EUROPEAN COMMISSION
DIRECTORATE-GENERAL FOR COMMUNICATIONS NETWORKS, CONTENT AND TECHNOLOGY

Future Networks
Next-Generation Internet

Brussels, 7 January 2021
CNECT.E.3.022/TDH

SUBJECT: Your contribution to the Study on Domain Name System (DNS) Abuse

Dear Sir, / Dear Madam,

A safe and secure Domain Name System (DNS) is of paramount importance for the digital economy and society. Malicious activities on the DNS, generally referred to as "DNS Abuse", are a frequent and serious problem affecting online security and undermining users' trust in the internet. On one hand, DNS Abuse is composed of cybersecurity threats (e.g. DDoS attacks, Spam, Phishing, Malware, Botnets) aiming at disrupting the DNS and the internet infrastructure or at exploiting it to perpetrate crimes. On the other hand, there is the distribution of illegal material on the internet, e.g. child sexual abuse material, material infringing Intellectual Property Rights (IPR), sales of counterfeit drugs, using domain names to do so.

Against this background, the European Commission commissioned Fasano Paulovics Società tra Avvocati and Institut Polytechnique de Grenoble (collectively "the Contractor") to carry out a Study on Domain Name System (DNS) Abuse, EC reference VIGIE 2020/0653 ("the Study").

The objectives of the Study are the following:

1. Define the DNS abuse phenomenon, identify and categorise recurring types of abuses, provide a broad and workable definition of DNS abuse taking into consideration the different abuse categories, their magnitude and their impact;
2. Provide a comprehensive description of the impact of DNS abuses on the European economy and society in comparison to the international level, and explore the possible impact of technological developments (such as IoT and 5G) on the magnitude and risks associated to DNS abuse;
3. Provide a comprehensive overview of the existing policies, applicable laws and relevant industry practices to address DNS abuse, assess the effectiveness of those measures, and identify possible gaps and shortcomings;
4. Provide recommendations for improvements in the different categories of remedies to address DNS abuses, in order to guide possible future policy development, and identify the possible actions needed at European level.

The findings of the Study will enable the European Commission to evaluate existing practices to address DNS abuse and assess whether complementary measures might be necessary or useful.

Commission européenne/Europese Commissie, 1049 Bruxelles/Brussel, BELGIQUE/BELGIË - Tel. +32 22991111
Office: BU33 03/050 - Tel. direct line +32 22983631

Thomas.DE-HAAN@ec.europa.eu

In carrying out the Study, the Contractor shall analyse relevant cybersecurity data (e.g., URL and domain name blacklists) and collect information from stakeholders, such as domain name registries and registrars, cybersecurity experts, blacklist providers, technical internet organisations, industry associations, rights holders associations, consumer protection organisations, and public authorities.

We hope that you will agree to collaborate with the Contractor in providing the information and data requested and if opportune, participate in workshops organised around certain themes of the Study. It will help substantiate the findings of the Study. The information and data collected will be aggregated and anonymized, unless a stakeholder requests their position to be disclosed.

Yours faithfully,

Olivier BRINGER
Head of Unit

Contact: Thomas DE HAAN, Thomas.DE-HAAN@ec.europa.eu, +32 229 83631

c.c.: Olivier BRINGER, Gemma CAROLILLO, Ivett PAULOVICS