NCAP DG Meeting

Monday September 19, 2022

Agenda

- Welcome and roll call
- Project status
- Study Two report outline
- Gaps, subjects for additional discussion, other concerns
    - TRT heuristics for assessing risk
- AOB

Study Two Report Outline

Executive Summary (TBD)

1. Introduction
   - Background, Methodology, Terminology

2. Précis of NCAP Study Two Reports
   - Case Study, Perspective Study, and Root Cause Report

3. Summary of NCAP Discussion Group Activities
   - NCAP Gap Analysis, Review of Available Datasets, Issue of Manipulation, Controlled Interruption, Review of Proposal for Measurements and Assessments Mechanisms, Workflow Development, Tabletop Exercises

Study Two Report Outline

4. Collective Findings from Study Two Reports and DG Activities
   - Name collision assessment is a risk management process, WIP

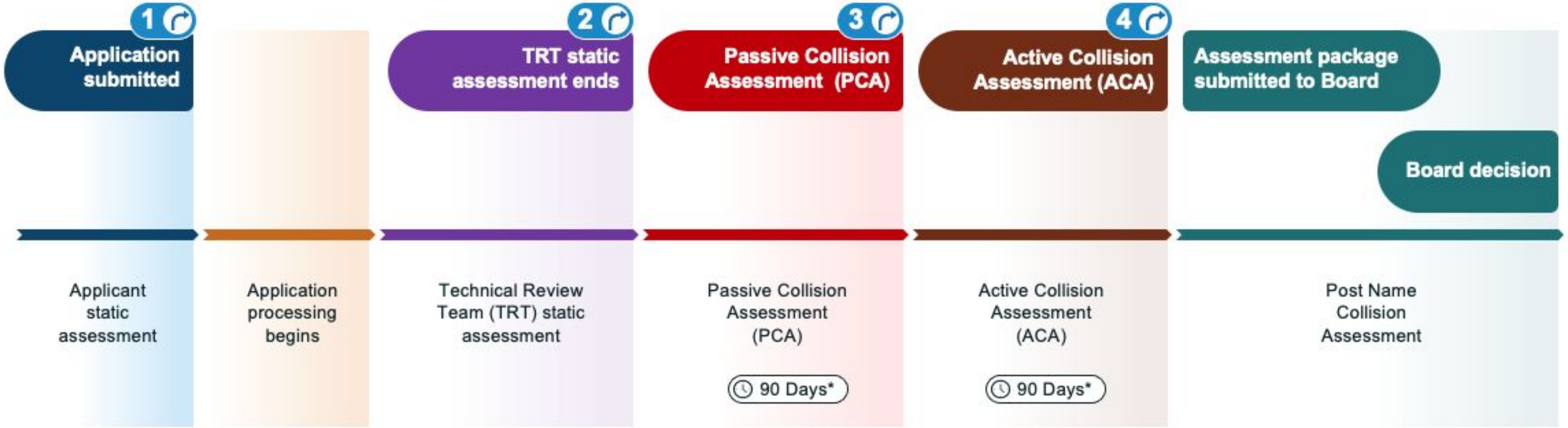
5. Board Questions
   - Name collision definition, negative answers, harm, risks of delegation, undelegated strings and collision strings, WIP

6. Recommendations
   - WIP

7. Advice to ICANN Board / Conclusion
   - WIP

New Figure – Assessment Timeline

Name Collision Assessment Timeline



1 Application submitted

2 TRT static assessment ends

3 Passive Collision Assessment (PCA)

4 Active Collision Assessment (ACA)

Assessment package submitted to Board

Board decision

Applicant static assessment

Application processing begins

Technical Review Team (TRT) static assessment

Passive Collision Assessment (PCA)

90 Days*

Active Collision Assessment (ACA)

