ENS War Stories:

Protecting Web3 from Web2-Based Attacks

Alexander Urbelis

urbelis.eth

General Counsel / CISO, ENS Labs Ltd.

Malika Gazalieva

malikat.eth

Legal research associate, ENS Labs Ltd.

Whoami

Alexander Urbelis / urbelis.eth

- General Counsel / CISO of ENS
- Former CISO of NFL
- Professor of Law, King's College, London
- DNS-based intel platform creator
- Technology Advisory Board of Human Rights First
- Member of the UL Security Council
- Background in defense and intelligence in the US
- Co-host of a Hacker-focused radio show in NY
- Published in FT, CNN, The Intercept, 2600 Magazine
- Was a hacker way before it was cool

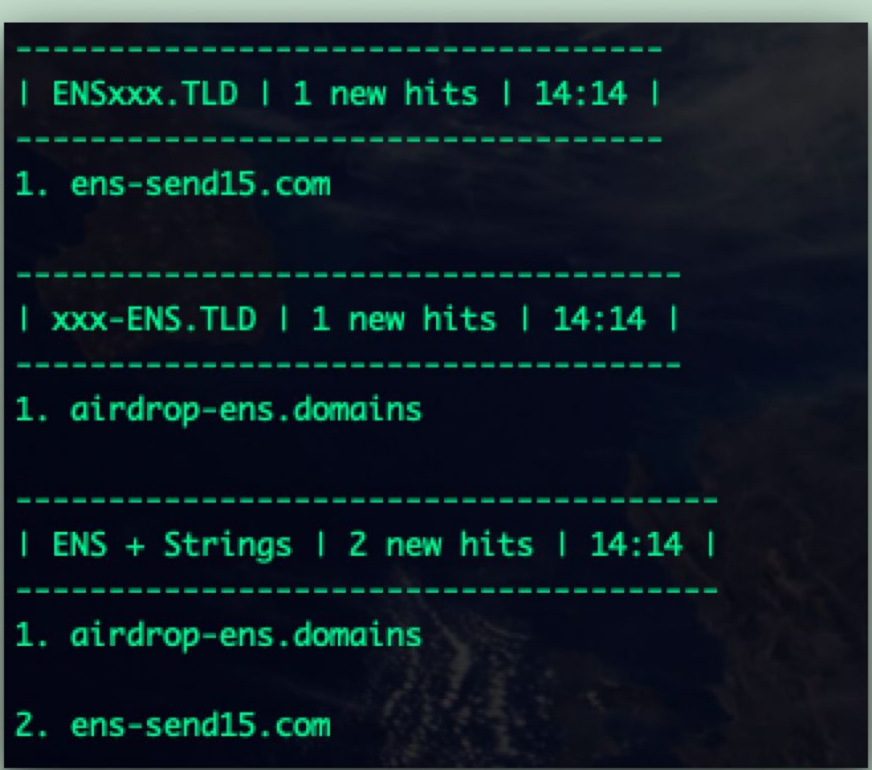
Whoami

Malika Gazalieva / malikat.eth

- Legal Research associate of ENS
- Former Senior consultant at Deloitte / TMT sector
- Tax Tool Developer for SMEs
- LLM in IP and Information Law at King’s College, London
- Participant in WIPO Academy
- Member of the AI & Law Society at KCL
- Thesis in Space Law, Environment & Technologies
- Internship at the Space Committee

The DNS is Dangerous

Bad Guys Abound



```
-----------------------------------
| ENSxxx.TLD | 1 new hits | 14:14 |
-----------------------------------
1. ens-send15.com

------------------------------------
| xxx-ENS.TLD | 1 new hits | 14:14 |
------------------------------------
1. airdrop-ens.domains

--------------------------------------
| ENS + Strings | 2 new hits | 14:14 |
--------------------------------------
1. airdrop-ens.domains

2. ens-send15.com
```

