by MistTrack (MistTrack.io) on 11 January 2024
- $808,304 (USDC) — reported by MistTrack (MistTrack.io) on 11 January 2024
- ~$300,000 – reported by Quetzal article published on 3 May 2024

According to the creators, they claimed to have stolen over **$5 million** in the **first week alone**.

Associated Medusa Drainer Tags and Smart Contracts:

We identified several addresses tagged to Medusa Drainer activity:

- **Medusa Drainer 1**: 0xFa757575CaA049e5cFD96a2783da2C85663f0Da817
  - Refer to the metasleuth.io report for a summary.
  - This wallet is also linked to accounts on Rarible and OpenSea.
- **Medusa Drainer 2**: 0x111117d0c05573b49B32eF30Dc031dD9eD022099
  - Refer to the metasleuth.io report for a summary

    - This wallet has active accounts on both Rarible and OpenSea.
    - This address was actively used to funnel phishing contracts. Interestingly, it sometimes returned leftover gas ("change") from transactions.

- **Fake_Phishing26988**: 0x1x1a42605d92c210e4be47a6363046c591659ab444
    - Referenced in MistTrack's malicious activity report.
- **Fake_Phishing268902**: 0x009515EfabCccdBAfA485f3919d94C85Ff23Ba75D
    - Mentioned in Quetzal's drainer report.
- **Fake_Phishing328573**: 0xaC65360aF5a8AE5ec45AD0Bf2A7Ec063a38e2161
    - Flagged by CryptoEvgen for involvement in Medusa Drainer withdrawals.
- **Fake_Phishing328557**: 0xda2dF35CDDA2C26D2473AAB2Ca1d6C15d58Ddd96e
    - Participated in a known Medusa Drainer-linked withdrawal.

🔄 Transaction and Victim Analysis via AMLBot.com

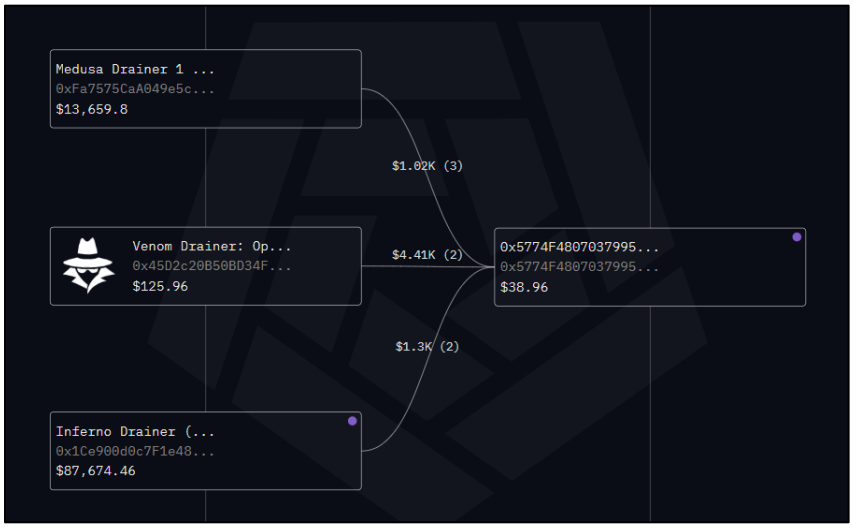
An on-chain analysis of incoming transactions to the known addresses reveals the following:

- **Total stolen funds**: ~$5,500,000 USD (calculated based on token value at the time of each transaction).
    - This figure casts doubt on the creators' claim of earning over $5 million in their *first week*, unless a significant number of additional, untagged addresses were used.
    - In particular, the wallet [**663f0da817**] interacted with **Bybit Thief 2025**, who routed **0.67467505 BTC** (approximately **$56,208.85 USD**) through the same address.
- **Median value per transaction**: ~$3,800 USD
    - The distribution is highly skewed, with a few large hacks contributing the majority of the stolen funds.
- **Total number of incoming transactions per address**: ~1,547
    - Represents an upper bound of potential victim interactions with the drainer.
- **Estimated number of unique victims**: ~870 unique sender addresses were identified.
    - Suggests a more conservative but realistic victim count.

On-Chain Links – Inferno, Venom, and Medusa Drainers

Blockchain analysis through Arkham.com has revealed that the **Inferno**, **Venom**, and **Medusa** drainers have conducted transactions with the wallet address **0x5774F4807037995f56604e3AA1Efc4fe06D478Ea**, which is likely associated with the **eXch[.]ch** non-KYC exchange.

A screenshot illustrating these interactions is provided below.



🔗 On-Chain Transaction Flow Analysis – Medusa Drainer

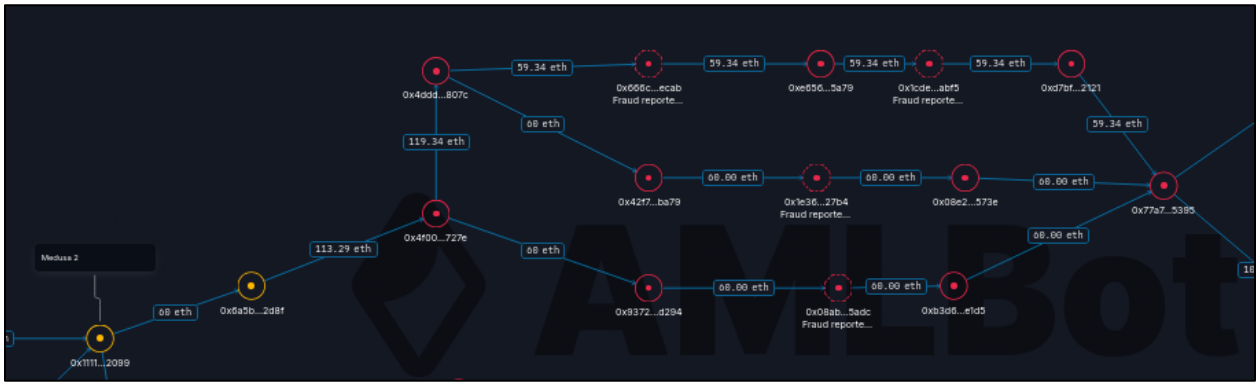
AMLBot team conducted an in-depth on-chain investigation using AMLBot Pro, focusing primarily on two key addresses labeled as Medusa Drainer 1 and Medusa Drainer 2. These tags were previously identified in scam analysis reports.

Tracked Addresses:

- **Medusa Drainer 1: 0xFa7575CaA049e5cFD96a2783da2C85663f0Da817** (NFT listed: Unidentified contract 97322167-c8bc-4828-9c87-ec9f7058fdd2 – linked to the phishing domain pendlev2.top)
- **Medusa Drainer 2: 0x111117d0c05573b49B32eF30Dc031dD9eD022099**
    - Used extensively for deploying phishing smart contracts and initializing malicious transactions.

🐙 Medusa Drainer 2: Fund Movement Overview

A transaction graph was built to trace how funds flowed through the Medusa Drainer 2 address. According to a report by @CryptoEvgen, the address served as a collection hub for victim funds, pooling approximately **180 ETH** before dispersing them through intermediaries.

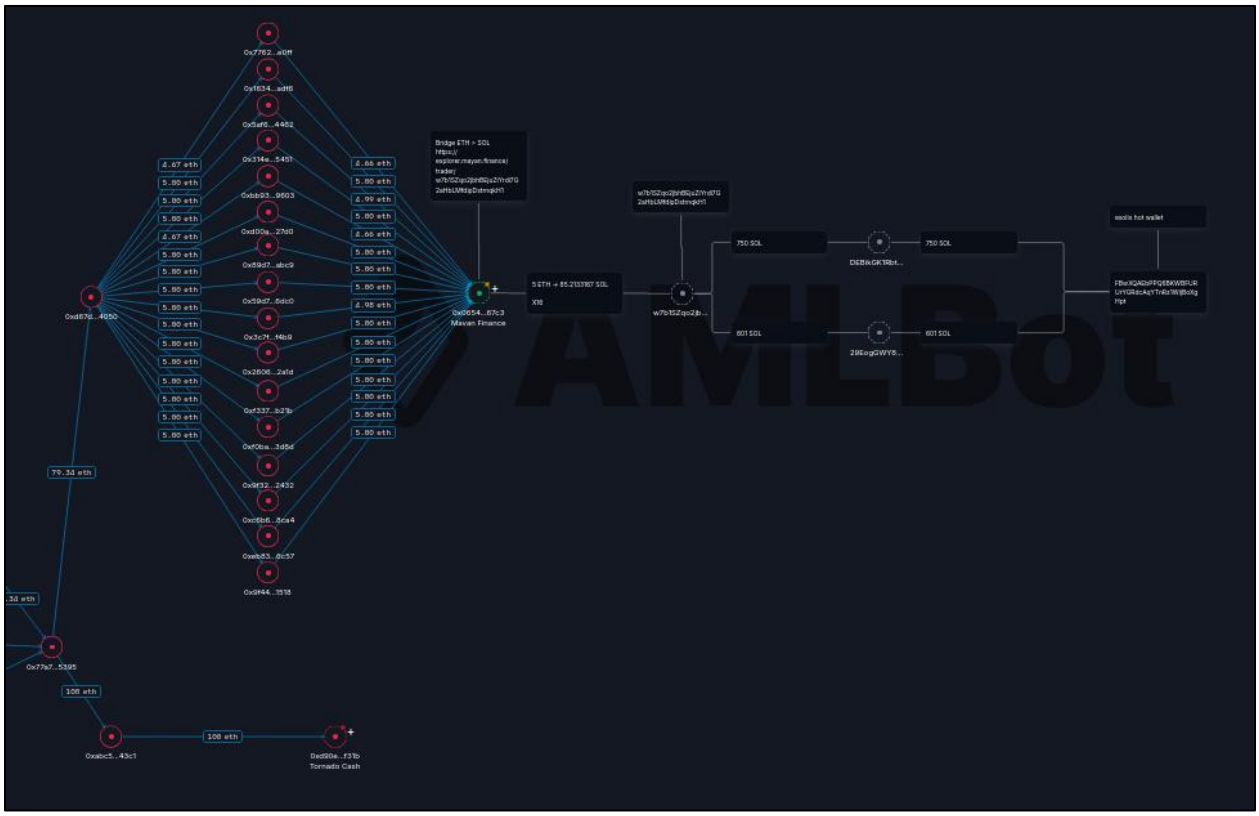


Note: *Transaction graph for **Medusa Drainer 2** built using AMLBot Pro.*

Key Steps in the Transaction Flow:

- Funds first routed through a disposable address:
    - 0x77a78d9e12b94825c02595aebc208915df495395
- On **18 October 2024**, the total amount was split:
    - **100 ETH** sent to **Tornado Cash** – anonymized and untraceable beyond this point.
    - **80 ETH** sent through **Mayan Finance Bridge**, migrating assets to the **Solana blockchain**.
        - Final destination: **1350 SOL** deposited into the **EXOLIX exchange**.
- At this point, further tracing ends due to a lack of public transparency from EXOLIX.

