Q&A Pod Transcript
Plenary Session DNS Abuse: Consideration of the Issues
Tuesday, 20 October 2020 10:30-12:00 CEST

1. ... you still have time to shave..., *Warren Kumari*
   -Say it isn't so

2. For spam- does this represent purely bulk unxolicted emails? Or do the spam emails also contain/deliver other forms of technical abuse such malware and/or phishing? In other words, if a spam email also contains/delivers other forms of abuse, how is the abuse categorized?, *Elisabeth Behsudi*
   -Live answered

3. What does reported threats mean? Are those actual threats or only reported? In our experience we are receiving more false postives than actual threats, *Luc Seufer*
   -A reported security threat is one that has been reported to one or more of the reputation providers that we use for DAAR. We do not investigate beyond the domain showing up in the reputation provider. With respect to false positives, studies have indicated the actual false positive rates found on the reputation providers we use are actually quite low.

4. These decreases do not look like what my members are describing as increased abuse of domains that play off misuse of their brands vis a vis phishing and spam. I feel like the increase should show in phishing as well. Much of phishing is perpetuated via spam. How do the numbers reconcile this? Shouldn't they be parallel?, *Lori Schulman*
   -Live answered

5. Also, for the 10 registries that appear to be the worst actors, what compliance measures have been taken? Their status to date? Thanks., *Lori Schulman*
   -Live answered

6. David, how much of your data is self-reported by contract parties, and how much is independently reported?, *Steve DelBianco*
   -All of the data we're using is derived from reputation providers. It is possible that contracted parties. could be reporting their own domains to the reputation providers, but this is probably unlikely.

7. the DAAR data seem to show a high concentration of bad behavior in a very limited number of actors. What learnings and actions can be derived from this insight?, *Jorge Cancio*
   -As mentioned, the absolute numbers can be misleading as there will likely always be some percentage of abuse in every TLD. If a TLD has a large number of registrations, the absolute number of abusive domains will be high, even if the percentage is quite low. With that said, we in OCTO have reached out to

registries and registrars which are outliers in terms of abuse to help those contracted parties understand the issues. In most cases, this has resulted in reduction of abuse.

8. in the DNSTCIR graph what's the different between invalid and nxdomains, *Wafa Dahmani*

   -No, it was between pandemic-related domains registered vs. those that showed up in reputation lists for phishing or malware.

   <q> (Not necessarily about DAAR)

9. One of the methods by which abuse is monitored is by asking users to "mark it spam", "report phishing" but the data gathered from users is not complete, there is considerable under-reporting of the scale of abuse. Is there a possibility that the abuse reporting process becomes responsive by itself with a view to encourage wider use of the reporting tools? A user reports, without any form of "incentive" or "reward" - in the form of a feedback, or better, action on the abuse marked and reported by that particular user, because some of these processes are BOT processes without any manual attention. Could the user reporting system be doubled as an interactive tool that prompts action and provides a feedback?, *Sivasubramanian Muthusamy*

   -It is possible and figuring out how to improve reporting might be an area of future research.

10. David, do you track percentage of abuse related domains by registry and registrar? Goran often speaks of a "few bad apples." Are they identifiable?, *Jonathan Zuck*

    -If you look in the DAAR reports, you can see in Figure 13 (etc) certain outliers. Those are the folks we reach out to.

11. David, has your team started attribution yet to identify the cybercrime operators who cause all these issues? It looks like 70% of all phishing/malware is caused by a few APT crews, like Emotet., *Theo Geurts*

    -We can and do identifier registries and registrars, but we cannot identify the underlying cybercrime operators that are obtaining domain names via those registries and registrars for malicious use.

12. My interpretation of this data is not that malicious behavior has gone down - it has not - but that it is concentrated into fewer domains. Is that the correct interpretation?, *Mark Svancarek*

    -We in OCTO try to provide the data as objectively and without interpretation as we can. The intent of DAAR is to provide trustable information for the community to help inform discussions.

13. As per the sadag report new gTLDs are misused for cyber attacks, what mitigation measures and registries responsible?, *Shiva Upadhyay*

-I believe it safe to say pretty much all TLDs that allow for the general public to register are subject to being misused. As for the mitigation measures, the contracted parties are probably in a better position to answer that.

