topDNS Best Practice Series Part 6: Addressing, evidencing, and mitigating abuse in Web3

The topDNS webinar on “Addressing, evidencing, and mitigating abuse in Web3” was held on 12 December 2023. This was the sixth in a series of topDNS best practice webinars which showcase what the domain name industry is doing to fight DNS abuse. The webinar was moderated by **Lars Steffen**, Head of International, Digital Infrastructures & Resilience at eco – Association of the Internet Industry.

The specific aim of the webinar was to identify and suggest remediation methodologies to reduce victimisation among online harms in Web3, given that Web3 creates new opportunities for online harm, bad actors, and malicious activities. The details on this initiative were presented by:

- **Chris Lewis-Evans**, Director of Governmental Engagement & Internet Abuse Mitigation, CleanDNS
- **Federico Costa,** Co-founder & CTO, Freename

In his introduction, Chris Lewis-Evans explained that CleanDNS manages abuse handling and mitigation services and accepts reports on abuse within the normal Internet, Web3, and the IP space. On his part, Federico Costa illustrated how Freename acts as the guide to the Web3 domains’ activity platform which enables users to own their TLDs and to understand and register Web3 domains.

Chris proceeded to describe how abuse types can be both common and unique, given that online harms and malicious activities encompass a wide range of negative actions and behaviours that manifest in the digital realm, and that these can have significant consequences for individuals, organisations, or society as a whole. While many of the abuses commonly occur online, there are also abuses that are unique or much more prevalent to Web3. As Chris articulated, CleanDNS and Freename luckily have an evolving understanding of how they can detect and mitigate harms on the Internet, particularly in the context of Web3 adoption.

In examining harms and their impacts in the context of Web3, both Chris and Federico spelt out the range of online and malicious activities. While some of these aspects include malware, botnets, data breaches, non-consensual image sharing, and online predation, the most prominent format that they highlighted was phishing, meaning that Web3 requires an increased concentration on factors such as private keys and fake applications. Moreover, in Web3 databases such as blockchain, spam NFTs (unsolicited non-fungible tokens) can exploit vulnerabilities in smart contracts, causing security risks and financial harms to users. A further issue requiring uppermost attention was seen to be CSAM (child sexual abuse material), with one of the challenges involving the storing of content into the IPFS (InterPlanetary File System).

Regarding other forms of harm, Chris homed in on financially motivated aspects, with one of his insights regarding the unique DeFi (the term used to describe a new category of financial services based on blockchain technology for decentralisation). The keypoint here was seen to be the ability to define aspects such as DeFi and to evidence the different types of harms that can be tackled. Other forms of regulatory harms were noted as the selling of illicit substances, unregulated pharma, and acceptable use policy violations. Furthermore, when it comes to online harassment and human rights violations, both Chris and Federico pointed out how standard Internet harms also have implications for Web3 platforms. These include harms such as cyberbullying, stalking and harassment, doxing (the release of personal information), trolling (deliberately upsetting others), and catfishing (creating a fake identity). Overall, they advised arriving at a consistent definition of what abuse entails and what is needed to evidence abuse in order for appropriate action to be taken.

Chris proceeded to state that a guide to evidencing and reporting online harms is essential to address and combat malicious Internet activities effectively and in a timely manner. In documenting the evidence, he accentuated just how important screenshots are: for example, if there is a list of NFTs "pushed into" a wallet, being able to capture and show their inaccuracy is paramount. From his angle, Federico also stressed how important it is to not only track and copy the wallet address, but also the smart contract address. If, for example, a token has been used or there has been interaction with a smart contract, each kind of integration is tracked on the blockchain with a specific transaction identity. He proceeded to note that copying and keeping track of these is important for documenting evidences regarding potential stealing of personal assets or other types of harm.

Further effective approaches including saving messages, recording full URLs, downloading content, user information, preserving metadata, supporting statements, maintaining detailed records, and recording full email header data.