An additional transaction flow chart is provided below.



*Note: Transaction graph for **Medusa Drainer 2** built using [AMLBot Pro](#).*

Medusa Drainer 1: Continued Movement and Laundering

While Medusa Drainer 2 was used for early-stage phishing contract deployment, Medusa Drainer 1 remains active with sporadic withdrawal patterns. A notable portion of the ETH has been routed through various services for laundering and obfuscation:

Notable Transfers & Services Used:

- **~312 ETH** transferred to **TradeOgre** and **Railgun** — Railgun being a well-known privacy protocol.

- **COW Protocol** frequently used to swap tokens before withdrawals.
- Final destinations include **gambling platforms** such as **Stake**, and exchanges like **Bybit** and **TradeOgre**.

Transaction Flow Summary:

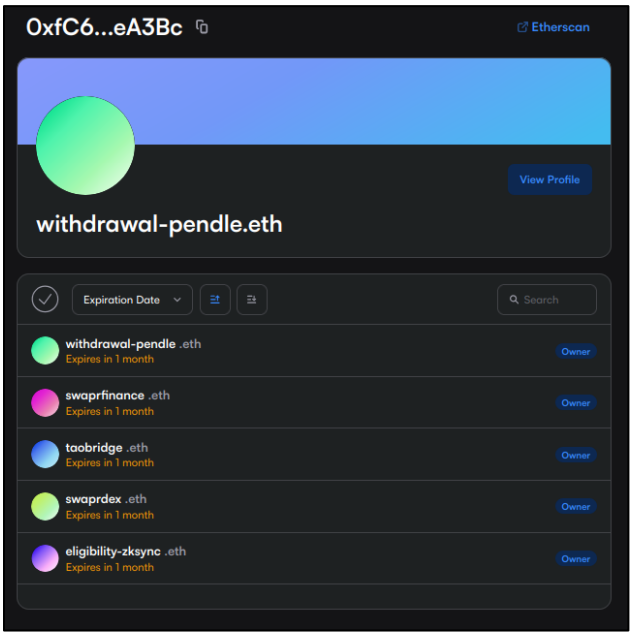
- **22 February – 23 May 2024**:
    - ~300 ETH moved to **TradeOgre** via intermediate wallets.
- **24 May – 18 October 2024**:
    - ~180 ETH laundered through **Tornado Cash** and **Mayan Finance Bridge**.
- Smaller amounts (e.g., **8 ETH**) routed through intermediaries to **Bybit**, which saw outgoing transactions from **21 April to 30 August.**

🧩 🎃 Cross-Linking Clues: ENS Domains and Medusa Drainer Overlap in a Key Intermediate Wallet

Further investigation into one of the intermediate wallets has revealed valuable insights into the fund transfer trail following interactions with the **Stake gambling platform**. This address received funds from **0xfC6C479CBB9dB178E5F959CFc56d790B1D3eA3Bc**, a wallet tied to several **ENS (Ethereum Name Service) domains**.

For context, **ENS domains** function similarly to web domains in traditional Web2 systems—e.g., "google.com"—but are instead mapped to blockchain addresses. These human-readable names are often registered temporarily and can help identify behavioral patterns or track affiliations between threat actors.

ENS Domains Linked to 0xfC6C479CBB9dB178E5F959CFc56d790B1D3eA3Bc (registered on **Opensea.io**):



- withdrawal-pendle.eth (registered on 25 April 2024)
- swapdex.eth (registered on 19 September 2021)
- taobridge.eth (registered on 26 April 2024)
    - Archived version redirects to taobridge.org (inactive)
    - Further investigation revealed a likely structurally similar site: taobridge.xyz
    - Publicly reported as malicious: Scam Report
- swapfinance.eth
- eligibility-zksync.eth (registered on 21 May 2024)

Transaction Footprint & Ties:

- This wallet received funds from **TradeOgre**, similar to other addresses in the Medusa Drainer laundering chain.
- It also **interacted with** fatfeemiffleman.eth—not to be confused with fatfee.eth—a known **guarantor** (trusted person) in the **TwitterFunhouse** community (a 'marketplace' for illegal, cracked, and stolen accounts).
    - This operator was previously linked to **Pink Drainer** and exposed in a prior investigation, which traced their identity back to a **Macedonian developer**.
    - Their role extended beyond guarantor services, suggesting deeper involvement in scam facilitation.
        - ❖ Full background: Heiner's Pink Drainer investigation (Archived)

🕸 Broader Drainer Ecosystem Ties:

This intermediate address appears consistently connected to multiple **major drainer groups**, including:

- **Angel Drainer**
- **Inferno Drainer**
- **Pink Drainer**
- **Ace Drainer**

The convergence of these interactions, ENS registrations, and service overlaps points to a shared infrastructure or close-knit operational network among the top-tier drainer operators.

💰 Final Trace: Latest Known Destination of Medusa Drainer Proceeds

Tracing the transaction flow to Bybit and TradeOgre reveals that, via the intermediate address **0x8fc43d983a8e807705120f5ec6493c561f6db33c**, an additional **25 ETH** was transferred to the wallet **0xb83b5790f2bb98f72cf7294e71d56e3c0ba5363b**.

This later address remains active and is currently holding **approximately 50 ETH**, while around **445 weETH (~$973,000)** and **178 wstETH (~$441,000)** have passed through it. A substantial share of these funds—specifically the **178 wstETH**—was deposited into the **Zircuit Restaking Pool**, marking this address as the **latest confirmed location of Medusa Drainer's stolen assets**.

Behavior Consistency:

The transactional pattern closely mirrors that of **Medusa Drainer 1**, — receiving ETH via the **COW Protocol** and subsequently converting it through a sequence of ETH derivatives in ERC-20 form. The systematic conversion and rewrapping of Ethereum includes:

- **ETH → eETH → weETH / wstETH → stETH → wstETH**

These token swaps likely aim to obfuscate traceability while maintaining liquidity and minimizing slippage—typical tactics in professional laundering operations.

Key Transactions:

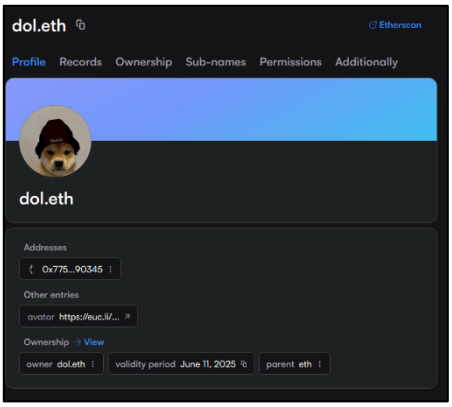
- [445 weETH to Zircuit (TX)]
- [178 wstETH to Zircuit (TX)]

Suspect Address:

- [Wallet 0xb83b5790f2bb98f72cf7294e71d56e3c0ba5363b] (registered on **Opensea.io**; linked to t.me/ClaimCake (display name: "PancakeSwap - CAKE")

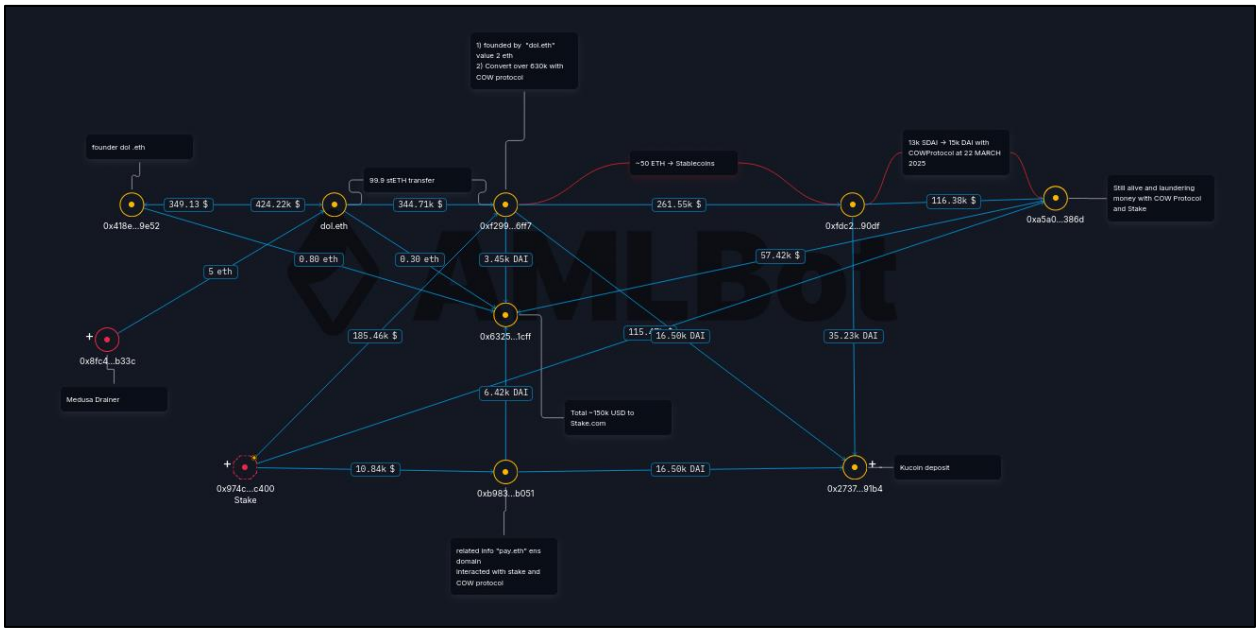
This address should be monitored closely as it may either serve as a final destination before off-ramping or as a temporary holding point pending further laundering activity.

Connections Between Medusa Drainer 1 and dol.eth



The address **0x775b404e48ff523032ce9cc5483de2fef7690345** (registered on **Opensea.io** in **April 2024**), which is involved in a transaction chain with **Medusa Drainer 2**, is also the registrant of the ENS domain **dol.eth**. This address has shown significant activity on the **COW Protocol**, where it consistently converted **ETH** and **stETH** into stablecoins such as **USDT**, **USDC**, **sDAI**, and **DAI**.

It was also involved in the transfer of approximately **100 stETH**, suspected to be illicitly obtained. These funds were sent to **0xf2999210f49f5210ffcbdb07b14d3b8792236ff7**, where they were split evenly: one half was routed through the **COW Protocol**, while the other half was sent to an intermediate address **0xfdc2790f3c0186f914b43c3be47bcbffabb290df**. From there, the funds ultimately reached a previously identified wallet (**0xFdc2790f3c0186f914B43C3bE47BcBFFAbb290df**) in the form of **stablecoins**.



