Comments on "Name Collision Analysis Project (NCAP) Study 1 Final Report"

VeriSign, Inc.
June 16, 2020

Verisign appreciates the opportunity to comment on the Name Collision Analysis Project (NCAP) Study 1 Proposed Final Report.[1] We would also like to thank Scarfone Cybersecurity and the NCAP Work Party of ICANN's Security and Stability Advisory Committee (SSAC), as well as ICANN's Office of the CTO (OCTO) for their efforts and commitment to produce the report. The report provides a helpful recounting of the name collision research program of the past several years. However, to provide further context in reading the report, we would like to respond to a few of the report's statements and conclusions.

The report puts forth four major findings in Section 6. We comment on three of these and add two additional points below.

1. The first point claims that "There does not appear to be any recent academic research into the causes of name collisions or new name collision mitigation strategies." The report's interpretation of "recent" seems arbitrary, given that several peer-reviewed publications were released in 2016 and 2017, which is certainly current in the research publication lifecycle. The report also states, "the volume of work on name collisions has greatly decreased." But academic or scientific literature doesn't necessarily have to be repeated to remain relevant, especially once fundamentals are in place.

   As the first systematic studies of the robustness of internal network services under name collision attacks, the 2016 and 2017 academic papers are indeed the "recent research." They provide valuable insights that were not codified and considered prior to ICANN's creation of the Collision Occurrence Management Framework in 2014 and offer the basis for further research (including a follow-up paper from 2017[2] not referenced in the report). Subsequent research includes remediation proposals mentioned in the academic literature and on the NCAP DG mailing list.[3]

---

[1] Scarfone, Karen. *Managing the Risks of Top-Level Domain Name Collisions — Findings for the Name Collision Analysis Project (NCAP) Study 1.* Scarfone Cybersecurity, May 7, 2020. https://www.icann.org/en/system/files/files/managing-risks-tld-2-name-collision-07may20-en.pdf

[2] Nesterov, Ilya, and Maxim Goncharov. *All Your Emails Belong to Us: Exploiting Vulnerable Email Clients via Domain Name Collision*. Presented at Black Hat Asia 2017, March 28-31, 2017. https://www.blackhat.com/docs/asia-17/materials/asia-17-Nesterov-All-Your-Emails-Belong-To-Us-Exploiting-Vulnerable-Email-Clients-Via-Domain-Name-Collision-wp.pdf

[3] See, e.g., McPherson, Danny. "Additional comments on the comments to the Scarfone draft," NCAP-Discuss mailing list, May 6, 2020. https://mm.icann.org/pipermail/ncap-discuss/2020-May/000356.html

2. The second point focuses on the lack of instances of name collision problems being reported to ICANN or reported publicly through other means. The report uses this as grounds for claiming "controlled interruption has already proven an effective mitigation strategy." But lack of evidence does not support the conclusion that there are no problems, or as many have stated during NCAP DG calls, "Absence of evidence is not evidence of absence."[4] It may simply mean that the problems are *not being detected* (or if they are, they're not being exploited or reported[5]). Furthermore, it should be clear to the reader that as "the volume of new postings of name collision-related problems has dropped sharply over the past few years," so has the volume of new gTLD delegations (Figure 1).

   The Controlled Interruption framework has never undergone a thorough assessment of various name collision attack scenarios, including those recently highlighted in the 2016 and 2017 literature that identify numerous vulnerabilities that present undetectable Man-in-the-Middle (MitM) attacks. And although the report states that "most of the harm or potential for harm should have occurred during the 90-day controlled interruption periods," this again assumes that Controlled Interruption is effective at disrupting name collision attack vectors, including MitM. Data that could have been used to assess effectiveness was not collected during Controlled Interruption, as we note next. The October 2015 Name Collisions Final Report simply concluded that the "controlled interruption approach offers the most value and presents the least risk," offering rationale but lacking experimental results or formal comparison with proactive alternatives such as string-by-string remediation.[6] (Recall, for comparison, the demonstrated effectiveness of the proactive, per-string outreach for .CBA[7] [8], which measurably reduced the frequency of collision occurrences prior to delegation, when the impact was still visible in root zone traffic.)

