DNS OPERATORS' DECISION-MAKING GUIDE TO ADDRESS TECHNICAL ABUSE

REF: 20-108 | July 21, 2020

Acting at the DNS level can be justified to remediate technical/infrastructure abuse in order to protect the stability and security of the global infrastructure of the internet. DNS operators rely on a variety of internal and external resources to identify, evaluate and take action to remediate technical abuse[1]. While establishing whether a domain is being used to perpetrate technical abuse tends to produce binary results (i.e. the domain is or is not engaged in technical abuse), care should nonetheless be taken to ensure that action at the DNS level to remediate said abuse is appropriate and proportionate.

A general approach to addressing technical abuse may be based upon the following steps:

- Identification or notification of the alleged technical abuse associated with the domain(s)
- Evaluation of scope of abuse
- Determination of the choice of appropriate and proportionate action
- Technical actions to ensure recourse and remediation

The table below lists a set of structuring questions that DNS Operators can use at each step to determine a course of action to address technical abuse on a voluntary basis.

	Structuring Questions
IDENTIFICATION AND NOTIFICATION	• Is the domain within the DNS Operator's zone? • Does the notice allege technical abuse? • Does the notice contain all the necessary components[2] for identifying abuse and taking action, as appropriate? • Does the notice come from a court of applicable jurisdiction? • Does the notice come from a trusted, repeating or ad-hoc source? • Is there an agreement between the DNS Operator and this specific notifier?

EVALUATION OF ABUSE
Multi-factor analysis to evaluate the scope and authenticity of alleged abuse
	According to the type of technical abuse, what should DNS Operators take into consideration when evaluating alleged abuse, to ensure that the action taken is appropriate and proportionate?
	• Conduct own investigation (with help of 3rd parties if required) to determine:
	  ○ That it is not a false positive
	  ○ Whether the abuse is still active (hasn't already been mitigated by someone else)
	  ○ Where the abuse is taking place (single link, single URL, entire site?)
	• Is it likely that the domain has been compromised, such that the registrant should be contacted?

[1] See scope in Annex at the end of this document.

[2] Minimum Notice Components for Technical Abuse (REF: 20-109)

	• Is the alleged abuse related to a sublevel or third level domain? Should action be taken?
CHOICE OF ACTION Choice of the measure used to address the abuse	According to the type and level of technical abuse, what determines the choice of action? • Should the DNS Operator act or should other actors act[3] (e.g. hosting provider)? • If ordered by a court of applicable jurisdiction, is the specified action technically implementable? • What type of action[4] should be taken? • Should the registrant be notified[5]?
RECOURSE AND REMEDIATION Recourse Mechanisms available to registrants	• According to each type of technical abuse and type of notice: • When is there notification to the registrant (when applicable)? • What recourse mechanisms[6] are available to the registrant?

[3] Refer to *Criteria E/2B - Procedural Due Diligence* in the Domains & Jurisdiction Operational Approaches

[4] Refer to *Criteria F - Types of Action* in the Domains & Jurisdiction Operational Approaches

[5] Refer to Criteria H - Notification to *Registrants* in the Domains & Jurisdiction Operational Approaches

[6] Refer to *Criteria I - Recourse for Registrants* in the Domains & Jurisdiction Operational Approaches

ANNEX

OPERATIONAL CRITERIA A - TYPES OF ABUSES[7]

DNS Operators receive cross-border requests to take action against domain names allegedly associated with technical abuse. Listed below are descriptions of different types of technical abuses, for which Registries and Registrars often receive such requests.[8]

1. Technical abuses

Domain names can be misused to propagate different types of technical abuse, including but not limited to the following:

a. **Malware** is malicious software, installed on a device without the user's consent, which disrupts the device's operations, gathers sensitive information, and/or gains access to private computer systems. Malware includes viruses, spyware, ransomware, and other unwanted software.[9]

b. **Phishing** occurs when an attacker tricks a victim into revealing sensitive personal, corporate, or financial information (e.g. account numbers, login IDs, passwords), whether through sending fraudulent or "look-alike" emails, or luring end users to copycat websites. Some phishing campaigns aim to persuade the user to install software, which is in fact malware.

c. **Pharming** is the redirection of unknowing users to fraudulent sites or services, typically through DNS hijacking or poisoning. DNS hijacking occurs when attackers use malware to redirect victims to their own site instead of the one initially requested. DNS poisoning causes a DNS server to respond with a false IP address bearing malicious code.[10] Phishing differs from pharming in that the latter involves modifying DNS entries, while the former tricks users into entering personal information.

d. **Botnets** are collections of Internet-connected computers that have been infected with malware and commanded to perform activities under the control of a remote administrator.[11]

e. **Fast-flux hosting** is used to disguise the location of Web sites or other Internet services, or to avoid detection and mitigation efforts, or to host illegal activities. Fast-flux techniques use the DNS to frequently change the location on the Internet to which the domain name of an Internet host or name server resolves.[12]

---

[7] This list of technical abuses is abstracted from the Domains & Jurisdiction Operational Approaches document as reordered by the Contact Group (See Criteria A - Types of Abuses). The list is accessible at: https://www.internetjurisdiction.net/uploads/pdfs/Papers/Domains-Jurisdiction-Program-Operational-Approaches.pdf

[8] These lists are illustrative and not intended to be exhaustive.

[9] See M3AAWG & London Action Plan, Operation Safety-Net: best practices to Address Online Mobile and Telephony Threats (2015) ("Operation Safety-Net"), at https://www.m3aawg.org/system/files/M3AAWG_LAP-79652_IC_Operation_Safety- Net_Brochure-web2-2015-06.pdf; "Malware" page at the U.S. Federal Trade Commission website, at https://www.consumer.ftc.gov/articles/0011-malware

[10] See the Public Interest Registry's Domain Name Anti-Abuse Policy, at https://pir.org/policies/org-idn-policies/anti-abuse- policy/; entries for DNS hijacking and DNS poisoning in the Kaspersky Lab Encyclopedia, at https://encyclopedia.kaspersky.com/glossary/dns-hijacking/

[11] See "A Glossary of Common Cybersecurity Terminology," National Initiative for Cybersecurity Careers and Studies, at: https://niccs.us-cert.gov/about-niccs/glossary#B

[12] See the Public Interest Registry's Domain Name Anti-Abuse Policy, at https://pir.org/policies/org-idn-policies/anti-abuse-policy/ 7 Interpol, "Online child abuse material: Q & A" (January 2017). [7]https://www.interpol.int/Media/Files/Crime-areas/Crimes- against-children/Online-Child-Abuse-%E2%80%93-Questions-and-Answers/

f. **Spam** is unsolicited bulk email, where the recipient has not granted permission for the message to be sent, and where the message was sent as part of a larger collection of messages, all having substantively identical content.[13] Spam is included here to address when it is used as a delivery mechanism for technical abuse.

[13] See "The Definition of Spam" by The Spamhaus Project, at https://www.spamhaus.org/consumer/definition/