Note: *Transaction graph showing connections between Medusa Drainer 1 and dol.eth built using [AMLBot Pro].*

Stake Withdrawal Analysis Related to Medusa Drainer

As part of the on-chain investigation, a data request was submitted to **Stake** to obtain information about withdrawals from deposit addresses linked to **Medusa Drainer 1**. The request returned detailed records for two specific Ethereum addresses:

Deposit Address 1: 0x8261f516b0221633f2343baa5944f9f67874dbda

- **Blockchain:** Ethereum
- **Withdrawal Assets:** ETH, USDT
- **Approximate Withdrawal Volume:** ~$300,000
- **Activity Window:** 26 July 2024 –20 January 2025
- **Connected Recipient Addresses:**
    - 0xA5A062cEadC6C212b04C76987354372327be386D
    - 0xf2999210F49F5210FfcBDb07b14d3b8792236FF7
    - 0xE4e2620d05D4B2004A6EE3E183b94D0DEB881B98
    - 0x5022F184b7E9E05A0cc60811806Ad7Bc6A972b61
    - 0xB98310E85D68b888eEc216cDFb9Ce1Ef545cB051
    - 0xb09e1335aE962c6a88C7018e3393784b760638B2
    - 0x0DDbAb11Aac0301f32964F76a029Bdef0c92f6f5
    - 0x6cB33dF933eC7aac60F2640D07a5E744317651Af

Deposit Address 2: 0xe7d6bd1b2a8a764ef2722f41e939db4936ff048b

- **Blockchain:** Ethereum
- **Withdrawal Assets:** TRON, Monero (XMR), ETH, BTC
- **Approximate Withdrawal Volume:** ~$650,000 (in USDT, DAI, USDC) and ~$450,000 in XMR
- **Activity Window:** 6 October 2024 –14 December 2024
- **Connected Recipient Addresses:**
    - Ethereum:
        - 0x86e5d3c1edfe442bd276508ad897e6154cb05c39
        - 0x0CB6aa8C9fBe844ba979Fa6DAD1473bD394a2db1
        - 0xa3442e789768C43Bd6DA036d1F6F26998432dc58
        - 0xe8c8E2bfa900A05E8B2115b8f3Efeb9D17F9FdAB
    - Tron:

        - TTt4eiHpCXxMToHvhbwDy9AYgbvNkjhcfn
        - THqqfBjJLm5S8SS4dhUSnCEksyZJ1LrW6i
        - TJaRSHSicV51wbJ6RAzK53WUVPNjE6FTD8
        - TQDMqzNgpCeBo7G8WNQazckRAXikWdCeX1
        - TAHvN5vBJGwY2g2TWDvpJ5VQL62bbGVJjy
        - TJZ2MNXdhSLgknNvmDRPNbppHaLn4VjzcS
        - TNN36i7aD4c26wJTZLtUS2tUFVV2WW5dLz
        - TM2KGMRG5KzsMbQWSdDh9ByShknm1zkh5j
        - TYmmUt6R4db6oW8DNwUxMGb18VNgbUD6MH
        - TQuvUgiipVEu1wTonkh1sRgjAqJwN48R5i
    - Monero:
        - rffGCKC7Mk4cQ5aUGg8pfRe3MPC7Cy8gfe:661320
        - rdPeCfko28cCLNbY8noXGV4ycZ3TGCSnM:0
        - rffGCKC7Mk4cQ5aUGg8pfRe3MPC7Cy8gfe:441743
    - Bitcoin:
        - bc1qvg7nrph4pgqpjrlpj6rqf8hnamsvg3r6k0yvrm
        - bc1qv0y2d8vcnu38tcf0xu8v7nx2xhtzzdcl94s3xf
        - bc1q0fztyvvf6lr35serala4g8tg54uav3w9azds50

The withdrawal figures shown above reflect the total outflows from the analyzed Stake deposit addresses **associated with Medusa Drainer**, not the full scope of stolen assets. Due to fund cycling (e.g., routing through liquidity pools, bridges, and swaps), the same wallet could receive assets multiple times in different forms or denominations.

Key Findings

- **Initial Fund Flow:**

  The stolen assets were initially routed directly to **TradeOgre** and **Binance**. However, over time — likely for operational security — the laundering strategy evolved. Funds began to split into two (occasionally three) distinct paths:

    - One branch typically passes through the **COW Protocol** before reaching **Stake**, often via multiple intermediate wallets.
    - The other branches frequently loop through the **COW Protocol** to convert into **stablecoins** or native **ETH**, then either settle in final destinations or return to **Stake** for further laundering cycles.

- **24 May 2024 – Cross-Drainer Fund Mixing:**

  On this date, assets from **Medusa Drainer 2** were mixed with funds from victims associated with the **PINK Drainer**. The mixed funds were divided into three parts of **60 ETH** each and sent to a single address: 0x77a78d9e12b94825c02595aebc208915df495395.

  From there, a portion was bridged via **Mayan Finance** to the **Solana** blockchain and later deposited into the **Exolix** exchange through a Solana wallet.

- **Latest Stake Withdrawals:**

  Withdrawals from **Stake** were last observed at the below address:

  - 0xa5a062ceadc6c212b04c76987354372327be386d, totaling **445 weETH** and **178 wstETH**. These funds were then deposited into the **Zircuit Restaking Pool**.

- **Active Address Highlight:**

  The address 0xa5a062ceadc6c212b04c76987354372327be386d remains active and is currently the most operational wallet linked to the laundering operation.

- **Notable Identity Clue – dol.eth:**

  A key address appearing in the fund flow chain, 0x775b404e48ff523032ce9cc5483de2fef7690345 — is registered under the ENS domain **dol.eth**, making it the most personalized entity identified so far. It also received a **direct transfer of 5 ETH** from **Medusa Drainer 2**, further linking it to the laundering network.

🧮 🔗 📋 Social Media and On-Chain Analysis Summary

MedusaDrainer follows patterns commonly seen in similar crypto threat actors — making a sudden appearance, operating intensively for a short period, and then vanishing. Telegram accounts directly tied to the operation (e.g., **@taomazov**, **@medusadrainersupport**, **@mazovdusa**) were active in prominent drainer development Telegram chats like **Drainer's Heaven**. Based on recent posts from **@mazovdusa**, the group has ceased operations and is not expected to return. However, the **medusa.services** website remains online, and indicators suggest they may not be entirely dormant—activity continues both on Telegram and through on-chain transactions, pointing to the possibility of a future reactivation or rebrand under a different identity.

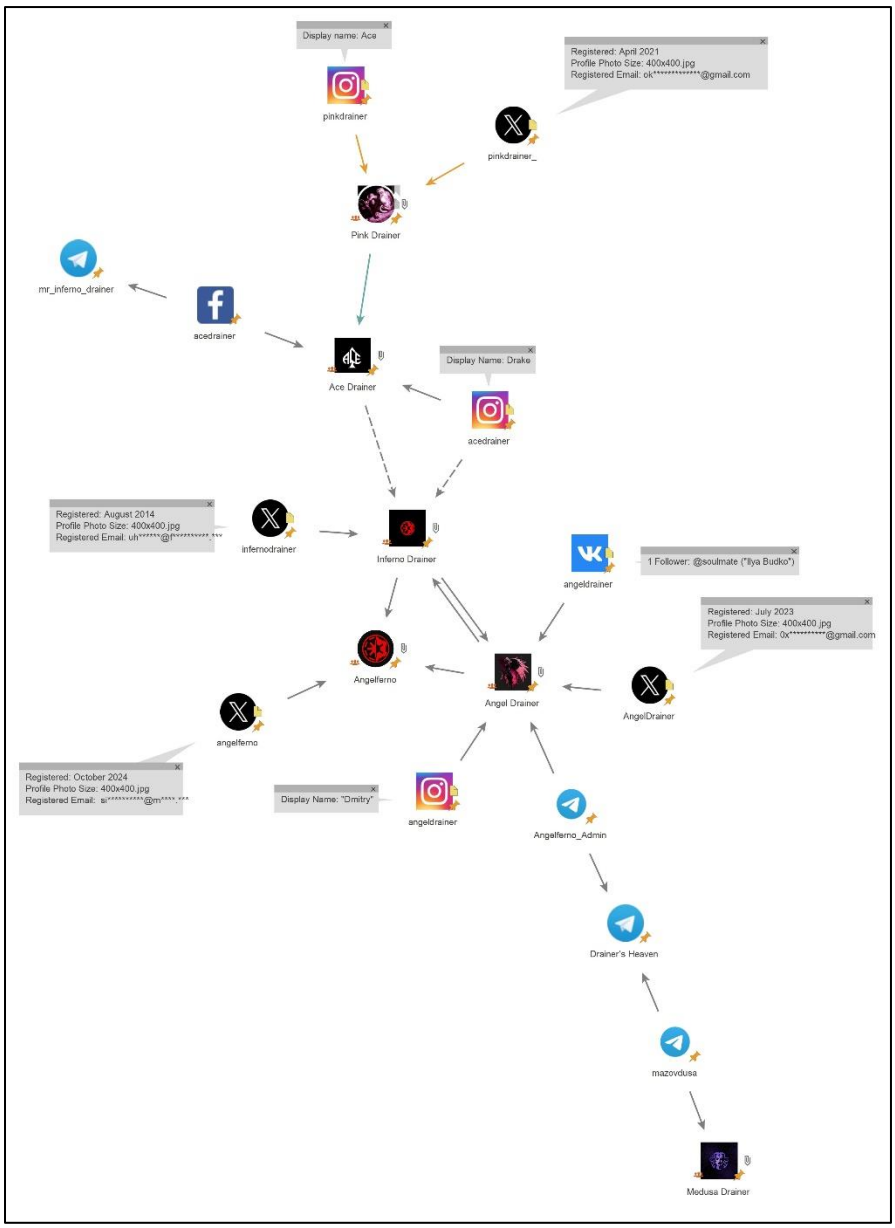
According to **ScamSniffer's 2024 drainer activity data**, phishing domains associated with Medusa Drainer have steadily declined since their peak in March. This downturn aligns with the appearance of the "**Medusa Drainer Scammer Alert**" message, signaling the start of their decline.

An in-depth investigation published in the **ETHSecurityCommunity** Telegram group uncovered direct ties between scam service providers, various drainer developers, and one of the most prominent entities in this ecosystem — **Pink Drainer**. The drainer community has clearly taken notice: the original Medium link to the investigation has been deleted and is now only accessible via **Webarchive.org**. Following this, several related Telegram channels, including **Twitter Funhouse** (mentioned in the report), switched to restricted or private modes.

Notably, there are several overlapping connections between **Medusa**, **Pink**, **Ace**, **Inferno**, and **Angel** Drainers. The Instagram account **“pinkdrainer”** uses the display name **“Ace”**, which aligns with a Facebook account named **“acedrainer”**—this Facebook profile is linked to a previous Telegram handle associated with **Inferno Drainer** (**t.me/mr_inferno_drainer**). Additionally, another Instagram profile with the handle **“acedrainer”** and display name **“Drake”** is visually linked to **Inferno Drainer** through its use of the group's logo.

