Nadezhda Arteeva,
ICANN@NextGen

DNS ABUSE IN THE EU

Why is it important and how to tackle it?

WHAT IS DNS ABUSE?

- Difficult to define because "New types of abuse are commonly created, and their frequency waxes and wanes over time." (ICANN Security and Stability Advisory Committee, 2021)
- Recent EU report suggests it "is any activity that makes use of domain names or the DNS protocol to carry out harmful or illegal activity."

THE EVOLUTION OF THE ISSUE

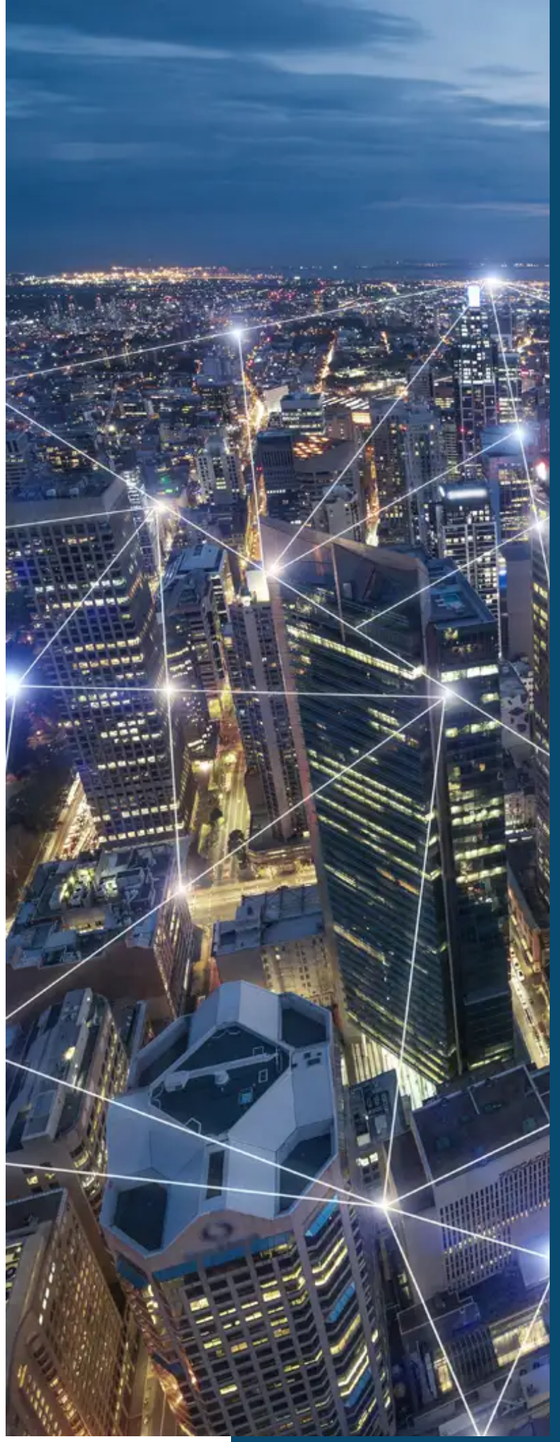
- The contractual provisions governing DNS abuse originally came from policy work done by the ICANN community in 2009 and 2010 through the Registration Abuse Prevention Working Group (RAPWG).
- More than six years ago, in SAC077, the SSAC wrote about ICANN's proposed marketplace health index:
  - "To develop and maintain effective metrics of security and stability of the gTLD ecosystem, ICANN will have to undertake auditing activity, including mandating future disclosure of aspects of registry and registrar operations and behavior, in a form that emphasizes consumer protection over industry norms."
- Not much has been done in the following years, the response has been critiqued, especially during the pandemic (see Krebs, 2020), however, now the issue is one of the top ICANN's agendas.

WHAT LETS DNS ABUSE HAPPEN?

- 2021 study suggests that:
  - Registration contact data is redacted for 57% of all generic Top-level Domain (gTLD) names
  - Only around 11.5% of domains may belong to natural persons who are subject to GDPR
  - 85% of gTLD domain registrants can no longer be identified
- Long lifetime of a DNS abuse report - 32 days (Forsberg, 2022)
- Lack of knowledge about DNS abuse and required actions if encountered

HOW TO TACKLE DNA ABUSE IN THE EU?

- Selecting providers with more validation standards for domain registrations (ex.: customer validation approach)
- Initiate prevention and remediation solutions (ex.: proactive detection of suspicious domain names containing targeted brand keywords)
- Increase adoption of security controls (ex.: registry locks)
- Better standards in top-level domains (TLDs) (ex.: blocking programs — leveraged by the Donuts DPML program)



BIBLIOGRAPHY

- European Commission, Directorate-General for Communications Networks, Content and Technology, Paulovics, I., Duda, A., Korczynski, M. (2022). *Study on Domain Name System (DNS) abuse*, https://data.europa.eu/doi/10.2759/616244
- Forsberg, L. (2022, January 26). DNS Abuse: Everyone's Problem. Dotmagazine. https://www.dotmagazine.online/issues/the-heart-of-it/building-trustworthiness/dns-abuse
- ICANN Security and Stability Advisory Committee. (2021). SSAC Report on an Interoperable Approach to Addressing Abuse Handling in the DNS (No. SAC115). ICANN. https://www.icann.org/en/system/files/files/sac-115-en.pdf
- ICANN Security and Stability Advisory Committee. (2016, January). SAC077: SSAC Comment on gTLD Marketplace Health Index Proposal. ICANN. https://www.icann.org/en/system/files/files/sac-077-en.pdf
- Krebs, B. (2020, April 16). Sipping from the Coronavirus Domain Firehose. Krebsonsecurity. Retrieved June 7, 2022, from https://krebsonsecurity.com/2020/04/sipping-from-the-coronavirus-domain-firehose/