Created a DNS-based threat intel system

We identify malicious domains daily

Cloudflare → Hiding the Host

Attacks / fraud persist

Volume and velocity are alarming

Propelled on X / Twitter

Linktree usage is common

Wallet drainer smart contract

Attacks stood up surprisingly quickly

The Attacks

Pernicious and persistent

Can cause significant losses

Security threat coming
from web2 domains

An onboarding issue for web3

/

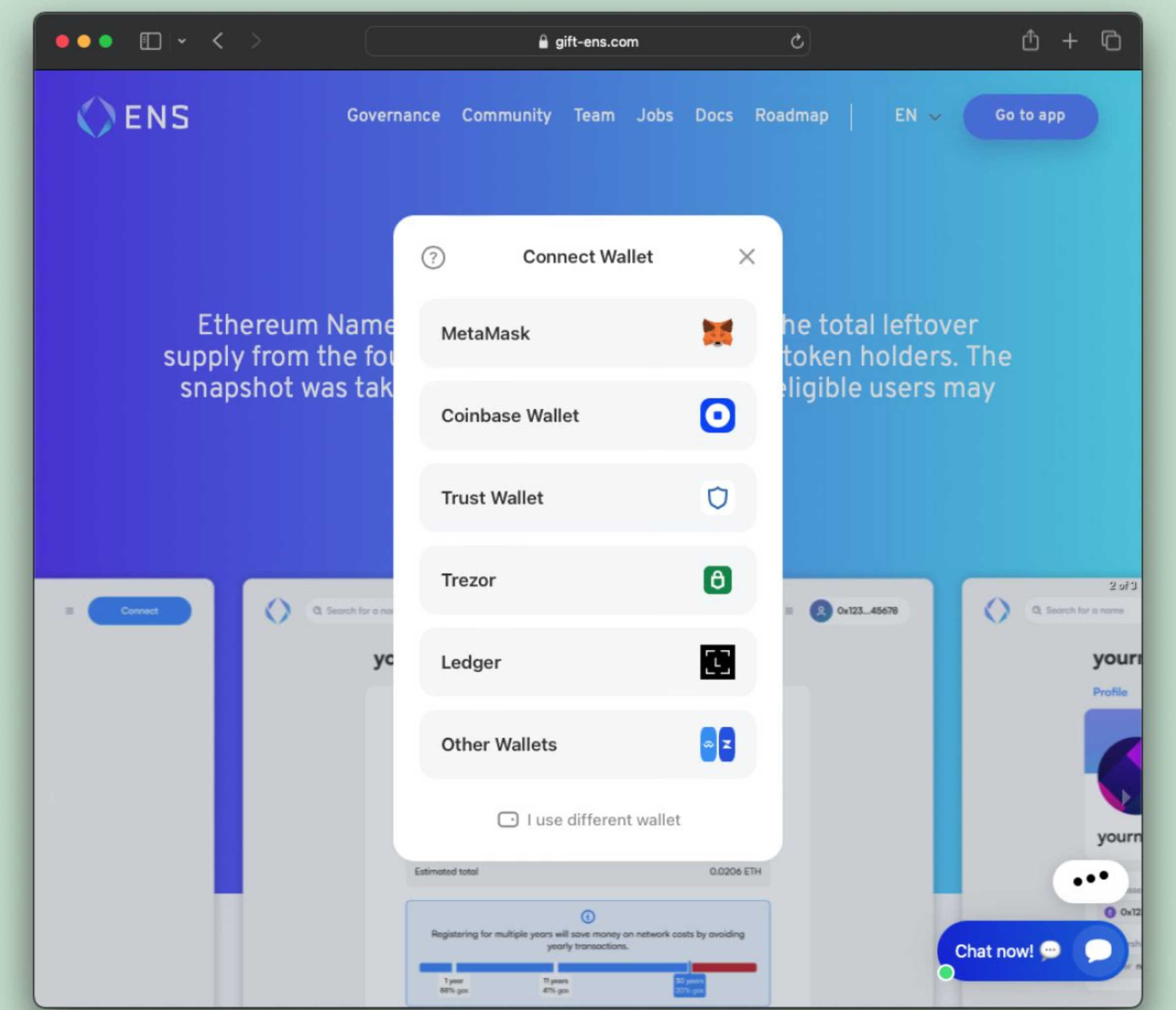
\

/

\

/

\



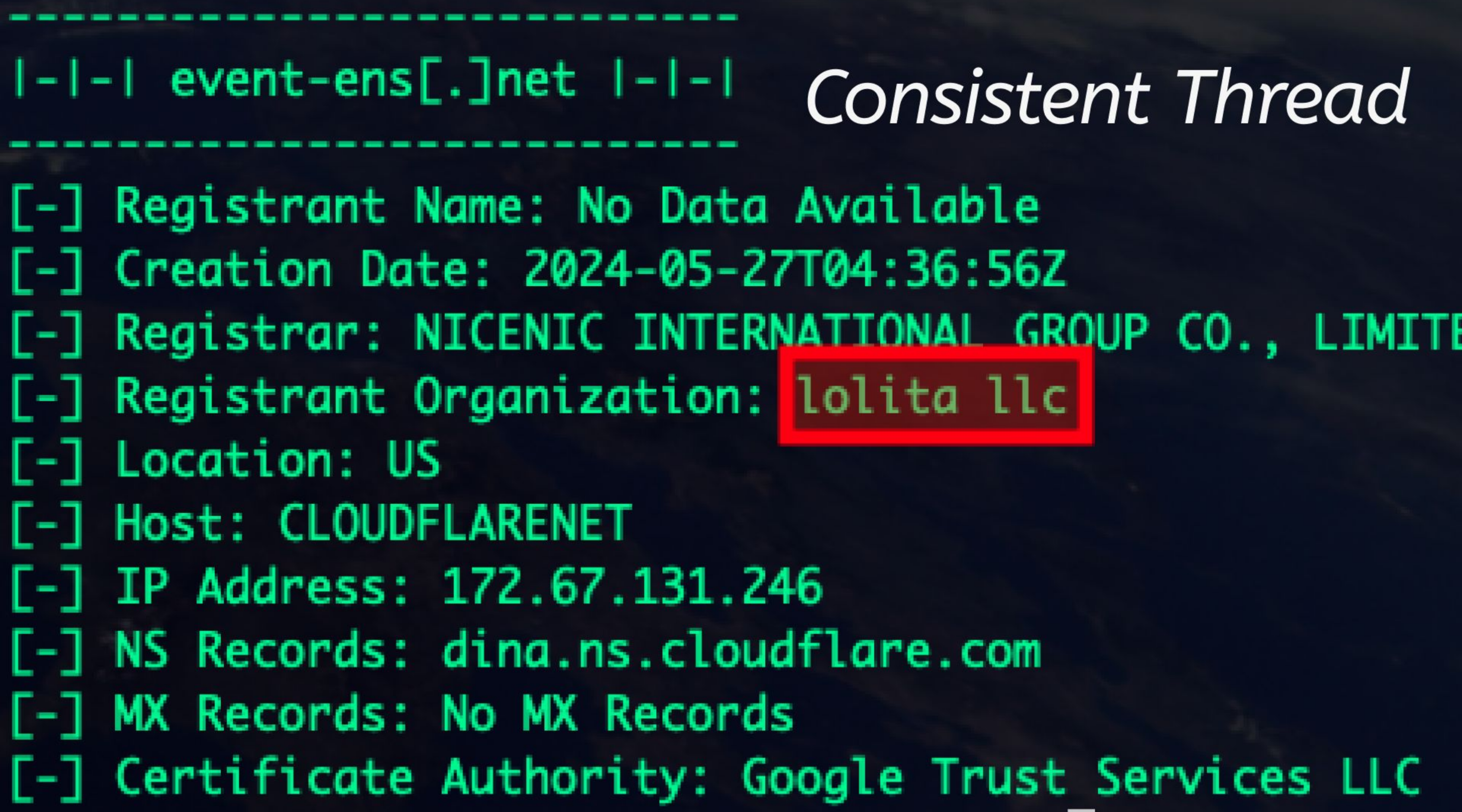
Ethereum Name
supply from the fo
snapshot was tak

he total leftover
token holders. The
eligible users may