Our social media investigation also found that **@mazovdusa** is a member of a private Telegram group named **“Drainer’s Heaven”** (ID: **2398309960**), which is also joined by **@Angelferno_Admin** (User ID: **7578452222**), further indicating cross-collaboration or shared infrastructure between these actors.

Below is a graph depicting the social media relationships between Medusa, Pink, Ace, Inferno, and Angel Drainers.



The **on-chain investigation** confirmed that the stolen assets ultimately flowed to several known services: **TornadoCash**, **Exolix**, **Bybit**, **Railgun**, **TradeOgre**, and **Stake**.

Notably, a substantial portion of funds — approximately **$445,000** — was transferred to **Zircuit**, originating from wallet **0xb83b5790f2bb98f72cf7294e71d56e3c0ba5363b**, which still holds around **50 ETH**. On the path to Zircuit, the assets were frequently routed through **COW Protocol** for token swaps. Additionally, **Medusa Drainer 2** withdrawals included **180 ETH** linked to another actor affiliated with **Pink Drainer**.

Domains & Server Infrastructure

The primary domain associated with the Medusa Drainer operation is **medusa.services**, registered on **25 October 2024** via **PDR Ltd. d/b/a PublicDomainRegistry.com**. The domain is protected by **Cloudflare**, and its **favicon hash** is **435747183**.

Server banner analysis reveals a **Cache-Status: "Netlify Edge"**, indicating the use of **Netlify (netlify.com)**—a platform commonly used for building and deploying websites. The website lists a **Telegram Premium contact** under the handle **@mazovdusa**.

The jQuery script located at "assets/js/script.js" on **medusa.services** includes inline comments in **Russian**, potentially suggesting the developer's origin or linguistic background.

Further infrastructure analysis via fofa.info identified:

- **20 unique IPs** across **16 subnets**, all hosted on **Amazon Web Services (AWS)**
- **17 servers located in Ashburn, Virginia**
- **1 server in Columbus, Ohio**
- **1 server in Mumbai, India**

A detailed summary table of the infrastructure findings is provided below.

Servers	IP Geolocation	Notes
52.219.110.218, AMAZON-02	Columbus	https://medusa.services-s3bucket**petadoption**cb20dce5-1xrl7dzw3vzdi.s3.us-east-2.amazonaws.com Server: AmazonS3 Server: AmazonS3 X-Amz-Id-2: fR9eJzkcl0fTUt/uvSxMuuVn591iZbwuwuAe5dAcAEhTwtqqvJR5AA8IBn6VVd4Y0uoL55b72h0= X-Amz-Request-Id: YYGK9B8EKAHVHVDZ
52.216.216.1, AMAZON-02	Ashburn	dev.medusa.services.s3.amazonaws.com X-Amz-Id-2: 4W1RnqqySOQdkfs7k5q/PLnnABp8kiaKuhxX2bK7uooWaqDn9F59doPoF/0XP9atkAEIHW+sdaE= X-Amz-Request-Id: H9PD9E7QF7SE6NMR
3.5.29.50, AMAZON-AES	Ashburn	medusa.services-s3bucket**petadoption**cb20dce5-19dvoixbafl77.s3.amazonaws.com

		X-Amz-Id-2: 2LFbpNqOwslkUvi67gh/utjJUFqeXynhJNIMihsHHXCtyGIjteANMroQEf5OAzZSAVQKbkCgrgI= X-Amz-Request-Id: 92C9M4TNWJ0KSQ8E
3.5.29.185, AMAZON-AES	Ashburn	https://medusa.services-s3bucket**petadoption**cb20dce5-19dvoixbafl77.s3.amazonaws.com X-Amz-Id-2: NaxA+Nwm8IwZHsgjmsbAst7wwKwFYio2zpWuD3h8U0sSCgV7kH04egtQjotZlzXX4JzF1I+KVEM= X-Amz-Request-Id: X05SKVD54CXP0VW4
3.5.29.23, AMAZON-AES	Ashburn	medusa.services-s3bucket**petadoption**cb20dce5-ls73efo1ev06.s3.amazonaws.com X-Amz-Id-2: lwCFGVdaPxXYeTJLiKYN8YmHP2K7hthrg8oZkJBdshDsdp5KuTwNXT2FlHmZGg+BddeCSqbTmn0jDC46BRG6XGUZhGR6rGCB X-Amz-Request-Id: 9CGJK7B0EXRCHBQX
52.217.138.177, AMAZON-02	Ashburn	medusa.services-s3bucket**petadoption**cb20dce5-1rxg06ddwvq8.s3.amazonaws.com X-Amz-Id-2: GdWWw6JyB/GPN6UXrvAnREvN5O+mndxJ9dBaanFl9+BXayviVbP2Z74KFpx7KS9J3eJkOJiR/0xorfJYqpwTFQHxy8zZPeD/ X-Amz-Request-Id: 6V0MDTBJYR9991SX
52.219.160.206, AMAZON-02	Mumbai	medusa.services-s3bucket**petadoption**cb20dce5-18snnbxszyb9a.s3.ap-south-1.amazonaws.com X-Amz-Id-2: cycBpdg04lBh8Mved9uzaO+IkX7hBRf492AvuPOJu9K9s8BLnlRIWqgk9cU05oRcoqyDW7bIG20= X-Amz-Request-Id: YDWK7HB0Z1V3KQPV
3.5.6.134, AMAZON-AES	Ashburn	https://medusa.services-s3bucket**petadoption**cb20dce5-1srluoz6schrh.s3.amazonaws.com X-Amz-Id-2: 6Pz+mADXVjZqrmoaEtkD49sZvaHhFZGmIx54a9ndreJ+nrLJg0yX2YXjj7CaEuvhVJ2W+HemQXB53nO2oh4j7g== X-Amz-Request-Id: Y3QZ78HBRTRJZ5Z0
54.231.135.121, AMAZON-02	Ashburn	medusa.services-s3bucket**petadoption**cb20dce5-1srluoz6schrh.s3.amazonaws.com X-Amz-Id-2: Ps91EWibjcQ0ON3OuypjaDfNMKrZ2+MgEZ7Bkzd9tXLPmOD2xtow2KYSnzdKbiqmf8Z1+sq/ffA= X-Amz-Request-Id: DZX0ANPFVAE9GSST
3.5.30.32 AMAZON-AES	Ashburn	https://medusa.services-s3bucket**petadoption**cb20dce5-1gmheft3h66dd.s3.amazonaws.com X-Amz-Id-2: 3TaYq2vkJP9PcaCdVybSJSr2iXVftvsk9mx8hhU5J1eIv8XDYtWZMuF7XfZB2hF9nfmeYIyDDFk= X-Amz-Request-Id: QAY3X7B6C3J71B2G

52.217.85.212, AMAZON-02	Ashburn	medusa.services-s3bucket**petadoption**cb20dce5-1gmheft3h66dd.s3.amazonaws.com X-Amz-Id-2: XrF2MMlLjMJoIo+ynzbewpbVCETiyhP7Jo/Xt/kd8HjexyPJ786+sRFBdVB2aRl+i4KNo0MJNpE= X-Amz-Request-Id: 7G4PBJ5SXEQ2XD75
52.216.44.65, AMAZON-02	Ashburn	https://medusa.services-s3bucket**petadoption**cb20dce5-1rxg06ddwvq8.s3.amazonaws.com X-Amz-Id-2: CERBrddJqhX7fqid0pH/CE63c6Ej5yKqI16IqH5ewBJ92hh7oTHwKfRsY+0Bw+cShUYO/Nv75jPBXy8Gv9CNvyPNjdZVZm0m X-Amz-Request-Id: MA22MYN7MST0B3H7
3.5.29.76, AMAZON-AES	Ashburn	https://medusa.services-s3bucket**petadoption**cb20dce5-lhy9vdtyj6gr.s3.amazonaws.com X-Amz-Id-2: sn08w4qWFwzbh8xUHKWSK+GY7DNPfR009jCzaQyA7i05kl+cIZoihAV1q1ZzJpya9z9xbD0pAuM= X-Amz-Request-Id: G0E1GZFMKJCKTZ11
16.182.36.113, AMAZON-02	Ashburn	medusa.services-s3bucket**petadoption**cb20dce5-lhy9vdtyj6gr.s3.amazonaws.com X-Amz-Id-2: X5ljzi/j2No7tjo3ibikSUr+xnH5BF0gVzGF1NnM/p+vJIzzbB00iOJZfg443y5CWmNj638eOAM= X-Amz-Request-Id: F20Z9HH872C3M6ZB
16.15.185.152, AMAZON-AES	Ashburn	https://medusa.services-s3bucket**petadoption**cb20dce5-1v45rsfb6i0ng.s3.amazonaws.com X-Amz-Id-2: H+hdZUN+0fPFPOIgKaaBOQQXZ6OmoyFoLpZ6BpI7GVaN4BhezBOnGSsWeK/+2gYpKUftmtXcx8E= X-Amz-Request-Id: E1KMJZKJWKTRRJJD
3.5.25.152, AMAZON-AES	Ashburn	https://medusa.services-s3bucket**petadoption**cb20dce5-gbcn430m9d7n.s3.amazonaws.com X-Amz-Id-2: KNNee4YlbCTqHFxCpxJvGrazmG+x0fauc3kM9b+1524ak/FYeDrq1oUafE9nXt53p5MnTOOrlMI= X-Amz-Request-Id: 86YHTTTP6NVVXXED
3.5.25.147, AMAZON-AES	Ashburn	medusa.services-s3bucket**petadoption**cb20dce5-1v45rsfb6i0ng.s3.amazonaws.com X-Amz-Id-2: l9H5ZeYLNKt/AiAx7MfxWoJxtEPxx7hOi/ZH1R9k0TtONwukQTMLElJ/n42wjcCB2xVDHlm1/do= X-Amz-Request-Id: B03RQGQKQQ2YZ8AZ
54.231.199.41, AMAZON-02	Ashburn	medusa.services-s3bucket**petadoption**cb20dce5-gbcn430m9d7n.s3.amazonaws.com X-Amz-Id-2: 31y+s7i5jgB4txhhMdBWS3vaO8D4ord55RSMmlfbTbo4cVh3Lxro5QAno2l7A2DGS2CqeYgHUqI=

		X-Amz-Request-Id: 3VFT18F9NHZ7BQX5
52.217.160.73, AMAZON-02	Ashburn	https://medusa.services.s3.amazonaws.com X-Amz-Id-2: 6ALaT4zm7S6wpxL7Nq/Ik/nYPIYtgrkJXDCoxhFIQEvz8Ob5DF9tr5MT+FQVp67ZaRRt3HAeFpM= X-Amz-Request-Id: 1Y52XF3HG60ZGJ7V
3.5.27.148, AMAZON-AES	Ashburn	medusa.services.s3.amazonaws.com X-Amz-Id-2: ro+0OW9ULTwWFblxps3E7qIf+7sVxz2ENsvoxjabr2KtxrYsH9UYmoecCXOOgfiDjkkx8OPslTBEn0dQ91VJf9i3r3a3fvwi X-Amz-Request-Id: ZYEPJA1C23M726BS

NFT Phishing Activity Linked to Medusa Drainer Ethereum Address 1

We have analysed the NFT domains (transfers) made by the Medusa Drainer ETH Address 1 via etherscan.io.