3. The third point claims that many of the root causes of name collisions have been found by "researching a particular leaked TLD to find its origin, not be examining datasets." Several of the documents, papers, and presentations referenced in the report[9] utilize holistic views of DNS traffic patterns to identify underlying causes and commonalities of name collision risks. While individual TLD investigations may be better suited for targeted remediation strategies, broad general analyses of datasets are more

---

[4] For example, Warren Kumari stated at the April 1, 2020 meeting, "I do want to make sure that we remember that absence of evidence is not evidence of absence" (transcript p. 11). NCAP Discussion Group Meetings, April 1, 2020. https://community.icann.org/display/NCAP/1+April+2020

[5] The ongoing flow of .CORP queries to CORP.COM stands as an example of known but unexploited risks.

[6] JAS Global Advisors. *Mitigating the Risk of DNS Namespace Collisions.* Final report, October 28, 2015. https://www.icann.org/en/system/files/files/name-collision-mitigation-final-28oct15-en.pdf See Section 3.1.6.

[7] Kane, Patrick S., Indelicarto, Thomas C., and McPherson, Danny. *Re: ICANN's Proposal to Mitigate Name Collision Risks – .CBA Case Study.* Letter to ICANN Board of Directors, September 15, 2013. https://www.verisign.com/assets/report-cba-analysis.pdf

[8] Kaliski, Burt. *Name Collision Mitigation Requires Qualitative Analysis.* CircleID, November 13, 2013. http://www.circleid.com/posts/20131113_name_collision_mitigation_require_qualitative_analysis_part_3_of_4/

[9] See references [53], [62], [75], [81], and [83] in the Study 1 Final Report.

© 2020 VeriSign, Inc. All rights reserved.

appropriate tools for name collision research, including the insights that help inform proactive (i.e., pre-delegation) mitigation of name collisions, as shown in the referenced literature.

Furthermore, we observed in our preliminary comments on the Phase 2 report in 2014[10] that proper risk mitigation requires feedback on effectiveness. This is reflected in the following proposed improvement to one of the report's recommendations:

- "RECOMMENDATION 9: ICANN monitor the implementation of controlled interruption by each registry to ensure proper implementation and compliance, **and to assess effectiveness in mitigating risk**." (emphasis in original)

We also stated:

- "One practical way to assess the effectiveness of controlled interruption for the new gTLD operator to provide periodic samples of DNS queries and responses for analysis. Similar to the DITL project that seeks to understand DNS activity at the root servers, an organization like DNS-OARC could run an ongoing project to study 'Day-in-the-Controlled-Interruption' data sets provided by registry operators, root server operators and other participants in the DNS ecosystem."

We made the case to ICANN at the time that the introduction of Controlled Interruption provided a unique opportunity to measure how the replacement of NXDOMAIN responses by loopback addresses would affect the query behavior of installed systems that previously assumed a new gTLD was not part of the global DNS. Once Controlled Interruption was complete and the new gTLD was part of the global DNS, the opportunity to see how installed systems responded would be gone. But it's not too late to incorporate such a measurement scheme for future delegations.

The Study 1 Final Report states that "much of the publicly available information on the known harm of name collisions is not relevant for evaluating current and future risks because it is outdated." But inasmuch as DNS is one of the longest established internet protocols, historical information should endure well. The report acknowledges as "noteworthy" Verisign's reference in its comments from 2013 to lessons that can be learned from "… the introduction of .info over a decade ago" (Sec. 3.3.3.) So if information from a 2001 launch could remain relevant in 2013, then surely recent works in 2016 and 2017, highlighting various classes of name collision attacks that were not previously known and could be used as potential assessment criteria when combined with DNS data, could be used to evaluate current and future risk profiles of new gTLDs.

