Q&A Pod Transcript
Plenary Session: Understanding Reputation Block Lists
Thursday, 17 June 2021 10:30-12:00 CEST

1. I was under the impression ICANN OCTO was looking into ranking RBLs in terms of reliable reporting / false positives. Has anything come from that study? Thanks. ?, *Crystal Ondo - Google*

   -Thanks for bringing this up Crystal. We are working on it and this will be one of the points that I will be addressing in today's presentation.

2. In the design and implementation of reputation block lists, what is the degree of importance and attention given to false positives that occur to the limitations of AI, unattended blocks created based on a certain criteria that can not always be precise, and malicious inclusions by bad actors among those who provide inputs to the block lists?, *Sivasubramanian M*

   - In our case it's very important. The more errors that exist in the data, the harder it will be to convince people to use the data.

   - Thanks for this, Sivasubramanian: I appreciate Carel's point above, as false positives and removal post-remediation are very important to domain owners whose domains have been abused.

3. And, is the process is removal of false positives as swift as the process of inclusion in an RBL?, *Sivasubramanian M*

   - Speaking about abuse.ch (in particular URLhaus), there is an easy to use "Report False Positive" button where anyone can report false positives to the team. Such reports are being asnwered in time and necessary actions taken.

   -Our removal process is available to any end user online, and can be done immediately without having to wait for us. Our datasets are updated every minute.

4. '@Jonnaa, Can you tell us the ICANN future programs for the capaity building program on this matter as it is very critical for the security prospective, *Syed Iftikhar Shah*

   - Hello Syed, ICANN org's Office of the CTO (OCTO) has a Technical Engagement team that conducts webinars, trainings and events around the world. You can see a recent general description here: https://www.icann.org/en/blogs/details/how-icann-strengthened-its-technical-engagement-around-the-world-23-4-2021-en. ICANN org also offers the ICANN Learn online platform, where courses on various topics can be accessed: https://www.icann.org/news/multimedia/42. If you are a member of a community

structure, we welcome your suggestions on additional content and priority topics we should be covering. Thank you!

5. What incentives are there for reputation blocklists to keep freshness of data, meaning, removing domains or IPs where the reasons for the inclusion have been fixed?, *Rubens Henrique Kuhl Junior*

   - Speaking about abuse.ch (in particular URLhaus), a domain nam / URL will automatically be flagged as clean once the threat has been ceased. Usually, there is no human interaction involved in this process.

   -As we want to be able to update our datatsets as fast as we can, there is an incentive for us to keep the dataset small. So if we believe something is not a threat anymore, it will automatically expire.

6. Roman, the report false positive button is a good start., *Sivasubramanian M*

7. Can you speak in relation to the impact that a domain name being under a New TLD known to be a significant source of malicious action has on a domain? Is everyone under that TLD affected, even if in a minor way?, *Mark Datysgeld*

   - I can speak as a registry of a gTLD flagged as such and yes: every domain in that TLD (.work at the time) was flagged—legitimate consumers who wanted to use email addresses in the .work namespace were flagged as spam by multiple retail blocklists despite their legitimacy. I believe the algorithms have improved since then, however, this was quite early in the new gTLD roll-out.

   -Speaking about abuse.ch, the reputation of a TLD has no impact on the listing process

8. will the potential inclusion of registrar in the new ICANN DAAR dara be factored in to RBLs to help reduce false positives?, *Jothan Frakes*

   - We at OCTO are working on developing concrete RBL evaluation method for all of the projects that will utilize RBLs including but not limited to DAAR.

9. We're seeing an increasing number of spam mails sent from large U.S. providers. At the same time they do not offer a point of contact that responds within a reasonable timeframe. Still our customers expect us to fix their problems. What's the best place to start address these issues - ICANN, RIPE, anyone else?, *Marcus Fauré*

   - The provider itself. They are in the best position to fix issues.