Our analysis of NFT-related domain transfers linked to **Medusa Drainer Ethereum Address 1** (via etherscan.io) reveals phishing infrastructure tied to the following wallet:

- **0x111117d0c05573b49b32ef30dc031dd9ed022099**

We identified **9 domains** associated with this address, which redirect to **8 distinct active phishing websites**. These domains are designed to impersonate and target well-known **brands and blockchain protocols**, as outlined below.

Protocol / Project	Official Domain	Phishing Domains
Lido (stETH / DAO)	lido.fi	- foundation-lido.net - foundation-lido.com - reward-steth.org - reward-steth.com
Aave	aave.com	- aave-gift.net
BlazeStake	stake.solblaze.org	- airdrop-blaze.org
PoolStake	peetdefi.gitbook.io peetdecentralized.finance	- poolstake-hub.org
Origin Protocol	originprotocol.com	- get-originether.com

Our investigation uncovered **8 historical domains** previously associated with Medusa Drainer activity. These domains **currently redirect to 7 distinct active phishing websites**.

A summary of the mappings between historic domains and their corresponding active phishing sites is presented in the table below.

NTF Transfer	Redirected Domain
bzeth.org	airdrop-blaze.org
stethprize.org	foundation-lido.com

staave.net	aave-gift.net
poolstaked.com	poolstake-hub.org
getstether.com	reward-steth.org
coinsteth.net	reward-steth.com
originethers.com	Inactive
oeth.ai	get-originether.com

Additional WHOIS record analysis is presented in the table below. Five domains were registered in **February 2025**, while three were registered in **March 2025**.

Phishing Domain	Registration Details	Further Investigation
foundation-lido.net	Registrar: NICENIC INTERNATIONAL GROUP CO., LIMITED Registered: 14th February 2025	
bzeth.org	Registrar: NICENIC INTERNATIONAL GROUP CO., LIMITED Registered: 8th March 2025 Registrant Name: Francoise Rivas Registrant Country: French Polynesia	whoxy.com/company/59220668
airdrop-blaze.org	Registrar: NICENIC INTERNATIONAL GROUP CO., LIMITED Registered: 10th March 2025 Registrant Company: **Jacobs Ltd PLC**	whoxy.com/company/74076404
foundation-lido.com	Registrar: NICENIC INTERNATIONAL GROUP CO., LIMITED Registered: 14th February 2025	
stethprize.org	Registrar: NICENIC INTERNATIONAL GROUP CO., LIMITED Registered: 8th February 2025 Registrant Name: Bryce Hickman Registrant Country: Korea Democratic Republic	whoxy.com/company/58959170
aave-gift.net	Registrar: NICENIC INTERNATIONAL GROUP CO., LIMITED Registered: 7th February 2025	
staave.net	Registrar: NICENIC INTERNATIONAL GROUP CO., LIMITED Registered: 9th December 2024	
poolstaked.com	Registrar: NICENIC INTERNATIONAL GROUP CO., LIMITED Registered: 3rd October 2024	
poolstake-hub.org	Registrar: NICENIC INTERNATIONAL GROUP CO., LIMITED Registered: 15th January 2025 Registrant company: **Jacobs Ltd PLC**	
getstether.com	Registrar: NICENIC INTERNATIONAL GROUP CO., LIMITED Registered: 20th August 2024	

reward-steth.org	Registrar: NICENIC INTERNATIONAL GROUP CO., LIMITED Registered: 14th December 2024 Registrant company: **Jacobs Ltd PLC**	
coinsteth.net	Registrar: NICENIC INTERNATIONAL GROUP CO., LIMITED Registered: 6th June 2024 Registrant company: Julien Maddox (5 domains) Registrant country: Guinea-bissau	whoxy.com/company/58565918
reward-steth.com	Registrar: NICENIC INTERNATIONAL GROUP CO., LIMITED Registered: 14th December 2024	
originethers.com	Registrar: NICENIC INTERNATIONAL GROUP CO., LIMITED Registered: 11th May 2024	
oeth.ai	Registrar: NICENIC INTERNATIONAL GROUP CO., LIMITED Registered: 16 April 2024 Registrant Name: Bryan Kaiser Registrant Organization: **lolita llc** Registrant Street: 37 Charles Street Registrant City: Manchester Registrant State/Province: Michigan Registrant Postal Code: 48158 Registrant Country: US Registrant Phone: +1.7344280917 Registrant Email: **montorerielz4@mail.com**	whoxy.com/company/67543715
get-originether.com	Registrar: NICENIC INTERNATIONAL GROUP CO., LIMITED Registered: 30th October 2024	

NFT Phishing Activity Linked to Medusa Drainer Ethereum Address 2

- **0xfa7575caa049e5cfd96a2783da2c85663f0da817**

An investigation into NFT tokens linked to the above Ethereum address revealed a total of **64 domains**. Among them, **12 domains are currently inactive**, while the remaining **52 actively redirect to various phishing websites**.

After removing duplicates, we identified **40 unique active phishing domains** targeting the following brands and blockchain protocols.

Brand / Protocol	Official Domain	# of Phishing Domains	Phishing Domains
Lido (stETH)	lido.fi	5	foundation-lido.net, foundation-lido.com, liquideth-claim.org, network-stether.net, steth-finance.com

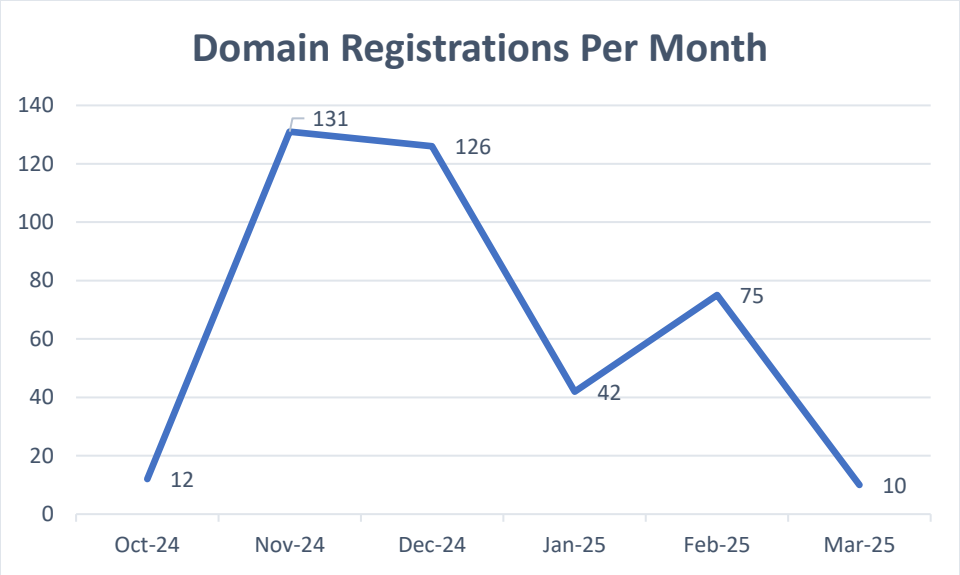
Chainlink	chain.link	4	link-awards.org, get-linktoken.net, airdrop-clink.org, gifts-linktoken.net
Injective	injective.com	3	gifts-injective.net, award-injective.net, injconnect.com
Ondo Finance	ondo.finance	3	awards-ondo.com, ondo-airdrop.com, event-ondo.net
ENS	ens.domains	2	rewards-ens.org, ens-network.net
Beam	beam.mw	2	beam-giveaway.net, giveaway-beam.com
Quant	quant.network	2	app-quant.net, event-quant.com
Synthetix	synthetix.io	2	airdrop-synthetix.org, event-snx.net
Aave	aave.com	1	protocol-aave.net
BlazeStake	stake.solblaze.org	1	giveaway-blaze.com
Compound	compound.finance	1	dashboard-compound.com
Fetch.ai	fetch.ai	1	fetch-foundation.com
Gala Games	gala.com	1	galagames-network.net
HEX	hex.com	1	app-hex.com
Origin Protocol	originprotocol.com	1	event-origineth.net
Realio	realio.fund	1	app-realio.org
Mantra	mantrachain.io	1	mantra-finance.net
SingularityNET	singularitynet.io	1	agix-gifts.com
PoolStake	peetdefi.gitbook.io peetdecentralized.finance	1	reward-poolstake.net, app-pooledeth.io, app-pooledeth.net
Shiba Inu	shibatoken.com	1	claim-shib.org
Render Network	rendernetwork.io	1	dashboard-render.com
dYdX	dydx.exchange	1	network-dydx.net

Although the registrant information appears to be false or intentionally misleading, our investigation uncovered **two key pivot data points** linked to **fake company names** used during domain registration:

- **Jacobs Ltd PLC** *(fake registrant name generated via fauxid.com)*
- **lolita llc** *(fake registrant name)*

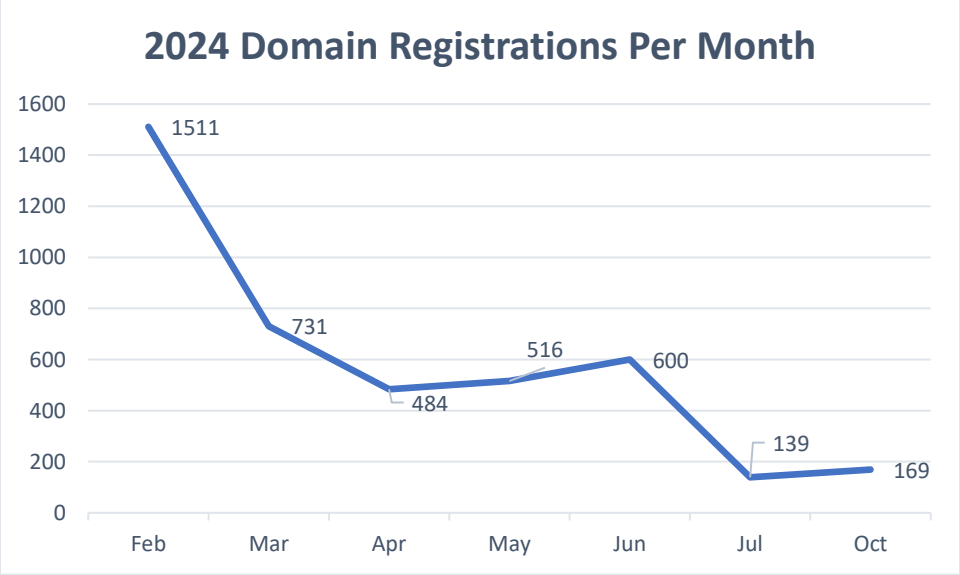
A **reverse WHOIS search** for "Jacobs Ltd PLC" on whoxy.com revealed **162 registered domains**, while a search on silentpush.com uncovered **423 domains** tied to the same name. All of these domains were registered through **NICENIC INTERNATIONAL GROUP CO., LIMITED**.

