RySG
gTLD Registries Stakeholder Group

ICANN | RrSG
Registrar Stakeholder Group

# CPH DNS Abuse Work Group Community Update

ICANN 72
VIRTUAL ANNUAL GENERAL

# CPH DNS Abuse WG Community Outreach

| No. | TOPIC | LEAD |
|---|---|---|
| 1 | Welcome and Introduction | Reg Levy, Tucows |
| 2 | Update on Work Outputs:<br>• RySG<br>• RrSG | Various |
| 3 | RrSG Approaches to BEC Scams | Reg Levy, Tucows |
| 4 | Appeal Mechanisms Following DNS Abuse Mitigation | Owen Smigelski, NameCheap |
| 5 | Trusted Notifier Framework | Keith Drazek, Verisign |
| 6 | Q&A and CPH Questions for the community | Reg Levy, Tucows |

# CPH Definition of DNS Abuse

**DNS Abuse** is composed of five broad categories of harmful activity insofar as they intersect with the DNS: malware, botnets, phishing, pharming, and spam when it serves as a delivery mechanism for the other forms of DNS Abuse.

Full details are available on the RrSG website and the RySG website.

# RySG Output on DNS Abuse

| TOPIC | REFERENCE |
| --- | --- |
| Recommendations for DAAR; Joint work with OCTO | • RySG DAAR Working Group Final Report |
| Education: Registry Actions for DNS Abuse | • Combatting DNS Abuse: Registry Operator Available Actions |
| Collaboration with PSWG | • Framework on Domain Generating Algorithms (DGAs)<br>• Framework for Registry Operators to Respond to Security Threats |
| Joint work with RrSG | • Trusted Notifier Framework |
| CCTRT Recommendations | • Review of CCTRT recommendations as relates to DNS Abuse |
| IDN Homoglyph Attacks; Joint work with IPC | • Resource explaining homoglyph attacks and potential mitigations |

# RrSG Output on DNS Abuse

| TOPIC | STATUS |
|---|---|
| Guide to Registrar Abuse Reporting | PUBLISHED |
| Registrar Approaches to the COVID-19 crisis | PUBLISHED |
| ✨ Appeals Mechanisms following DNS Abuse Mitigation | NEWLY PUBLISHED |
| ✨ Approaches to Business Email Compromise (BEC) scams | NEWLY PUBLISHED |
| ✨ CPH Trusted Notifiers Framework | NEWLY PUBLISHED |
| ✨ CPH Guide to DNS Abuse Reporting<br>*(update to Guide to Registrar Abuse Reporting)* | UPDATE COMING SOON |
| Triage tool for registrants dealing with DNS Abuse | IN DEVELOPMENT |
| IDN homoglyph domain attacks | IN PROGRESS WITH RYSG |
| Incentive Programs for Combatting DNS Abuse | IN PROGRESS |

# Approaches to Business Email Compromise (BEC) Scams

- BEC Fraud: a social engineering hack
- Not as frequent as phishing, but has a higher impact
- May use a domain name (ceo@company.net, ceo@c0mpany.com) or not (randomstring@emailprovider.tld)
- Approaches to combat BEC Fraud
- Approaches for registrars (incident response approach)

# Appeals Mechanisms following DNS Abuse Mitigation

- Highlights protections to ensure registrants are not subject to unfounded abuse complaints and have the ability to “appeal” actions against abuse through various mechanisms:
  - All DNS abuse complaints should be based on material, actionable reports that include verifiable evidence.
  - Internal, support-based appeals (e.g. through customer support flow)
  - Internal ombuds
  - Courts of competent jurisdiction (including public ombuds, consumer agencies, or law enforcement)
- Not intended to facilitate or protect abuse

# CPH Trusted Notifier Framework

## Overview

- Notes that several RRs and RYs already rely on TNs to address both DNS Abuse and website content abuse questions.
- Relies on the Framework to Address Abuse in scoping out key aspects of TN:
  (1) expertise and accuracy;
  (2) documented relationship with the RR/RY;
  (3) defined process for notification.