Estimated total 0.0206 ETH

Registering for multiple years will save money on network costs by avoiding yearly transactions.

Consistent Thread

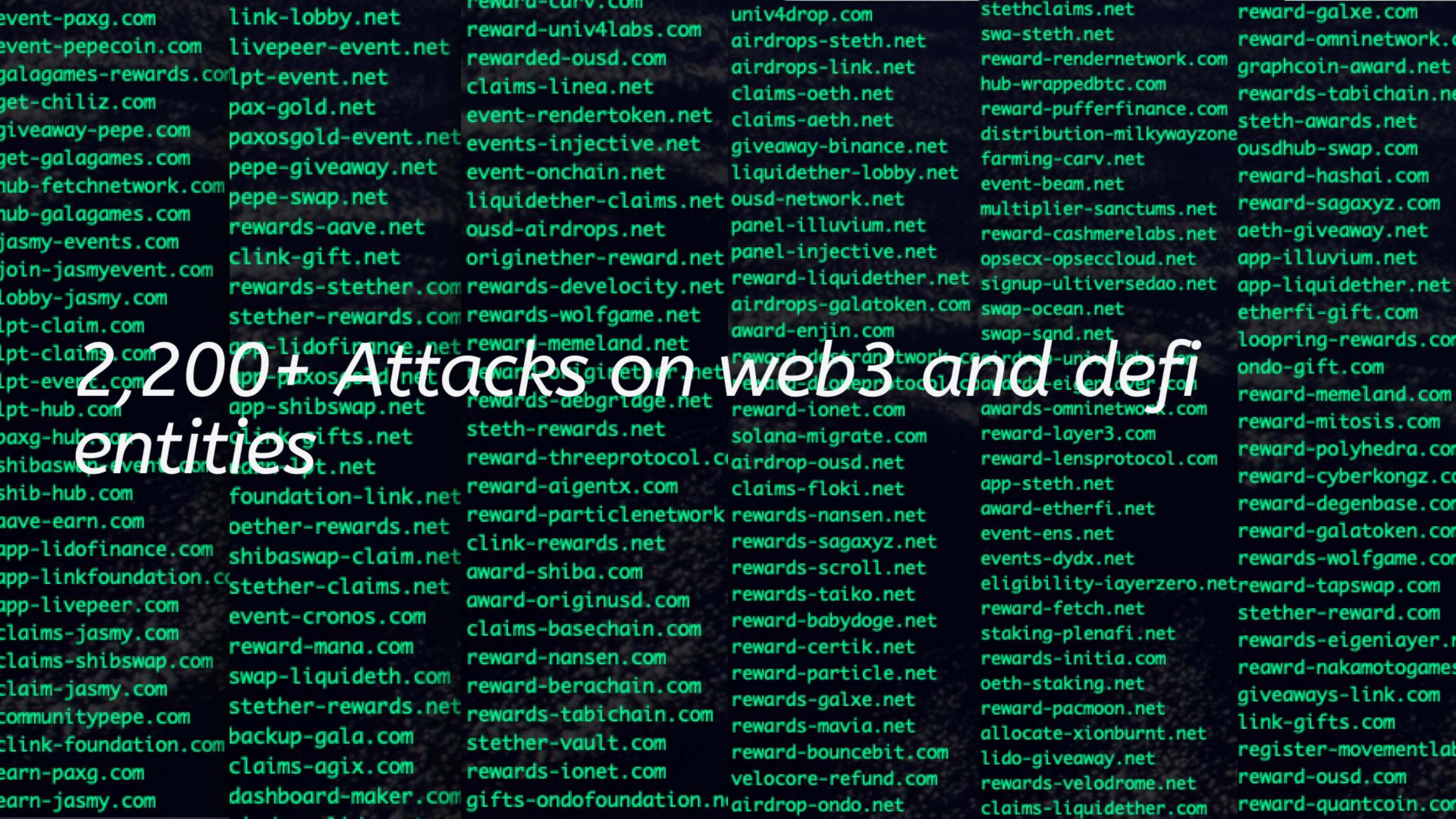


```
-----------------------------------

|-|-| event-ens[.]net |-|-|

-----------------------------------
[-] Registrant Name: No Data Available
[-] Creation Date: 2024-05-27T04:36:56Z
[-] Registrar: NICENIC INTERNATIONAL GROUP CO., LIMITE
[-] Registrant Organization: lolita llc
[-] Location: US
[-] Host: CLOUDFLARENET
[-] IP Address: 172.67.131.246
[-] NS Records: dina.ns.cloudflare.com
[-] MX Records: No MX Records
[-] Certificate Authority: Google Trust Services LLC
```