[10] Verisign. *Preliminary Comments on "Mitigating the Risk of DNS Namespace Collisions" Phase One Report.* March 31, 2014. http://forum.icann.org/lists/comments-name-collision-26feb14/pdfNPWfDHk1pu.pdf Submitted to comments-name-collision-26feb14 mailing list, March 31, 2014. https://forum.icann.org/lists/comments-name-collision-26feb14/msg00010.html

© 2020 VeriSign, Inc. All rights reserved.

4. We would draw attention to the fact that, due to an expansion of scope introduced in ICANN's Request for Proposal (RFP) for the study,[11] a significant portion of the Study 1 Final Report is directed to namespace usage issues that, as we have argued previously, are beyond the definition of a name collision. (This is in no way a fault by the report contractor, who was simply following the scope of work given in the RFP.)

   The SSAC proposal, as revised by ICANN OCTO, and the RFP are both clear in their terminology, as is the ICANN Board resolution that mandated this work:

   - "**Name Collision** refers to the situation where a name that is defined and used in one namespace may also appear in another."[12] (emphasis in original)

   - "Name collision refers to the situation in which a name that is used in one namespace may be used in a different namespace, where users, software, or other functions in that domain may misinterpret it.

     "In the context of top level domains, the term 'name collision' refers to the situation in which a name that is used in the global Domain Name System (DNS) namespace defined in the root zone as published by the root zone management (RZM) partners ICANN and VeriSign (the RZM namespace) may be used in a different namespace (non-RZM), where users, software, or other functions in that domain may misinterpret it."[13]

   - "A name collision occurs when an attempt to resolve a name used in a private name space (e.g. under a non-delegated Top-Level Domain, or a short, unqualified name) results in a query to the public Domain Name System (DNS). When the administrative boundaries of private and public namespaces overlap, name resolution may yield unintended or harmful results. This class of as-yet undelegated strings is referred to as 'Collision Strings.'"[14]

   Despite the precision of "another [namespace]," "different namespace," "RZM namespace" vs. "non-RZM," and "private namespace," the RFP asserts that this "high-level definition" of name collision also includes the case where a name is re-registered within the *same* namespace, i.e., within the RZM namespace itself (Section 2.3.3, case

[11] ICANN. *Project Overview for the Name Collision Analysis Project (NCAP) Study 1* Request for Proposal, July 9, 2019. https://www.icann.org/en/system/files/files/rfp-ncap-study-1-09jul19-en.pdf

[12] ICANN OCTO. *SSAC Proposal for the Name Collision Analysis Project (Revised by ICANN Office of the CTO)* . February 2019. https://community.icann.org/download/attachments/79437474/NCAP%20Proposal%20for%20Board%20%28revised%20by%20OCTO%20based%20on%20V2.5BTClean%29%20REDACTED.pdf?api=v2 See Section2.1.

[13] Section 2.3.3 of the RFP.

[14] ICANN Board. Consideration of .CORP, .HOME, and .MAIL and other Collision Strings. Approved Board Resolutions, November 2, 2017. https://www.icann.org/resources/board-material/resolutions-2017-11-02-en#2.a

© 2020 VeriSign, Inc. All rights reserved.

B.c). Indeed, the RFP even considers the case where an entire TLD is delegated[15] to a new registry operator as falling within the project's scope (Section 2.3.3, case B.b). The Study 1 Final Report, following the RFP as directed, repeats the error and even gives a name to these same-namespace reuses: "Re-registered name collisions."

Namespace usage issues related to the re-registration of the same name in the global DNS, as the report appropriately recounts, were "extensively discussed in SAC 010 … and SAC 011, both from June 2006." But a review of both references[16] [17] makes clear that these advisories involve no concerns that "a name that is used in one namespace may be used in a different namespace" — a collision between namespaces. The advisories' concerns are rather about the reuse of the same name, in the same namespace, at a different time, by "a different party."