10. Carol and Leg Levy, it is good that you consider it important to make the RBLs reliable, but how alert is the design of the process for false positives, and how

swift is the process of removal? Often any attention, if at all, comes after inflicting harm over a long period of time., *Sivasubramanian M*

11. Is a domain name listed but not resolving, to be considered as “whitelisted” (i.e. removed from the reputation list)?, *Steinar Grøtterød*

    -In our, registrar, experience, this is not the case. We often get malformed reports of abuse that we cannot verify (the full URL is not included). So “example.tld” may not resolve but “example.tld/phish” does—without the full URL, we are not able to confirm that abuse exists on the domain and, if the domain is not resolving for us (even if there are valid nameservers), there’s little action we can take.

    I encourage all reporters to provide as much evidence as possible when submitting abuse reports, as this speeds our ability to mitigate.

12. '@Carel the point is the provider is not responsive, *Marcus Fauré*

13. Are they any guaranty or fail-safe in place to ensure that RBL providers always follow some transparent guidelines and aren't abused by reporters willing to harm legitimate third parties? Are the reviewing processes disclosed somewhere?, *Luc Seufer*

14. We work closley with many blacklist providers to ensure that we’re doing our best to keep the intetnet space clean however, once action has been taken, or it’s been reported as a false positive, I’ve reached out to many of these blacklist providers and it proves difficult to get domains removed from the list, even after providing proof to them such as; the domain is parked. Blocklist providers, are a business and when bulk action is taken, it often takes a long time to be removed which is reputational damage to the company. What can be done to ensure that blocklist are working in realtime, and keeping more accurate data?, *Keiron Tobin*

    - Live answered

15. Question to all speakers: Do you have differential approach for ASCII and IDN domains for including them in your blacklists or it's absolutely the same approach? Thank you!, *Vadim Mikhaylov*

    - Speaking about abuse.ch, the fact whether the domain is ASCII or IDN doesn't have any impact on a listing

16. Hello from Taiwan! This is Ken-Ying, a Taiwan lawyer. I have the following questions:

    1. Who is responsible for creating the Blocklist? ICANN or registries or registrars or an independent third party?

2. Would this “responsible entity” be reviewing the “content” of a website in order to determine whether it is malicious? Based on what standard? Local law standards or ICANN policy?
3. Would the Blocklist be limited to the activities defined as “DNS Abuse” by ICANN? (such as only those we just voted on at the beginning of this meeting). My point is that DNS abuse or cyberthreat may be evolving, perhaps the list shall not be confined to only certain specific activities?, *Ken-Ying Tseng*

- Hi Ken. 1- Speaking from ICANN org’s side, ICANN does not create or maintain any RBL. We use RBLs that are provided by third parties such as those on today’s panel. 3- Blocklists could be focused on any threat type. We at ICANN only use those focused on Malware, Phishing, Botnet C&C as well as Spam as a delivery mechanism.

- 1. Each retail blocklist manages its own creation, although sometimes they are informed by other blocklists.
2. As the speakers just indicated, some operate on algorithms and others manually review.
3. This also depends on the blocklist itself—DNS Abuse has a very specific meaning, as indicated by the first public poll in this session—but some retail blocklists will also report, for example, trademark or copyright as “abuse”, despite the fact that these are most often content-based complaints.

17. '@roman. What is "malicious content"? Does it include TM infringement as well?, *Vivek Goyal (COO-LdotR)*

    -Speaking about URLhaus, the scope is malware only. The listing policy is available here:
    https://urlhaus.abuse.ch/api/#policy

18. This may already exist and it would be helpful if ICANN published the list of RBLs is uses and how to contact them (e.g., URL and email address) to initiate the investigation of alleged abuse., *Craig Schwartz (fTLD - .BANK)*

    - We publish the list of RBLs we use per project. An example is the DAAR project. You can find the list of RBLs used in the info page, methodology paper as well as at the end of every month, DAAR monthly report. Please see here https://www.icann.org/octo-ssr/daar

19. question to all speakers: How can you want to prevent RBLs from getting politisised at global level? what is exactly the relation between unilateral digital sanctions and RBLs processes? and do you think about its impact on digital trust in internet governance domain ? thanks, *Mokabberi*

    - I'm not sure if I am the right person to asnwere this. The listing policy of abuse.ch (URLhaus) is transparent and an entry will auto removed once the

threat (malware payload) disappears. There is no way to influce this process in a way that a URL/domain stays listed when the threat has been ceased. Speaking about policits, CH is a neutral country. We do not know any national security letters or similar. Did that answere your question at all?