2,200+ Attacks on web3 and defi entities



```
event-paxg.com
event-pepecoin.com
galagames-rewards.com
get-chiliz.com
giveaway-pepe.com
get-galagames.com
hub-fetchnetwork.com
hub-galagames.com
jasmy-events.com
join-jasmyevent.com
lobby-jasmy.com
lpt-claim.com
lpt-claims.com
lpt-event.com
lpt-hub.com
paxg-hub.com
shibaswap-event.com
shib-hub.com
aave-earn.com
app-lidofinance.com
app-linkfoundation.c
app-livepeer.com
claims-jasmy.com
claims-shibswap.com
claim-jasmy.com
communitypepe.com
clink-foundation.com
earn-paxg.com
earn-jasmy.com

link-lobby.net
livepeer-event.net
lpt-event.net
pax-gold.net
paxosgold-event.net
pepe-giveaway.net
pepe-swap.net
rewards-aave.net
clink-gift.net
rewards-stether.com
stether-rewards.com
app-lidofinance.net
app-paxosgold.net
app-shibswap.net
clink-gifts.net
claim-lpt.net
foundation-link.net
oether-rewards.net
shibaswap-claim.net
stether-claims.net
event-cronos.com
reward-mana.com
swap-liquideth.com
stether-rewards.net
backup-gala.com
claims-agix.com
dashboard-maker.com

reward-carv.com
reward-univ4labs.com
rewarded-ousd.com
claims-linea.net
event-rendertoken.net
events-injective.net
event-onchain.net
liquidether-claims.net
ousd-airdrops.net
originether-reward.net
rewards-develocity.net
rewards-wolfgame.net
reward-memeland.net
reward-originether.net
rewards-debgridge.net
steth-rewards.net
reward-threeprotocol.c
reward-aigentx.com
reward-particlenetwork
clink-rewards.net
award-shiba.com
award-originusd.com
claims-basechain.com
reward-nansen.com
reward-berachain.com
rewards-tabichain.com
stether-vault.com
rewards-ionet.com
gifts-ondofoundation.n

univ4drop.com
airdrops-steth.net
airdrops-link.net
claims-oeth.net
claims-aeth.net
giveaway-binance.net
liquidether-lobby.net
ousd-network.net
panel-illuvium.net
panel-injective.net
reward-liquidether.net
airdrops-galatoken.com
award-enjin.com
reward-destranetwork.co
reward-dolomeprotocol.c
reward-ionet.com
solana-migrate.com
airdrop-ousd.net
claims-floki.net
rewards-nansen.net
rewards-sagaxyz.net
rewards-scroll.net
rewards-taiko.net
reward-babydoge.net
reward-certik.net
reward-particle.net
rewards-galxe.net
rewards-mavia.net
reward-bouncebit.com
velocore-refund.com
airdrop-ondo.net

stethclaims.net
swa-steth.net
reward-rendernetwork.com
hub-wrappedbtc.com
reward-pufferfinance.com
distribution-milkywayzone
farming-carv.net
event-beam.net
multiplier-sanctums.net
reward-cashmerelabs.net
opsecx-opseccloud.net
signup-ultiversedao.net
swap-ocean.net
swap-sand.net
airdrop-univ4labs.com
awards-eigenlayer.com
awards-omninetwork.com
reward-layer3.com
reward-lensprotocol.com
app-steth.net
award-etherfi.net
event-ens.net
events-dydx.net
eligibility-iayerzero.net
reward-fetch.net
staking-plenafi.net
rewards-initia.com
oeth-staking.net
reward-pacmoon.net
allocate-xionburnt.net
lido-giveaway.net
rewards-velodrome.net
claims-liquidether.com

reward-galxe.com
reward-omninetwork.c
graphcoin-award.net
rewards-tabichain.ne
steth-awards.net
ousdhub-swap.com
reward-hashai.com
reward-sagaxyz.com
aeth-giveaway.net
app-illuvium.net
app-liquidether.net
etherfi-gift.com
loopring-rewards.co
ondo-gift.com
reward-memeland.com
reward-mitosis.com
reward-polyhedra.co
reward-cyberkongz.c
reward-degenbase.co
reward-galatoken.co
rewards-wolfgame.co
reward-tapswap.com
stether-reward.com
rewards-eigeniayer.
reawrd-nakamotogames
giveaways-link.com
link-gifts.com
register-movementlab
reward-ousd.com
reward-quantcoin.co
```