14. To Lori's questions, can we identify the 8-10 bad actor parties that ICANN keeps saying are the concentration of bad acts / abuse -- and explain what ICANN compliance plans to do about those parties?, *Fabricio Vayra*
-'@Fabricio, see Jamie Hedlund's reponse to Steve DelBianco's answer below and reproduced here: "Last year, we completed an audit of virtually all registry operators to assess their compliance with their DNS security threat obligations (particularly Spec 11 3(b)). The final report on that audit can be found on icann.org/compliance. A similar audit of registrars has been delayed due to the pandemic but we hope to launch it later this year. It will primarily examine registrars' obligations under RAA 3.18, and will focus initially on registrars with apparently high concentration of abuse (phishiing, malware, botnets) under management as well some registrars with large numbers of abusive names but low concentration. We hope to publish that report in 2Q or 3Q of next year."

15. Mark asked in the chat, "My interpretation of this data is not that malicious behavior has gone down - it has not - but that it is concentrated into fewer domains. Is that the correct interpretation?" Can you please address this?, *Reg Levy - Tucows*
-In speaking with my team, they say "It is hard to conclude that from the data presented today as one needs to look at the commutative distribution (where for instance 80% of the data is located) over time. We have that data, we can look into it."

16. '@David - can you confirm that the list of Reputation Data Providers and data feeds at this page is still accurate/complete? https://www.icann.org/octo-ssr/daar-faqs/#security-threats, *Alex Deacon*
-Yes, those are the reputation providers used in DAAR

17. for Jeff: is the SSAC report going to advice any policy development effort and/or any update of contractual provisions?, *Jorge Cancio*
-At this point the report is not finalized, however, in its current form it does not suggest update of contractual provisions.

18. '@David Conrad we are working in the Tunisan CERT on Passive DNS (using the DNS logs implement a dashboard of indicators on malwares and ransomwares... in order to have an idea about the local cyberspace and have an idea about infected users....) can we have some support with regard to the work done within ICANN., *Wafa Dahmani*
-We'd be happy to help as we can. Please drop a note to octo@icann.org.

19. Domain Generation Algorithms (DGA) are an automation technique designed to generate (and later register these domain names) domain names in a particular

fashion. These registered domains are sometimes used as a part of malware distribution.
Can ICANN Org develop best practices and provisions in its agreements with Registries and Registrars that make it harder for attackers to use DGA's for malicious purposes?, *Mohit Batra*

20. Thank you David Conrad., *Sivasubramanian Muthusamy*

21. Jeff, is there an official report coming from SSAC on this? If so, is there a reason this was not available prior to this meeting?, *Reg Levy - Tucows*
-Process within SSAC for escalation from WP to full SSAC is the delay.

22. Mason, do you know who funded the Interisle report?, *Reg Levy – Tucows*
-Live answered

23. Domains under the control of criminals increasingly carry content that depends on the end-user visiting the page. This can be done with cookies, http headers and data obtained abusively from social networks or advertising networks. Unless the visiting user is identified as vulnerable with respect to the abusers' objectives, no malicious content is transmitted.
This makes any given abused domain much less likely to be discovered. Could this be an explanation of the apparent downward trend in domains observed as involved in phishing incidents? *Werner Staub*
-Werner, it very well could. One of the ever present issues is that criminals, fraudsters are always looking for and utilizing new methods to avoid detection by threat hunters.

24. Mason, could you explain how the redaction of the WHOIS is impacting the detection of phishing? I believe the tracking of the persons behind the phishing attempts may be harder but the number of abused domain names remain the same. Thank you., *Luc Seufer*
-Thanks Luc. It makes it hard to correlate bad actors and take down networks. You are well aided by the investigatory side of Whois.