90 Days*

Post Name Collision Assessment

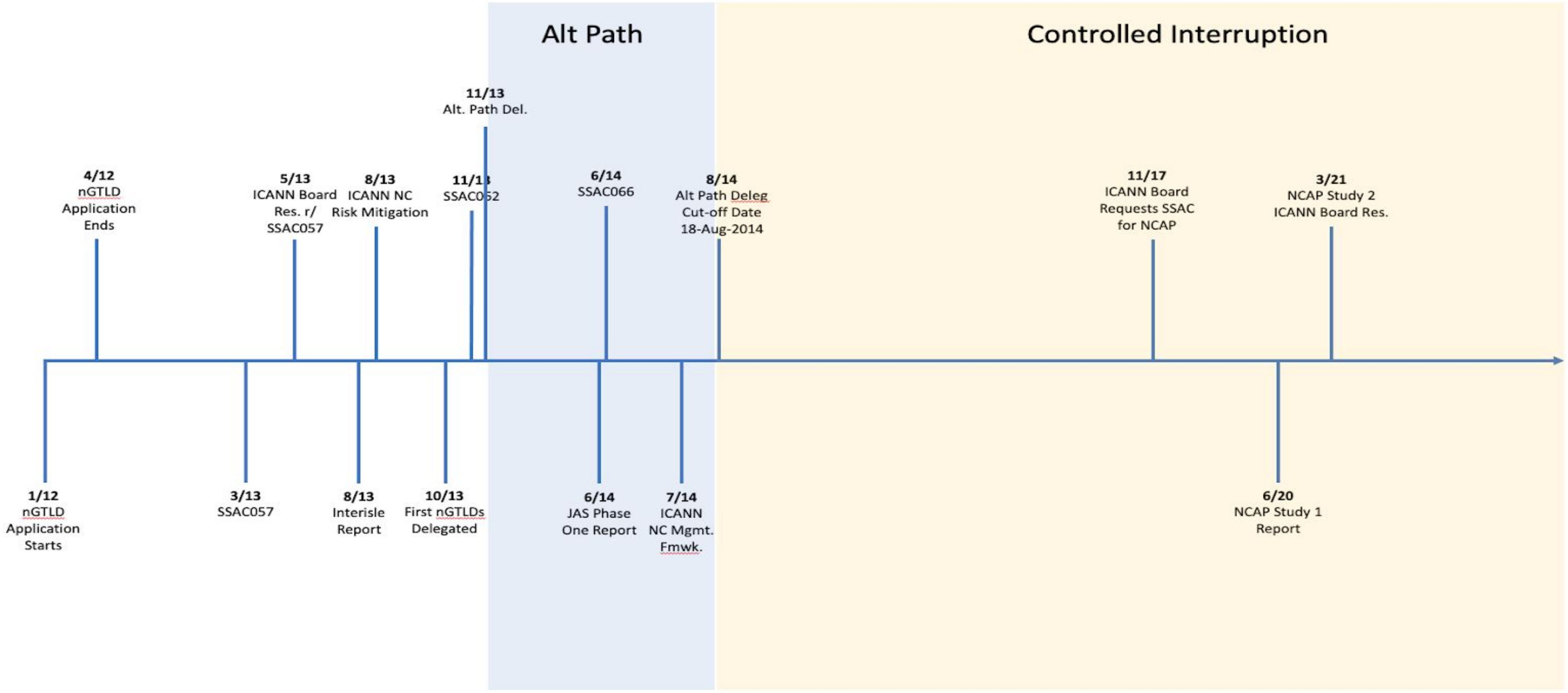
Offramp Options

1 – Applicant decision only

2,3, & 4 – TRT identifies risk in its written report; notifies Board and Applicant who consider mitigation, remediation, or withdrawal; OR no risk concerns and assessment proceeds to next step

*: 90 days of data collection followed by time for report and decision

New Figure – Historical Timeline



Alt Path

Controlled Interruption

1/12 nGTLD Application Starts

4/12 nGTLD Application Ends

3/13 SSAC057

5/13 ICANN Board Res. r/ SSAC057

8/13 Interisle Report

8/13 ICANN NC Risk Mitigation

10/13 First nGTLDs Delegated

11/13 SSAC062

11/13 Alt. Path Del.

6/14 JAS Phase One Report

6/14 SSAC066

7/14 ICANN NC Mgmt. Fmwk.

8/14 Alt Path Deleg Cut-off Date 18-Aug-2014

11/17 ICANN Board Requests SSAC for NCAP

6/20 NCAP Study 1 Report

3/21 NCAP Study 2 ICANN Board Res.

“If you don't know where you've come from, you don't know where you're going” – Maya Angelou

Gaps, subjects for additional discussion, etc.

- Guidance to TRT for name collision risk assessment
- What else? Speak up!

TRT Heuristics for Assessing Risk

1. Do the queries originate from some common networks/ASNs?
    a. Yes: Action: Direct outreach to network operator
        i. Example: .CONSUL outreach to originating source
        ii. Implication: Risk/harm is contained to a particular entity. Still could be a large risk/harm in some scenarios such as .INTERNAL
    b. No: Action: Analyze the SLDs and labels for commonalities.

2. Do the queried names contain common SLDs or other labels?
    a. Yes: Action: Associate common strings with networks, software, services, etc.
        ii. Example: Windows Defender in .TCS. .DLINK, .BELKIN, .BBROUTER, etc.
        iii. Implication: Outreach to address the root cause may remediate the risk. Common SLDs could offer a mechanism to block the registration of that SLD (e.g., alternate path to delegation). SLDs or other labels could be indicators of root cause (e.g., identify some type of software or system that is leaking the queries). Some types of leakage are associated with end consumer devices that may require long remediation times or may not be feasible (e.g., ISP routers and D-Link
    b. No: Action: Additional research into querying sources, strings, and root cause.

4. Do the queries come from a diverse set of networks or networks/ASNs and a diverse set of SLDs?
    a. Yes: Action: Additional bespoke investigation into what could be causing the leak.

5. Are there any other indicators of heightened risk based on source IP addresses or the labels sent (e.g.. known exploitable DNS-SD protocols such as WPAD, ISATAP, etc.)?

6. Is there any reason to believe that PCA would be impactful/harmful?

7. Is there any reason to believe that ACA would not succeed in disruption and notification?

AOB