Tracking & Threat Detection

Consistent infrastructure

Consistent DNS configuration

Wrote bash script to track NS record changes every ten minutes

NS records → Cloudflare = attack

wget -m [target domain]

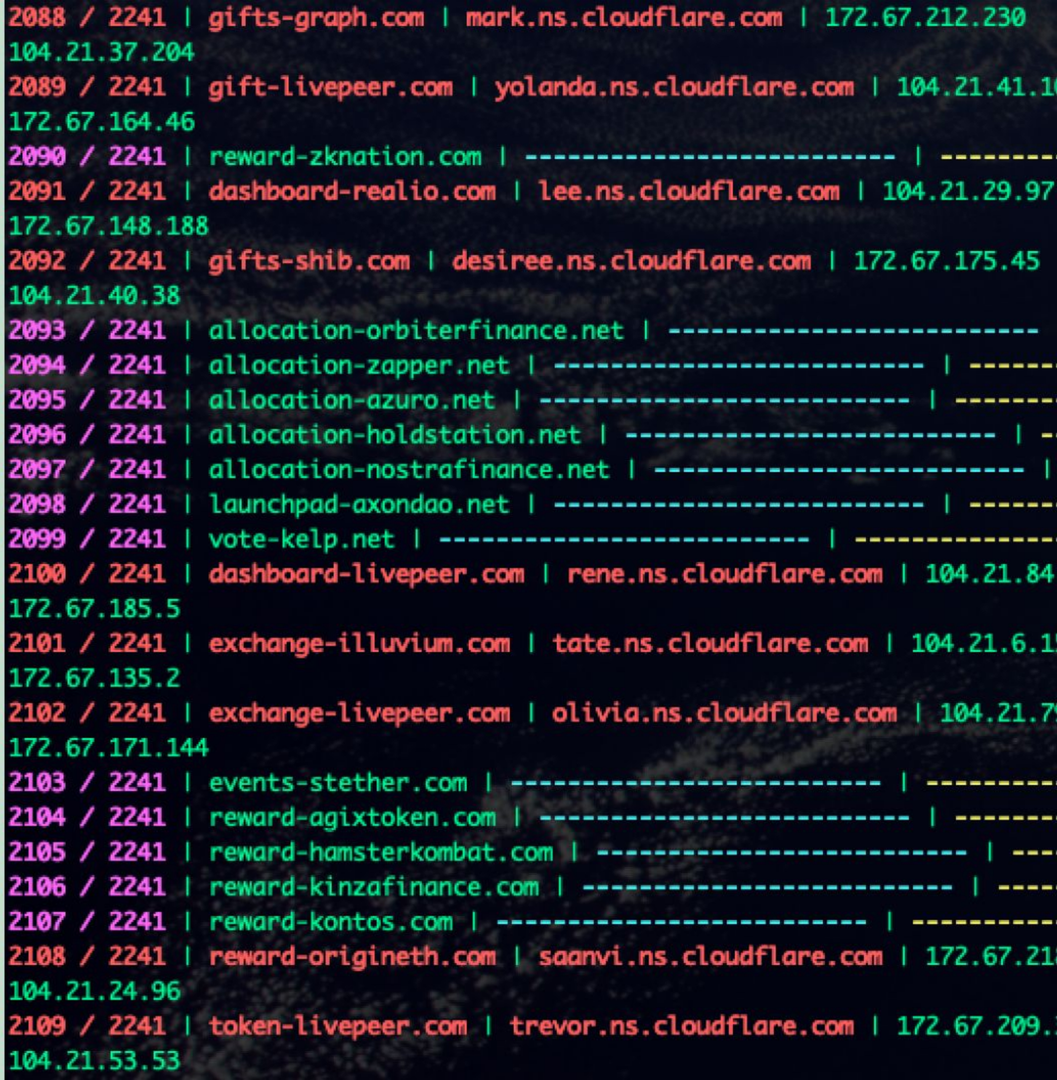
Evidence and indicators

Reliable early warning system

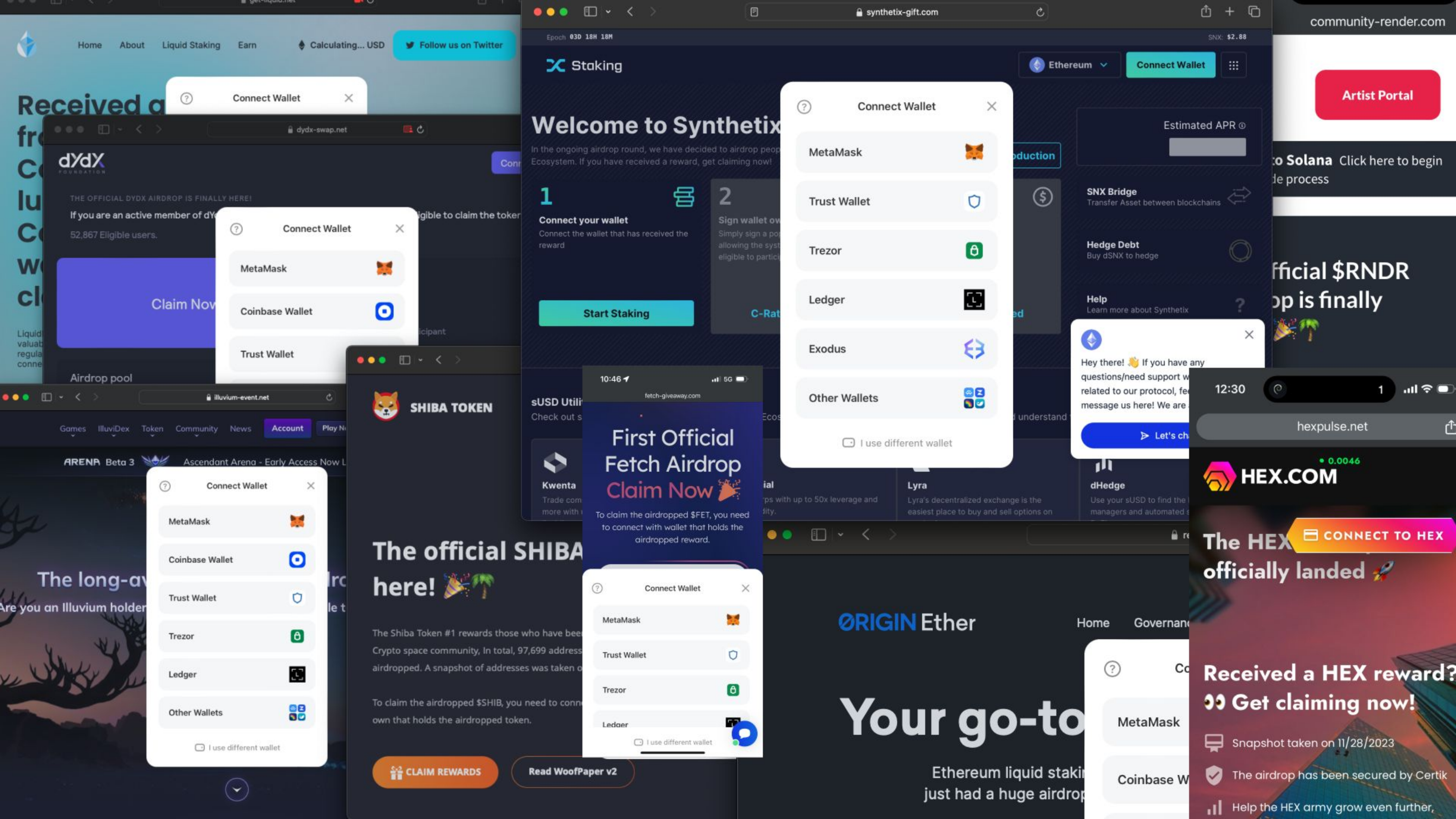
/

\

/



```
2088 / 2241 | gifts-graph.com | mark.ns.cloudflare.com | 172.67.212.230
104.21.37.204
2089 / 2241 | gift-livepeer.com | yolanda.ns.cloudflare.com | 104.21.41.1
172.67.164.46
2090 / 2241 | reward-zknation.com | -------------------------- | --------
2091 / 2241 | dashboard-realio.com | lee.ns.cloudflare.com | 104.21.29.97
172.67.148.188
2092 / 2241 | gifts-shib.com | desiree.ns.cloudflare.com | 172.67.175.45
104.21.40.38
2093 / 2241 | allocation-orbiterfinance.net | --------------------------
2094 / 2241 | allocation-zapper.net | -------------------------- | ------
2095 / 2241 | allocation-azuro.net | -------------------------- | -------
2096 / 2241 | allocation-holdstation.net | -------------------------- | -
2097 / 2241 | allocation-nostrafinance.net | -------------------------- |
2098 / 2241 | launchpad-axondao.net | -------------------------- | ------
2099 / 2241 | vote-kelp.net | -------------------------- | -------------
2100 / 2241 | dashboard-livepeer.com | rene.ns.cloudflare.com | 104.21.84
172.67.185.5
2101 / 2241 | exchange-illuvium.com | tate.ns.cloudflare.com | 104.21.6.1
172.67.135.2
2102 / 2241 | exchange-livepeer.com | olivia.ns.cloudflare.com | 104.21.7
172.67.171.144
2103 / 2241 | events-stether.com | -------------------------- | ---------
