topDNS Best Practice Series: How is DNS Abuse Actually Measured?

On 8 October 2025, eco – Association of the Internet Industry hosted the 10th session of its topDNS Best Practice Series, titled “How is DNS Abuse Actually Measured?”.

The webinar was moderated by Lars Steffen, Head of Digital Infrastructures, Resilience and International at eco.

Reports from the constituencies were provided by:

- **Maciej Korczyński**, Professor, KOR Labs
- **Sourena Maroofi**, Founder, URLAbuse
- **Rowena Shoo**, Director of Programs & Policy, NetBeacon Institute

Together, they came together for a deep dive into how DNS abuse is measured in practice, and explored the advantages, challenges, and limitations of different methods.

Introduction

The 10th session of the topDNS Best Practice Webinar Series explored how DNS abuse is detected, measured, and mitigated. **Lars Steffen**, Head of Digital Infrastructures, Resilience and International at eco, opened the webinar by welcoming the three core participants and emphasizing the importance of collaboration across multiple stakeholders, including registries, registrars, hosting providers, and security researchers. As Lars noted, topDNS is a collaborative initiative focused on DNS abuse, with sponsors and additional supporters providing support in the topDNS webinars and workshop sessions throughout each year.

DNS abuse encompasses a wide spectrum of malicious activity, including phishing, malware distribution, compromised websites, and other forms of harm that exploit the Domain Name System. The session highlighted that measuring DNS abuse is complex: it requires rigorous data collection, careful analysis, and structured mitigation approaches.

Subsequently, the speakers discussed the methodological and technical challenges inherent in defining, detecting, and acting on DNS abuse. They also explored how measurement can inform mitigation strategies, prioritize interventions, and support cross-industry coordination.

Maciej Korczyński, KOR Labs

Maciej Korczyński, Professor at Grenoble Alpes University and researcher at KOR Labs, presented the methodology used by KOR Labs for systematic, multi-level measurement of DNS abuse. His talk, titled "Evidence to Action: Measuring Abuse Persistence", described how their research platform monitors and analyzes the lifecycle of malicious online activity – from detection to mitigation.

He noted that, at KOR Labs, the system ingests multiple types of inputs, including malicious URLs, phishing URLs, and malware delivery URLs. It performs both passive data information and active collection (interactive crawling), retrieving page content and transaction traces (HAR logs). KOR Labs collects artifacts related to downloaded resource fingerprints.

The platform examines websites at three levels:

1. **Root domains** – the highest level of domain hierarchy.
2. **Fully Qualified Domain Names (FQDNs)** – subdomains that may be hosting malicious content.
3. **URLs** – specific malicious web addresses.

In addition, it performs active scans of various DNS records and collects registration information. Based on this comprehensive dataset, KOR Labs provides contextual risk and reputation assessments, performs domain classifications, and measures uptimes.

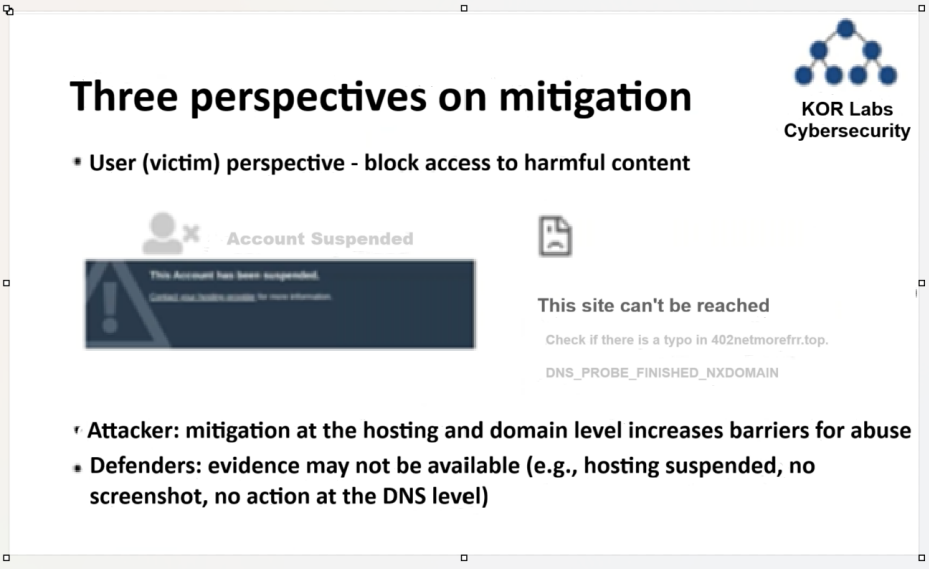
Maciej explained that the definition of uptime can vary slightly across research studies, but generally it represents the time elapsed between a URL being blocklisted (by the Anti-Phishing Working Group, for example) and its mitigation at the DNS or hosting level.

