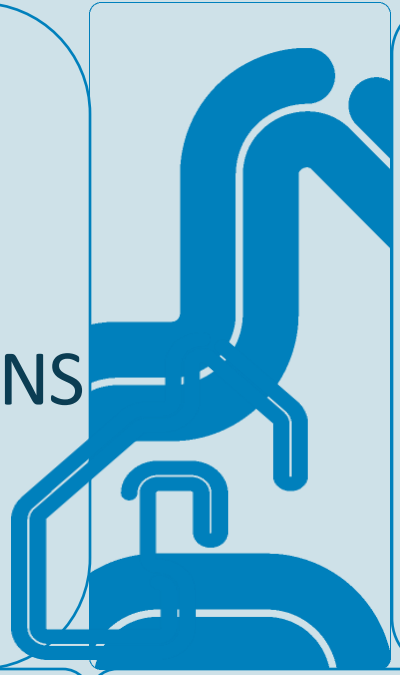
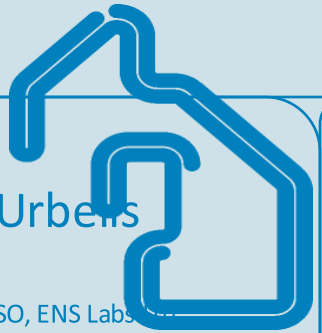
Web2 Woes & Web3 Warfare: Detecting & Dissecting DNS Abuse