A summary chart illustrating monthly domain registration activity is included below.



Data from whoxy.com reveals that **"lolita llc"** is the registrant for a total of **16,318 domain names**. However, searches on **silentpush.com** indicate that **4,149 domains** are registered under this name, with **4,138 of these domains** being registered through **NICENIC INTERNATIONAL GROUP CO., LIMITED**. The remaining **11 domains** were registered via **1API GmbH**.

All of these domains were registered in **2024**, and a summary chart showing monthly domain registration patterns, based on **Silentpush.com** data, is provided below.



The two identified registrant data points— **"Jacobs Ltd PLC"** and **"lolita llc"**—should be closely monitored for any new phishing domain registrations.

NFT Phishing Activity Linked to Fake_Phishing328573:

- **0xaC65360aF5a8AE5ec45AD0Bf2A7Ec063a38e2161**

We identified **7 domains** associated with this address, which redirect to **6 distinct active phishing websites**. These domains are designed to impersonate and target well-known **brands and blockchain protocols**, as outlined below.

Protocol / Project	Official Domain	Initial Phishing Domains	Redirected Phishing Domain
BlazeStake	stake.solblaze.org	genesis-eth.net	blaze-airdrop.com
Lido (stETH / DAO)	lido.fi	– stethprize.org – getstether.com – claimsteth.org – stethgift.net	– foundation-lido.com – reward-steth.org – reward-steth.com – stether-finance.org
PoolStake	peetdefi.gitbook.io peetdecentralized.finance	poolstaked.com	poolstake-hub.org
Origin Protocol	originprotocol.com	originethers.com	Inactive

Expanding Phishing Domain Monitoring Through Unique Snippets Analysis

Through further analysis via Fofa.info, we examined the unique snippets linked to phishing domains. This helped us expand the infrastructure monitoring and potentially develop rules for identifying new phishing domains.

The following snippets, associated with various brand protocols and potential phishing servers, were identified during this analysis.

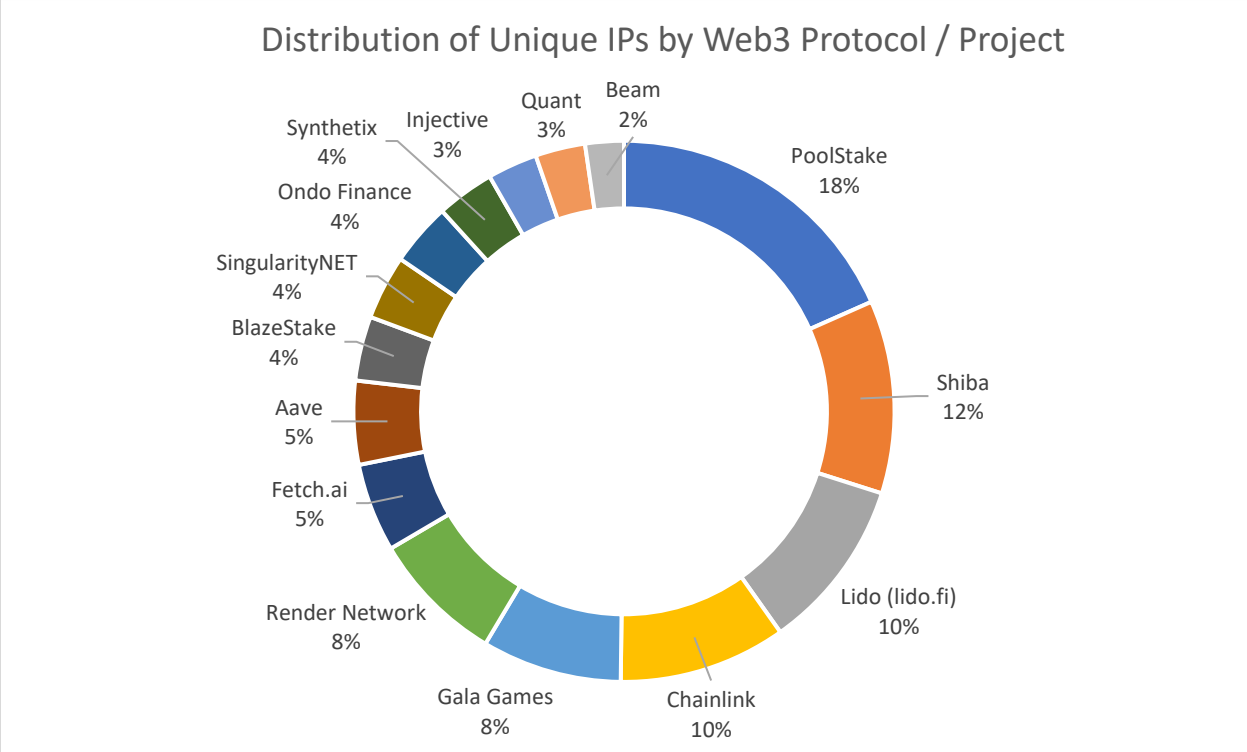
Unique Snippets	Protocol Brand	Number of Servers
1681484233 (favicon hash)	Lido (lido.fi)	**290** servers detected 282 (US); 2 (BG); 2 (HK); 2 (ZA); 1 (RU) **107** unique IP addresses
title=="Blaze - Liquid Staking"	BlazeStake	**104** servers detected (Cloudflare, US) **40** unique IP addresses
0xae7ab96520DE3A18E5e111B5EaAb095312D7fE84 (Lido Staked Ether address) && title=="Blaze - Liquid Staking"	BlazeStake	**64** servers detected (Cloudflare, US) **26** unique IP addresses
2017642785 (favicon hash)	Aave	**10** servers detected (US)
title=="Aave - Open Source Liquidity Protocol"	Aave	**124** servers detected (US) 95 (US); UK (10); MD (6); NL (4); RU (4) **52** unique IP addresses
1230563828 (favicon hash)	PoolStake	**614** servers detected (Cloudflare, US) **191** unique IP addresses

		Pooled Staking for Ethereum - PoolStaked (353 results) Liquid Staking for Ethereum - LiquidEther (261 results)
-1523901802 (favicon hash)	Origin Protocol	**6** servers detected **4** (US); **2** (RU) **4** unique IP addresses
1720176043 (favicon hash)	Chainlink	**549** servers 457 (US), 63 (HK), 7 (UK), 2 (JP), 1 (BG) **104** unique IP addresses Blockchain Oracles for Hybrid Smart Contracts | Chainlink (**464** results) Chainlink: Airdrop Event has already started (**7** results) ChainLink (**4** results)
-1049881231 (favicon hash)	Injective	**97** servers 74 (US), 19 (DE), 4 (SG) **31** unique IP addresses Injective Hub - Access Unlimited DeFi Markets (**61** results)
1758103197 (favicon hash)	Ondo Finance	**98** servers 97 (US) 1 (MY) **39** unique IP addresses
1535523138 (favicon hash)	ENS	**33** servers (Cloudflare, US) **13** unique IP addresses
title=="Beam Airdrop is Here! | Merit Circle"	Beam	**98** servers (Cloudflare, US) **24** unique IP addresses
1641416809 (favicon hash)	Quant	**114** servers (Cloudflare, US) **31** unique IP addresses
-776987632 (favicon hash)	Synthetix	**77** servers 62 (US), 6 (RO), 4 (AU), 2 (DE), 1 (CA) **36** unique IP addresses
-617263435 (favicon hash)	Compound	**75** servers (Cloudflare, US) **23** unique IP addresses
1076535611 (favicon hash)	Fetch.ai	**227** servers 178 (US), 49 (UK)

		55 unique IP addresses Fetch AI: Open platform to build AI Apps & Services (211 results) Access 1 Million AI Agents (2 results) BlockAgent - AI Agents platform for Blockchain Observability (2 results)
-511910750 (favicon hash)	Gala Games	**317** servers (Cloudflare, US) **87** unique IP addresses
-1602356927 (favicon hash)	HEX	**54** servers (Cloudflare, US) **16** unique IP addresses
1246193725 (favicon hash)	Realio	**6** servers 4 (LT), 2 (US) **2** unique IP addresses
"mantra-finance.net"	Mantra	**18** servers (US) **5** unique IP addresses
"MANTRA - A Security First L1 Blockchain for Real World Assets"	Mantra	**37** servers 28 (US), 4 (UK), 2 (HK), 2 (JP), 1 (SE) A Security First L1 Blockchain for Real World Assets | MANTRA (27 results)
1462188057 (favicon hash)	SingularityNET	**72** servers 62 (US), 5 (DE), 2 (HK), 1 (IN), 1 (JP) **40** unique IP addresses
title=="SingularityNET - Next Generation of Decentralized AI"	SingularityNET	**11** servers (US) **4** unique IP addresses
Shib | D3 - Official Identity "Shib | D3 - Official Identity Service For Top Web3 Communities"	Shiba	**391** servers **390** (US), 1 (SE) **120** unique IP addresses
-1325884221 (favicon hash)	Shiba	**31** servers 20 (US), 8 (HK), 3 (IN) **23** unique IP addresses
title=="Render Network"	Render Network	**178** servers 161 (US), 11 (KR), 6 (FR) **67** unique IP addresses
-537092978 (favicon hash)	Render Network	**27** servers 17 (US), 6 (FR), 3 (KR), 1 (HK) **16** unique IP addresses
title=="Airdrop dYdX"	dYdX	**13** servers (US)

		5 unique IP addresses
-1119305046 (favicon hash)	dYdX	**22** servers (US) **11** unique IP addresses

A chart illustrating the distribution of unique IP addresses by protocol / project is provided below. The analysis was conducted using relevant criteria, such as **favicon hash**, selected from the table above.