Mitigation may occur through actions by authoritative name servers, suspension of the website's hosting, or deactivation of the hosting account. Data collection integrates passive monitoring (DNS queries, network traces) with active methods (interactive crawling, content downloads, fingerprinting). Screenshots and HAR logs document content and behavior, while resource fingerprints help classify domains as either maliciously registered or compromised.

Uptime measurement is a central metric. KOR Labs defines uptime as the time elapsed from a URL being blocklisted to its mitigation at the DNS or hosting level. This allows analysis of both mitigation speed and effectiveness across various infrastructures.

Maciej emphasized three key perspectives on mitigation:

- **User (victim) perspective:** Abuse should be neutralized as quickly as possible to prevent users from exposure to phishing or malware.
- **Attacker perspective:** Mitigation should ideally occur at both the hosting and domain levels to reduce the potential for reuse of malicious infrastructure. If only hosting is suspended, attackers can re-register elsewhere and point the domain to new infrastructure within seconds. If only the domain is suspended, attackers can register new domains and continue operations.
- **Defenders' perspective:** Hosting providers, registrars, and registry operators face challenges – particularly around evidence availability. If hosting is suspended first, defenders at the DNS level may not see sufficient evidence to justify further action, creating coordination gaps.



As Maciej noted, several case studies illustrated real-world complexity. For example, phishing websites targeting financial institutions were mitigated at different levels – some via DNS record suspension (with server hold status indicating registry action), others through hosting account suspension. Subdomain hosting services like Firebase add further complexity, as malicious activity could occur without affecting the primary domain. In these cases, mitigation happens at the URL or subdomain level rather than the domain name level.

One particularly interesting example showed a domain that was initially mitigated at the DNS level (NXDOMAIN), then later restored – possibly after the registrant contested the action – before ultimately being properly mitigated at the website level with a 404 error.

Key Insights from KOR Labs' Approach:

- Multi-level tracking provides a nuanced understanding of online abuse.
- Mitigation speed varies depending on whether action is taken by registries, registrars, or hosting providers.
- Attackers exploit infrastructure gaps, making continuous monitoring essential.
- Collecting and interpreting evidence is not trivial, and measurements require careful analysis.

Sourena Maroofi, URLAbuse

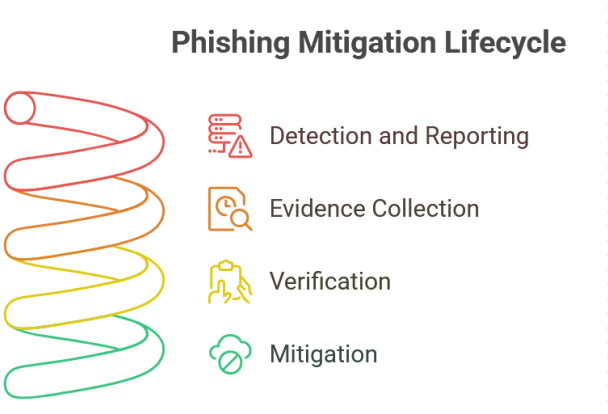
Sourena Maroofi, Founder of URLAbuse, presented insights on phishing trends, the takedown procedure, role of blocklist feeds in detection, and the evolving methodologies behind identifying and mitigating phishing activity. His talk examined both data trends and structural challenges within the DNS abuse ecosystem, focusing on evidence collection, coordination, and modern detection methods.

Sourena began by comparing phishing statistics from Interisle and NetBeacon. Both datasets, derived from COMAR-based methodologies, showed a consistent increase in malicious registered domains, going higher every year. From 2024 to 2025, both reports indicated increases of 8% (Netbeacon) and 35% (Interisle) respectively.

Despite ongoing efforts by registries, registrars, and security organizations, phishing continues to rise. Sourena emphasized that the challenge is not individual capability, but rather gaps in coordination and information sharing among the different actors in the ecosystem.

He outlined the typical lifecycle of phishing mitigation:

1. **Detection and Reporting:** Blocklists, security vendors, or individual analysts identify suspicious URLs.
2. **Evidence Collection:** Screenshots, metadata, and network traces are gathered to verify phishing activity.
3. **Verification:** Reports are sent to registries or registrars for confirmation.
4. **Mitigation:** If verified, domains or hosting accounts are suspended or blocked.



Sourena emphasized that the collection of actionable evidence is the main bottleneck in this process. Coordination often breaks down between entities at the handoff points between detection, verification, and mitigation.

Phishing campaigns increasingly use sophisticated evasion techniques including geolocation restrictions, time-based activation, and specific user-agent configurations, making automated evidence collection difficult. Registrars require concrete proof – typically screenshots and network data – before taking action. This positions blocklists as critical intermediaries that bridge technical verification with operational enforcement.

Furthermore, Sourena shared examples from URLAbuse's work, such as phishing campaigns targeting U.S. toll systems that displayed fake pages only to users in specific states. Large-scale campaigns often register hundreds of domains daily, requiring precise timing and contextual knowledge to capture valid evidence.

He noted that WHOIS records alone are insufficient, since they do not demonstrate active malicious behavior. The key question became: "Who is in the best position to collect evidence?" His answer: blocklists themselves have the methodological insight, and can collect evidence at the right time with the right parameters.

He then distinguished between two primary types of blocklists:

- **Traditional Blocklists** rely on email honeypots, third-party reports, and reverse IP lookups. While simple and scalable, they often produce false positives due to inconsistent naming, unverified reports, or shared hosting environments (e.g., CDNs).
- **Modern Blocklists** leverage automated detection, machine learning, and campaign tracking to identify phishing domains more reliably. They standardize naming conventions, follow campaign evolution, and continuously refine accuracy through expert feedback.

At URLAbuse, each domain is manually verified before being listed, ensuring transparency about why it was blocklisted. This approach increases trust and allows users and partners to understand the rationale behind each entry.

Sourena also described URLAbuse's daily operations, which include the following: analyzing phishing and phishing-as-a-service infrastructures; training and refining machine learning detection models; scanning hundreds of millions of Fully Qualified Domain Names (FQDNs); and verifying third-party reports and preparing evidence packages for takedown actions.

Finally, he encouraged greater collaboration across the ecosystem:

- **Reporters** can obtain tokens to submit phishing URLs, with submissions made publicly accessible.
- **Registries and registrars** can use URLAbuse data to support takedowns.
- **Researchers** can leverage the dataset to train or benchmark detection systems.

He concluded that strengthening the connections and coordination among evidence collectors, blocklists, and mitigation actors is critical to reducing phishing persistence.

Key Insights from URLAbuse Approach:

- Phishing is rising continuously, driven by both campaign complexity and gaps in coordination.
- Evidence collection is the central challenge, especially for geographically or temporally targeted campaigns.
- Modern blocklists using machine learning and campaign tracking improve accuracy and standardization.
- Collaboration across reporters, registries, and blocklists is essential for effective mitigation.

Rowena Shoo, NetBeacon Institute

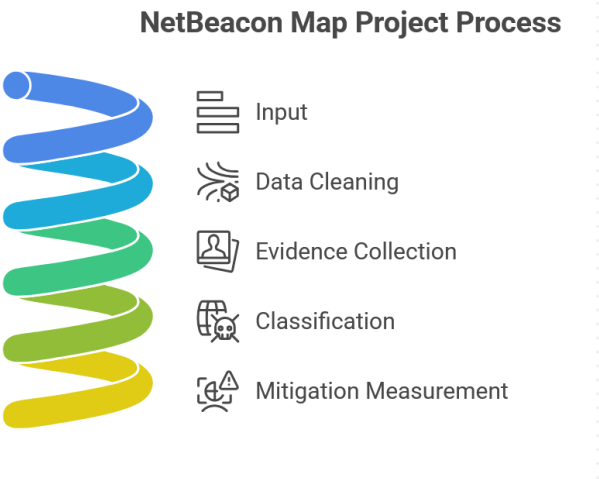
Rowena Shoo, from the NetBeacon Institute, presented an overview of NetBeacon Map, a measurement and analytics platform designed to understand the distribution and mitigation of DNS abuse. NetBeacon was created in 2021 by the Public Interest Registry, operating with external focus while collaborating with TLD registries, registrars, hosting providers, and stakeholders outside the industry. Its mission is to foster a safer Internet by analyzing DNS abuse including phishing, pharming, malware delivery, botnets, and spam when used as a delivery mechanism.

Rowena focused on NetBeacon Map, developed in collaboration with KOR Labs to understand how DNS abuse is distributed across the ecosystem, where it concentrates, whether it is being mitigated, and whether domains are maliciously registered or represent compromised websites.

This distinction between maliciously registered domains and compromised websites is critical because compromised websites are typically not appropriate for DNS-level mitigation due to potential collateral damage.

The NetBeacon MAP project follows a structured, evidence-based process:

- **Input:** Four reputation blocklists provide the initial dataset.
- **Data Cleaning:** KOR Labs performs deduplication, removes IP addresses, and filters out "special domains" (e.g., URL shorteners, dynamic DNS providers, or file-sharing services) inappropriate for DNS-level mitigation.
- **Evidence Collection:** Screenshots, fingerprints, and metadata are gathered to determine whether domains are maliciously registered or compromised.
- **Classification:** A proprietary system developed by KOR Labs for MAP – independent of earlier AFNIC and SIDN work – applies multiple indicators to make this determination.
- **Mitigation Measurement:** KOR Labs tracks whether harm has stopped, regardless of who acts (registry, registrar, or host), taking a holistic and attribution-agnostic approach.



Different TLDs and registrars often show varying proportions of malicious versus compromised domains, as domains typically need to exist for some time before being compromised. Measurements occur at regular intervals over 30 days, allowing analysis

of mitigation speed and persistence. Because the project prioritizes accuracy over coverage, providers may observe fewer cases in MAP than in their own abuse desks. Each month's dataset is treated as a standalone snapshot, with domains counted when identified as abusive rather than when registered.

Rowena emphasized that NetBeacon's mitigation measurements are holistic and attribution-agnostic. When a domain shows as "mitigated," it means the harm has stopped – but this could have occurred through registry action (server hold); registrar action (client hold); hosting provider suspension; and law enforcement intervention. This comprehensive approach focuses on outcomes rather than attributing responsibility to specific entities.

Addressing the prevention of malicious registrations, Rowena noted this as an emerging challenge. While much of the industry focuses on post-evidence mitigation, high volumes of malicious registrations require earlier intervention. MAP data reveals that such registrations are often clustered in specific campaigns targeting particular registrars or registries. She recommended:

- Analyzing previously mitigated domains for common traits (e.g., domain strings, client accounts, registration timing, API usage, or payment method).
- Watching for emerging naming patterns such as "GovDash" and "ComDash."
- Using payment-provider anti-fraud tools to assess registration risk at the point of purchase.

As Rowena noted, one registrar successfully reduced abuse by restricting cryptocurrency payments to trusted customers. These proactive measures, she said, complement reactive mitigation.

Rowena concluded by highlighting NetBeacon Reporter, a companion project connecting defenders (registries, registrars, and hosting providers) with report submitters. The system verifies reports as they flow through, providing evidence to support takedown actions. She encouraged participants to explore and adopt NetBeacon's free tools and workflows to strengthen global mitigation efforts.

Key Insights from NetBeacon Institute Approach:

- DNS abuse is unevenly distributed across the ecosystem; understanding local patterns is critical.
- MAP's academically rigorous, transparent methodology distinguishes malicious from compromised domains – essential for appropriate mitigation.
- Mitigation measurements are holistic and attribution-agnostic, capturing whether harm has ceased across all intervention levels.

- Proactive pattern recognition and anti-fraud measures help prevent abuse at registration, complementing reactive mitigation.
- Open data and collaborative tools promote transparency and continuous improvement across the DNS abuse mitigation ecosystem.

Conclusion

The session concluded that effectively tackling DNS abuse requires more than technical precision – it demands coordination, transparency, and shared responsibility across the entire Internet ecosystem.

From rigorous, evidence-based measurement frameworks developed by KOR Labs, to advanced detection and verification processes led by URLAbuse, to NetBeacon's open and collaborative analytics platforms, the webinar showcased how diverse initiatives are aligning toward the same goal: reducing abuse persistence and improving the safety and reliability of the Domain Name System.

As Lars Steffen from eco emphasized in closing, there is no single solution or "one-stop shop" for combating DNS abuse. Meaningful progress depends on sustained collaboration among registries, registrars, hosting providers, security researchers, and reporting networks. Through continued partnership and knowledge exchange – including initiatives like topDNS, NetBeacon, and URLAbuse – the Internet community is building a stronger, more resilient foundation for DNS abuse prevention and mitigation.

Reference

- topDNS webinar recordings and reports: topdns.eco