DNS Abuse Mitigation

Susan Chalmers (US Department of Commerce, NTIA)
Karel Douglas (Telecom. Authority of Trinidad and Tobago, USRWG Co-Chair)
Laureen Kapin (US Federal Trade Commission, Co-Chair GAC PSWG)
Chris Lewis-Evans (UK National Crime Agency, Co-Chair GAC PSWG)

Guest Speakers:
Russ Weinstein (ICANN Global Domains and Strategy)
Peter Jansen (EURid)

ICANN77

14 March 2023

ICANN | GAC
Governmental Advisory Committee

Agenda

1. Overview of proposed DNS Abuse Contract Amendments and the DNS security threats they are designed to address
2. EURid: .eu, .ɛu & .ɐю and DNS Abuse
3. Day 0 GAC Capacity Development Workshop on DNS Abuse
4. GAC discussion to determine next steps

Summary of Proposed Changes (Contract Amendments)

- Adds to existing obligations in Registrar Accreditation Agreement (RAA) & Registry Agreement (RA)
- Clarifies registrar / registry abuse contacts are readily accessible
- Adds a requirement to provide confirmation of receipt of an abuse report
- Adds a definition of DNS Abuse for purpose of the agreements
- Adds new obligation to take mitigation action to stop or disrupt DNS Abuse.

New draft ICANN Advisory: Describes the new requirements and provide clarity on the implementation and enforcement of such requirements, including several examples.

Reference: Amendments and draft ICANN Advisory available in the public comment proceeding

Proposed Changes: Adding Definition of DNS Abuse

A definition of DNS Abuse for purposes of the RA and RAA.

For the purpose of the RAA, RA, and draft Advisory, *DNS Abuse* means:

- Malware
- Botnets
- Phishing
- Pharming
- Spam, when spam serves as a delivery mechanism for the other forms of DNS Abuse listed

Registry Agreement: Specification 11 3(b) - replaces the term "security threats" with the defined term DNS Abuse.

Reference: Amendments and draft ICANN Advisory available in the public comment proceeding

Registrar Proposed Changes

New point: 3.18.2 (Registrar Accreditation Agreement)

*When Registrar has **actionable evidence** that a Registered Name sponsored by Registrar is being used for DNS Abuse, Registrar **must promptly** take the **appropriate mitigation action(s) that are reasonably necessary** to stop, or otherwise disrupt, the Registered Name from being used for DNS Abuse. Action(s) may vary depending on the circumstances, taking into account the cause and severity of the harm from the DNS Abuse and the possibility of associated collateral damage.*

Reference: Amendments and draft ICANN Advisory available in the public comment proceeding