# CPH Trusted Notifier Framework

## Purpose

- Framework intended to serve as a guide for parties considering entering into TN arrangements.
- Also explains the role, responsibilities, and expectations of TNs, in the mitigation of abuse—both DNS Abuse and website content abuse.

# CPH Trusted Notifier Framework

## TN Role and Expectations

- Has a strong, demonstrated expertise in the subject matter;
- Operates with a consistent adherence to a high level of substantive and procedural due diligence
- Stands behind its reporting and is committed, in writing, to a low false positive rate and the accuracy of its notices; and
- Has a clearly enumerated process for registrants to challenge the TN's recommendations.

# CPH Trusted Notifier Framework

## Notifiers vs Trusted Notifiers

- Might be expert notifiers with high degree of confidence, but doesn't make them TNs.
- TN status is only conferred when a RR or RY agrees to put such trust into the notices from that notifier—when the RR or RY enter into an agreement with that TN.
    - "[t]the overarching criterion […] is reputation over time: how long the notifier has been active, its track record on the market and, more importantly, whether it is willing to defend its notices and stand by the operator in case of litigation."

# CPH Trusted Notifier Framework

## Choice of Action

- A RR or RY may accord the notice from the TN with a heightened level of deference but still take steps necessary to ensure that the processes set forth in its written arrangement were followed and that the notice seems credible and accurate.
- Ultimately, must still be the RR/RY decision to act.

# CPH Trusted Notifier Framework

## Relationship with Registrar (RR) / Registry (RY)

- TN arrangements are codified in writing between a notifier and the party to be notified, either a RY or a RR. Should provide a level of understanding and comfort to each as to processes and due diligence.
- Potential legal ramifications and exposure to taking action at the DNS level (particularly to remedy issues that are outside ICANN's remit), these arrangements should also address apportionment of liability. Either party may have a need to include representations and warranties and/or indemnification provisions, to incentivize expectations of transparency, due diligence and ensuring that actions taken based on the notice of a TN, particularly in situations where the notice was to protect commercial interests, were appropriately and properly made.

# CPH Trusted Notifier Framework

## Due Diligence by TNs

- TNs, as subject matter experts, are expected to conduct thorough due diligence before sending an abuse notice to a RR or RY. Not doing so could result in a higher rate of false positive reports, loss of “trust” and potential legal exposure of the RR/RY and the TN.
  - Substantive Due Diligence - making certain that the alleged abuse is properly investigated, substantiated, and documented.
  - Procedural Due Diligence - RR/RY may for certain types of abuse require that more appropriate parties are contacted first (e.g., website operator → registrant → hosting provider → registrar → registry).
- A RR or RY, and a TN may mutually define their own thresholds for substantive and procedural due diligence.

# CPH Trusted Notifier Framework

## Transparency and Due Process

- TNs and RR/RYs should consider a level of transparency into their relationships as well as potential recourse mechanisms for registrants.
- I&J notes “a two-dimensional approach”:
  - sharing statistics on abuse reports and actions taken, and
  - publishing the decision-making criteria (e.g., abuse policy, thresholds for action), abuse point of contact and procedure to appeal or request recourse.

# CPH Trusted Notifier Framework

## Potential Future Work

- Living document capable of iteration and evolution.
- As the number of TNs grows, it is possible that RR/RYs will be faced with administrative/operational challenges.
- CPH will consider potential optional mechanisms and relationships that could deliver economies of scale, while allowing each RR/RY to continue to exert their own judgement over their respective TN agreements, policies, and any course of action taken.

**DNS Abuse** is composed of five broad categories of harmful activity insofar as they intersect with the DNS: malware, botnets, phishing, pharming, and spam when it serves as a delivery mechanism for the other forms of DNS Abuse.

1) What information do you use and how do you use it to assess DNS Abuse levels?
2) What are your concerns regarding DNS Abuse?
3) Are you seeing practices from registrars or registries you find helpful?