Chris and Federico's consequent recommendations on reporting the harm included a range of options: for instance, reporting to the platform; contacting law enforcement (which is imperative if there is a criminal offence); using third-party reporting tools; contacting support organisations; seeking legal advice; encouraging collective reporting; monitoring and following up; and, ultimately, prioritising one's safety. With regard to the latter, Chris noted that, given the availability of multiple high-quality cybersecurity professionals, what can make the most sense is to report the abuse and request for it to be dealt with by a technical party.

Relevant fields for data mapping

In sharing information on relevant fields for data mapping, Federico stated how important it is to keep track on the blockchain environment and free domains. In dealing with the blockchain, assets are dealt with in the digital environment with their own specific characteristics. While Web3 identifiers contain records, it differs from the standard domain, given that the DNS records are stored into the identifier itself in the blockchain and not outside. In this respect, records are an important feature of the NFT entities, allowing users to customise their own resolving preferences. Each identifier contains information to resolve specific payment addresses, to manage DNS information, IPFS websites, domain redirects and much more. In the Web3 namespaces registry, a record is managed through a Key-Value combination. Given a Key, there is a corresponding value associated that could be inserted as a text or a message, an address, a URL, a TXT record, an A record, a CNAME record, an NS record, or wallet addresses. Furthermore, as Federico remarked, users can set their own records directly in the Web3 name registrars, while developers can configure their own records or resolve specific records using APIs, SDK or directly interacting with the Smart Contract. Last but not least, Federico noted how browsers resolve these records via APIs or gateways.

In responding to a query regarding how to identify the blacklists for Web3 and what tools are available for these, Federico also explained that there are currently different platforms that can collect this kind of data. One example that he noted related to the Chain Analysis company that keeps track of all the blockchain transactions and sees whether value has been stolen or whether transaction has occurred. Federico also drew attention to Tenderly, which helps to stimulate the execution of the transaction before it is written. He also acknowledged that there is currently no mechanism such as the classic DNS RPZ (Response Policy Zones) for propagating blacklist information, with companies such as Freename and CleanDNS running reporting tools and collecting data to resolve such situations.

In complying with the viewpoint of another attendee, Chris agreed that CSAM should clearly not be downloaded. In a similar vein, he noted that PII (Personally Identifiable Information) should also not be downloaded, with this being illegal in many countries. In such instances, his advisable approach was to record and report on the full string from where such content has been displayed.

Availability of data to support reports

In contrast to conventional web systems, Federico once again clarified that the Web3 space resides within the blockchain, signifying a distinct approach in data management and storage. In availing of data to support reports, he noted how one should bear in mind that Web3 entities are not directly affiliated with any one person. Federico also stated that it makes sense to link to blockchain wallets, meaning that an asset itself can be linked to – and even defined by – a blockchain. This linkage can be administered by a human user or controlled through a software application. Federico also recommended to support reports via airdrop activities, which can conduct the establishment of Web3 entities. Other important factors noted included behaviour across namespaces: as every transaction is visible on blockchain, everyone can keep track of everything and can see how the money flows.

Mitigation of harms in Web3

In addressing the mitigation of harms, Chris stated the security by design, noting just how important it is to integrate security measures into Web3 applications and platforms, and how essential it is to build blocklists into browser integration to prevent access to harm. In turning towards the factor of regulatory frameworks, he pinpointed that some of the Web3 principles entail community self-governance regulations built in by the users, enabling users to manage the governance. Furthermore, he regarded reporting of harms – via standard evidence packages or reporting to law enforcement – as imperative in enabling mitigative action.

Summary of recommendations

In their conclusion of the webinar, Chris and Federico summarised five recommendations:

- A common abuse reporting tool;
- Creation and maintenance of evidencing standards;
- Ongoing measurement, tracking and reporting on trends, volumes and demographics;
- A framework for commitment to mitigate harms in the Web3 marketplace;
- The creation of community/platform norms.

In drawing to a close, Federico emphasised that such standard checks and prevention can lead to the avoidance of downloading abuse content or CSAM, with standardisation activities and data analytic tools helping to progressively move Web3 into the future.