25. There are a lot of calls for Proactive approach, can anyone explain how to predict future actions in situations where nothing bad have been done yet for the domains in quesion?, *Maxim Alzoba*
-Live answered

26. Do you have plans to involve RIRs into the process (all internet abuse happens over IP) ?, *Maxim Alzoba*
-Live answered

27. QUESTION to David or any of the panelists - Why do we seem to have such a discrepency between the ICANN data you refer to and other data? For instance, the DNS Abuse in gTLDs Study we commissioned on the CCTRT found "a clear

upward trend in the absolute number of phishing and malware domains in new gTLDs." That guided much of our work and recommendation 15 in particular ?, *David Taylor*
-I'm not sure there is a major discrepancy. If you look over time at DAAR reports you can see an increase in absolute numbers for newTLDs as security threats shifted towards new opportunities likes the newer TLDs. Note that todays slide were normalized to percentages so not absolute numbers..

28. Q for Chris L-E: Can you share details on "60 percent of reported data breaches are attributed to phishing and malware" - do you have details about the figures, sources for the figures and can you elaborate what means they are "attributed", perhaps you can explain the modus operandi?, *Monika Ermert (eLance journalist)*
    -Live answered

29. Can someone please give example of PROACTIVE measures. I've heard that: .EU requires identity verification for some registrations, which causes many bad actors to abandon the registration, *Steve DelBianco*
    -Live answered

30. thank you David, *Wafa Dahmani*

31. How could we deal with the incrase number of training phishing domain names registered which are not stricly malicious but could be caught for it, *Alexandre Hugla (Gandi)*
    -IMO a notifier/reporter standardized system would allow such testing domains to be registered so that they were "known harmless"

32. '@Steve, Contractual compliance audits are an example of proactive measures. Last year, we completed an audit of virtually all registry operators to assess their compliance with their DNS security threat obligations (particularly Spec 11 3(b)). The final report on that audit can be found on icann.org/compliance. A similar audit of registrars has been delayed due to the pandemic but we hope to launch it later this year. It will primarily examine registrars' obligations under RAA 3.18, and will focus initially on registrars with apparently high concentration of abuse (phishiing, malware, botnets) under management as well some registrars with large numbers of abusive names but low concentration. We hope to publish that report in 2Q or 3Q of next year., *Jamie Hedlund*
    -Live answered

33. All - one of the points made yesterday during the discussion about ICANN Meetings was that every session should have a purpose, constructive dialogue, and then end with action items and deliverables. So, we have had some dialogue on the issue of DNS Abuse, but what was the goal of this session and what are the action items and deliverables. In other words, how is this session furthering the work of ICANN? [NOTE, I am not criticizing, but rather trying to

draw out why we are having this session in light of the fact that we have had these plenaries now for years), *Jeffrey Neuman*

34. Maybe I'm misunderstanding, but for cases where a domain name is used in a way that is abusive -- selling counterfeit products, for example -- comparing <BRANDNAME.com> to Amazon or eBay (i.e., you don't shut the whole site down just because there is counterfeiting happing) doesn't seem like the appropriate comparison. Why are registrars reluctant to pull the lever they have to shut down such activity?, *Jonathan*

35. '@Steve I should have added that in the Compliance context, "proactive" is action taken that is not responsive (or reactive) to complaints submitted to us., *Jamie Hedlund*

36. Question for James: Would Trusted Notifier arrangements be a good mitigation for all the noise you mentioned?, *Mark Svancarek*

    -Live answered

37. To any of the panelists - what are your views on feasibility of measuring number of victims or impact at the end user side - are there metrics or tools that capture impact of particular types of abuse? I assume each incident may have multiple victims? would number of reports me a better indicator of the impact/number of victims?, *Gangesh Varna*

    -With good source data that would be an excellent augmentation to abuse reporting models.

38. Regarding enforcement in general against "bad actors" or anyone else alleged to have an abusive name under registration, Compliance has relatively limited tools authorized under our agreements. For example, we do not have authority to order suspension or deletion of a name. For complaints against registrars, we validate whether a registrar investigated and responded to reports of abuse, and whether any action it took was consistent with its abuse policies., *Jamie Hedlund*

39. Would CPH be willing to explore TMCH integration to show would-be registrants a warning message before completing potentially-infringing domain registrations - for all gTLDs?, *Brian King (MarkMonitor)*