2104 / 2241 | reward-agixtoken.com | -------------------------- | -------
2105 / 2241 | reward-hamsterkombat.com | -------------------------- | ---
2106 / 2241 | reward-kinzafinance.com | -------------------------- | ----
2107 / 2241 | reward-kontos.com | -------------------------- | ----------
2108 / 2241 | reward-origineth.com | saanvi.ns.cloudflare.com | 172.67.21
104.21.24.96
2109 / 2241 | token-livepeer.com | trevor.ns.cloudflare.com | 172.67.209.
104.21.53.53
```



get-liquid.net

Home About Liquid Staking Earn Calculating... USD Follow us on Twitter

Received a fr C lu C w cl

Liquid valuab regula conne

Connect Wallet

dydx-swap.net

dYdX FOUNDATION

THE OFFICIAL DYDX AIRDROP IS FINALLY HERE!

If you are an active member of dY ...igible to claim the token

52,867 Eligible users.

Claim Now

Airdrop pool

...icipant

Conn

Connect Wallet

MetaMask

Coinbase Wallet

Trust Wallet

synthetix-gift.com

Epoch 03D 18H 18M

SNX: $2.88

Staking

Ethereum

Connect Wallet

Welcome to Synthetix

In the ongoing airdrop round, we have decided to airdrop peop... Ecosystem. If you have received a reward, get claiming now!

1 Connect your wallet

Connect the wallet that has received the reward

Start Staking

2 Sign wallet ow... Simply sign a po... allowing the syst... eligible to partici...

C-Rat

...duction

...ed

Estimated APR

SNX Bridge Transfer Asset between blockchains

Hedge Debt Buy dSNX to hedge

Help Learn more about Synthetix

sUSD Utili... Check out s...

...Ecos...

...l understand

Kwenta Trade com... more with...

...ial ...ps with up to 50x leverage and ...ity.