SSAC and the NCAP Working Party should correct this error in further communications to ensure that this imprecise representation of name collision does not further propagate and add confusion to an already confusing topic. Re-registration practices and policies are important, but compared to name collisions, as we've said before, the issues are as different as "apples and oranges."[18]

5. Finally, it is important to keep in mind that the Study 1 Final Report is just one deliverable within ICANN's name collision management program and does not necessarily represent ICANN's recommendations on this matter. ICANN OCTO stated on the NCAP mailing list regarding the independence of report author Karen Scarfone, the cybersecurity writer at Scarfone Cybersecurity,[19]

   - "OCTO has told Karen all along that she should feel free to reach whatever conclusion she felt warranted by the research she's done. We have not attempted to undermine her professional integrity by leading her in any particular direction."

[15] The RFP's language is unusual at this point: "Registrant Alice uses .EXAMPLE as a TLD in the public DNS and then lets the registration expire." Registrants don't register TLDs or let them expire. The confusion in roles here underscores that the "re-registration" use cases are extraneous to the project's intent.
[16] ICANN SSAC. *SSAC Advisory SAC0010. Renewal Considerations for Domain Name Registrants.* June 2006. https://www.icann.org/en/system/files/files/renewal-advisory-29jun06-en.pdf
[17] ICANN SSAC. *SSAC Advisory SSAC0011 Problems Caused by the Non-Renewal of a Domain Name Associated with a DNS Name Server.* June 2006. https://www.icann.org/en/system/files/files/renewal-nameserver-07jul06-en.pdf
[18] Osterweil, Eric. "NXDomain responses under existent TLDs are _not_ the same as NXDomain responses under applied-for strings," comments-name-collision-05aug13 mailing list, September 11, 2013. https://forum.icann.org/lists/comments-name-collision-05aug13/msg00038.html
[19] Larson, Matt. "Draft final Study 1 report," NCAP-Discuss mailing list, April 24, 2020. https://mm.icann.org/pipermail/ncap-discuss/2020-April/000275.html

© 2020 VeriSign, Inc. All rights reserved.

This approach to the design and management of Study 1 has thereby allowed Scarfone Cybersecurity to provide an independent, unilateral assessment of name collision risks. However, ICANN OCTO also stated,[20]

- "OCTO has responsibility within the org to perform Study 1 and report back to the Board with the results. We have contracted a significant amount of that work to Karen, but the ultimate responsibility for this work is OCTO's on behalf of the org."

Even though the contractor may unilaterally make recommendations for future name collision work, the import of these recommendations remains unclear because the project is managed by and is ultimately accountable to ICANN OCTO, who has yet to provide any judgment on the report. The final report and accompanying statements from OCTO therefore need to state clearly which parties are responsible for the underlying recommendations put forth to the ICANN Board, to avoid any potential confusion within the ICANN community.

Notwithstanding these concerns about ultimate accountability, the views of the report's author remain an important contribution to the community. In particular, when the Study 1 Final Report states in Section 6, "the recommendation is that Studies 2 and 3 should not be performed as currently designed," this statement implies that the contractor has an ideal or more appropriate design in mind. It would be beneficial to the ICANN community that ICANN request advice from the author, as a subject-matter expert and the sole author of the recommendations in the report, in redesigning the work tasks of future Studies 2 and 3.

We appreciate ICANN's and Scarfone Cybersecurity's efforts on this project and the opportunity for public comments. With the Study 1 Final Report complete, we encourage ICANN to continue and expand its current program of global engagement and outreach on name collision risks. Verisign remains committed to collaboration on these efforts, and we expect that ICANN will likewise find support from other industry partners in helping mitigate the risk of name collisions in the global DNS.

[20] Larson, Matt. "Re: Draft final Study 1 report," NCAP-Discuss mailing list, April 24, 2020. https://mm.icann.org/pipermail/ncap-discuss/2020-April/000277.html

© 2020 VeriSign, Inc. All rights reserved.