Source-Code Analysis of Phishing Domains

Our analysis of the source code within the phishing domains revealed significant code similarities. We identified **11 relevant JavaScript files** and **1 stylesheet (CSS)**. These phishing domains employ random names for the JavaScript files, which differ across various domains. For example, the phishing domain **foundation-lido.net** contains the following JavaScript files:

JavaScript snippet	Description
uSRXQAtPVGZyQJYwaPNFv.js	– a JavaScript (or TypeScript) configuration that defines metadata and access endpoints for multiple **EVM-compatible blockchains**. – The code acts as a registry or lookup object that allows a blockchain-related application (like a wallet, explorer, dApp frontend, or SDK) to interface with different EVM-compatible chains. – Some chains use Etherscan clones, others use BlockScout or custom tools
bXBRBXGzYLxvPXS.js	– The code provides the developer Session ID for contact: 05c78f6352a461383a0ee289d33d41c3bdc8c752509d92f88e13c515edccd9f704 – This Session ID is provided across all the phishing domains

UQrHstcEWN.js	– The code provides the developer Session ID for contact: 05c78f6352a461383a0ee289d33d41c3bdc8c752509d92f88e13c515edccd9f704
UYydzVpUvvDWvNA.js	– The code provides the developer Session ID for contact: 05c78f6352a461383a0ee289d33d41c3bdc8c752509d92f88e13c515edccd9f704
KEKOmeCX.js	– The code provides the developer Session ID for contact: 05c78f6352a461383a0ee289d33d41c3bdc8c752509d92f88e13c515edccd9f704
PHOABBXfWSVGyyUE.js	– The code provides the developer Session ID for contact: 05c78f6352a461383a0ee289d33d41c3bdc8c752509d92f88e13c515edccd9f704
gFSxvSxVv.js	– The code provides the developer Session ID for contact: 05c78f6352a461383a0ee289d33d41c3bdc8c752509d92f88e13c515edccd9f704
EKRhKuADnMxOTMvE.js	– The code provides the developer Session ID for contact: 05c78f6352a461383a0ee289d33d41c3bdc8c752509d92f88e13c515edccd9f704
KziWNJ.js	– The code provides the developer Session ID for contact: 05c78f6352a461383a0ee289d33d41c3bdc8c752509d92f88e13c515edccd9f704
YjXIUtpKRM.js	– The code provides the developer Session ID for contact: 05c78f6352a461383a0ee289d33d41c3bdc8c752509d92f88e13c515edccd9f704
tmkUInnzBZAwNMMvCwCVvtWE.js	– The code provides the developer Session ID for contact: 05c78f6352a461383a0ee289d33d41c3bdc8c752509d92f88e13c515edccd9f704

We conducted a similar analysis on the source code of **airdrop-blaze.org**. A summary of the findings is provided below.

Javascript snippet	Description
vaoxGn.js	– The code defines configurations for various **EVM-compatible blockchain networks**, including Ethereum Mainnet, Layer 2s (Arbitrum, Optimism, zkSync), sidechains (Polygon, BSC, etc.), and alternative L1s (Avalanche, Fantom, Celo, etc.) – The **multicall3** contract is reused across nearly all networks, always at the same address: **0xca11...ca11**. It's a standard contract with a known deployment, used for batching JSON-RPC calls.
FAoIvQbRGNvnTxwypHZUm.js	– a JavaScript (or TypeScript) SDK dealing with Web3-related functionality, **WalletConnect**.
NwYSHBVDCJzUZIIRLQncJG.js	– The code enables a **Web3Modal** wallet explorer that allows users to search, filter, and connect to various wallets, including injected, manual, and recommended wallets. It uses debounce for real-time search, infinite scroll with *IntersectionObserver*, and preloads wallet icons. The system supports **WalletConnect** integration for Web3 wallet connections, with mobile and

		desktop platform support. It also handles connection errors, retries, and dynamic wallet fetching.
SIPSdM.js	–	The code provides the developer Session ID for contact: 05c78f6352a461383a0ee289d33d41c3bdc8c752509d92f88e13c515edccd9f704
ouKsDOVsImeqtDIr.js	–	The code provides the developer Session ID for contact: 05c78f6352a461383a0ee289d33d41c3bdc8c752509d92f88e13c515edccd9f704
KxYMfOmoTSBWuKmnKrPA.js	–	The code provides the developer Session ID for contact: 05c78f6352a461383a0ee289d33d41c3bdc8c752509d92f88e13c515edccd9f704
AMBqDnryCyrFgEzJBRRzyAon.js	–	The code provides the developer Session ID for contact: 05c78f6352a461383a0ee289d33d41c3bdc8c752509d92f88e13c515edccd9f704
TuJyhKtwzXHwoqwtJ.js	–	The code provides the developer Session ID for contact: 05c78f6352a461383a0ee289d33d41c3bdc8c752509d92f88e13c515edccd9f704
QuZMZBDCRFmOiwxAwuLwSpYs.js	–	The code provides the developer Session ID for contact: 05c78f6352a461383a0ee289d33d41c3bdc8c752509d92f88e13c515edccd9f704
WvUjnwRSMszOr.js	–	The code provides the developer Session ID for contact: 05c78f6352a461383a0ee289d33d41c3bdc8c752509d92f88e13c515edccd9f704
UrkzDYoXurNuN.js	–	The code provides the developer Session ID for contact: 05c78f6352a461383a0ee289d33d41c3bdc8c752509d92f88e13c515edccd9f704

Additional searches were conducted to examine snippets within the source code of phishing sites. A search for the contract **"0xae7ab96520DE3A18E5e111B5EaAb095312D7fE84"**, which appears across several phishing sites, yielded **840 results** (covering **378 unique IP addresses**) via fofa.info. These results are distributed across the following website titles:

- Lido Airdrop - Liquid Ethereum (ETH) Rewards (**279** results)
- Blaze - Liquid Staking (**64** results)
- Synth - Metronome - Synthesizing the Future of DeFi (**39** results)
- Vesper App | Pools | Ethereum (**34** results)

This analysis can help identify additional phishing sites linked to these servers.

The **Ethereum contract "0xae7ab96520DE3A18E5e111B5EaAb095312D7fE84"**, found in the source code of the phishing site **airdrop-blaze.org**, is associated with **"DRAINER_CHAINS"** and interacts with this specific contract.

The source code of the malicious sites also contains the snippet **"id="drainer-button"**. A search for this snippet across the source-code search engine **publicwww.com** revealed **122 websites** that contain this specific snippet.

🔍 🪄 🔗 Investigating Potential Links to CryptoGrab Drainer

CryptoGrab Drainer maintains an extensive social media presence, presenting itself as a legitimate company registered in both **London, UK**, and **Ontario, Canada**. However, their UK-based company was dissolved on **4 March 2025**. The company had been registered through a proxy individual.

An in-depth analysis of CryptoGrab was conducted by **Certik**. CryptoGrab is known for offering various phishing services targeting cryptocurrency users, including the **Nova Drainer** and more traditional seed phrase phishing techniques. Certik's investigation suggests that CryptoGrab is likely managed from **Russia**.

CryptoGrab operates an affiliate network and provides its affiliates with a wide range of phishing attack methods. The group also maintains a wallet drainer, the **Nova Drainer**, which has been estimated to have stolen at least **$3 million** at current valuations.

Certik's analysis identified the **Nova Drainer modal phishing contract**:

- **0x000003845129254E67E3EcEf365c8c4fA0600000** ("CG_Magic")

Additionally, two **NFT assets** were found to be associated with this contract.

NFT Asset / Domain	Redirected Phishing Domain	Notes
genesis-eth.org	blaze-ethereum.org	Same source-code as Medusa Drainer
StakeEther.net	liquideth-claim.org	Same source-code as Medusa Drainer

The address **0x000003845129254E67E3EcEf365c8c4fA0600000** ("CG_Magic") has been found to be interacting with another known Drainer, identified as **"devildrainer.eth"** or **"monkeydrainer"** (according to **RootOne**). A transaction analysis of these interactions is available via **Arkham** here.

For more advanced analysis, users are advised to consult **AMLBot.com**.

Further investigation revealed that the **contract creator** of **0x000003845129254E67E3EcEf365c8c4fA0600000** is associated with the address:

- **0x79fF3EcA7E54222761C0a070bda2b4f119A90897**
  (funded by Fake_Phishing322870 on etherscan.io)

Fake_Phishing322870 has been linked to **21 NFTs** tied to phishing domains similar to those used by **Medusa Drainer**. Below is a summary table.

NTF Transfer	Redirected Domain	Used by Medusa Drainer
yieldeth.net	blaze-network.net	NO
stethcoin.net	foundation-lido.net	YES
univ4lab.net	Inactive	
poolstaked.org	reward-poolstake.net	YES
o-ether.org	airdrop-origineth.net	NO
getstether.org	reward-steth.org	YES
stethreward.org	reward-steth.org	YES
stethnetwork.org	reward-steth.com	YES

univ4labs.net	app.uniswap.org/swap (not phishing)	YES
stakingreward.org	steth-finance.com	YES
reward-link.net	airdrop-linktoken.org	NO
wsteth.net	app-lidonetwork.org	NO
stether.net	reward-steth.com	YES
stethclaims.org	reward-steth.org	YES
coinsteth.org	steth-finance.com	YES
stethevent.com	steth-finance.com	YES
etherfi.gift	Inactive	
StakeEther.net	liquideth-claim.org	YES
ldosteth.com	Inactive	

An additional address identified by **Certik.com** is:

- **0x00000751E8310fE25912aFD7B347C2612b400000** (“CG_Contract”)

The address **0x00000751E8310fE25912aFD7B347C2612b400000** was found to have received a transaction from **angel-drainer.eth**. A screenshot of this interaction is provided below, based on **Arkham.com** analysis.

An **NFT domain** was identified as being connected to the address **[612b400000]**: **fund-eth.org**, which redirects to **blaze-ethereum.org**.

This address **[612b400000]** is funded by **0x35647496bc5a7770f17b9ce160ace56c89e60df7** (**Fake_Phishing228342** on etherscan.io).

Fake_Phishing228342 was found to be linked to the following **NFT phishing domains**.

NTF Transfer	Redirected Domain	Used by Medusa Drainer
yield-eth.net	reward-blaze.com	NO
link-rewards.org	Inactive	
link-get.com	hub-linktoken.org	NO
apylink.org	gift-clink.org	NO
link-protocol.net	app-linktoken.net	NO
link-gift.org	airdrop-linktoken.org	NO
earn-link.com	app-link.io	NO
quant.gift	Inactive	

Interestingly, the phishing sites tied to the Fake Phishing addresses above all use the same source code and layout found in Medusa Drainer NFT phishing sites.

Investigating the Background of CryptoGrab

A brief investigation into **CryptoGrab** reveals potential connections to **Russia** and **Iran**, with affiliates operating in multiple countries.

Our analysis identified **8 unique email addresses** potentially associated with the **CryptoGrab** entity. A summary of these email addresses is provided in the table below.