Alexander Urbelis
urbelis.eth
General Counsel / CISO, ENS Labs

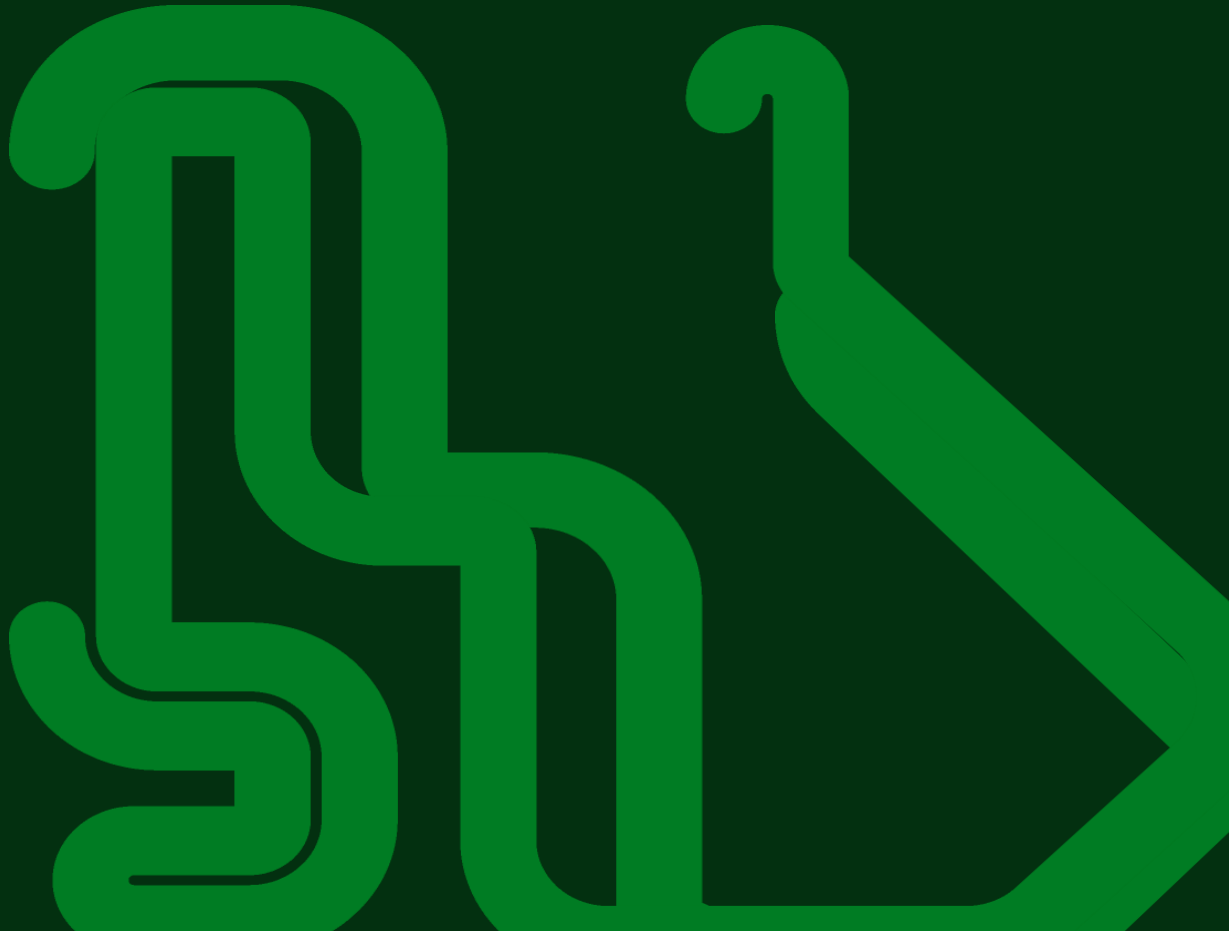
ens

.eth
.cb.id
.base
.linea
.uni

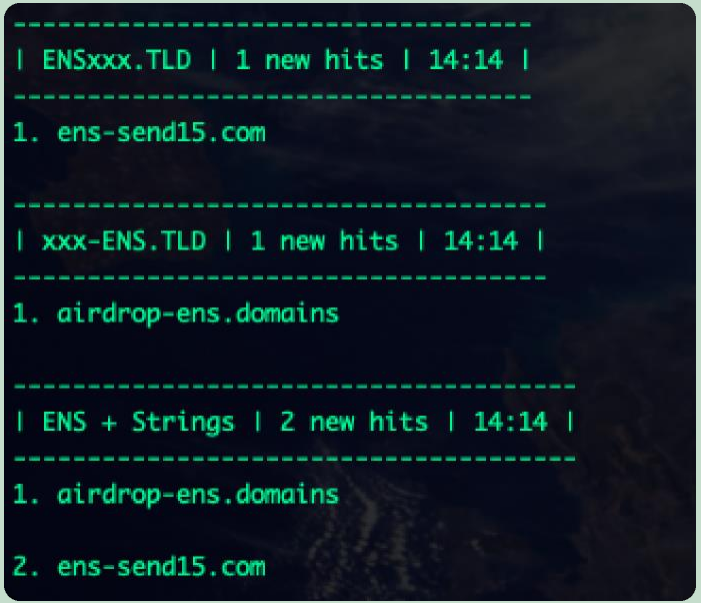
whoami

- General Counsel / CISO of ENS
- Former CISO of NFL
- Professor of Law, King's College, London
- DNS-based cyber threat 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