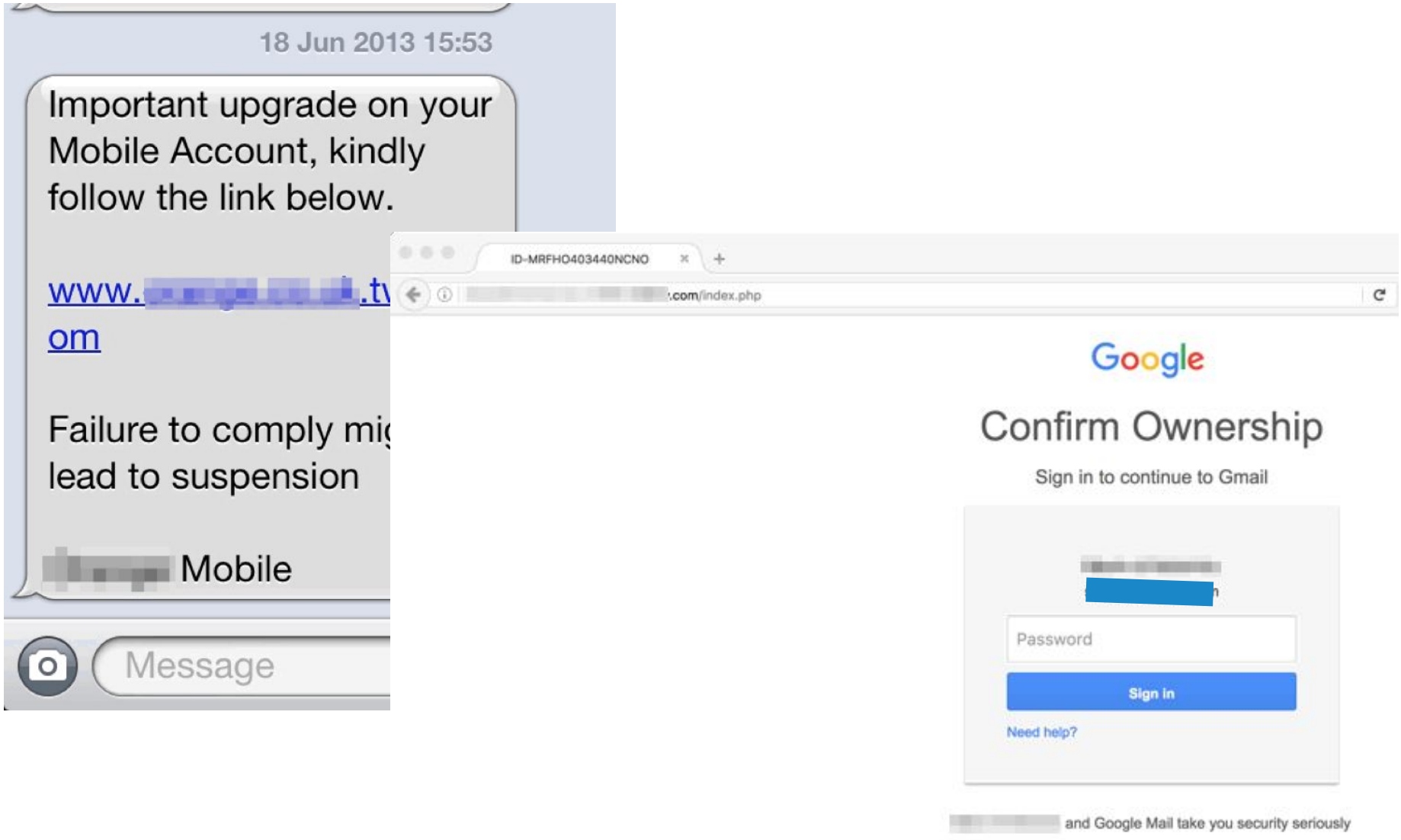
Registry Proposed Changes

New Specification 6 Section 4.2 (Registry Agreeement)

DNS Abuse Mitigation. Where a Registry Operator ***reasonably determines, based on actionable evidence****, that a registered domain name in the TLD is being used for DNS Abuse, Registry Operator* ***must promptly take the appropriate mitigation action(s) that are reasonably necessary to contribute to stopping, or otherwise disrupting****, the domain name from being used for DNS Abuse. Such action(s)* ***shall, at a minimum****, include: (i) the referral of the domains being used for the DNS Abuse, along with relevant evidence, to the sponsoring registrar; or (ii) the taking of direct action, by the Registry Operator, where the Registry Operator deems appropriate. Action(s) may vary depending on the circumstances of each case, taking into account the severity of the harm from the DNS Abuse and the possibility of associated collateral damage.*

Reference: Amendments and draft ICANN Advisory available in the public comment proceeding

Examples of DNS abuse covered



Examples of DNS abuse covered

Ransomware

Blackmails you

Spyware

Steals your data

Adware

Spams you with ads

Agenda

1. Overview of proposed DNS Abuse Contract Amendments and the DNS security threats they are designed to address
2. **EURid: .eu, .ɛu & .ɐɧo and DNS Abuse**
3. Day 0 GAC Capacity Development Workshop on DNS Abuse
4. GAC discussion to determine next steps

Agenda

1. Overview of proposed DNS Abuse Contract Amendments and the DNS security threats they are designed to address

2. EURid: .eu, .ɛu & .ɐɥo and DNS Abuse

3. **Day 0 GAC Capacity Development Workshop on DNS Abuse**

4. **GAC discussion to determine next steps**

Day 0 Capacity Development Workshop on DNS Abuse

Timeline for GAC Input on Contract Amendments

Today - June 21	All GAC reps provide input on Google Doc
June 22 - 29	GAC small group incorporates inputs into first draft
—	
June 30 - July 6	First draft to GAC for feedback/amendments
—	
July 7 - 10	GAC small group incorporates feedback
July 11 - 12	Draft circulated for review and finalization
July 13	Final GAC input submitted to Public Comment Process

GAC Discussion to Determine Next Steps

Questions for consideration in the public comment process:

1. What are the positive aspects of these amendments?
2. Are the obligations sufficiently clear to be enforceable?
3. Thoughts on the proposed definition of DNS Abuse? (too broad/too narrow? sufficiently flexible?)
4. Thoughts on the role of the *ICANN Advisory on the Amendments*?
    a. Intended to be an evolving document?
    b. Sufficiently informative as to:
        i. What is “actionable” evidence?
        ii. What is “prompt?”
        iii. Escalation paths/When registry should take action vs. referring

GAC Discussion to Determine Next Steps

Questions for consideration in the public comment process:

5. What issues remain with regard to DNS Abuse?
    a. What subject matter areas may be appropriate for the planned PDPs?
        i. Before the next round of new gTLDs?
    b. The role of Public Interest and Registry Voluntary Commitments?
    c. Dealing with recidivist bad actors (registrants or registrars/registries that are havens for illicit activities)
    d. Priority/ideal timing for these issues?
6. Other issues?