Lyra Lyra's decentralized exchange is the easiest place to buy and sell options on

dHedge Use your sUSD to find the ... managers and automated s...

Connect Wallet

MetaMask

Trust Wallet

Trezor

Ledger

Exodus

Other Wallets

□ I use different wallet

Hey there! 👋 If you have any questions/need support w... related to our protocol, fe... message us here! We are ...

Let's ch...

community-render.com

Artist Portal

...to Solana Click here to begin ...le process

...fficial $RNDR ...op is finally 🎉🌴

illuvium-event.net

Games IlluviDex Token Community News Account Play N...

ARENA Beta 3 Ascendant Arena - Early Access Now L...

The long-a... ...ro

Are you an Illuvium holder... ...le t...

Connect Wallet

MetaMask

Coinbase Wallet

Trust Wallet

Trezor

Ledger

Other Wallets

□ I use different wallet

SHIBA TOKEN

The official SHIBA here! 🎉🌴

The Shiba Token #1 rewards those who have bee... Crypto space community. In total, 97,699 address... airdropped. A snapshot of addresses was taken o...

To claim the airdropped $SHIB, you need to conn... own that holds the airdropped token.

CLAIM REWARDS

Read WoofPaper v2

10:46 5G

fetch-giveaway.com

First Official Fetch Airdrop Claim Now 🎉

To claim the airdropped $FET, you need to connect with wallet that holds the airdropped reward.

Connect Wallet

MetaMask

Trust Wallet

Trezor

Ledger

□ I use different wallet

ORIGIN Ether

Home Governan...

Your go-to

Ethereum liquid staki... just had a huge airdrop

Co...

MetaMask

Coinbase W...

12:30

hexpulse.net

0.0046

HEX.COM

CONNECT TO HEX

The HEX ... officially landed 🚀

Received a HEX reward? 👀 Get claiming now!