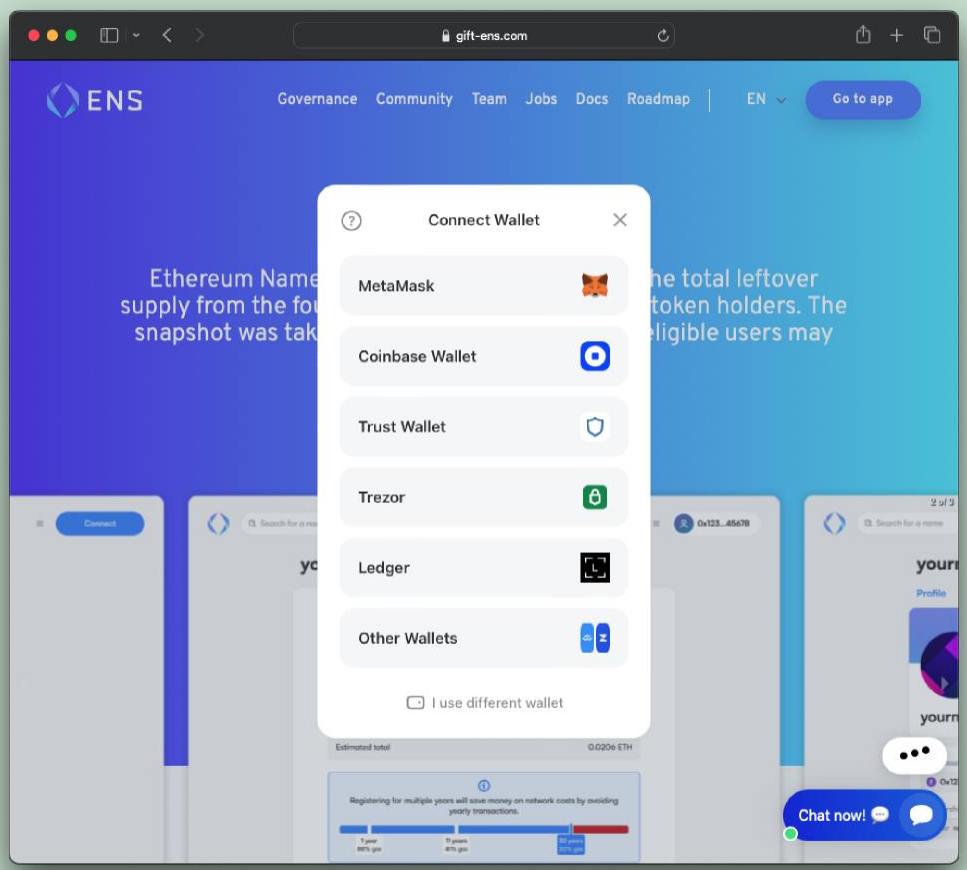
The DNS is Dangerous



Bad Guys Abound



- 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

Clear case of DNS Abuse

Chicken & egg reporting issue

Law enforcement not available

An onboarding concern for web3


|-|-| event-ens[.]net |-|-|
Consistent Thread
[-] Registrant Name: No Data Available
[-] Creation Date: 2024-05-27T04:36:56Z
[-] Registrar: NICENIC INTERNATIONAL GROUP CO., LIMITED
[-] 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

Tracking & Threat Detection

Consistent infrastructure

Consistent DNS configuration

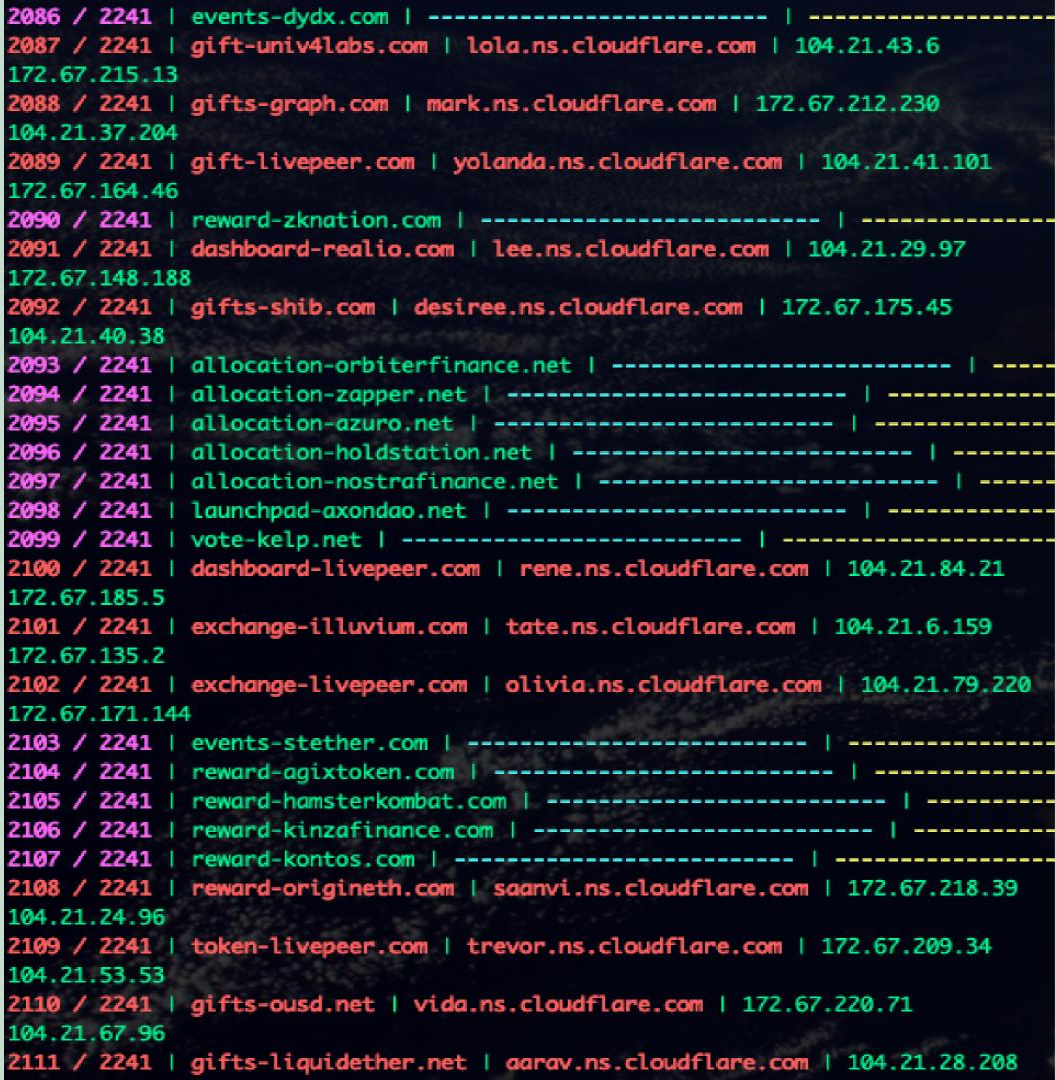
Wrote bash script to track NS record changes every ten minutes

