Joint AFRALO-AfrICANN Meeting
ICANN71 Virtual Policy Forum

Wednesday, 16 June 2021

DNS Abuse Mitigation Strategies

We, the African ICANN Community members participating in the ICANN 71 Virtual Policy Forum in the *Hague* and attending the Joint AFRALO/AfrICANN meeting on Wednesday, 16 June 2021, discussed the issue of Domain Name System (DNS) Abuse and the importance of having a unified strategy for DNS abuse mitigation that includes all stakeholders.

DNS Abuse is a broad term that essentially refers to the use of the DNS in conducting fraudulent and/or malicious acts over the Internet. To be able to respond to DNS abuse incidents as well as eliminate them as much as possible, collaboration among all relevant stakeholders is necessary. ICANN as the primary entity responsible for the security and stability of the DNS plays a key role in ensuring that technical issues that allow the misuse of the DNS are identified and resolved; reaching out to relevant stakeholders to address relevant deployment issues, such as distributed denial-of-service (DDOS) attacks that use the DNS and raise awareness and promote good practices.

A successful DNS Abuse mitigation strategy needs to consider the following elements:

- Methods and quality of abuse reporting
- Ability to identify where the threats lie, whether within a specific domain or from a technical point of view - such as threats due to deployment issues
- Providing incentives that promote the adoption of good practices
- Standardizing definitions and methods of mitigation
- Educational material and raising awareness
- Collaboration among all stakeholders. Collaboration is a main and essential element for efficient and effective DNS abuse mitigation.

Current efforts that address the DNS abuse mitigation strategy elements include:

- ICANN Domain Abusive Activity Reporting (DAAR) project, which is a good start for studying and reporting domain name registration and security threats across top-level domain (TLD) registries. The system allows TLD registries to see where the threats are concentrated within the TLD and how this threat changes over time. Thus, the system gathers and provides information that could be helpful to mitigate DNS Abuse.

However, wider registry participation is necessary to identify threats within more TLDs. We also propose inclusion of people and institutions interested and involved in monitoring DNS abuse as observers in groups such as TLD-OPS that is within the Country Code Name Supporting Organization (ccNSO)

- The responsibility for working on resolving DNS design and deployment issues that have enabled DNS abusive acts does not primarily fall on ICANN, but on DNS operators and network operators as well as manufacturers. However, ICANN should improve on their outreach to the stakeholders, to make them aware of the unresolved issues and promote the solutions.
- Working on maintaining an up to date registrants' database previously known as WHOIS. However, as this is still a work in progress it is still uncertain that cybersecurity practitioners would be able to obtain registrant's data related to abusive domains involved in botnets, malware or other forms of fraud in a timely manner. Similarly timely responses in relation to phishing and trademark infringement are still doubtful.

Recommendation:

Looking at the aforementioned DNS abuse mitigation strategy elements and some of the current efforts in this regard it is evident that collaboration between stakeholders is essential. Therefore, we suggest that ICANN creates a platform through which all stakeholders can work together to implement the above DNS abuse mitigation strategy elements , raise awareness and share information and data. The platform would allow stakeholders to agree on broad mitigation methods definitions, actions, tools, and try to balance security and privacy issues.

Drafting. Team

1. Hadia ELminiaw, hadia@tra.gov.eg
2. Chokri Ben Romdhane, chokribr@gmail.com
3. Kaddyjatou Drammeh, kaddyjatou2@gmail.com
4. Sarah Kiden, skiden@gmail.com
5. Barrack Otieno otieno.barrack@gmail.com