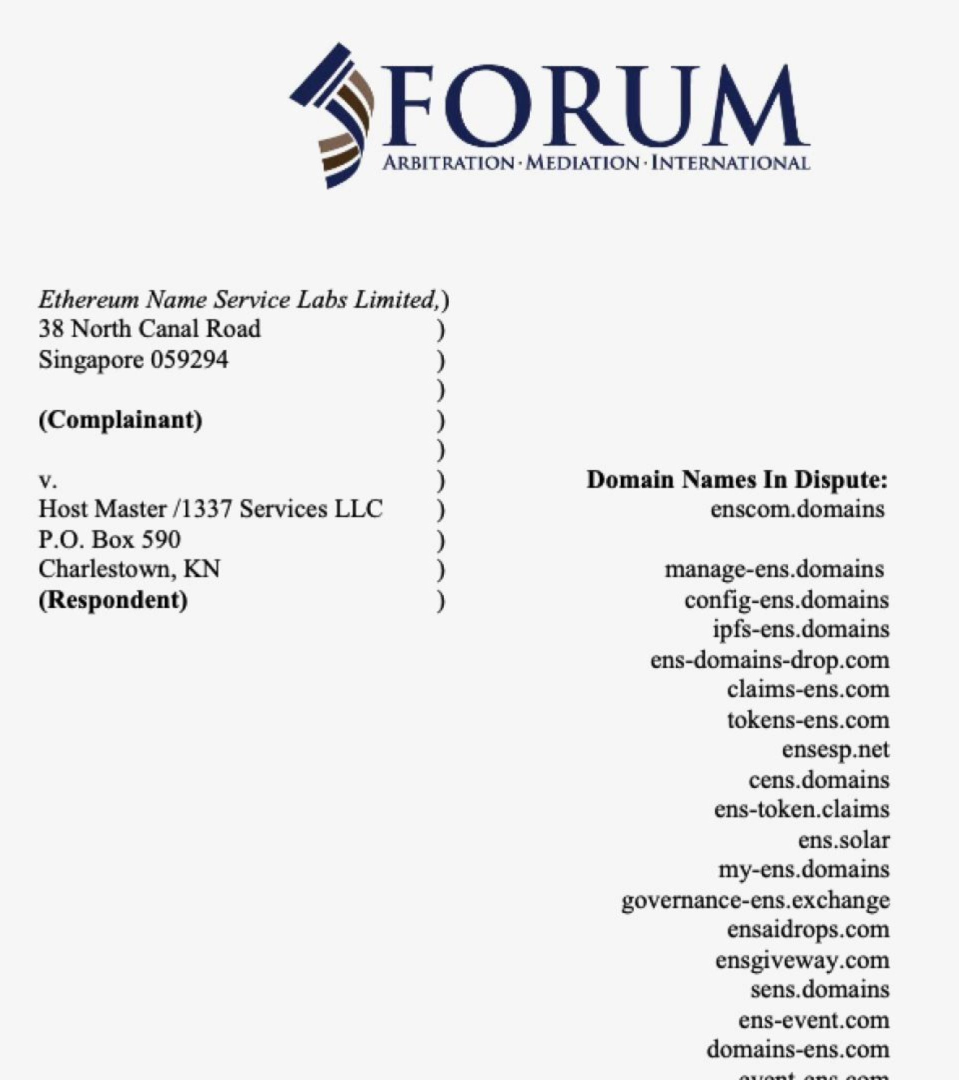
Snapshot taken on 11/28/2023

The airdrop has been secured by Certik

Help the HEX army grow even further,

What to do about all this?

UDRPs
/
Takedowns
/
Blacklists
/
Reports
/



FORUM
ARBITRATION · MEDIATION · INTERNATIONAL

Ethereum Name Service Labs Limited,)
38 North Canal Road)
Singapore 059294)
)
(Complainant))
)
v.)
Host Master /1337 Services LLC)
P.O. Box 590)
Charlestown, KN)
(Respondent))

Domain Names In Dispute:
enscom.domains

manage-ens.domains
config-ens.domains
ipfs-ens.domains
ens-domains-drop.com
claims-ens.com
tokens-ens.com
ensesp.net
cens.domains
ens-token.claims
ens.solar
my-ens.domains
governance-ens.exchange
ensaidrops.com
ensgiveway.com
sens.domains
ens-event.com
domains-ens.com
event-ens.com

A Modest Proposal

Share intel amongst the ecosystem

Pool resources

Reclaim every domain

Change the law

Web3 on the Offense

Come together and file the largest UDRP Complaint ever

Common grievance | Registration pattern | Same rights at issue

Reclaim all 2,200+ threat actor domains

Gather intel from registrations / domains

Warning shot to threat actors

Community is safer together

Thank You for Listening

Let's share intelligence be in touch

Alexander Urbelis

urbelis.eth

General Counsel / CISO, ENS Labs Ltd.

Malika Gazalieva

malikat.eth

Legal research associate, ENS Labs Ltd.