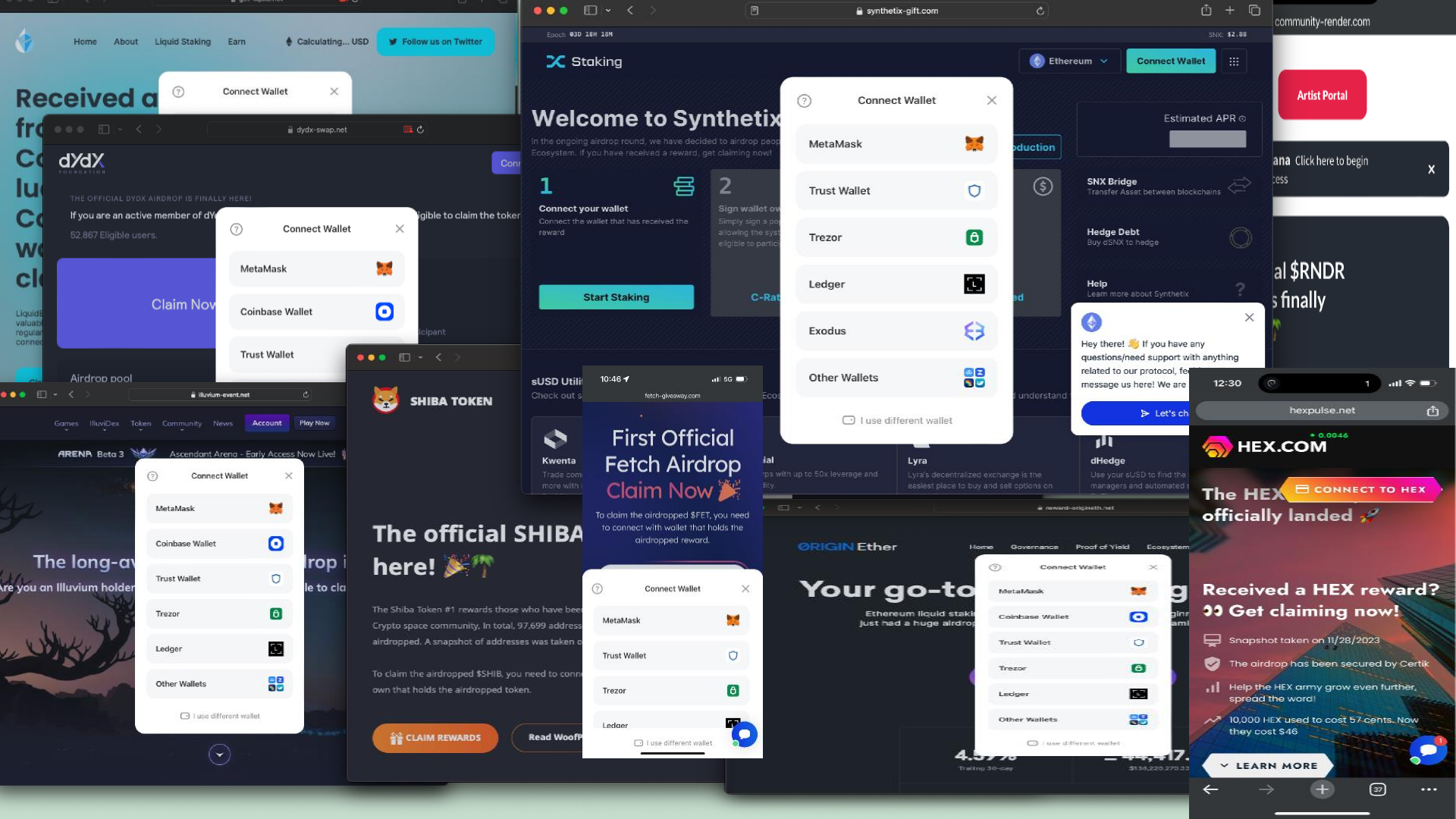
NS records -> Cloudflare = attack

wget -m [target domain]