Email Address	Source	Notes
cryptograb-forums@outlook.com	Slivup.net, 2022 (Russian forum dedicated to the exchange of private courses on earnings, business and much more)	Associated with username "CryptoGrab" Registered IP: 45.93.11.129 (ASN AS44477: (STARK INDUSTRIES SOLUTIONS LTD); ISP: Perviy TSOD LLC; IP Geolocation: Warsaw, Poland)
cryptograb-forums@outlook.com	Osint.industries	Skype ID: live:.cid.b9537e51ae74a978 Name: **Arseniy Pilotov (Арсений Пилотов)** Microsoft ID: B9537E51AE74A978 Location: **Russia** Email hints: **cr *** @mail.ua**
masoomkaramianfar@gmail.com	BreachForums.to, 2022	Associated with username "CryptoGrab" IP address: 176.53.134.183 (XServer Europe; IP Geolocation: Paris, France; using VPN service Troywell VPN (Poland))
Bulletproofmask7@yahoo.com	Twitter, 2022	Associated with username "Cryptograb" on Twitter Display Name: "Mardzhori Klark"
Bulletproofmask7@gmail.com	Recovery email for Bulletproofmask7@yahoo.com	
cryptograb_auto@proton.me	stopforumspam.com, June 2024	Associated with username "CryptoGrab" and IP address: 23.106.56.11 (ISP: Leaseweb UK Limited, London, United Kingdom)
cryptograb_auto@proton.me	Osint.industries	Linked to Medium.com account "Cryptograb" (username: **cryptograb_auto**)
cryptograb_auto@proton.me	Osint.industries	Registered account on **Pedsovet.su** (Russian platform)
cryptograb2@outlook.com	stopforumspam.com, January 2025	Associated with username "cryptograb", and IP address:

		118.179.44.67 (ISP: AmberIT Limited, Farīdpur, Dhaka Division, Bangladesh)
cryptograb2@outlook.com	Osint.industries	Registered accounts on Bandlab, Doctissimo (France), Mastodon, Hackernoon, Lichess.org, GitHub, Tumblr
cryptograb09@outlook.com	stopforumspam.com, January 2025	Associated with username “cryptograb1” and IP address: 203.190.14.173 (ISP: Daffodil Online Ltd, Purbadhala, Mymensingh Division, Bangladesh)
cryptograb09@outlook.com	Osint.industries	Registered accounts on Microsoft (ID: BA81BB628A86410D), Bandlab, Roll20, Mastodon, Gaia Online
cryptograb7@outlook.com	stopforumspam.com, December 2024	Associated with username “cryptograb” and IP address: 118.179.44.67 (ISP: AmberIT Limited, Farīdpur, Dhaka Division, Bangladesh)
cryptograb7@outlook.com	Osint.industries	Registered accounts on BeatStars (ID: MR7283630; Location: **Russia**); Microsoft (ID: 2CEA1CCA3B1B187C; Location: **Russia**), Roll20, Replit, Band.us

Further analysis of the username “cryptograb” has revealed the online accounts listed below.

Platform	Username	Notes
letterboxd.com	cryptograb	Location: Russia Website: cryptograb.io
github.com	cryptograb	Repository: exodus
about.me	cryptograb	Bradley Robertson (officer of CryptoGrab Limited dissolved in March 2025); Bio: Web Developer, Software Engineer, and Project Manager in London
pastebin.com	cryptograb	Location: Russia
telegram.org	cryptograb	Website: cryptograb.io Channel: cryptograb_info
Opensea.io	cryptograb	0x6F6D0118c8b5C20e75E798f4C5320E57842823E3

A **Telegram group** named **“crypto_life_chat”** ([Chat] CryptoGrab; ID: -1001414162744) was found to be owned by the **Telegram username Sezar_mr** (display name: “0mid”; ID: 568330379). This user was linked to multiple **Iranian Telegram groups and channels**. Further investigation revealed his **Iranian phone number** (**989374036051**, **Irancell, Iran**), associated with the name **“Kaveh Delbandi, Faridokht**

Dibay” (کاوه دلبندی, فریدخت دیبای). The name displayed on **CallApp** is **“Seyyed Mohammad Reza”** (سید محمد رضا).

Additional findings uncovered a **Telegram channel** under the username **“MedusaDrainer_scam”** (ID: -1001916540595), created on **15 December 2023**. The channel has **333 subscribers** as of **9 April 2025** and contains content related to **CryptoGrab**, with links to their website **cryptograb[.]io** and a reviews channel **cryptograb_reviws** (display name: “Payments|Review CryptoGrab Affilate”; ID: -1001534115465).

In particular, two messages in the **“MedusaDrainer_scam”** channel were forwarded by a **Telegram user** named **“Drainer Crypto | Angel|Inferno”**.

🔍🖼️🕵️🔗 Investigating the Potential Link Between NFT Phishing Domains and MS Drainer Developer “Pakulichev”

On **21 December 2023**, **Scamsniffer.io** published an article titled **“From Google to X Ads: Tracing the Crypto Wallet Drainer’s $58 Million Trail”**, in which they identified the developer of **MS Drainer**, a tool highly used in phishing ads. According to their findings, **10,072 phishing websites** using **MS Drainer code** were active between **March and December 2023**, targeting brands and protocols like **Zapper**, **Lido**, and **Radiant**.

The article also highlighted a **victim address**:

- **0x13e382dfe53207e9ce2eeeab330f69da2794179e**, which was found to interact with **NFT phishing domains** similar or identical to those used by **CryptoGrab** and **Medusa Drainers** (e.g., **stethclaims.org**, which redirects to **reward-steth.org**).

The **MS Drainer code** was first advertised on a forum on **22 January 2023**, distinct from other wallet drainers that typically charge a **20% fee**, including **Medusa Drainer**.

The developer of **MS Drainer**, initially identified as **“pakulichev”**, later changed their username to **“Phishlab”**. Code similarities, integrations, and modules within the **MS Drainer** were found to match the code used by **NFT phishing domains** linked to **Medusa** or **CryptoGrab**.

Pakulichev provided a link to their **Telegram account** under the same username (**ID: 349286731**, name: “Pavel”). Their Telegram account was registered via **79227987912**, which was linked to **Akulichev Pavel Alekseevich**, based out of **Surgut, Russia**.

While the code similarities between **MS Drainer** and the **Medusa Drainer** are evident, it is possible that **Medusa Drainer** was developed by a different individual/team.

🌓🧠☑️🚫 Recommended Actions for Web3 Users and Businesses to Protect Against Phishing and Malicious Activity

As the Web3 ecosystem continues to evolve, so too does the sophistication of malicious actors who target users through phishing sites and other deceptive tactics. The rise of phishing domains impersonating legitimate protocols, as well as the complex network of wallet drainers, underscores the importance of awareness and proactive security measures. To protect both individuals and businesses in the Web3 space, the following actions are highly suggested:

1. For Web3 Users:

- **Be Aware of Phishing Sites Impersonating Protocols**

Phishing sites targeting Web3 users have become increasingly sophisticated, with many sites now imitating well-known brands and protocols. These sites often redirect to malicious domains designed to steal private keys, seed phrases, or drain crypto wallets. Users need to be aware when clicking on unfamiliar sites or links, especially those sent through unsolicited messages, social media promotions, or fake airdrop announcements.

Adopt a **zero-trust** approach. Only use verified links and official domains cross-checked with social media channels. Suspicious links should be tested in sandboxed environments such as Browser.lol, any.run, or scanned with VirusTotal or urlscan.io.

- **Double-Check All Addresses**

Clipboard hijackers may alter addresses while copying. Always verify the full wallet address before confirming a transaction. Be cautious with QR codes—they can link to drainers disguised as payment requests.

- **Employ Web3 Security Tools for Wallet Verification and Protection**

Web3 users should use available tools to ensure their wallets are secure. **Blockchain explorers** (such as **Etherscan.io**) can help trace transactions and the addresses interacting with their wallets. Additionally, wallet protection tools such as hardware wallets (e.g., Ledger, Trezor) and browser extensions that monitor suspicious activity or services like **ScamSniffer** or **Revoke.cash** to identify and revoke malicious token approvals. Tools like **AMLBot.com** are essential for identifying malicious addresses, tracking stolen funds, and blocking potentially fraudulent transactions before they occur.

- **Diversify Wallets and Devices**

Don't keep all assets in one wallet. Spread funds across different wallets or even devices. Use different browsers or isolated containers like **Firefox Multi-Account Containers** for higher-risk interactions.

- **Multisignature Wallets**

Set up multisig wallets requiring multiple approvals for transfers. Even if one signer is compromised, unauthorized fund movements are blocked.

- **Enable 2FA Everywhere**

Use robust 2FA—preferably app-based (e.g., Authy, Google Authenticator). Avoid SMS or call-based 2FA, as they're vulnerable to **SIM swapping**.

- **Use Strong Passwords and Managers**

Create long, complex passwords with varied characters and manage them via trusted password managers (e.g., Bitwarden, 1Password).

- **Keep Software Updated**

Ensure that your OS, browser, wallet apps, and plugins are always up to date to prevent exploitation via known vulnerabilities.

2. For Businesses:

- **Continuous Blockchain Monitoring**

Businesses operating in the Web3 space need to continuously monitor blockchain activity to identify and respond to malicious actors targeting their users. Regular **blockchain analysis** can help detect suspicious transactions and flag interactions with **malicious addresses** tied to phishing campaigns or wallet draining activities. Platforms like **AMLBot.com** enables businesses to identify malicious wallet interactions, flag stolen assets, and visualize fund movement.

- **Implement Full-Spectrum Investigation Services**

For a more comprehensive approach to security, businesses should partner with services that specialize in investigating the full scope of phishing attacks and identifying related actors. Investigations can reveal hidden connections between multiple malicious domains, wallets, and social media activity, helping businesses understand the tactics and infrastructure used by these attackers. This type of deep investigation is crucial for responding to threats within a reasonable timeframe and preparing for future incidents.

- **Blockchain Transaction Blocking**

By integrating advanced tools and services, businesses can block or filter transactions originating from known malicious addresses. **Smart contract monitoring**, combined with **real-time transaction blocking** systems, can prevent funds from reaching fraudsters' wallets. Blockchain analytics platforms like **AMLBot.com** can assist with identifying these addresses in advance and alerting businesses to take immediate action, such as blacklisting addresses or freezing funds.

• Segment Internal Systems

For service providers and exchanges, isolate wallet infrastructure and implement role-based access control (RBAC) with strict key management policies to reduce insider risk.

3. Phishing Domain Enforcement

Beyond individual protections and transaction monitoring, businesses and users must focus on enforcement against phishing domains. **Online enforcement services** can help take down phishing websites by submitting reports to relevant authorities, domain registrars, registries, CDNs, hosting and upstream providers. Taking these sites down from the internet helps prevent them from deceiving users and minimizes the overall risk to the Web3 ecosystem.

4. Recovery Services via AMLBot.com

For users and businesses that fall victim to a phishing attack, recovery options are available. **AMLBot.com** offers services to track stolen funds, monitor transactions, and potentially recover assets lost to phishing schemes. This includes working with exchanges, bridges, and enforcement bodies to potentially freeze and recover funds. Using blockchain analytics tools for real-time monitoring can improve the likelihood of asset recovery and provide a safety net for Web3 participants.

Conclusion

In the rapidly evolving world of Web3, security remains a top priority. By remaining alert, using Web3 security tools, and partnering with blockchain analytics providers, users and businesses can protect themselves against malicious phishing attacks. Proactive monitoring, investigation services, and enforcement actions against phishing domains can help mitigate the risks associated with these types of attacks, ensuring a safer environment for all participants in the decentralized ecosystem.