20. do the RBLs report false positives to each other?, Jonathan Zuck

    - I think this is an important topic. I am not aware about any established processes between RBL providers where false positive reports are being exchanged. Of course, that doesn't mean that such a process / system doesn't exist. If such one exists, abuse.ch is not part of it (yet).

21. Thanks Samaneh and I'll review. Is contact information for the RBLs also provided within the referenced materials?, *Craig Schwartz (fTLD - .BANK)*

    - The contacts are unfortunately not there but you can contact me if you needed help.

22. I maintain the Public Suffix List and am curious if there are ways that subdomains are determined using the PSL and if there is a way we can (cas a volunteer peoject) have support from you to identify names where submissions could be identified in the PRs or otherwise to address them so that they are blocked before being added if there is a bad actor submitting it?, *Jothan Frakes*

    - Live answered

23. '@ Keiron Yes, it is a cumbersome, unworkable process, almost an impossible process to get the false positive removed in time, *Sivasubramanian M*

24. Dear Moderator, Could you please raise my queston too? thank you., *Mokabberi*

    - Thank you for the question, Mokabberi. I have seen that Roman typed an answer to your question.

25. Why do many RBLs do not provide any evidence in their reports? Without evidence or specific reference that allows verification of the report, it makes taking action exceedingly difficult, *Volker Greimann*

    - Speaking about spam based RBLs, I think the main issue is redacting spam samples in an automated and secure way. I see many threat actors using email thread hijacing thesed days, stealing email conversations and then use them to spread malware. There are a) PI in these conversations that can't be revealed and b) possible data/info that may reveal the receiving endpoint (usually a spam trap). Speaking about abuse.ch (URLhaus), we always share evidence (the offensive URL concerned along with the payload received).

26. Another important question, and I note that Roman has noted that non-resolving domains appear to be removed from the RBLs, but 'resolution' or mitigation of a threat is of cours, not as simple as does it resolve or not (e.g. fixing a compromised domain, or indeed where a domain is 'repossessed' by a registrar, or nameservers are changed so that the threat no longer exists but potentially remain 'live' from a technical point of view. How is this taken into account in RBLs? This is pertinent when considering metrics such as DAAR and perceived rates of abuse -especoally where mitiagation is not being well measured., *Alan Woods*

27. '@Samaneh. Does DAAR make its sources public?, *Vivek Goyal (COO-LdotR)*

    - Yes. You can find them at the end of every DAAR monthly report. https://www.icann.org/octo-ssr/daar

28. Many people outside the industry have no idea who ICANN is, and if we're unable to take action, due to evidence etc, they tell us that 'they're going to report us to ICANN'. ICANN in itself, could be classed as an RBL with the amount of complaints you must receive, so if you're doing your job correctly and reading the abuse complaints that you're receiving, how are you justifying paying 3rd party RBL's for data that you may already have?, *Keiron Tobin*

29. '@Samaneh, Is there any specific ICANN initiatve to promote unique and central approach to mitigate the silo approachs for RBLs as you highlighed as a key issue (silos appraoches for RBLs) on the subject matter? In case there is such initiative(s) can you share their exact titles., *Syed Iftikhar Shah*

    - No. RBLs are completely independent of the ICANN processes.

30. Have you researched the governance and accountability issues around reputation lists?, *Peter Koch (DENIC eG)*

    - Hi Peter. Excellent question. We did not. and I am not aware of any research out there about this aspect of it.

31. Question to the dear speakers: How can you want to prevent RBLs from getting politisised at global level? what is exactly the relation between unilateral digital sanctions and RBLs processes? and do you think about its impact on digital trust in internet governance domain ? thanks, *Mokabberi*

    - We may not get to it live, but I think this goes to my point about false positives—where reporting of a domain is malicious, whether for political reasons or other—that must be mitigated. Transparency about methodology, including removal post-mitigation and false positives, is extremely important when attempting to make a determination about whether or not to work with a retail blocklist.

32. @dear Roman, that did not answer my question., *Mokabberi*

33. If This RBLs processes it is not fair and transparent itself it could badly affect ICANN community Reputation., *Mokabberi*