Evidence and indicators

Reliable early warning system




Connect Wallet
MetaMask
Coinbase Wallet
Trust Wallet
Trezor
Ledger
Exodus
Other Wallets
I use different wallet
Staking
Ethereum
Connect Wallet
Welcome to Synthetix
Start Staking
Estimated APR
SNX Bridge
Hedge Debt
Help
dYdX
Claim Now
Airdrop pool
SHIBA TOKEN
The official SHIBA here!
CLAIM REWARDS
First Official Fetch Airdrop
Claim Now
To claim the airdropped $FET, you need to connect with wallet that holds the airdropped reward.
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, spread the word!
10,000 HEX used to cost 57 cents. Now they cost $46
LEARN MORE
Artist Portal
Hey there! If you have any questions/need support with anything related to our protocol, message us here! We are
Let's ch
Kwenta
Lyra
dHedge
ORIGIN Ether
Your go-to
Ethereum liquid staki
just had a huge airdro
Home
Governance
Proof of Yield
Ecosystem
ARENA Beta 3
Ascendant Arena - Early Access Now Live!
The long-av
Are you an Illuvium holder
Games
IlluviDex
Token
Community
News
Account
Play Now
Follow us on Twitter
Calculating... USD
Liquid Staking
Earn
About
Home

What to do about all this?

UDRPs /

Takedowns / Blocklists

/

Reports /

Always reactive, always chasing

How to get ahead of the game?

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))

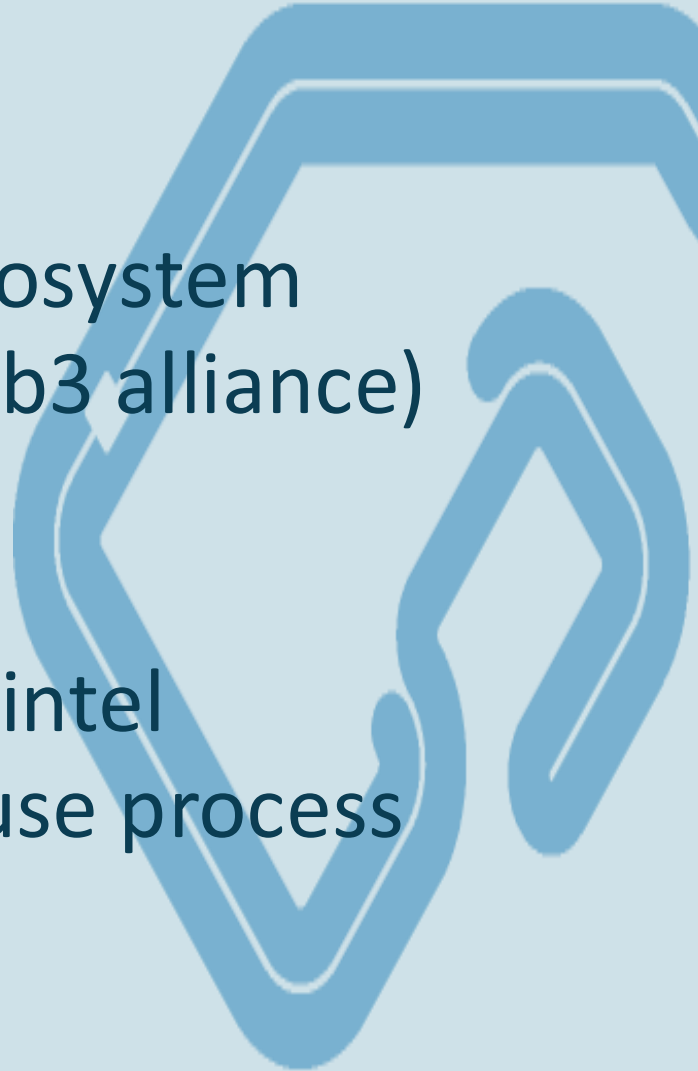
Domain Names In Dispute:
enscom.domains

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
free-ens.com
mint-ens.com
mainnet-ens.domains
clalm-ens.domains

COMPLAINT IN ACCORDANCE WITH
THE UNIFORM DOMAIN NAME DISPUTE RESOLUTION POLICY

A Modest Proposal

Share intel amongst the ecosystem
Disperse through SEAL (web3 alliance) alliance)
Prioritize abuse reporting
Reclaim domains & collect intel
Evolve the UDRP / DNS abuse process



Web3 on the Offense

Common grievance | Registration pattern | Same rights at issue
Come together and file the largest UDRP Complaint ever
Reclaim thousands of malicious threat actor domains
Warning shot to threat actors that we are watching
Gather intel from registrations / domains / logs
Law enforcement involvement / US interest
Evolve DNS Abuse reporting process
Community is safer together

Thank You for Listening

Let’s share intel, be in touch, and connect in Dublin Dublin

Alexander Urbelis
urbelis.eth

General Counsel / CISO, ENS Labs Ltd.

alex@ens.domains

Telegram: aurbelis

X / Twitter: aurbelis

Signal: alex.8998

LinkedIn: