Public Comment on the Preliminary Issue Report on DNS Abuse Mitigation

Abstract
With this comment we aim to highlight the need for additional transparency for effective DNS abuse mitigation. Based on our collaborative research on *transient domains*, we show that a measurable fraction of malicious domains evade current detection and reporting frameworks due to the lack of fine-grained and timely access to zone change information. We recommend that the forthcoming Policy Development Process explicitly address the visibility gap in DNS operations as a prerequisite for effective mitigation and accountability.

Comment
We welcome the opportunity to contribute to the discussion initiated by the Preliminary Issue Report on DNS Abuse Mitigation. The report correctly identifies contractual and procedural mitigation gaps, but it overlooks a more fundamental one that affects the entire DNS abuse lifecycle: the lack of structural visibility into how domains appear, change, and disappear from the DNS.

Our recent work in collaboration between the University of Twente, CAIDA, Stanford University, and SIDN Labs has shown that the current data-sharing model provides only a limited and delayed view of the DNS namespace. In our study, *DarkDNS: Revisiting the Value of Rapid Zone Updates* (IMC 2024)[1], we measured a persistent visibility gap in the ICANN Centralized Zone Data Service (CZDS), where at least one percent of newly registered domains never appear in the daily zone snapshots. These *transient domains* exist for less than 24 hours and are frequently associated with abuse, including phishing and spam campaigns. Because of their short lifetime, they evade both compliance checks and post hoc analyses, effectively operating in the blind spots of the DNS ecosystem.

Without more timely visibility into zone changes, any policy and security intervention will remain reactive. The lifecycle of transient domains is shorter than the reporting and enforcement cycles of registrars, which means that abuse is often completed before detection. A more structural and near real-time view of DNS changes would allow researchers, registries, and trusted operators to better quantify abuse, identify systemic vulnerabilities, and evaluate the actual impact of policy and security measures.

In addition, in our recent ICANN83 presentation (*Lost in Transit: A First Look at Residual Traffic from Transient Domains*) [2] we showed that improved visibility would directly help recursive resolvers to flush transient domains from caches, reducing the collateral effects of stale malicious entries. Timely access to zone change data would also allow Certificate Authorities to revoke certificates bound to already expired domains, improving the trustability of the TLS ecosystem and extending the security benefit beyond DNS into the broader Internet trust infrastructure.

Increased transparency should not stop at near real-time zone deltas. It should also include easier and more structured processes for access to registration data in bulk and at scale.

Facilitating controlled access for vetted security researchers and operational experts would enable correlation of attacker behaviour across different registries and registrars, using privacy-preserving identifiers such as anonymized but correlatable hashes. This would provide visibility into coordinated abuse campaigns and systematic misuse of registrar services, which remain largely opaque today. Access to reliable registration timestamps and consistent registrar identifiers would also enable the detection of bulk and automated registration patterns, as highlighted in the INFERMAL study referenced in the Preliminary Issue Report. These improvements would strengthen evidence-based approaches to identifying registrars that systematically enable or tolerate abusive behaviour.

We recognize that real-time and large-scale data sharing raises operational and privacy considerations. However, a controlled, auditable, access-vetted model, analogous to the transparency framework deployed by Certificate Transparency (which logs certificate issuance in append-only public logs, enabling auditors to monitor certificate issuance and detect abuse), could enable safe and effective sharing of near real-time zone changes and registration information.. Reviving the concept of Rapid Zone Update Sharing [3] within a modernized transparency framework would be a concrete step toward closing the visibility gap that enables DNS abuse to proliferate.

We therefore recommend that the GNSO Council explicitly incorporate the need for *augmented visibility (i.e., additional registration information) and more fine-grained visibility (i.e., real-time updates)* into the upcoming Policy Development Process on DNS Abuse Mitigation. Without addressing this foundational issue, any policy will continue to operate with limited situational awareness and constrained effectiveness.

Sincerely,
Raffaele Sommese (University of Twente),
Gautam Akiwate (Stanford University),
KC Claffy (CAIDA)

References:

[1] Sommese, Raffaele, Gautam Akiwate, Antonia Affinito, Moritz Müller, Mattijs Jonker, kc claffy. "DarkDNS: Revisiting the Value of Rapid Zone Update." ACM Internet Measurement Conference (IMC), Nov. 2024, https://doi.org/10.1145/3646547.3689021

[2] Sommese, Raffaele, “Lost in Transit: A First Look at Residual Traffic from Transient Domains”, ICANN 83 Presentation - SSAC Lightning Talk https://static.sched.com/hosted_files/icann83/5b/Rafaelle%20Sommese%20ICANN%2083%20Lost%20in%20Transit.pdf?_gl=1*1gtvc4b*_gcl_au*MTk3NjE4NjY2MS4xNzU3NDk1NzY3*FPAU*MTk3NjE4NjY2MS4xNzU3NDk1NzY3

[3] Verisign. Application for Registry Service: “Rapid Zone Updates” (2007). https://www.icann.org/en/system/files/files/memo-dnsupdate-service.pdf.